Pseudo linear transformations and evaluation in Ore extensions.

André Leroy[*]

Abstract

The relations between evaluation of Ore polynomials and pseudo-linear transformations are studied. The behavior of these transformations under homomorphisms of Ore extensions, in particular with respect to algebraicity, is analyzed leading to characterization of left and right primitivity of an Ore extension.

Necessary and sufficient conditions are given for algebraic pseudo-linear transformations to be diagonalizable. Natural notions of (S, D) right and left eigenvalues are introduced and sufficient conditions for a matrix to be (S, D) diagonalizable are given.

1 Introduction

Skew polynomial rings were introduced by Oystein Ore in 1933 [0] but some earlier works related to the differential case already appeared e.g. in Landau (see [La]) We will mainly be interested in the case when the coefficients belong to a division ring but occasionally we will have to work with more general rings, so let A be a ring, $S \in \text{End}(A)$ and D a left S-derivation i.e. D is an additive endomorphism of A such that

$$\text{for any } a, b \in A \qquad D(ab) = S(a)D(b) + D(a)b \qquad (1.1)$$

A skew polynomial ring (also called Ore extension) $A[t; S, D]$ consists of polynomials $\sum_{i=0}^{n} a_i t^i$, $a_i \in A$ which are added in the usual way but are multiplied accordingly to the following commutation rule

$$\text{for any } a \in A \qquad ta = S(a)t + D(a) \tag{1.2}$$

In an attempt to study modules over $K[t; S, D]$, K a division ring, we are forced to consider pseudo-linear transformations since they translate the action of the indeterminate. This situation is completely similar to the standard relations between modules over $k[t]$, k a field, and linear algebra. This similarity is based on some common properties shared by these polynomial rings and skew polynomial rings; division algorithm, "unique" factorization into irreducibles,... These properties were established in the skew case by Ore himself and used later by Jacobson (cf. [J]) to study pseudo-linear transformations.

Let K be a division ring and V be a K vector space. A pseudo-linear transformation is an additive map $T : V \to V$ such that

$$T(\alpha v) = S(\alpha)T(v) + D(\alpha)v \quad \text{for } \alpha \in K, \ v \in V \tag{1.3}$$

We will often use the abbreviation $(S, D)PLT$ for a pseudo-linear transformation with respect to the endomorphism S and the S-derivation D. Jacobson [loc. cit.] was mainly interested in irreducibility (absence of invariant subspace), indecomposability (absence of direct summand) normal form (matrices over $K[t; S, D]$ are (S, D) similar to diagonal matrices whose elements are the invariant factors).

In the second section of this paper we will recall the folklore of (S, D) similarity give examples and show how the use of $(S, D)PLT$ enables us to generalize formulas of earlier work connected to skew evaluation.

An important particular feature of $(S, D)PLT$ (or even of usual K linear transformations when K is a non commutative division ring) is the absence of a Cayley Hamilton theorem. In the third section, we analyze this problem and give different necessary and sufficient conditions for T, an $(S, D)PLT$ to be algebraic we show that this property is preserved under the image of an $(S', D')C.V.$ polynomial $p(t) \in K[t; S, D]$ (see definition 3. 1). These considerations enable us to exhibit a class of skew polynomial rings for which all the $(S, D)PLT$'s on finite-dimensional vector spaces are algebraic. We obtain an analogue of the Amitsur-Small's theorem namely a characterization of skew polynomial rings which are primitive. In this characterization the notion of (S, D)-algebraicity plays the role of (usual) algebraicity.

In section 4, we first consider the question of diagonalization of an algebraic $(S, D)PLT$ and we obtain different necessary and sufficient conditions for the existence of a basis consisting of eigenvectors, e.g. we show that the minimal polynomial of the pseudo-linear transformation must be the minimal polynomial of the set of eigenvalues. In the second part of this section, assuming $S \in Aut(K)$, we introduce the notions of right and left "(S, D) eigenvalues" for a matrix $A \in M_n(K)$ we show that this set is (S, D) closed and that if it consists of n (S, D) conjugacy classes then A is (S, D) similar to a diagonal matrix (cf. definition 1.3 (b) for the notion of (S, D) conjugacy classes).

Let us now end this introduction with a few notations.

For any element a in a ring A equipped with an endomorphism S and an S-derivation D we have, in $A[t; S, D]$, and for any $n \in \mathbb{N}$

$$t^n a = \sum_{i=0}^{n} f_i^n(a) t^i \tag{1.4}$$

where the maps $f_i^n \in \mathrm{End}\,(A, +)$ consist of the sum of all products with i factors S and $n - i$ factors D. This formula generalizes (1.2) and will be in its turn generalized in section 2 (cf. remark 2.11).

In earlier works we introduced (cf. [LL1], [LL2]) a natural notion for the evaluation $f(a)$ of a polynomial $f(t) \in R = A[t; S, D]$ at some elements $a \in A : f(a)$ is the remainder of $f(t) = \sum_{i=0}^{n} a_i t^i$ divided on the right by $t - a$ i.e. $f(t) = q(t)(t - a) + f(a)$, for some polynomial $q(t) \in A[t; S, D]$. It is easy to show by induction that $f(a) = \sum_{i=0}^{n} a_i N_i(a)$ where the maps N_i are defined by induction in the following way : For any $a \in A$ $N_0(a) = 1$ and $N_{i+1}(a) = S(N_i(a))a + D(N_i(a))$. This natural notion seems to be important and we offer in section 2 another perspective on it in terms of pseudo-linear transformations leading to generalizations of formulas obtained earlier.

2   Basic properties and examples.

Let K, S, D, V be a divison ring, an endomorphism of K, a (left) S-derivation and a left K-vector space respectively.

Definition 1. *A map $T : V \to V$ such that*

$$\begin{aligned} T(v_1 + v_2) &= T(v_1) + T(v_2) &\quad &\text{for } v_1, v_2 \in V \\ T(\alpha v) &= S(\alpha)T(v) + D(\alpha)v &\quad &\text{for } \alpha \in K \;\; v \in V \end{aligned}$$

is an (S, D) pseudo-linear transformation of V.

The abbreviation (S, D) PLT will stand for an (S, D) pseudo-linear transformation.

If V is finite-dimensional and $\underline{e} = \{e_1, \ldots, e_n\}$ is a basis of V let us write $Te_i = \sum_{j=1}^{n} a_{ij} e_j$, $a_{ij} \in K$ or with matrix notation $T\underline{e} = A\underline{e}$ where $A = (a_{ij}) \in M_n(K)$. The matrix A will be denoted $M_{\underline{e}}(T)$ and $\Delta(T)$ will stand for the set $\{M_{\underline{e}}(T) | \underline{e}$ is a basis of $V\}$.

Lemma 2. *a) Let $T : V \to V$ be an (S, D) PLT then V becomes a left module over $R = K[t; S, D]$ via $f(t) \cdot v = f(T)(v)$ for $f(t) \in R$ and $v \in V$. Conversely, any left R-module V gives rise to an (S, D)PLT on V via $T(v) = t \cdot v$.*

b) If V_1 is a vector space isomorphic to V and $\sigma : V \to V_1$ is an isomorphism then $\sigma \circ T \circ \sigma^{-1}$ is an (S, D) PLT on V_1.

Proof The easy proofs are left to the reader.

Part b) of the above lemma motivates the following

Definition 3.   a) Let V and V_1 be isomorphic vector spaces and let T and T_1 be $(S, D)PLT$'s on V and V_1 respectively. T_1 is similar to T if there exists an isomorphism $\sigma : V \to V_1$ such that $T_1 = \sigma \circ T \circ \sigma^{-1}$.

b) Let A, S, D be a ring, an endomorphism of A and an S-derivation of A respectively. Two elements $a, b \in A$ are (S, D) conjugate if there exists $c \in A$, c invertible, such that $b = S(c)ac^{-1} + D(c)c^{-1}$. We will use the notations $a \underset{S,D}{\sim} b$ to express that a and b are (S, D) conjugate and $a^c := S(c)ac^{-1} + D(c)c^{-1}$. It is easy to check that $\underset{S,D}{\sim}$ is an equivalence relation on A.

Proposition 2.4. Let V and V_1 be isomorphic left K-vector spaces of finite dimension , say n, and let T and T_1 be $(S, D)PLT$'s on V and V_1 respectively. Extend S and D in the natural way from K to $M_n(K)$ and denote $U := M_n(K)[t; S, D]$ and $R := K[t; S, D]$. Then the following are equivalent

(i) T is similar to T_1.

(ii) There exists an isomorphism $\sigma : V \to V_1$ such that $T_1 = \sigma \circ T \circ \sigma^{-1}$.

(iii) The R-module structure on V induced by T is isomorphic to the R-module structure on V_1 induced by T_1.

(iv) $M_{\underline{e}}(T) \underset{S,D}{\sim} M_{\sigma(\underline{e})}(T_1)$ for any basis $\underline{e}$ of V and some K isomorphism $\sigma : V \to V_1$.

(v) $M_{\underline{e}}(T) \underset{S,D}{\sim} M_{\underline{u}}(T_1)$ in $M_n(K)$ for some basis $\underline{e}$ of V and some basis $\underline{u}$ of V_1.

(vi) $M_{\underline{e}}(T) \underset{S,D}{\sim} M_{\underline{u}}(T_1)$ in $M_n(K)$ for any basis $\underline{e}$ of V and any basis $\underline{u}$ of V_1.

(vii) $\{M_{\underline{e}}(T)|\underline{e}$ is a basis of $V\} = \{M_{\underline{u}}(T_1)|\underline{u}$ is a basis of $V_1\}$.

(viii) $\dfrac{U}{U(t - M_{\underline{e}}(T))} \cong \dfrac{U}{U(t - M_{\underline{u}}(T_1))}$ as left U-modules for any basis $\underline{e}$ and $\underline{u}$ of V and V_1 respectively.

In particular if $V_1 = V$, $T_1 = T$, $\sigma = id_V$, (vi) above shows that for any basis $\underline{e}$, $\underline{u}$ of V the matrices $M_{\underline{e}}(T)$ and $M_{\underline{u}}(T)$ are (S, D) conjugate and the set $\Delta(T) = \{M_{\underline{e}}(T)|\underline{e}$ is a basis of $V\}$ is an (S, D) equivalence class in $M_n(K)$.

Proof The equivalence of the five first assertions is easy.

(v) $\leftrightarrow$ (vi) Let $\underline{e}'$ and $\underline{u}'$ be basis of V and V_1 respectively. there exist $P, Q \in GL_n(K)$ such that $\underline{e}' = P\underline{e}$ and $\underline{u} = Q\underline{u}'$ then $M_{\underline{e}'}(T)P\underline{e} = M_{\underline{e}'}(T)\underline{e}' = T\underline{e}' = TP\underline{e} = S(P)T\underline{e} + D(P)\underline{e} = (S(P)M_{\underline{e}}(T) + D(P))\underline{e}$ and we conclude $M_{\underline{e}'}(T) = S(P)M_{\underline{e}}(T)P^{-1} + D(P)P^{-1}$. Similarly we have $M_{\underline{u}}(T_1) = S(Q)M_{\underline{u}'}(T_1)Q^{-1} + D(Q)Q^{-1}$. So $M_{\underline{e}'}(T) \underset{S,D}{\sim} M_{\underline{e}}(T)$, $M_{\underline{u}}(T_1) \underset{S,D}{\sim} M_{\underline{u}'}(T_1)$. By hypothesis $M_{\underline{e}}(T) \underset{S,D}{\sim} M_{\underline{u}}(T_1)$ and by transitivity we get $M_{\underline{e}'}(T) \underset{S,D}{\sim} M_{\underline{u}'}(T_1)$.

(vi) $\to$ (vii) By symmetry it is enough to show that for any basis $\underline{e}$ of V we have $M_{\underline{e}}(T) = M_{\underline{u}}(T_1)$ for some basis $\underline{u}$ of V_1. By (v) we know $M_{\underline{e}}(T)^P = M_{\underline{u}'}(T_1)$ (notation as in Definition 3 (b)) for some $P \in GL_n(K)$ and some basis $\underline{u}'$ of V_1. Let

$\underline{u}$ be the basis of V_1 defined by $\underline{u} = P^{-1}\underline{u}'$. it is easy to check $M_{\underline{u}}(T_1) = M_{\underline{u}'}(T_1)^{P^{-1}}$ and so $M_{\underline{u}}(T_1) = M_{\underline{e}}(T)$ as desired.

(vii) $\rightarrow$ (iv) If $M_{\underline{e}}(T) = M_{\underline{u}}(T_1)$ $\underline{e}$ basis of V, $\underline{u}$ basis of V_1. It suffices to define σ by $\sigma(\underline{e}) = \underline{u}$.

(vi) $\rightarrow$ (viii) By hypothesis we know there exists $P \in GL_n(K)$ such that $M_{\underline{e}}(T) = M_{\underline{u}}(T_1)^P$ and this implies that $(t - M_{\underline{e}}(T))P = S(P)(t - M_{\underline{u}}(T_1))$ in $U = M_n(K)[t; S, D]$. It is then easy to check that there exists a well defined U-module isomorphism between $\dfrac{U}{U(t - A)}$ and $\dfrac{U}{U(t - B)}$, where $A = M_{\underline{e}}(T)$ and $B = M_{\underline{u}}(T_1)$. Explicitly this isomorphism ψ is given by

$$\psi(1 + U(t - A)) = P + U(t - B)$$

(viii) $\rightarrow$ (vi) If ψ is an isomorphism of U-modules between $\dfrac{U}{U(t - A)}$ and $\dfrac{U}{U(t - B)}$, let $\psi(I + U(t - A)) = P + U(t - B)$. Since ψ is surjective we easily conclude that there exists $C \in M_n(K)$ such that $CP = I$ and, as is well known, this implies that P is invertible. Since ψ is a morphism of left U-modules we get $(t - A)P \in U(t - B)$. So $S(P)(t - B) + S(P)B + D(P) - AP \in U(t - B)$ and thus $S(P)B + D(P) = AP$ i.e. $A = B^P$. Using $A = M_{\underline{e}}(T)$ and $B = M_{\underline{u}}(T_1)$ we obtain the desired conclusion $M_{\underline{e}}(T) \underset{S,D}{\sim} M_{\underline{u}}(T_1)$. The final assertions are now easy to check.

Remarks 2.5. a) If $S \in Aut(K)$ we can also add to the above equivalences the following one :

(ix) $\dfrac{U}{(t - M_{\underline{e}}(T))U} \cong \dfrac{U}{(t - M_{\underline{u}}(T_1))U}$ as right U-modules where $\underline{e}$ and $\underline{u}$ are basis of V and V_1 respectively.

This is easily proved using the fact that for any $B \in M_n(K)$ left division by $t - B$ can now be performed in U.

b) Most of the above is part of folklore but has been recalled for the convenience of the reader.

c) Of course it is also possible to define PLT's with respect to an endomorphism σ and a right σ-derivation δ (i.e. $\delta(ab) = \delta(a)\sigma(b) + a\delta(b)$). They correspond to right A-modules where $A = K[T; \delta, \sigma]$ in which polynomials are written with coefficients on the right and the commutation law is $at = t\sigma(a) + \delta(a)$ for $a \in K$. For $a, b \in K$, we define $a \widetilde{\sim}_\sigma b$ if there exists $c \in K \smallsetminus \{0\}$ such that $b = c^{-1}a\sigma(c) + c^{-1}\delta(c)$. If $S \in Aut(K)$ and D is a left S derivation then $(K[t; S, D])^{op} \cong K^{op}[t; S^{-1}; -DS^{-1}]$ i.e. $-DS^{-1}$ is a left S^{-1} derivation of K^{op} and so a right S^{-1} derivation of K. It is worthwhile to remark that $a \underset{S,D}{\sim} b$ iff $a \underset{-DS^{-1}, S^{-1}}{\sim} b$. These observations will shed some light on definitions and apparent lack of symmetry in section 4.

d) Even if $M_{\underline{e}}(T) = 0$ this does not mean that $T = 0$. In fact the zero map $0 : V \rightarrow V : v \mapsto 0$ is not a PLT if $D \neq 0$.

e) Even if $M_{\underline{e}}(T)$ is invertible this does not mean that T is bijective. In fact it may happen that $M_{\underline{e}}(T) = 0$ but $M_{\underline{e}}(T)$ is invertible for some other basis $\underline{e}$ of V.

Let us consider, for instance, the case $V = K$ and $T = D$. Of course D itself is a PLT and $D(1) = 0$ so $M_{\{1\}}(D) = 0$.

f) If T_1, T_2 are (S, D) PLT in a K vector space $V, T_1 + T_2, T_1 \circ T_2, \ \alpha T_1 (\alpha \in K)$ are not necessarily pseudo-linear transformations.

Example 2.6. Of course $D : K \to K$ is an (S, D) PLT. More generally any $c \in K$ gives rise to an (S, D) PLT on K denoted T_c and defined by

$$T_c(x) := S(x)c + D(x) \quad \text{for } x \in K \tag{2.7}$$

It is easy to check that all the (S, D) PLT's on K are of this form (e.g. $D = T_0$).

To convince the reader of the importance of these maps, let us mention that they give back.

a) The maps $N_i : K \to K$ used in [LL1] [LL2] (cf. §1 for definition) which can be seen as generalization of both the standard i^{th} power and i^{th} norm. If fact $T_c^i(1) = N_i(c)$ for $i \geq 0$ (see Theorem 2.8 b) hereafter).

b) The left R-module structure on K in relation with evaluation at c defined in [LL1] Remark 2.8. Explicitely this R-module structure was given by $g(t)*x = g(c^x)x$ for $x \in K \ \ g(t) \in R = K[t; S, D]$. In fact this R-module structure is nothing else but the one given by T_c (cf. Remark 2.11 (a) below).

Let us notice that the maps T_c defined by (2.7) have a meaning also for an element c in a ring A equipped with an endomorphism S and a S-derivation D.

Recall from the introduction that the N_i's are maps from K to K defined by induction : For $a \in K$, $N_0(a) = 1$ and $N_{i+1}(a) = S(N_i(a))a + D(N_i(a))$. Let us also define for $i \geq j \ \ h_j^i(T_c) \in \text{End}(A, +)$ to be the sum of all products with j symbols S and $i - j$ symbols T_c (e.g. $h_0^i(T_c) = T_c^n$, $h_n^n(T_c) = S^n$) with these notations we easily prove the following.

Theorem 2.8. *Let A be a ring, $S \in \text{End}(A)$ and D an S-derivation of A. For $f(t) = \sum_{i=0}^n a_i t^i \in R = A[t; S, D]$, and $c, x \in A$ we have*

a)

$$f(t)x = \sum_{j=0}^{n} \left(\sum_{i=j}^{n} a_i h_j^i(T_c)(x) \right) (t - c)^j \tag{2.9}$$

In particular we have $(f(t)x)(c) = f(T_c)(x)$ and $f(c) = f(T_c)(1)$.

b) If x is invertible in A then for any $n \in \mathbb{N} \ \ N_n(c^x)x = T_c^n(x)$ and $f(T_c)(x) = \sum_{i=0}^n a_i N_i(c^x)x$. In particular we get $N_n(c) = T_c^n(1)$ and we obtain the classical formula $f(c) = \sum_{i=0}^n a_i N_i(c)$. We also have $f(T_c)(x) = f(c^x)x$.

Proof We will prove formula 2.9 by induction on $\deg f(t) = n$. Let us first assume that the polynomial $f(t)$ is of the form $f(t) = t^n$.

For $n = 0$ both sides of 2.9 boil down to x.

For $n = 1$ we have $tx = S(x)(t - c) + T_c(x) = h_1^1(T_c)(x)(t - c) + h_0^1(T_c)(x)$.

Assuming the formula 2.9 valid for $f(t) = t^n$ we compute :

$$t^{n+1}x = t \left(\sum_{j=0}^{n} h_j^n(T_c)(x)(t - c)^j \right)$$

and using the case $n = 1$ we get :

$$
\begin{aligned}
t^{n+1}x &= \sum_{j=0}^{n} \left[S(h_j^n(T_c)(x))(t-c)^{j+1} + T_c(h_j^n(T_c)(x))(t-c)^j \right] \\
&= \sum_{j=1}^{n} \left[S(h_{j-1}^n(T_c)(x)) + T_c(h_j^n(T_c)(x)) \right] (t-c)^j \\
&\qquad + S(h_n^n(T_c)(x))(t-c)^{n+1} + T_c(h_0^n(T_c)(x)) \\
t^{n+1}x &= \sum_{j=1}^{n} h_j^{n+1}(T_c)(x)(t-c)^j + h_{n+1}^{n+1}(T_c)(x)(t-c)^{n+1} + h_0^{n+1}(T_c)(x)
\end{aligned}
$$

and finally we obtain $t^{n+1}x = \sum_{j=0}^{n+1} h_j^{n+1}(T_c)(x)(t-c)^j$ as required.

Now if $f(t) = \sum_{i=0}^{n} a_i t^i$ we easily compute

$$
f(t)x = \sum_{i=0}^{n} a_i t^i x = \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{i} h_j^i(T_c)(x)(t-c)^j \right)
$$

and hence

$$
f(t)x = \sum_{j=0}^{n} \left(\sum_{i=j}^{n} a_i h_j^i(T_c)(x) \right) (t-c)^j
$$

as we wanted to prove.

Let us now prove the particular case; the remainder of $f(t)x$ divided by $t - c$ is, by definition, the evaluation of $f(t)x$ at c, i.e. $(f(t)x)(c)$. This remainder is also the independant term of the R.H.S. of 2.9 we obtain

$$
(f(t)x)(c) = \sum_{i=0}^{n} a_i h_0^i(T_c)(x) = \sum_{i=0}^{n} a_i T_c^i(x) = f(T_c)(x)
$$

as desired. For $x = 1$ this last formula gives $f(c) = f(T_c)(1)$.

b) Let us prove the formula $N_n(c^x)x = T_c^n(x)$ by induction on n. For $n = 0$ the formula boils down to $x = x$. Assume the formula true for $n \in \mathbb{N}$ and let us compute

$$
\begin{aligned}
N_{n+1}(c^x)x &= \left[S(N_n(c^x))c^x + D(N_n(c^x)) \right] x \\
&= \left[S(N_n(c^x))(S(x)cx^{-1} + D(x)x^{-1}) + D(N_n(c^x)) \right] x \\
&= S(N_n(c^x)x)c + (S(N_n(c^x))D(x) + D(N_n(c^x))x \\
&= T_c(N_n(c^x)x) = T_c^{n+1}(x).
\end{aligned}
$$

From this it is easy to establish $f(T_c)(x) = \sum a_i N_i(c^x)x$. For $n = 1$ these formulas become $N_n(c) = T_c^n(1)$ and $f(T_c)(1) = \sum_{i=0}^{n} a_i N_i(c)$. But by a) above we have $f(c) = f(T_c)(1)$ and so we conclude $f(c) = \sum_{i=0}^{n} a_i N_i(c)$. The last formula is now clear : $f(T_c)(x) = \sum a_i N_i(c^x)x = f(c^x)x$. $\qquad \square$

As a corollary we obtain a formula which generalizes the standard one (e.g. [LL2], 2.1) for the evaluation of a product of polynomials at a point $c \in A$.

Corollary 2.10.   *Let A, S, D be as in Theorem 2.8 and let $f(t), g(t)$ be polynomials in $R = A[t; S, D]$. Then for any $c \in A$ we have $(f(t) \cdot g(t))(c) = f(T_c)(g(c))$. In particular if $g(c)$ is invertible in A we have $(f(t) \cdot g(t))(c) = f(c^{g(c)})g(c)$.*

Proof Since A is an $A[t; S, D]$ left module via the action of T_c, we have $(f \cdot g)(T_c) = f(T_c) \cdot g(T_c)$. Hence the last formula of part a) of the above theorem implies that $(f \cdot g)(c) = (f \cdot g)(T_c)(1) = f(T_c)(g(T_c)(1)) = f(T_c)(g(c))$. Now, if $g(c)$ is invertible in A we have, thanks to the last formula of the above theorem, $f(T_c)(g(c)) = f(c^{g(c)})g(c)$ and so $(f \cdot g)(c) = f(c^{g(c)})g(c)$.

Remarks 2.11.

a) For any element c in a division ring K, we introduced in [LL1] a left R-module structure via $f(t) * x = f(c^x)x$; $x \in K^*$. Since $f(c^x)x = f(T_c)(x)$ it is now clear that this R-module structure in K is the one induced by T_c.

b) For $c = 0$, $T_c = D$ and $h_i^n(T_c) = f_i^n$ where the f_i^n's are defined in section 1 (cf. (1.4)).

c) Formula 2.9 also gives the quotient of the division of $f(t)x$ by $t - c$: $f(t)x = q(t)(t - c) + f(T_c)(x)$ where

$$q(t) = \sum_{j=1}^{n} \left(\sum_{i=j}^{n} a_i h_j^i(T_c)(x) \right) (t - c)^{j-1}$$

d) Formula 2.9, for $x = 1$, can potentially be used for checking the multiplicity of a root. In this respect the expression $\sum_{i=j}^{n} a_i h_j^i(T_c)(1)$ is the analogue of the standard j^{th} derivative of $f(t)$ evaluated at c.

As noticed earlier if K is a division ring, $S \in \text{End }(K)$ and D an S-derivation of K, then S and D extend in a natural way to $M_n(K)$. Still denoting by S and D the extended maps we may associate to every matrix $C \in M_n(K)$ the map $T_C : M_n(K) \to M_n(K) : X \mapsto S(X)C + D(X)$. Of course this is a PLT on $V = M_n(K)$. Let us remark that for any i, $1 \le i \le n$, the K subspace consisting of the ith row is T_C-stable. We thus get a PLT on a vector space isomorphic to K^n. Up to the end of the paper we will use the notation T_C, $C \in M_n(K)$, for this last PLT. To make this clear and for easy further references we state the

Definition 2.12.   *Let K, S, D stand for a division ring, an endomorphism of K and an S-derivation. For $C \in M_n(K)$, we define a map T_C on the vector space K^n of rows by*

$$T_C : K^n \to K^n : v \mapsto S(v)C + D(v)$$

where $v = (\alpha_1, \ldots, \alpha_n) \in K^n$ $S(v) = (S(\alpha_1, \ldots, S(\alpha_n))$ $D(v) = (D(\alpha_1), \ldots, D(\alpha_n))$.

Proposition 2.13.   *Let $T : V \to V$ be an (S, D) PLT on a left K vector space V. If $\dim_K V < \infty$ then T is similar to T_A where $A = M_{\underline{e}}(T)$ and $\underline{e}$ is any basis of V.*

Proof Let $(e_1, \ldots, e_n)$ be a basis of V. Define a linear map $\sigma : V \to K^n$ by $\sigma(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ the row with 1 in the ith entry and 0 elsewhere. By definition T is similar to $T_1 = \sigma \circ T \circ \sigma^{-1}$ defined on K^n. For $(\alpha_1, \ldots, \alpha_n) \in K^n$ and $M_{\underline{e}}(T) = A = (a_{ij}) \in M_n(K)$ let us compute

$$
\begin{aligned}
T_1(\alpha_1, \ldots, \alpha_n) &= \sigma(T(\sum \alpha_i e_i)) = \sigma \left(\sum_{j=1}^n \left(\sum_{i=1}^n S(\alpha_i) a_{ij} + D(\alpha_j) \right) e_j \right) \\
&= \left(\sum_{i=1}^n S(\alpha_i) a_{i1} + D(\alpha_1), \ldots, \sum^n S(\alpha_i) a_{ij} + D(\alpha\chi_j), \ldots \right) \\
&= T_A(\alpha_1, \ldots, \alpha_n) \qquad \square
\end{aligned}
$$

3 Algebraicity of a P.L.T.

In this section we will investigate polynomials in a PLT. Let us first recall from [LL1] the following

Definition 3.1. *A polynomial $p(t) \in R = K[t; S, D]$ is a c.v. polynomial with respect to an endomorphism S' and an S'-derivation D' of the division ring K, if for any $x \in K$ we have*

$$
p(t)x = S'(x)p(t) + D'(x) \tag{3.2}
$$

The notion of c.v. polynomials with respect to (S', D') appears naturally while investigating K-ring homomorphisms $\psi : R' = K[t'; S', D') \to R = K[t; S, D]$. In this case $\psi(t')$ is a cv polynomial in R. The name comes from the fact that polynomials of the form $at + b$ are cv polynomials (with respect to $(S' = I_a \circ S, \; aD + D_{b,S'}))$ and they define a "change of variables".

If T is an (S, D) PLT on V and $g(t) = \sum b_i t^i \in R = K[t, S, D]$ $g(T)$ will stand for $\sum b_i T^i \in \text{End } (V, +)$. For $A \in M_n(K)$ $g(A) = \sum b_i N_i(A) = \sum b_i T_A^i(I_n)$ where S and D have been extended to $M_n(K)$ in the natural way and $I_n \in M_n(K)$ is the standard identity matrix of size $n \times n$.

Lemma 3.3. *Let $T : V \to V$ be a PLT with respect to (S, D) and let $g(t) = \sum_{i=0}^n b_i t^i \in K[t; S, D]$. Then with the above notations*

a)

$$
g(T)(\alpha v) = \sum_{j=0}^n \left(\sum_{i=j}^n b_i f_j^i(\alpha) \right) T^j(v) \text{ for } v \in V \text{ and } \alpha \in K \tag{3.4}
$$

(Recall that $f_j^i \in \text{End } (K, +)$ is the sum of all words of length i with j letters S and $i - j$ letters D).

In particular

$$
T^n(\alpha v) = \sum_{j=0}^n f_j^n(\alpha) T^j(v) \tag{3.5}
$$

b) If $\underline{e} = (e_1, \ldots, e_n)$ is a basis of V and $A = (a_{ij}) = M_{\underline{e}}(T) \in M_n(K)$ then $g(T)(e_i) = \sum_{j=1}^{n} g(A)_{ij} e_j$ for $i = 1, \ldots, n$ or in matrix form

$$M_{\underline{e}}(g(T)) = g(M_{\underline{e}}(T)) \tag{3.6}$$

c) If $p(t) \in R = K[t; S, D]$ is a c.v. polynomial with respect to (S', D') then $p(T)$ is a PLT with respect to $(S'D')$. In this situation we have

- 1) $p(\{M_{\underline{e}}(T) | \underline{e} \text{ is a basis of } V\}) = \{M_{\underline{e}}(p(T)) | \underline{e} \text{ is a basis of } V\}$

$$i.e. \quad p(\Delta(T)) = \Delta(p(T)) \tag{3.7}$$

- 2) If T and T_1 are similar (S, D) PLT's then $p(T)$ and $p(T_1)$ are similar (S', D') PLT's.

$$i.e. \quad T \sim T_1 \Rightarrow p(T) \sim p(T_1) \tag{3.8}$$

- 3) For $A \in M_n(K)$ the (S', D') PLT's on $V = K^n$ defined by $p(T_A)$ and $T_{p(A)}$ are equal

$$i.e. \quad p(T_A) = T_{p(A)} \tag{3.9}$$

- 4) If $A \in M_n(K)$ and $P \in GL_n(K)$ then $p(S(P)AP^{-1} + D(P)P^{-1}) = S'(P)p(A)P^{-1} + D'(P)P^{-1}$.

$$i.e. \quad p(A^P) = p(A)^P \tag{3.10}$$

where the L.H.S. conjugation is relative to (S, D) and the R.H.S. conjugation is relative to (S', D').

d) If $g(T)$ is an (S', D') PLT then there exists a c.v. polynomial $r(t) \in R = K[t; S, D]$ with respect to (S', D') such that $g(T) = r(T)$.

Proof

a) Formula 3.5 can be proved either by a direct induction or by using the ring homomorphism $\psi : K[t; S, D] \to \text{End}(V, +)$ defined by $\psi(t) = T$ and $\psi(a) = L_a : V \to V : v \mapsto av$; $a \in K$, $v \in V$. Indeed in $R = K[t; S, D]$ we have the well known formula $t^n \alpha = \sum f_i^n(\alpha) t^i$ for $\alpha \in K$ $n \in \mathbb{N}$ and applying ψ we get Formula (3.5).

b) It is enough to prove the result for $g(t) = t^m$. We proceed by induction :
For $m = 0$ we have $g(T)(e_i) = (id)(e_i) = e_i = \sum_{j=1}^{n} \delta_{ij} e_j = \sum_{j=1}^{n} (I)_{ij} e_j$. Assume the formula holds for $g(t) = t^m$ and let us compute :

$$T^{m+1} e_i = T(T^m e_i) \quad = \quad T \left(\sum_{j=1}^{n} N_m(A)_{ij} e_j \right)$$

$$= \sum_{j=1}^{n} S(N_m(A)_{ij})T(e_j) + D(N_m(A)_{ij})e_j$$

$$= \sum_{j=1}^{n}\sum_{k=1}^{n} S(N_m(A)_{ij})A_{jk}e_k + \sum_{k=1}^{n} D(N_m(A)_{ik})e_k$$

$$= \sum_{k=1}^{n} \left[\sum_{j=1}^{n} S(N_m(A))_{ij}A_{jk} + D(N_m(A))_{ik} \right] e_k$$

$$= \sum_{k=1}^{n} N_{m+1}(A)_{ik}e_k$$

as desired.

c) If $p(t) \in R = K[t; S, D]$ is an $(S'D')$ c.v. polynomial we have for any $\alpha \in K$ $p(t)\alpha = S'(\alpha)p(t) + D'(\alpha)$. By making use of the homomorphism ψ defined in the proof of a) above we get $p(T)L_\alpha = L_{S'(\alpha)} \circ p(T) + L_{D'(\alpha)}$ and hence $p(T)(\alpha v) = S'(\alpha)p(T)(v) + D'(\alpha)v$, for any $\alpha \in K$ and any $v \in V$. This shows that $p(T)$ is an (S', D') PLT.

  1) Formula (3.6) shows that we have $p(\Delta(T)) \subset \Delta(p(T))$. Now if $B \in \Delta(p(T))$ then $B = M_{\underline{u}}(p(T))$ for some basis $\underline{u}$ of V but then $p(M_{\underline{u}}(T)) = M_{\underline{u}}(p(T)) = B$ and so $B \in p(\Delta(T))$.

  2) If $T \sim T_1$ then Proposition 1.4 (vii) shows that $\Delta(T) = \Delta(T_1)$ hence $p(\Delta(T)) = p(\Delta(T_1))$ and, by using 1) above, we conclude $\Delta(p(T)) = \Delta(p(T_1))$ and Proposition 2.4 implies $p(T) \sim p(T_1)$.

  3) Let $\underline{c} = \{e_1, \ldots, e_n\}$ be the usual canonical basis for the space K^n of rows then $M_{\underline{c}}(p(T_A)) = p(M_{\underline{c}}(T_A)) = p(A)$ and $p(T_A)$ is the (S', D') PLT on K^n defined by $p(A)$.

  4) Let $A \in M_n(K)$ $P \in GL_n(K)$ $\underline{c}$ the canonical basis of K^n and $\underline{u}$ another basis of K^n s.t. $\underline{u} = P\underline{c}$. For $T = T_A$ the (S, D) PLT determined on K^n by A we have $M_{\underline{c}}(T) = A$ and $M_{\underline{u}}(T) = S(P)AP^{-1} + D(P)P^{-1} = A^P$ and $M_{\underline{c}}(p(T)) = p(A)$, by (3.6) above. Moreover, we also have

$$p(A)^P = S'(P)p(A)P^{-1} + D'(P)P^{-1} = M_{\underline{u}}(P(T))$$
$$= p(M_{\underline{u}}(T)) = p(A^P).$$

d) The fact that $g(T)(\alpha v) = S'(\alpha)g(T)(v) + D'(\alpha)v$ for $\alpha \in K$ and $v \in V$ implies that $g(T) \circ L_\alpha - L_{S'(\alpha)} \circ g(T) - L_{D'(\alpha)} = 0 \in \mathrm{End}\,(V, +)$. Hence if $\mathrm{Ann}_R V = 0$ we conclude that $g(t)$ itself is an (S', D') c.v. polynomial. Otherwise, $g(t)\alpha - S'(\alpha)g(t) - D'(\alpha) \in \mathrm{Ann}_R V = Rf(t) \supseteq f(t)R$ where $f(t)$ is a monic right invariant polynomial generating $\mathrm{Ann}_R V$. There exist $q(t), r(t) \in R$ $\deg r(t) < \deg f(t)$ such that $g(t) = q(t)f(t) + r(t)$ and we easily get, for any $\alpha \in K$, $r(t)\alpha - S'(\alpha)r(t) - D'(\alpha) \in Rf(t)$. Since $\deg r(t) < \deg f(t)$ we conclude $r(t)\alpha = S'(\alpha)r(t) + D'(\alpha)$ for $\alpha \in K$ i.e. $r(t)$ is an (S', D') cv polynomial. The fact that $r(T) = g(T)$ is clear from the equalities $g(t) = q(t)f(t) + r(t)$ and $f(T) = 0$.

Remarks 3.11. With the notations of the lemma we have, for $C \in C^{S,D}(A) = \{C \in M_n(K) \mid S(C)A + D(C) = AC\}$, $g(T_A)(vC) = g(T_A)(v)C$ for any $v \in K^n$. And we conclude that Ker $g(T_A)$ is a right $C^{S,D}(A)$-module. For $n = 1$ this gives back the classical fact (cf. [LL2] §3) that $E(g, a) = \{y \in K^* \mid g(a^y) = 0\} \cup \{0\}$ is a $C^{S,D}(a)$-right vector space.

As noticed earlier, if $p(t) \in R = K[t; S, D]$ is an (S', D') c.v. polynomial there exists a ring homomorphism $\varphi : R' = K[t'; S', D'] \to R = K[t; S, D]$. So any left R-module inherits an R'-module structure. The next proposition analizes this situation.

Proposition 3.12. Let $T : V \to V$ be an (S, D) PLT and let $\varphi : R' = K[t'; S', D'] \to R = K[t; S, D]$ be the K-ring homomorphism defined by an (S', D') c.v. polynomial $p(t) \in R$. The R'-module structure induced on V via φ by T corresponds to the R'-module structure given by the (S', D') PLT $p(T)$. In particular if $g(t') \in R'$ we have for $A \in M_n(K)$

$$g(p)(T_A) = g(T_{p(A)}) \tag{3.13}$$

and for $A \in M_n(K)$, $P \in GL_n(K)$

$$g(p)(A^P) = g(p(A)^P) \tag{3.14}$$

where $g(p) \in R$, T_A and $T_{p(A)}$ stand for an (S, D) and (S', D') PLT respectively, $A^P = S(P)AP^{-1} + D(P)P^{-1}$ and $p(A)^P = S'(P)p(A)P^{-1} + D'(P)P^{-1}$.

Proof By definition of the induced R'-module structure of V via φ we have for $g(t') = \sum_{i=0}^n a_i t'^i \in R'$ and $v \in V$ $g(t') \cdot v = \varphi(g(t')) \cdot v = g(p(t)) \cdot v = \sum_{i=0}^n a_i p(t)^i \cdot v = \sum_{i=0}^n a_i p(T)^i(v) = g(p(T))(v)$ and $p(T)$ in an (S', D') PLT as remarked in the lemma.

From these equalities we extract $g(p(t)) \cdot v = g(p(T))(v)$ and so $g(p)(T) = g(p(T))$. In particular $g(p)(T_A) = g(p(T_A)) = g(T_{p(A)})$ (by 3.9). We have, by making use of Theorem 2.8 and Formula (3.13), $g(p)(A^P)P = g(p)(T_A)(P) = g(T_{p(A)})(P) = g(p(A)^P)P$. This proves formula (3.14). $\qquad\square$

Notice that formula (3.14) was obtained for $n = 1$ $P = 1$ in [LL2]. This was called the composite function theorem. In this respect we could say that Proposition 3.12 generalizes the composite fonction theorem and says that the R'-module structure induced by φ on V is given by $p(T)$.

Definition 3.15.

a) *An (S, D) PLT $T : V \to V$ is algebraic if there exist $n \in \mathbb{N}^*$, $a_0, a_1, \ldots, a_n \in K$, $a_n \neq 0$ such that $a_n T^n + \cdots + a_1 T + a_0 I = 0$.*

b) *A set $\Delta \subset M_n(K)$ of matrices is (S, D) algebraic if there exists $g(t) = \sum a_i t^i \in K[t; S, D]$ such that $g(A) = \sum a_i N_i(A) = 0$ for any $A \in \Delta$.*

Remarks 3.16. a) Unlike classical linear transformations of a finite dimensional vector spaces over a commutative field, a pseudo-linear transformation need not be algebraic.

b) A finite set of matrices $\Delta \subset M_n(K)$ is always (S, D) algebraic. Indeed if $\Delta = \{A\}$ then $I, A, N_2(A), \ldots, N_{n^2}(A)$ are matrices in $M_n(K)$ and are left K-dependant. For $\Delta = \{A_1, \ldots, A_s\}$, $s \in \mathbb{N}$, it suffices to consider the left least common multiple in $R = K[t; S, D]$ of polynomials annihilating the A_i's.

Lemma 3.17. *Let T be an (S, D) PLT on V and $f(t) \in R = K[t; S, D]$.*

a) *If T is algebraic, its monic minimal polynomial f_T is invariant in R and $f_T R \subseteq R f_T = \operatorname{ann}_R V$ where the left R-module structure on V is induced by the action of T.*

b) *If f is semi-invariant (i.e. $(S', 0)$ c.v. polynomial) and $\underline{e}$ is a basis of V then $f(T) = 0$ if and only if $f(M_{\underline{e}}(T)) = 0$. In particular this is true if f is invariant.*

c) *If T_1 is an (S, D) PLT on V_1 similar to T, then T is algebraic if and only if T_1 is algebraic and moreover T and T_1 have the same monic minimal polynomial.*

Proof

a) is easy and left to the reader.

b) Of course if $f(T) = 0$ then Formula 3.6 shows that $f(M_{\underline{e}}(T)) = M_{\underline{e}}(f(T)) = 0$. On the other hand, if $f(M_e(T)) = 0$ then $M_{\underline{e}}(f(T)) = 0$ but, by Lemma 3.3, $f(T)$ is an $(S', 0)$ PLT and so for $v = \sum \alpha_i e_i \in V$ we have

$$f(T)v = f(T)\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} S'(\alpha_i) f(T)(e_i) = 0$$

c) This is straightforward since $T \sim T_1$ iff T and T_1 induce isomorphic left R-module structure on V and V_1 respectively and this implies $\operatorname{ann}_R V = \operatorname{ann}_R V_1$

$\square$

Theorem 3.18. *Let T be an (S,D)PLT on V and let $f(t) \in R = K[t; S, D]$ be a monic invariant polynomial. Then the following are equivalent.*

(i) *T is algebraic and f is its minimal monic polynomial.*

(ii) *$fR \subseteq Rf = \operatorname{ann}_R V$ where the left R-module structure on V is given by the action of T.*

(iii) *For any basis $\underline{e}$ of V, the (S,D)PLT on K^n, $T_{M_{\underline{e}}(T)}$ is algebraic and f is its minimal monic polynomial.*

(iv) *There exists a basis $\underline{e}$ of V such that the (S,D)PLT on K^n, $T_{M_{\underline{e}}(T)}$ is algebraic and f is its minimal monic polynomial.*

(v) *There exists a basis $\underline{e}$ of V such that the $f(M_{\underline{e}}(T)) = 0$ and f is of minimal degree among invariant polynomials annihilating $M_{\underline{e}}(T)$.*

(vi) $\Delta(T) = \{M_{\underline{e}}(T)|\underline{e}$ is a basis of $V\}$ is (S, D) algebraic and f is its minimal polynomial.

Proof Let us first remark that a monic invariant polynomial of degree m is in particular an $(S^m, 0)$ c.v. polynomial.

The implications (i) $\leftrightarrow$ (ii) and (iii) $\rightarrow$ (iv) are obvious.
(ii) $\leftrightarrow$ (iii) is a direct consequence of the above lemma and of the fact that for any basis $\underline{e}$ of V, T is similar to $T_{M_{\underline{e}}(T)}$.
(iv) $\leftrightarrow$ (v) is clear in view of Lemma 3.17 b).
(v) $\rightarrow$ (vi) Assume $f(M_{\underline{e}}(T)) = 0$ and let $M_{\underline{u}}(T) \in \Delta(T)$ then there exists $P \in GL_n(K)$ such that $M_{\underline{u}}(T) = M_{\underline{e}}(T)^P = S(P)M_{\underline{e}}(T)P^{-1} + D(P)P^{-1}$ and since f is an $(S^m, 0)$ c.v. polynomial we get, by Lemma 3.3 c) - 4 that $f(M_{\underline{u}}(T)) = S^m(P)f(M_{\underline{e}}(T))P^{-1} = 0$.
(vi) $\rightarrow$ (i) For any basis $\underline{e}$ of V we have $M_{\underline{e}}(f(T)) = f(M_{\underline{e}}(T)) = 0$. Hence $f(T) = 0$ and the minimality of $\deg f$ amongst $f \in Ann_R V$ is obvious from the already proved implication (i) $\rightarrow$ (vi). $\square$

We will now look to the question of the transfer of algebraicity via c.v. polynomials. We need the following easy but useful

Lemma 3.19. *Let $p \in R = K[t; S, D]$ be any polynomial of degree ≥ 1 and f any non zero polynomial in R. Then $Rf \cap K[p] \neq 0$ where $K[p]$ is the left K vector space generated by powers of $p : K[p] = \{\sum \alpha_i p^i | \alpha_i \in K\}$.*

Proof If $Rf \cap K[p] = 0$ then $K[p]$ embeds in R/Rf but $\dim_K K[p] = \infty$ and $\dim_K R/Rf < \infty$. $\square$

Theorem 3.20. *Let p be an (S', D') c.v. polynomial of degree ≥ 1 and let T be an (S,D)PLT on the vector space V. Then*

a) *T is algebraic iff the (S', D') PLT $p(T)$ is algebraic.*

b) *$\Delta \subset M_n(K)$ is (S, D) algebraic iff $p(\Delta)$ is (S', D') algebraic.*

Proof

a) Assume T is algebraic then $ann_R V = Rf \supseteq fR$ where f is the monic minimal polynomial of T. Thanks to the above lemma there exist $a_0, \ldots, a_l \in K$ s.t. $\sum a_i p(t)^i \in Rf$ and we conclude that $\sum a_i p(T)^i = 0$ i.e. $p(T)$ is algebraic.

Conversely if $p(T)$ is algebraic, say $g(p(T)) = 0$ then $g(p(t)) \in ann_R V$.

b) Assume $\Delta \subset M_n(K)$ is (S, D) algebraic and let $f(t) \in K[t; S, D]$ be such that $f(A) = 0$ for any $A \in \Delta$. By the lemma we have $Rf \cap K[p] \neq 0$ and thus there exists $a_0, \ldots, a_l \in K$ such that $0 \neq \sum_{i=0}^{l} a_i p(t)^i \in Rf(t)$. Let $g(t') = \sum_{i=0}^{l} a_i t'^i \in R' = K[t'; S', D']$ we have $g(p(t)) \in Rf$ and $g(p)(A) = 0$ (since in $M_n(K)[t; S, D]$ $t - A$ divides on the right $f(t)$ and so also $g(p(t))$). By making use of 3.14 we conclude that for any $A \in \Delta$ $g(p(A)) = 0$ i.e. $g(p(\Delta)) = 0$ and this shows that $p(\Delta)$ is $(S'D')$ algebraic. The converse is an easy application of Formula 3.14.

□

Corollary 3.21.

Let K, S, D be a division ring, an endomorphism of K and an S-derivation of K respectively. Suppose that :

- for any $n \in \mathbb{N}^*$ and any $A \in M_n(K)$, A is algebraic over $Z(K)$ the center of K.

- $R = K[t; S, D]$ contains an (id.,0) c.v. polynomial of degree ≥ 1.

Then every (S, D) PLT on a finite dimensional left K-vector space is algebraic.

Proof Let $T : V \to V$ be an (S, D) PLT and put $n = \dim V$. Let $g(t) \in R$ be an (id.,0) c.v. of degree ≥ 1 whose existence is asserted in hypothesis 2. Theorem 3.18 shows that T is algebraic iff $\Delta(T) \subset M_n(K)$ is (S, D) algebraic and by Theorem 3.20 $\Delta(T)$ is (S, D) algebraic iff $g(\Delta(T))$ is algebraic i.e. iff $\Delta(g(T))$ is algebraic. But hypothesis 1 implies that any conjugacy class in $M_n(K)$ is algebraic and so $\Delta(g(T))$ is algebraic as desired. □

The next remarks concern the hypothesis made in the above corollary.

Remarks.
a) The hypothesis 1) in the corollary is satisfied in particular when either K is locally finite dimensional over its center or when K is algebraic over its center $Z(K)$ which is in turn uncountable..

The hypothesis 1) is equivalent to asking that every linear transformation on a finite dimensional K vector space is algebraic.
b) The hypothesis 2) is satisfied when R is non simple and a non zero power of S is inner.

We will now give, as an application of the preceeding results, different characterizations of the primitivity of $R = K[t; S, D]$.

Theorem 3.23. *Let K, S, D be a division ring, an endomorphism of K and a S-derivation respectively. Then the following are equivalent*

(i) $R = K[t; S, D]$ is left primitive.

(ii) There exists a faithful left R-module V such that $\dim_K V < \infty$.

(iii) There exists a non algebraic (S, D) PLT $T : V \to V$ such that $\dim_K V < \infty$.

(iv) There exists a positive integer n and an (S, D) conjugacy class $\Delta^{S,D}(A) \subset M_n(K)$ which is not (S, D) algebraic.

(v) There exists $n \in \mathbb{N}$ and $A \in M_n(K)$ such that A is not annihilated by an invariant polynomial of R.

Proof (i) $\to$ (ii) This is clear since any left ideal of R is of the form $Rg(t)$ for some $g(t) \in R$ and $\dim_K R/Rg(t) = \deg g(t)$.

(ii) $\to$ (i) This comes from the fact that R is prime and for prime rings primitivity is equivalent to the existence of a faithful left R-module of finite length ([MR] Lemma 9.6.10).

(ii) $\leftrightarrow$ (iii) It suffices to notice that R-modules correspond to (S, D) PLT's and in this correspondence faithfulness corresponds to non algebraicity.

(iii) $\leftrightarrow$ (iv) Follows from equivalence (i) $\leftrightarrow$ (vi) in Theorem 3.18.

(iv) $\leftrightarrow$ (v) Also follows from Theorem 3.18. $\square$

Equivalence (i) $\leftrightarrow$ (v) of the above theorem gives a characterization of primitivity of $R = K[t; S, D]$ similar to the classical one obtained for $K[t]$ (and more generally for $K[t_1, \ldots, t_n]$) by Amitsur and Small (cf. MR Chap 9). We will soon give a characterization of the primitivity of R which avoids (S, D) evaluations. This will enable us to show that R is left primitive if and only if it is right primitive. For this we need the following.

Proposition 3.24. *Suppose there exists a non constant (S', D') c.v. polynomial p in $R = K[t; S, D]$ and let R' be the Ore extension $K[t'; S', D']$. Then*

a) *R' is left primitive if and only if R is left primitive.*

b) *If R' is right primitive then R is right primitive.*

Proof Let us prove that if R' is left (resp. right) primitive then R is left (resp. right) primitive. There is a ring embedding $\varphi : R' \to R$ define by $\varphi(a) = a$ for $a \in K$ and $\varphi(t') = p(t)$, hence we can replace R' by its image $\varphi(R') = K[p] \subset R$. So let us suppose that $K[p]$ is a left (resp. right) primitive subring of R and let m be a left (resp. right) maximal ideal in $K[p]$ which contains no non zero 2-sided ideal. Let M be a left (resp. right) maximal ideal of R containing Rm (resp mR). Since $Rm \neq R$ (resp. $mR \neq R$) we have $M \neq R$. Since m is maximal in $K[p]$ and $M \cap K[p] \supset m$ we conclude that $M \cap K[p] = m$. Assume M contains I a 2-sided ideal of R then $I \cap K[p] \neq 0$, by Lemma 3.19, and this contradicts the fact that m does not contain non zero 2-sided ideals. We conclude that M is a maximal left (resp. right) ideal of R which contains no non zero 2-sided ideals. It remains to show that if R is left primitive then R' is left primitive. Now if R is left primitive, Theorem 3.23 (iv) shows that there exists $\Delta^{S,D}(A)$, $A \in M_n(K)$, an (S, D) conjugacy class which is not (S, D)-algebraic and so $p(\Delta^{S,D}(A)) = \Delta^{S',D'}(p(A))$ is not (S', D') algebraic thanks to Formula 3.10 and Theorem 3.20 b. Theorem 3.23 (iv) enables us to conclude that $R' = K[t'; S', D']$ is left primitive. $\square$

Remark 3.25. Corollary 3.27 will show that the converse of (b) in the above proposition is also true.

It is now an easy task to express primitivity of $R = K[t; S, D]$ in terms of "usual" algebraicity over $Z(K)$ the center of K.

Theorem 3.26.

With the same notations as in Theorem 3.23, the following assertions are equivalent :

(i) $R = K[t; S, D]$ *is left primitive*

(ii) $R = K[t; S, D]$ *is right primitive*

(iii) *One of the following conditions holds*

    a - *R is simple*

    b - *R is not simple but S^ℓ is not an inner automorphism for any $\ell > 0$*

    c - *R is not simple, a non zero power of S is an inner automorphism and the (usual) polynomial ring $K[x]$ is primitive.*

(iv) *One of the following conditions holds*

    a' - *R is simple*

    b' - *R is not simple but S^ℓ is not an inner automorphism for any $\ell > 0$*

    c' - *R is not simple, a non zero power of S is an inner automorphism and there exists $n \in \mathbb{N}$ and $A \in M_n(K)$ such that A is not algebraic over $Z(K)$.*

Proof (i) $\rightarrow$ (iii) : If R is left primitive but a) and b) above are false then R is not simple and a non zero power of S is an inner automorphism so the center of R is non trivial (cf. [LTVP] Proposition 2.3). In particular there exists and $(Id, 0)$ c.v. polynomial $p \in R$ and thanks to the above proposition we conclude that $K[p] \cong K[x]$ is primitive.

(ii) $\rightarrow$ (iii) : Suppose R is right primitive but a) and b) are false then R is not simple and a non zero power of S is an inner automorphism. We conclude in particular that the center of R is non trivial. Since $S \in Aut(K)$ the left primitive ring R^{op} is equal to $K^{op}[t, S^{-1}, -DS^{-1}]$ and R^{op} has a non trivial center. Let $p \in R^{op}$ be a central no constant polynomial. Proposition 3.24 shows that $K^{op}[p]$ is left primitive and so $K[p] \cong K[x]$ is right primitive.

(iii) $\rightarrow$ (i) and (iii) $\rightarrow$ (ii) : We will prove these two implications simultaneously by showing that if one of the conditions a), b) or c) is satisfied then R is both left and right primitive. If R is simple then obviously R is left and right primitive. If R is not simple but no non zero power of S is inner then there exists a semi invariant monic polynomial $p \in R$ of degree $n \geq 1$ ([LLLM], Theorem 3.6) and $T := K[x; S^n] \cong K[p; S^n] \subset R$ but since no power of S^n is inner, the 2-sided ideals of $T = K[x; S^n]$ are all of the form Tx^i $i > 0$ and it is easy to check that none of them is contained in the maximal left ideal $T(x - 1)$ nor in the maximal right ideal $(x - 1)T$. So T is left and right primitive and Proposition 3.24 shows that R is left and right primitive. Let us now assume that c) is satisfied then the center of R is non trivial [loc. cit.] and if p is a non constant central polynomial then $K[x] \cong K[p]$ is right and left primitive and hence, using Proposition 3.24 again, we conclude that R is left and right primitive.

(iii) $\leftrightarrow$ (iv) : It is enough to prove that c) is equivalent to c'); but this follows from the classical Amitsur-Small's theorem which characterizes the primitivity of a polynomial ring in commuting variables over a division ring (cf. [MR] Chapter 9).□

We are now able to complete Proposition 3.24.

Corollary 3.27. *Let $p \in R = K[t; S, D]$ be an (S', D') c.v. polynomial of degree ≥ 1. Let R' denote the skew polynomial ring $K[t'; S', D']$. Then the following assertions are equivalent*

(i) *R' is left primitive.*

(ii) *R' is right primitive.*

(iii) *R is left primitive.*

(iv) *R is right primitive.*

Proof The obvious proof is left to the reader.   □

Remarks 3.28. 1) If $S \in Aut(K)$ the equivalence (ii) ↔ (iv) in Corollary 3.27 can be obtained directly using the fact that R is then a left and right principal ideal domain.

2) If $S \in Aut(K)$ the equivalence (ii) ↔ (iii) in Corollary 3.27 can be obtained via a corollary of a result due to Jategaonkar and Letzter (cf. GW] Corollary 7.17).

4   Eigenvalues and diagonalization.

We will use the results of Sections 2 and 3 to study eigenvalues and diagonalization of algebraic PLT's. We will also give sufficient conditions for $A \in M_n(K)$ to be (S, D) equivalent to a diagonal matrix. In this section we will assume that S is an automorphism and D an S-derivation of a division ring K. We recall without proof a few properties of invariant polynomials of $R = K[t; S, D]$.

Proposition 4.1. (cf. [LL1]) *With the above notations if a monic polynomial $f \in R$ is right invariant ($fR \subseteq Rf$) then :*

a) *$Rf = fR$,*

b) *f is an $(S^\ell, 0)$ c.v. polynomial where $\ell = \deg f$,*

c) *$g \in R$ divides f on the right iff $g \in R$ divides f on the left*

d) *For $a \in K$, if $f(a) = 0$ then $f(\Delta^{S,D}(a)) = 0$ where $\Delta_{(a)}^{S,D} = \{a^x = S(x)ax^{-1} + D(x)x^{-1} \mid x \in K^*\}$.*

e) *If $\Delta \subset K$ is (S, D)-algebraic and closed by (S, D)-conjugation then its monic minimal polynomial $f_\Delta \in R$ is right invariant and if $q \in K$ is such that $f_\Delta(q) = 0$ then $q \in \Delta$.*   □

Proposition 4.2. *Let T be an (S, D) PLT on a vector space V. If $\gamma_1, \ldots, \gamma_s \in K$ are eigenvalues belonging to different (S, D) conjugacy classes and $v_1, \ldots, v_s \in V$ are corresponding eigenvectors ($T(v_i) = \gamma_i v_i$, $i = 1, \ldots, s$) then $v_1, \ldots, v_s$ are left linearly independant.*

Proof Assume $v_1, \ldots, v_s$ are linearly dependant and choose a shortest depen-dance relation : $\sum_{i=0}^{\ell} \beta_i v_i = 0$ $\beta_i \in K$ $\beta_\ell = 1$. Applying T we get $\sum_{i=1}^{\ell}(S(\beta_i)\gamma_i + D(\beta_i))v_i = 0$ from this relation we substract $\sum_{i=0}^{\ell} \gamma_\ell \beta_i v_i = 0$ and we obtain $\sum_{i=1}^{\ell-1}(S(\beta_i)\gamma_i + D(\beta_i) - \gamma_\ell \beta_i)v_i = 0$. Since γ_ℓ is not (S, D) conjugate to γ_i, this equation is a shorter non trivial relation for the v_i's. This contradiction shows that the v_i's are linearly independant. □

Proposition 4.3. *Let $T : V \to V$ be an (S, D) PLT and $\alpha \in K$, $v \in V$ be an eigenvalue and its corresponding eigenvector : $T(v) = \alpha v$. Then :*

- $T^n(v) = N_n(\alpha)v = T_\alpha^n(1)v$ *for any $n \in \mathbb{N}$. More generally for any $g(t) \in R = K[t; S, D]$ we have $g(T)(v) = g(\alpha)v$.*

- *For $\beta \in K \smallsetminus \{0\}$, $T(\beta v) = \alpha^\beta \beta v$ where $\alpha^\beta = S(\beta)\alpha\beta^{-1} + D(\beta)\beta^{-1}$. More generally for any $g(t) \in R = K[t; S, D]$ $g(T)(\beta v) = g(\alpha^\beta)\beta v$.*

- *If $\dim_K V = n$ and $\underline{e} = (e_1, \ldots, e_n)$ is a basis of V, writing $v = \sum \alpha_i e_i$ and $\underline{v} = (\alpha_1, \ldots, \alpha_n)$ we have $S(\underline{v})M_{\underline{e}}(T) + D(\underline{v}) = \alpha \underline{v}$.*

Proof 1) Let us prove that $T^n(v) = N_n(\alpha)v$ by induction on $n \in \mathbb{N}$. If $n = 0$ we have $T^0 = id$ $N_0(\alpha) = 1$ and the formula is true. Now assume $T^n(v) = N_n(\alpha)v$ and let us compute $T^{n+1}(v) = T(N_n(\alpha)v) = S(N_n(\alpha))T(v) + D(N_n(\alpha))v = [S(N_n(\alpha))\alpha + D(N_n(\alpha))]v = N_{n+1}(\alpha)v$. From this we immediately get the conclusion $g(T)(v) = g(\alpha)v$.

2) Let us compute : $T(\beta v) = S(\beta)T(v) + D(\beta)v = (S(\beta)\alpha + D(\beta))v$. Hence $T(\beta v) = (S(\beta)\alpha\beta^{-1} + D(\beta)\beta^{-1})\beta v = \alpha^\beta \beta v$. From this and part 1) we easily obtain the more general result.

3) This is straightforward and is left to the reader. □

Let us denote $\Gamma_T := \{\alpha \in K | T(v) = \alpha v$ for some non zero $v \in V\}$.

Remarks 4.4. a) Proposition 4.3 2) shows that Γ_T is closed by (S, D) con-jugations. If $\dim_K V = n$ we will write $\Gamma_T = \Gamma_1 \cup \ldots \cup \Gamma_r$ where $\Gamma_i = \Delta^{S,D}(\gamma_i) = \{\gamma_i^x | x \in K^*\}$. Notice that $r \leq n$.
b) If $T = T_a : K \mapsto K$ then $\Gamma_T = \Delta^{S,D}(a) = \{S(x)ax^{-1} + D(x)x^{-1} | x \in K^*\}$.
c) If T and T_1 are similar (S, D) PLT's on V and V_1 respectively then $\Gamma_T = \Gamma_{T_1}$.
d) If $p(t) \in R = K[t; S, D]$ is an (S', D') c.v. polynomial then $p(\Gamma_T) \supseteq \Gamma_{p(T)}$.
The proofs of these remarks are left to the reader.
We now turn to algebraic PLT's.

Proposition 4.5. *Let T be an algebraic (S, D) PLT on V and let $f_T(t) \in R = K[t; S, D]$ be its minimal polynomial, the following are equivalent*

(i) $\alpha \in K$ is an eigenvalue for T (i.e. $\alpha \in \Gamma_T$)

(ii) $t - \alpha$ divides on the right the polynomial $f_T(t)$ in $R = K[t; S, D]$.

(iii) $t - \alpha$ divides on the left the polynomial $f_T(t)$ in $R = K[t; S, D]$.

Proof (i) $\rightarrow$ (ii) Let $v \in V \smallsetminus \{0\}$ be such that $T(v) = \alpha v$ and put $f_T = \sum a_i t^i \in R$ then $0 = f_T(T)(v) = f_T(\alpha)v$ (by Proposition 4.3. (1)), and so $f_T(\alpha) = 0$. Hence we conclude $t - \alpha$ divides f_T on the right in R.

(ii) $\rightarrow$ (iii) This is an easy and well known property of invariant polynomials (cf. 4.1)

(iii) $\rightarrow$ (i) Suppose we have $f_T(t) = (t - \alpha)g(t)$ in R. Since $f_T(t)$ is the minimal (monic) polynomial of T, there exists $v \in V$ s.t. $\omega := g(t)(v) \neq 0$ and we get $0 = f_T(t)(v) = T(\omega) - \alpha\omega$. $\square$

Corollary 4.6. *Let T be an algebraic (S, D) PLT on V and let $f_T(t) \in R$ be its minimal polynomial, then*

a) *Γ_T is an (S, D)-algebraic (S, D) closed subset of K and the minimal monic polynomial of Γ_T, f_{Γ_T} divides f_T in R.*

b) *f_T has roots in at most $n = \dim V$ (S, D) conjugacy classes*

Proof a) and b) are easy consequences of Propositions 4.2. and 4.5. $\square$

Let us write V_Γ (resp. V_{Γ_i} $i = 1, , \ldots, r$) for the vector space spanned by the eigenvectors of T (resp. the eigenvectors of T associated to an eigenvalue in Γ_i) (recall that $\Gamma = \cup_{i=1}^r \Gamma_i$).

Lemma 4.7. *With the above notations we have*

a) *$r \leq \min\{\deg f_T, \dim V\}$*

b) *For any $i \in \{1, \ldots, r\}$ V_{Γ_i} is a left R submodule of V. If f_{Γ_i} denotes the minimal monic polynomial of Γ_i, we have $Rf_{\Gamma_i} = annV_{\Gamma_i}$. Moreover $f_{\Gamma_i}f_{\Gamma_j} = f_{\Gamma_j}f_{\Gamma_i}$ for any $i, j \in \{1, \ldots, r\}$.*

c) *$V_\Gamma = \bigoplus_{i=1}^r V_{\Gamma_i}$ and if f_Γ denotes the minimal polynomial of Γ_T then*

1) *f_Γ divides f_T*

2) *$Rf_\Gamma = annV_\Gamma$*

3) *$f_\Gamma = \prod_{i=1}^r f_{\Gamma_i}$*

Proof a) Proposition 4.2 implies $r \leq \dim V$, on the other hand $\Gamma_i = \Delta^{S,D}(\gamma_i)$ where γ_i is not (S, D) conjugate to γ_j if $i \neq j$ and Proposition 4.5 shows that $f_T(\gamma_i) = 0$. But f_T can have roots in at most $\deg f_T$ distinct (S, D) conjugacy classes (cf. [LL3]) and hence $r \leq \deg f_T$.

b) Let us remark that if $\Gamma_i = \Delta^{S,D}(\gamma_i)$ then $V_{\Gamma_i} = Vect\{v \in V | T(v) = \gamma_i v\}$ this is clear since if $T(\omega) = \gamma_i^x \omega, \omega \in V, x \in K^*$, then $T(x^{-1}\omega) = \gamma_i x^{-1}\omega$ and so we need only take into account eigenvectors relative to γ_i. It is easy to observe that $\Gamma_i \subset \Gamma_T$ is an (S, D) algebraic subset of K and that $f_{\Gamma_i}(t)$, being divisible on the right by $t - \gamma_i^x$ for any $x \in K^*$, is such that $f_{\Gamma_i}(T)(V_{\Gamma_i}) = 0$. On the other hand if $g(t) \in R = K[t; S, D]$ is such that $g(T)(V_{\Gamma_i}) = 0$ and if $T(v) = \gamma_i v$ we have $T(xv) = \gamma_i^x xv$ for any $x \in K^*$, so $0 = g(T)(xv) = g(\gamma_i^x)xv$. Hence $g(\gamma_i^x) = 0$ for any $x \in K^*$ and finally $g(t) \in Rf_{\Gamma_i}$. The fact that f_{Γ_i} and f_{Γ_j} commute is an

obvious consequence of the fact that $f_{\Gamma_i} f_{\Gamma_j}$ and $f_{\Gamma_j} f_{\Gamma_i}$ are both the monic miminal polynomial of $\Gamma_i \cup \Gamma_j$.

c) For $i \in \{1, \ldots, r\}$. let $\{v_{i1}, v_{i2}, \ldots, \ldots v_{in_i}\}$ be a basis for V_{Γ_i} s.t. $T(v_{ij}) = \gamma_i^{x_{ij}} v_{ij}$ where $\Gamma_i = \Delta^{S,D}(\gamma_i)$ and $x_{ij} \in K^*$. We will show that the vectors $v_{11}, \ldots, v_{1n_1}$, $v_{21}, \ldots, v_{2n_2}, \ldots, v_{rn_r}$ are linearly independant over K. Assume at the contrary that $v_{11} = \sum_{j \neq 1} \alpha_{1j} v_{1j} + \sum_{\substack{i \neq 1 \\ j=1 \ldots n_i}} \alpha_{ij} v_{ij}$ is a minimal relation among the v_{ij}'s. By the standard method we get

$$\sum_{j \neq 1} \left(S(\alpha_{1j}) \gamma_1^{x_{1j}} + D(\alpha_{1j}) - \gamma_1^{x_{11}} \alpha_{1j} \right) v_{1j}$$

$$+ \sum_{\substack{i \neq 1 \\ j=1 \ldots n_i}} (S(\alpha_{ij}) \gamma_i^{x_{ij}} + D(\alpha_{ij}) - \gamma_1^{x_{11}} \alpha_{ij}) v_{ij} = 0$$

which is a shorter relation.

By minimality we conclude that for $i \neq 1$ and $j \in \{1, \ldots, n\}$ we have $S(\alpha_{ij}) \gamma_i^{x_{ij}} + D(\alpha_{ij}) - \gamma_1^{x_{11}} \alpha_{ij} = 0$. Since γ_i and γ_1 are not (S, D) conjugate this implies that $\alpha_{ij=0}$ for $i > 1$ and our initial relation is in fact a non trivial relation between $v_{11}, \ldots, v_{1n_1}$. But this is impossible since $\{v_{11}, \ldots, v_{1n_1}\}$ is a basis of V_{Γ_1} by hypothesis. From this it is easy to conclude that $V_{\Gamma} = \oplus V_{\Gamma_i}$ and the properties of f_{Γ} and the f_{Γ_i}'s are direct consequences of previous results. $\qquad\square$

As usual we will say that T is diagonalizable if there exists a basis of V consisting of eigenvectors. We need the easy technical but useful

Lemma 4.8. *Let $T : V \to V$ be an algebraic (S, D) PLT with minimal monic polynomial f_T and let $\Gamma = \Delta^{S,D}(\alpha)$, $\alpha \in K$, be an algebraic (S, D) conjugacy class with minimal polynomial f_{Γ}. If $f_{\Gamma} = f_T$ then T is diagonalizable. If $\dim V = n$ there exists a basis $\underline{e} = \{e_1, \ldots, e_n\}$ of V such that $T(e_i) = \alpha e_i$ i.e. $M_{\underline{e}}(T) = diag(\alpha, \ldots, \alpha)$.*

Proof Since $f_T = f_{\Gamma}$ we have $f_T(t) = (t - \alpha)q(t)$ for some polynomial $q(t) \in R = K[t; S, D]$. Let V_{Γ} be the vector space generated by the eigenvectors associated to eigenvalues in Γ. We have to prove that $V_{\Gamma} = V$. V_{Γ} is a left R-submodule of V and for any $v \in V$ we have $(T - \alpha)(q(T)(v)) = f_T(T)(v) = 0$; hence $q(T)(V) \subset V_{\Gamma}$ or in other words $q(t) \in ann_R(V/V_{\Gamma})$. Assume that V/V_{Γ} is non zero and let $h(t) \in R$ be a non constant monic polynomial such that $Rh(t) = ann_R(V/V_{\Gamma})$. By the above observations we conclude that $h(t)$ divides $q(t)$ and in particular $h(t)$ divides $f_T(t)$ and $1 \leq \deg h(t) < \deg f_T$. Let us write $f_{\Gamma} = f_T = gh$ for some $g \in R$. Since h is invariant we easily see from 4.1 that if $h(\gamma) = 0$, for some $\gamma \in \Gamma$, then for any $x \in K^*, h(\gamma^x) = S^{\ell}(x)h(\gamma)x^{-1} = 0$ where $\ell = \deg h$. This means that if there exists $\gamma \in \Gamma$ such that $h(\gamma) = 0$ then $h(\Gamma) = 0$ but this contradicts the fact that $f_{\Gamma} = f_T$ is the minimal polynomial for Γ. On the other hand if for any $\gamma \in \Gamma, h(\gamma) \neq 0$ then since $f_{\Gamma} = f_T = hg$, using Corollary 2.10, we get that $g(\Gamma) = 0$ which also contradicts the minimality of f_{Γ}. This shows that V/V_{Γ} must be the zero module and so $V = V_{\Gamma}$. Let $f_1, \ldots, f_n$ be a basis of V consisting of eigenvectors associated to $\alpha^{x_1}, \ldots, \alpha^{x_n}, \{x_1, \ldots, x_n\} \subset K^*$ respectively. Then the vectors $e_1 = x_1^{-1} f_1, \ldots, e_n = x_n^{-1} f_n$ form a basis of V such that $T(e_i) = \alpha e_i$ $i = 1, \ldots, n$ $\qquad\square$

Theorem 4.9. *Let T be an (S, D) PLT on a left K vector space V such that $\dim V = n$. Let f_T be its minimal monic polynomial and $\Gamma = \cup_{i=1}^r \Delta^{S,D}(\gamma_i)$ the set of eigenvalues of T. Then the following assertions are equivalent :*

(i) *T is diagonalizable,*

(ii) *there exists $\underline{e}$ a basis of V such that $M_{\underline{e}}(T)$ is diagonal (in other words $\Delta(T)$ contains a diagonal matrix),*

(iii) *there exists $\underline{e}$ a basis of V and $\{\delta_1, \ldots, \delta_n\} \subset K$ such that $T_{M_{\underline{e}}(T)} = T_{\delta_1} \oplus \cdots \oplus T_{\delta_n}$ where $\oplus_{i=1}^n T_{\delta_1} : K^n \longrightarrow K^n : (\alpha_1, \ldots, \alpha_n) \longmapsto (T_{\delta_1}(\alpha_1), , \ldots, T_{\delta_n}(\alpha_n)),$*

(iv) *$V_\Gamma = V$, where V_Γ is the vector space generated by the eigenvectors of T,*

(v) *$f_\Gamma = f_T$, where f_Γ is the minimal polynomial of Γ,*

(vi) *$\deg f_\Gamma = \deg f_T$,*

(vii) *$f_T = \prod_{i=1}^r f_{\Gamma_i}$, where f_{Γ_i} is the minimal polynomial of $\Gamma_i = \Delta^{S,D}(\gamma_i)$;*

(viii) *$\sum_{i=1}^n [K : C^{S,D}(\gamma_i)]_{right} = \deg f_T$ where $C^{S,D}(\gamma_i) = \{x \in K^* \mid \gamma_i^x = \gamma_i\} \cup \{0\}$ is a subdivision ring of K.*

Proof (i) $\rightarrow$ (ii) is clear : take $\underline{e}$ to be a basis consisting of eigenvectors.
(ii) $\rightarrow$ (iii) If $A = M_{\underline{e}}(T) = diag(\delta_1, \ldots, \delta_n)$ we obviously have $T_A = \oplus_{i=1}^n T_{\delta_i}$.
(iii) $\rightarrow$ (iv) If $T_{M_{\underline{e}}(T)} = \oplus_{i=1}^n T_{\delta_i}$ we have $M_{\underline{e}}(T) = diag(\delta_1, \ldots, \delta_n)$ and so $T(e_i) = \delta_i e_i$, thus $\underline{e} = \{e_1, \ldots, e_n\} \subset V_\Gamma$ and we conclude $V = V_\Gamma$.
(iv) $\rightarrow$ (v) This is clear since $f_\Gamma R = ann_R V_\Gamma = f_T R$.
(v) $\rightarrow$ (vi) This is clear.
(vi) $\rightarrow$ (vii) This is obvious in view of Lemma 4.7 c).
(vii)$\leftrightarrow$ (viii) Assume $f_T = \prod_{i=1}^r f_{\Gamma_i}$ then $\deg f_T = \sum_{i=1}^r \deg f_{\Gamma_i}$, but by [LL3] Theorem 5.10, we know that $\deg f_{\Gamma_i} = [K : C^{S,D}(\gamma_i)]_{right}$.
(vii) $\rightarrow$ (i) Let us define $V_i = Ker f_{\Gamma_i}(T)$ for $i = 1, \ldots, r$. Since $f_{\Gamma_i} \in R$ is invariant of degree say ℓ_i, we know that $f_{\Gamma_i}(T)$ is an $(S^{\ell_i}, 0)$ PLT and V_i is an R submodule of V containing V_{Γ_i} (Indeed, if $v \in V$ is such that $T(v) = \gamma_i v$ for some $\gamma_i \in \Gamma_i$ then $t - \gamma_i$ divides f_{Γ_i} on the right and so $f_{\Gamma_i}(T)(v) = 0$). Let $f_i \in R$ be such that $R f_i = ann_R V_i$. Since $f_i(T)(V_{\Gamma_i}) = 0$ we also have $f_i(\Gamma_i) = 0$ and we easily conclude that $f_i = f_{\Gamma_i}$. Lemma 4.8 above then shows that $V_{\Gamma_i} = V_i$. Now assume $f_T = \prod_{i=1}^r f_{\Gamma_i}$. If $r = 1$ Lemma 4.8 shows that T is diagonalizable. If $r > 1$ let us put $h_i = \prod_{j \neq i} f_{\Gamma_j}$ $i = 1, \ldots, r$. We claim $\sum_{i=1}^r h_i R = R$. Indeed if $\sum h_i R = gR = Rg$ $\deg g \geq 1$. Let $g_1 \in R$ be such that $h_1 = g g_1$. Since h_1 is the minimal polynomial of the S, D algebraic set $\cup_{j \neq 1} \Gamma_j$, there exists $d \in \cup_{j \neq 1} \Gamma_j$ such that $x = g_1(d) \neq 0$ but $h_1(d) = 0$ and Corollary 2.10 gives us $g(d^x) = 0$. Now assume $d \in \Gamma_\ell$ for some ℓ, $\ell \geq 1$, then since Γ_ℓ is closed by (S, D) conjugation we also have $d^x \in \Gamma_\ell$, but g divides h_ℓ also on the right since h_ℓ is invariant in R and we conclude that $h_\ell(d^x) = 0$ (cf. Proposition 4.1). Once more the invariance of h_ℓ then forces h_ℓ to annihilate Γ_ℓ but this contradicts the definition of h_ℓ and proves our claim : $\sum h_i R = R$. We

can thus write $\sum_{i=1}^r h_i q_i = 1$ and for $v \in V$ let us put $v_i = h_i(q_i(T))(v)$. We have $v = \sum v_i$, but $f_T = f_{\Gamma_i} h_i$ and so $f_{\Gamma_i}(T)(v_i) = (f_{\Gamma_i} h_i)(q_i(T)(v)) = 0$. This means that $v_i \in Ker f_{\Gamma_i}(T) = V_i = V_{\Gamma_i}$ (by the first paragraph above). We conclude that any $v \in V$ can be written $v = \sum v_i$, $v_i \in V_{\Gamma_i}$ i.e. $V = \oplus V_{\Gamma_i}$. This means that T is diagonalizable.

Let us mention a few observations in the form of a

Corollary 4.10. *Let T be an algebraic (S, D) PLT on a left K-vector space V and T_1 be an (S, D) PLT on a left K-vector space V_1. Then*

a) *If $T \sim T_1$ then T is diagonalizable if and only if T_1 is diagonalizable.*

b) *If T is diagonalizable then for any (S', D') c.v. polynomial $p \in R$, $p(T)$ is diagonalizable.*

c) *If T is diagonalizable and $\dim V = n$, there exists a basis $\underline{e} = (e_1, \ldots, e_n)$ of V such that $M_{\underline{e}}(T) = diag(\alpha_1, \ldots, \alpha_1, \alpha_2, \ldots, \alpha_2, \ldots, \alpha_r, \ldots, \alpha_r)$ where r is the number of (S, D) conjugacy classes containing eigenvalues of T.*

Proof a) Lemma 3.17 shows that T_1 is algebraic and $f_{T_1} = f_T$ hence if T is diagonalizable we have by the theorem $f_T = f_\Gamma$ and so $f_{T_1} = f_\Gamma$ which implies that T_1 is diagonalizable.
b) This is clear from the fact that $p(T)$ is also algebraic (cf. Theorem 3.20) and $\Delta(p(T)) = p(\Delta(T))$ (cf. 3.7). So if $\Delta(T)$ contains a diagonal matrix A then $p(A) \in \Delta(p(T)$ is easily seen to be diagonal and Theorem 4.9 (ii) gives the conclusion.
c) Theorem 4.9 and Lemma 4.7 show that $V = V_\Gamma = \oplus_{i=1}^r V_{\Gamma_i}$. But the final assertion from Lemma 4.8 implies that for any $i = 1, \ldots, r$ V_{Γ_i} has a basis $\{e_{i1}, \ldots, e_{in_i}\}$ such that $T(e_{ij}) = \alpha_i e_{ij}$ when $\Gamma_i = \Delta^{S,D}(\alpha_i)$ and so the basis $\underline{e} = \{e_{11}, \ldots, e_{1n_1}, e_{21}, e_{22}, \ldots, e_{2n_2}, \ldots, e_{r1}, \ldots, e_{rn_r}\}$ satisfies the required properties.

In this final part, we will look at (S, D) diagonalization of matrices. We will use the previous notations in particular up to the end we will assume that $S \in Aut(K)$. Let us first give the relevant definitions.

Definitions 4.11. *Let A be an $n \times n$ matrix in $M_n(K)$ and α, β be elements in K. Let u be a column in ^nK and v a row in K^n.*

a) *A is (S, D) diagonalizable if there exists $P \in GL_n(K)$ such that $S(P)AP^{-1} + D(P)P^{-1}$ is a diagonal matrix.*

b) *v is a left eigenvector for A associated to the left eigenvalues α if $S(v)A + D(v) = \alpha v$.*

c) *u is a right eigenvector for A associated to the right eigenvalues β if $Au - D(u) = S(u)\beta$.*

d) *$SpecA$ is the set of right and left eigenvalues of A.*

e) *u and v are orthogonal if $\sum_{i=1}^n v_i u_i = 0$ where $u = (u_1, \ldots, u_n)^t$ and $v = (v_1, \ldots, v_n)$.*

Let us make a few observations about these definitions.

Remark 4.12. a) $v \in K^n$ is a left eigenvector of A associated to α if and only if $T_A(v) = \alpha v$. This shows that definition b) above is natural since T_A plays the role of the classical linear transformation attached to a matrix.

b) The notions of right eigenvectors, right eigenvalues are also natural in view of the following : if $S \in Aut(K)$ then $(-DS^{-1}, S^{-1})$ is a right S^{-1} derivation and hence the application $L_A : {}^nK \to {}^nK : u \mapsto AS^{-1}(u) - DS^{-1}(u)$ is a right $(-DS^{-1}, S^{-1})$ PLT (cf. Remark 2.5 c)); R_A is the analogue of the classical linear transformation on the space ${}^nK$ of columns defined by A. Thus $\omega \in {}^nK$ is a right eigenvector for A associated to the right eigenvalues β if $R_A(\omega) = \omega\beta$ i.e. $AS^{-1}(\omega) - DS^{-1}(\omega) = \omega\beta$ hence $Au - D(u) = S(u)\beta$ where $u = S^{-1}(\omega) \in {}^nK$.

Proposition 4.13. *Let A be an $n \times n$ matrix over K, $v, v_1, \ldots, v_s$ be rows in K^n and $u, u_1, \ldots, u_r$ columns in ${}^nK$. Then*

a) *$SpecA$ is closed by (S, D)-conjugation, more precisely :*

   If $\alpha \in K$ is such that $S(v)A + D(v) = \alpha v$ then for $\gamma \in K^*$ $S(\gamma v)A + D(\gamma v) = \alpha^\gamma \gamma v$

   If $\beta \in K$ is such that $Au - D(u) = S(u)\beta$ then for $\gamma \in K^*$ $Au\gamma - D(u\gamma) = S(u\gamma)\beta^{\gamma^{-1}}$

b) *If $v_1, \ldots, v_s$ (resp. $u_1, \ldots, u_s$) are left eigenvectors (resp. right eigenvectors) for A associated to non (S, D) conjugate eigenvalues then $v_1, \ldots, v_s$ (resp. $u_1, \ldots, u_s$) are left (resp. right) linearly independant over K.*

c) *Left and right eigenvectors associated to non (S, D) conjugate eigenvalues are orthogonal.*

d) *$SpecA$ contains at most n (S, D) conjugacy classes.*

Proof a) This is left to the reader.

b) We have $T_A(v_i) = \gamma_i v_i$ for some $\gamma_i \in K$ and $i = 1, \ldots, s$. Since the γ_i's are assumed to be non (S, D) conjugate, Proposition 4.1 shows that $v_1, \ldots, v_s$ are left linearly independant. The map $R_A : {}^nK \to {}^nK : u \mapsto AS^{-1}(u) - DS^{-1}(u)$ is a right $(-DS^{-1}, S^{-1})$ PLT and the conditions $Au_i - D(u_i) = S(u_i)\beta_i$ mean that $S(u_i)$ is a right eigenvector of R_A associated to the right eigenvalue β_i i.e. $R_A(S(u_i)) = S(u_i)\beta_i$ and the analogue of Proposition 4.2 for right $(-DS^{-1}, S^{-1})$ PLT implies that the $S(u_i)$'s are right independant and so the u_i's are also right linearly independant over K.

c) Suppose that $v = (v_1, \ldots, v_n) \in K^n$ $u = (u_1, \ldots, u_n)^t \in {}^nK$ and $\gamma, \beta \in K$ are such that $S(v)A + D(v) = \gamma v$ and $Au - D(u) = S(u)\beta$. If $c := \sum v_i u_i \neq 0$ then $[\gamma v - D(v)]u = (S(v)A)u = S(v)(Au) = S(v)[S(u)\beta + D(u)]$ and so $\gamma vu = S(v)S(u)\beta + S(v)D(u) + D(v)u$ hence $\gamma c = S(c)\beta + D(c)$ and $\gamma = \beta^c$. This contradiction shows that $c = 0$.

d) Let $\gamma_1, \ldots, \gamma_r$ and $\beta_1, \ldots, \beta_s$ be respectively left and right eigenvalues for A and suppose that $\gamma_1, \ldots, \gamma_r, \beta_1, \ldots, \beta_s$ are not (S, D) conjugate. Let $u_1, \ldots, u_r \in {}^nK$ and $v_1, \ldots, v_s \in K^n$ be respective eigenvectors. By b) above we know that the columns $u_1, \ldots, u_r$ are right independant. Let $U_1 = (u_1, \ldots, u_r) \in M_{n \times r}(K)$ and

$\varphi : K^n \to K^r : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n)U_1$ a left linear map. Since the columns of U_1 are right independant we deduce that the left K space generated by the rows of U_1 is of dimension r and so dim $im\,\varphi = r$ (in particular, there exists a matrix $V_1 \in M_{r \times n}(K)$ such that $V_1 U_1 = I_r$). By b) and c) we deduce that the rows $v_1, \ldots, v_s$ are left linearly independant vectors in $Ker\,\varphi$ and so $r + s \le \dim ker\,\varphi + \dim im\,\varphi = n$.

$\square$

Lemma 4.14. *Let T be an algebraic (S, D) PLT on V with minimal monic polynomial f_T. If $\gamma \in K$ is such that $f_T(\gamma) \ne 0$ then $T - L_\gamma : V \to V : v \mapsto T(v) - \gamma v$ is a bijection.*

Proof Since f_T is an invariant polynomial in $R = K[t; S, D]$ the fact that $f_T(\gamma) \ne 0$ implies that $t - \gamma$ is neither a left nor a right factor of f_T. In this section we assume $S \in Aut(K)$ so that we can write $f_T(t) = (t - \gamma)q(t) + r$ for some $q(t) \in K[t; S, D]$ and $r \in K^*$. Let v be any vector of V then we easily check that $(T - L_\gamma)(q(T)(r^{-1}v)) = v$. On the other hand if $(T - L_\gamma)(\omega) = 0$ and $\omega \ne 0$ then γ is an eigenvalue and Proposition 4.5 shows that $t - \gamma$ divides f_T. This contradiction shows that $T - L_\gamma$ is injective.

$\square$

In the next theorem we give sufficient conditions for a matrix A to be diagonalizable. This theorem is the analogue of Theorem 8.2.3 in [Co1].

Theorem 4.15. *Let K, S, D be a division ring an automorphism of K and an S-derivation of K. Suppose that $A \in M_n(K), n \in \mathbb{N}$, is such that $specA$ consists of exactly n (S, D) conjugacy classes. Suppose moreover that either the set of left eigenvalues or the set of right eigenvalues of A is (S, D) algebraic then A is diagonalizable.*

Proof Let $\gamma_1, \ldots, \gamma_r \in K$ and $\beta_1, \ldots, \beta_s \in K$ be respectively non (S, D) conjugate right eigenvalues and non (S, D) conjugate left eigenvalues of A such that $r + s = n$. Suppose that $u_1, \ldots, u_r$ are columns in ^nK and $v_1, \ldots, v_s$ are rows in K^n such that $Au_i - D(u_i) = S(u_i)\gamma_i$ for $i = 1, \ldots, r$ and $S(v_j)A + D(v_j) = \beta_j v_j$ for $j = 1, \ldots, s$.

Put $U_1 = (u_1, \ldots, u_r) \in M_{n \times r}(K)$ and $V_2 = \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} \in M_{s \times n}(K)$.

Proposition 4.13 b) shows that the u_i's are right independant while the v_j's are left independant and we conclude as in Lemma 4.14 above that there exist $V_1 \in M_{r \times n}(K)$ and $U_2 \in M_{n \times s}(K)$ such that $V_1 U_1 = I_r$ and $V_2 U_2 = I_s$. Since we are also assuming that for $i = 1, \ldots, r$ and $j = 1, \ldots, s$, γ_i is not (S, D) conjugate to β_j we conclude thanks to Proposition 4.13 c) that $V_2 U_1 = 0$. Let us denote $V := \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} \in M_{n \times n}(K)$ and $W := (V_1 \cdot U_2) \in M_{r \times s}(K)$ we have

$$AU_1 = S(U_1)C + D(U_1) \quad \text{where} \quad C = diag(\gamma_1, \ldots, \gamma_r)$$
$$S(V_2)A = BV_2 - D(V_2) \quad \text{where} \quad B = diag(\beta_1, \ldots, \beta_s).$$

It is easy to check that $V(U_1 \quad U_2 - U_1 W) = I$, and we get $S(V)AV^{-1} + D(V)V^{-1} = \begin{pmatrix} S(V_1) \\ S(V_2) \end{pmatrix} (AU_1 \quad A(U_2 - U_1 W)) + \begin{pmatrix} D(V_1) \\ D(V_2) \end{pmatrix} (U_1 \quad U_1 - U_1 W)$ we easily

compute

the left upper block : $S(V_1)AU_1 + D(V_1)U_1 = S(V_1U_1)C + S(V_1)D(U_1) + D(V_1)U_1 = C + D(V_1U_1) = C$

left lower block : $S(V_2)AU_1 + D(V_2)U_1 = S(V_2U_1)C + S(V_2)D(U_1) + D(V_2)U_1 = 0$

right lower block $S(V_2)A(U_2 - U_1W) + D(V_2)(U_2 - U_1W) = (BV_2 - D(V_2))(U_2 - U_1W) + D(V_2)(U_2 - U_1W) = BV_2U_2 - D(V_2)U_2 + D(V_2)U_1W + D(V_2)U_2 - D(V_2)U_1W = B$.

Let us call $Y \in M_{r \times s}(K)$ the right upper block we thus have

$$S(V)AV^{-1} + D(V)V^{-1} = \begin{pmatrix} C & Y \\ O & B \end{pmatrix} \qquad (4.16)$$

By our hypothesis at least one of the sets $\Delta = \cup_{i=1}^s \Delta^{S,D}(\beta_i)$ OR $\Gamma = \cup_{j=1}^r \Delta^{S,D}(\gamma_j)$ is (S, D) algebraic. So let us suppose that Δ is (S, D) algebraic and denote $f_\Delta(t) \in R = K[t; S, D]$ its monic minimal polynomial. We know that f_Δ is invariant and Theorem 4.9 shows that f_Δ is also the minimal polynomial of the (S, D) PLT $T_B : K^s \to K^s$. Since for any $i \in \{1, \ldots, r\}, \gamma_i$ does not belong to Δ, the above lemma 4.14 shows that $T_B - L_\gamma : K^s \to K^s$ is a bijection and so for any $i = 1, \ldots, r$ there exists $x_i \in K^s$ such that $(T_B - L_\gamma)(x_i) = -y_i$ where y_i is the ith row of Y. We thus have $S(x_i)B + D(x_i) - \gamma_i x_i = -y_i$ and if we put

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in M_{r \times s}(K)$$ we get $S(X)B + D(X) - CX = -Y$. Now, consider the

matrix $U = \begin{pmatrix} I_r & X \\ 0 & I_s \end{pmatrix} \in M_{n \times n}(K)$ and let us compute

$$S(U) \begin{pmatrix} C & Y \\ 0 & B \end{pmatrix} U^{-1} + D(U)U^{-1}$$

$$= \begin{pmatrix} C & Y + S(X)B \\ 0 & B \end{pmatrix} \begin{pmatrix} I & -X \\ 0 & I \end{pmatrix} + \begin{pmatrix} 0 & D(X) \\ 0 & 0 \end{pmatrix} \begin{pmatrix} I & X \\ 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} C & Y + S(X)B - CX \\ 0 & B \end{pmatrix} + \begin{pmatrix} 0 & D(X) \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} C & 0 \\ 0 & B \end{pmatrix}$$

This and 4.16 show that $S(UV)A(UV)^{-1} + D(UV)(UV)^{-1} = \begin{pmatrix} C & 0 \\ 0 & B \end{pmatrix}$. We

similarly handle the case when the set of right eigenvalues of A is (S, D) algebraic. $\square$

References

[Co1]   P.M. Cohn *Skew Field Constructions*, London Math. Soc. Lecture Notes Series **27** (1977) Cambridge University Press.

[Co2]   P.M. Cohn *Free Rings and Their Relations.* Academic Press, New York, 1971.

[G.W.] K.R. Goodearl and R.B. Warfield *Introduction to Non Commutative Nœtherian Rings,* Vol. 16 London Math. Soc. Student Texts Cambridge University Press, 1989.

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

[La]   E. Landau *Ein Satz über die Zerlegung Homogener linear Differentialansdrüche in Irreduzible Faktoren,* J. reine Ange W. Math. **124** (1902) 115-120.

[LL1]   T.Y. Lam and A. Leroy *Homomorphisms between Ore extensions,* Comtemporary Mathematics **124** (1992) 83-110, (In Honor of Goro Azumaya's seventieth Birthday) A.M.S. publication.

[LL2]   T.Y. Lam and A. Leroy *Hilbert 90 Theorem over division rings,* Trans. Amer. Math. Soc. **345** (1994) 595-622.

[LL3]   T.Y. Lam and A. Leroy *Algebraic conjugacy classes and skew polynomial rings,* (1988) 153-203, in "Perpectives in Ring Theory" (F. Van Oystaeyen and L. Le Bruyn, eds Proceedings of the Antwerp Conference in Ring Thoery, Kluwer Academic Publishers.

[LLLM] T.Y. Lam, A. Leroy, K.H. Leung, J. Matczuk *Invariant and semi-invariant polynomials in skew polynomial rings,* "in Ring Theory 1989" (In Honor of S.A. Amitsur) **1** éd. L. Rowen, Israel Mathematical Conference, Proceedings Wizman Science Press of Israel 1989 247-261.

[LTVP] A. Leroy, J-P. Tignol, P. Van Praag *Sur les anneaux simples différentiels,* Communications in Algebra **10** (1982) 1307-1314.

[M.R.] J. McConnell and J.C. Robson *Non Commutative Nœtherian Rings,* J. Wiley, London New York ,1988 .

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

Université d'Artois
Faculté J.Perrin
Département de Mathématiques
Rue J. Souvraz
62307 LENS Cedex
France