Wedderburn Polynomials over Division Rings, II

T. Y. LAM, A. LEROY and A. OZTURK

Abstract: A polynomial $f(t)$ in an Ore extension $K[t;S,D]$ over a division ring K is a Wedderburn polynomial if $f(t)$ is monic and is the minimal polynomial of an algebraic subset of K. These polynomials have been studied in [LL_5], [DL] and [LL_4]. In the present paper, we continue this study and give some applications to triangularization, diagonalization and eigenvalues of matrices over a division ring in the general setting of (S,D)-pseudo-linear transformations. In the last section we introduce and study the notion of G-algebraic sets which, in particular, permits generalization of Wedderburn's theorem relative to factorization of central polynomials.

1. Introduction

This paper continues the study of Wedderburn polynomials started in [LL_5]. Wedderburn polynomials are least left common multiple of linear polynomials of the form $t-a$ in (skew) polynomial rings over division rings. They can be factorized linearly using Wedderburn's method. Before describing the content of the paper let us give a short account of the history of Wedderburn polynomials and Wedderburn's method thereby asserting their importance (for a more detailed survey the reader is referred to [Ro_2]).

Let K be a division ring with center F. Wedderburn proved in [We] that the minimal monic polynomial $f_a(t) \in F[t]$ of an algebraic element $a \in K$ can be written as a product of linear factors in $K[t]$: $f_a(t) = (t-a_n)(t-a_{n-1})\cdots(t-a_1)$. Moreover he showed that $a_1,\ldots,a_n$ are conjugate to a. The polynomial $f_a(t)$ admits many such factorizations and all of them are obtained by what is called the Wedderburn's method. This method is basically a repeated use of the following fact: if $f = gh \in K[t]$ is such that $f(a) = 0$ but $d := h(a) \neq 0$ then $g(dad^{-1}) = 0$. Using the above, Wedderburn also proved that every division algebra K of degree 3 has a maximal subfield which is Galois over the center F of K. Using the same method, Albert, in [A1], extended this result to division algebras of degree 4 and showed, in [A2], that a finite dimensional division ring which is ordered as a ring is commutative. In [Ja_1], Jacobson used Wederburn's method to obtain

easy proofs of Skolem-Noether and Hilbert 90 theorems. Other results that can be obtained by Wedderburn's method concern

- division rings with involutions.
- the structure of the multiplicative group of a division ring (e.g. it is proved in [RS_2] that the multiplicative group of a division ring of degree 3 or 5 is solvable).
- reduced K-theory.

Recently Wedderburn polynomials have been used to present a generalized notion of non commutative symmetric function without the help of quasi determinants (Cf. [DL]). This presentation shows that Wedderburn's method give back the non commutative Vieta's formula and Miura decomposition. Let us also mention that Wedderburn polynomials sometimes appear under other names such as polynomials with separate zeros (Cf. [Tr]) or polynomials with zeros in generic position (Cf. [GGRW], [GR], [GRW]). This paper contains yet another application of the Wedderburn polynomials: they can be used to characterize diagonalizable matrices with coefficients in a division ring.

Let us now briefly describe the content of the paper. In the sequel R stands for an Ore extension $R = K[t; S, D]$, where K is a division ring, S an endomorphism of K and D a S-derivation of K.

In Section 2 we recall some basic facts and notations from our previous paper ([LL_5]).

In the third section we present various relations involving the rank of algebraic sets and, using these, we find back some of the features of Wedderburn polynomials presented in our previous work.

Section 4 is devoted to companion matrices. They show up naturally in the study of the action of $t\cdot$ on R/Rf and are very useful tools while we characterize when a product of W-polynomials is again a W-polynomial. This characterization generalizes the (S, D)-metro equation from [LL_5].

In Section 5 we analyse the problems of diagonalization and triangularization of matrices over a division ring. We work in the general (K, S, D)-setting as described above. We first consider the case of a companion matrix and then, supposing $S \in Aut(K)$, we analyse the case of a general square matrix via the companion matrices of its invariant factors. In particular, we will show that a square matrix $A \in M_n(K)$ is (S, D)-diagonalizable (resp. (S, D)-triangularizable) if and only if the invariant factors are Wedderburn polynomials (5.12) (resp. product of linear polynomials (5.14)).

We also define and study left and right eigenvalues of a matrix $A \in M_n(K)$ and get analogues of classical results for commutative polynomials.

The last section is concerned with the notion of G-algebraic sets. They give, in particular, another approach to the Wedderburn's theorem on factorization of central polynomials. In this last section we only consider the "classical" case i.e. we assume that $S = \mathrm{Id}$ and $D = 0$.

2. **Recapitulation**

Let us start with a brief review of basic definitions, notations and contents of our previous paper "Wedderburn polynomials over division rings, I". We will refer this paper by "Wed1" (Cf. [LL_5]). Let us start with a triple (K, S, D), where K is a division ring, S is a ring endomorphism of K, and D is a (S, Id)-derivation on K. The latter means that D is an additive endomorphism of K such that, for $a, b \in K$, $D(ab) = S(a)D(b) + D(a)b$. In the sequel of the paper a (S, Id)-derivation will just be called a S-derivation. We will occasionally need the symmetric notion of a (Id, σ)-derivation δ, where σ is an endomorphism of K and δ is an additive map such that, for $a, b \in K$, $\delta(ab) = a\delta(b) + \delta(a)\sigma(b)$. In particular, when S is an automorphism of K and D is an S-derivation, the map $-DS^{-1}$ is a (Id, S^{-1})-derivation.

In the general (K, S, D)-setting, we can form the Ore ring of skew polynomials $K[t; S, D]$. More details about this ring and its properties can be found in the introduction of "Wed1" or in [Co_3].

In case $D = 0$ (resp. $S = \mathrm{Id}$), we write $K[t; S]$ (resp. $K[t; D]$) for the skew polynomial ring $K[t; S, 0]$ (resp. $K[t; \mathrm{Id}, D]$). Of course, when $(S, D) = (\mathrm{Id}, 0)$ (we refer to this as the "classical case"), $K[t; S, D]$ boils down to the usual polynomial ring $K[t]$ with a *central* indeterminate t.

Throughout this paper, we'll write $R := K[t; S, D]$. R is a right euclidian domain (hence, in particular, a left principal ideal domain). For $f(t) \in R$ and $a \in K$ there exist $q(t) \in R$ and $b \in K$ such that

$$f(t) = q(t)(t - a) + b\,, \text{ we then define } f(a) := b$$

See [LL_1], [LL_2] or Wed1 for details. A subset $\Delta \subseteq K$ is algebraic if there exists a polynomial $g \in R$ such that $g(x) = 0$ for all $x \in \Delta$. For $f \in R$ we put $V(f) := \{a \in K | f(a) = 0\}$. This set is obviously algebraic and we say that a polynomial $f \in R$ is a Wedderburn polynomial if f is monic and is of minimal degree among polynomials annihilating $V(f)$. An element $a \in K$ is P-dependent over an algebraic subset Δ if any polynomial annihilating Δ also annihilates a.

A subset B of an algebraic set Δ is called a P-basis for Δ if no element $b \in B$ is P-dependent over $B \setminus \{b\}$ and all elements of Δ are P-dependent over B. All the P-bases of Δ have the same cardinal called the rank of the algebraic set Δ and denoted by $\operatorname{rk} \Delta$.

An element $b \in K$ is (S, D)-conjugate to an element $a \in K$ if there exists $c \in K \setminus \{0\}$ such that $b = S(c)ac^{-1} + D(c)c^{-1}$, in this case we write $b := a^c$ and the set $\{a^x | x \in K \setminus \{0\}\}$ will be denoted $\Delta^{S,D}(a)$ (or just $\Delta(a)$ when no confusion is possible) and called the (S, D)-conjugacy class of a.

For $a \in K$, we define the (S, D)-centralizer of a, denoted by $C^{S,D}(a)$, to be the set $C^{S,D}(a) := \{x \in K \setminus \{0\} \mid a^x = a\} \cup \{0\}$. This is a division subring of K.

Of course, similar notions exist for the case of a (Id, σ)-derivation δ. For instance an element $b \in K$ is (δ, σ)-conjugate to an element $a \in K$ if there exists $c \in K \setminus \{0\}$ such that $b = ca\sigma(c^{-1}) + c\delta(c^{-1})$. The set of elements (δ, σ)-conjugate to an element a will be denoted $\Delta^{\delta,\sigma}(a)$. It is an easy exercise to remark that, when σ is an automorphism of K, we have $\Delta^{S,D}(a) = \Delta^{-DS^{-1},S^{-1}}(a)$ (Cf. 6.1).

For $h \in R$ and $x \in K \setminus V(h)$ we define $\phi_h(x) := x^{h(x)}$. This map appears naturally while evaluating a product gh at an element $x \in K \setminus V(h)$:

$$gh(x) = g(\phi_h(x))h(x). \tag{2.1}$$

Let us recall that $\phi_h(\Delta(a)) \subseteq \Delta(a)$ i.e. ϕ_h preserves the (S, D)-conjugacy classes. While computing ϕ_h within a single (S, D)-conjugacy class $\Delta(a)$, another map appears naturally: for $x \in K \setminus 0$, $\phi_h(a^x) = a^{h(a^x)x}$. We thus define a map $\lambda_{h,a} : K \longrightarrow K$ by setting:

$$\lambda_{h,a}(x) = \begin{cases} h(a^x)x & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

The map $\lambda_{h,a}$ is a right $C := C^{S,D}(a)$-linear and $\ker \lambda_{h,a} = \{x \in K \setminus \{0\} \mid a^x \in V(h)\} \cup \{0\}$. If an algebraic set Γ is contained in a conjugacy class $\Delta(a)$, say $\Gamma = a^Y$ for some $Y \subseteq K \setminus \{0\}$, then $V(f_\Gamma) = a^{YC}$, where YC is the right $C = C^{S,D}(a)$-vector space generated by Y. Moreover one has $\operatorname{rk} \Gamma = \deg f_\Gamma = \dim_C YC$ (Cf. [LL$_2$]). We also have $\operatorname{rk}(V(h) \cap \Delta(a)) = \dim_C \ker \lambda_{h,a}$ (Cf. Wed1). Let us also remark that, for $f, g \in R$, we have $\lambda_{fg,a} = \lambda_{f,a}\lambda_{g,a}$.

3. **Rank theorems**

In this section we will present various relations involving the rank of an algebraic set. Our first objective is to relate the rank of $V(gh)$

and the ranks of $V(g)$ and $V(h)$. Let us first recall the following result from Wed1 (Cf. [LL_5, Corollary 4.4]).

Lemma 3.1. *If Δ_i $(1 \leq i \leq r)$ are algebraic sets located in different (S,D)-conjugacy classes $\Delta^{S,D}(a_i)$ of K, then:*

1. *The set $E_i := \{x \in K \setminus \{0\} \,|\, a_i^x \in \Delta_i\} \cup \{0\}$ is a right vector space over $C_i := C^{S,D}(a_i)$.*
2. *$\mathrm{rk}\left(\bigcup_{i=1}^r \Delta_i\right) = \sum_{i=1}^r \mathrm{rk}\,\Delta_i = \sum_{i=1}^r \dim_{C_i} E_i$.*

Of course, this lemma applies to the set $V(f) := \{x \in K \,|\, f \in R(t-x)\}$ of right roots of a polynomial $f \in R$. For $f \in R = K[t;S,D]$ and $a \in K$, we also introduce the following notations: $V'(f) := \{x \in K \,|\, f \in (t-x)R\}$ and $E(f,a) = \{x \in K \setminus \{0\} \,|\, a^x \in V(f)\} \cup \{0\}$. $E(f,a)$ is a right $C^{S,D}(a)$-vector space.

Corollary 3.2. *Let $f \in R = K[t;S,D]$ be a monic polynomial of degree n. With the above notations one has:*

1. *$V(f)$ intersects at most $n = \deg(f)$ (S,D)-conjugacy classes, say $V(f) = \bigcup_{i=1}^r (V(f) \cap \Delta(a_i))$, with $r \leq n$.*
2. *$\mathrm{rk}\, V(f) = \sum_{i=1}^r \dim_{C_i} E(f,a_i) \leq \deg(f)$, where $C_i = C^{S,D}(a_i)$. The equality holds if and only if f is a Wedderburn polynomial.*
3. *$V'(f) \cup V(f)$ intersects at most $n = \deg(f)$ (S,D)-conjugacy classes.*

Proof. (1). Let us recall that any polynomial $f \in R = K[t;S,D]$ can be factorized as a product of irreducible polynomials: $f = p_1 \cdots p_l$. Moreover if $f = q_1 \cdots q_s$ is another such factorization then $l = s$ and there exists a permutation $\pi \in S_l$ such $R/Rp_i \cong R/Rq_{\pi(i)}$ (this means that R is a UFD, Cf. [Co_2]). On the other hand, it is well known and easy to check that $R/R(t-a) \cong R/R(t-b)$ if and only if $\Delta(a) = \Delta(b)$ (Cf. Theorem 4.9 for a further generalization). It is then clear that the number of conjugacy classes containing right roots of f is bounded by $\deg(f)$.

Alternatively one can apply Lemma 3.1 to the algebraic set $V(f)$ to prove this result. This is left to the reader.
(2). Decomposing $V(f)$ into the (S,D)-conjugacy classes it intersects, we can write $V(f) = \bigcup_{i=1}^r \Delta_i$ where $\Delta_i = V(f) \cap \Delta(a_i)$ and $E(f,a_i) = \{x \in K \setminus \{0\} \,|\, f(a_i^x) = 0\} \cup \{0\}$. The above Lemma 3.1 then yields the desired formulas and the additional statement comes from the fact that f is a Wedderburn polynomial if and only if $\mathrm{rk}\,(V(f)) = \deg(f)$.
(3). As in (1) above, this is again a direct consequence of the fact that $R = K[t;S,D]$ is a UFD. □

Notice the following important special case: $E(f,0)$ is easily seen to be the solution space of the differential equation $f(D) = 0$ and $C^{S,D}(0) = K_D$ is the constant subdivision ring of K. Amitsur's well-known theorem states that the dimension over K_D of the solution space of the equation $f(D) = 0$ is bounded by the degree of the polynomial f (Cf. [Am]). This is now clear: this dimension is one of the dimensions appearing in the expression of $\operatorname{rk} V(f)$.

Lemma 3.3. *Let V be a right vector space over a division ring C and $\phi, \psi \in End_C V$. If $v_1, v_2, \ldots, v_r$ is a basis for $\ker\psi$ and $u_1, u_2, \ldots, u_s \in V \setminus \ker\psi$ then the following are equivalent:*

i) *The set $\{v_1, \ldots, v_r, u_1, \ldots, u_s\}$ is a basis for $\ker\phi\psi$.*

ii) *The set $\{\psi(u_1), \psi(u_2), \ldots, \psi(u_s)\}$ is a basis for $\operatorname{Im}\psi \cap \ker\phi$.*

In particular, we have

$$\dim_C \ker(\phi\psi) = \dim_C \ker\psi + \dim_C(\operatorname{Im}\psi \cap \ker\phi).$$

Proof. The easy proof is left to the reader. □

Theorem 3.4. *Let g, h be polynomials from R, then*

$$\operatorname{rk} V(gh) = \operatorname{rk} V(h) + \operatorname{rk}(\operatorname{Im}\phi_h \cap V(g)).$$

In particular, we always have

$$\operatorname{rk} V(gh) \leq \operatorname{rk} V(h) + \operatorname{rk} V(g).$$

Proof. Let us put $f = gh$ and remark that, thanks to Lemma 3.1, it is enough to prove that, for any $a \in K$, we have $\operatorname{rk}(V(gh) \cap \Delta(a)) = \operatorname{rk}(V(h) \cap \Delta(a)) + \operatorname{rk}(\operatorname{Im}\phi_h \cap V(g) \cap \Delta(a))$. Using the definitions and results recalled at the end of Section 2, we get, for a in K, $\lambda_{f,a} = \lambda_{g,a}\lambda_{h,a}$. In particular, $\ker\lambda_{h,a} \subseteq \ker\lambda_{f,a}$. Moreover, if C stands for $C^{S,D}(a)$, we have $\operatorname{rk}(V(f) \cap \Delta(a)) = \dim_C \ker\lambda_{f,a}$; $\operatorname{rk}(V(h) \cap \Delta(a)) = \dim_C \ker\lambda_{h,a}$; $\operatorname{Im}\phi_h \cap \Delta(a) = a^{\operatorname{Im}\lambda_{h,a}\setminus\{0\}}$ and $\operatorname{rk}(V(g) \cap \operatorname{Im}\phi_h \cap \Delta(a)) = \dim_C(\operatorname{Im}\lambda_{h,a} \cap \ker\lambda_{g,a})$. So we finally must prove that

$$\dim_C \ker\lambda_{f,a} = \dim_C \ker\lambda_{h,a} + \dim_C(\operatorname{Im}\lambda_{h,a} \cap \ker\lambda_{g,a}).$$

But this is exactly what is given by Lemma 3.3. □

As an application of the above result let us give another proof of the main part of the "factor theorem" [LL_5], Theorem 5.1. Recall that a polynomial f is Wedderburn if and only if it is monic and $\operatorname{rk} V(f) = \deg f$ (Cf. Wed1).

Corollary 3.5. *If g, h are monic polynomials in R such that gh is a Wedderburn polynomial then g and h are Wedderburn.*

Proof. The above theorem implies that $\operatorname{rk} V(g)+\operatorname{rk} V(h) \geq \operatorname{rk} V(gh) = \deg gh = \deg g + \deg h$. This implies $\operatorname{rk} V(g) = \deg g$ and $\operatorname{rk} V(h) = \deg h$. □

Recall from Wed1, that if $\Delta \subseteq K$ is an algebraic set, we denote by f_Δ the monic polynomial of minimal degree annihilating Δ, and we put $\overline{\Delta} = \{x \in K | \, f_\Delta(x) = 0\}$.

Theorem 3.6. *Let $h \in R$ and $\Delta \subseteq K$ be an algebraic set disjoint from $V(h)$. Then:*

1. *$\phi_h(\Delta)$ is an algebraic set.*
2. *$[f_\Delta, h]_l = f_{\phi_h(\Delta)}h$, where $[f_\Delta, h]_l$ denotes the monic least left common multiple of f_Δ and h.*
3. *$\operatorname{rk} \phi_h(\Delta) = \operatorname{rk} \Delta - \operatorname{rk} (\overline{\Delta} \cap V(h))$. In particular, $\operatorname{rk} \phi_h(\Delta) = \operatorname{rk} \Delta$ iff $\overline{\Delta} \cap V(h) = \emptyset$.*
4. *$\deg((f_\Delta, h)_r) = \operatorname{rk} (\overline{\Delta} \cap V(h))$, where $(f_\Delta, h)_r$ denotes the monic right greatest common divisor of h and f_Δ.*

Proof. (1) and (2) Let us write $[f_\Delta, h]_l$ for the monic least left common multiple of f_Δ and h. Let $g, g' \in R$ be such that $[f_\Delta, h]_l = gh = g'f_\Delta$. Then for $x \in \Delta$, we have $0 = (g'f_\Delta)(x) = (gh)(x) = g(\phi_h(x))h(x)$. Hence, since $h(x) \neq 0$, $g(\phi_h(x)) = 0$. This shows that $\phi_h(\Delta)$ is algebraic and $f_{\phi_h(\Delta)}$ divides g on the right. Hence $f_{\phi_h(\Delta)}h$ divides $[f_\Delta, h]_l$ on the right. On the other hand $f_{\phi_h(\Delta)}h$ annihilates Δ and is thus right divisible by both f_Δ and h. This proves (2).
(3) Decomposing the algebraic sets $\Delta, \phi_h(\Delta)$ and $\overline{\Delta} \cap V(h)$ in conjugacy classes and using the above Lemma 3.1 we see that it is enough to show that, for any $a \in K$, $\operatorname{rk} (\phi_h(\Delta) \cap \Delta(a)) = \operatorname{rk} (\Delta \cap \Delta(a)) - \operatorname{rk} (\overline{\Delta} \cap V(h) \cap \Delta(a))$. Let us put $Y := \{y \in K \setminus \{0\} | a^y \in \Delta \cap \Delta(a)\}$ and denote by YC the right $C := C^{S,D}(a)$-space generated by Y. We have $\operatorname{rk} (\Delta \cap \Delta(a)) = \operatorname{rk} (\{a^y | y \in Y\}) = \dim_C YC$, $\operatorname{rk} (\overline{\Delta} \cap V(h) \cap \Delta(a)) = \operatorname{rk} (\{a^y | y \in YC \text{ and } h(a^y) = 0\}) = \dim_C(YC \cap \ker \lambda_{h,a})$ and $\operatorname{rk} (\phi_h(\Delta) \cap \Delta(a)) = \dim_C \lambda_{h,a}(YC)$. The required equality is an easily seen to be an immediate consequence of the relation between the dimension of the kernel of $\lambda_{h,a}$ and the dimension of its image.
(4) As is well known, one has $\deg(f_\Delta) + \deg(h) = \deg([f_\Delta, h]_l) + \deg((f_\Delta, h)_r)$. Using statement (2) above we get $\deg(f_\Delta) = \deg(f_{\phi_h(\Delta)}) + \deg((f_\Delta, h)_r)$. In other words $\operatorname{rk} (\Delta) = \operatorname{rk} (\phi_h(\Delta)) + \deg((f_\Delta, h)_r)$. Formula (3) then yields the result. □

Example 3.7. Let K be a division ring (we assume that $S = \mathrm{Id}, D = 0$) and $a, x \in K$, $x \notin \{0, -1\}$, be such that $\{a, a^x, a^{1+x}\}$ are distinct elements. Consider the polynomial $h(t) = t - a^{1+x} \in K[t]$ and $\Delta =$

$\{a, a^x\}$. It is easy to check that $V(h) \cap \Delta = \emptyset$, $V(h) \cap \overline{\Delta} = \{a^{1+x}\}$. Notice also that $h(a^x)x = a^x x - (1+x)a + a^{1+x} = -a + a^{1+x} = -h(a)$ and thus $\phi_h(a^x) = a^{h(a^x)x} = a^{h(a)} = \phi_h(a)$. This gives $\phi_h(\Delta) = \{a^{a-a^{1+x}}\}$. Of course, formula (3) of the previous Theorem 3.6 can be checked on this particular example. This also shows that it is necessary to take $V(h) \cap \overline{\Delta}$ and not merely $V(h) \cap \Delta$ in this formula.

Let us recall that a subset $\{a_1, \ldots, a_n\}$ of an algebraic set Δ is a P-basis for Δ if the monic polynomial f such that $Rf = \bigcap_{i=1}^{n} R(t - a_i)$ is of degree n and annihilates Δ. As a corollary let us mention the following interesting fact:

Corollary 3.8. *For $h \in R$, let $\{a_1, \ldots, a_n\}$ be a P-basis for $V(h)$ and $\{b_1, \ldots, b_s\} \subset K \setminus V(h)$. Then the set $\{a_1, \ldots, a_n, b_1, \ldots, b_s\}$ is P-independent if and only if $\{\phi_h(b_1), \ldots, \phi_h(b_s)\}$ is P-independent.*

Proof. Let us put $\Gamma := \{a_1, \ldots, a_n\}$ and $\Delta := \{b_1, \ldots, b_s\}$. $\Gamma \cup \Delta$ is P-independent if and only if $\deg([f_\Delta, f_\Gamma]_l) = n + s$. Since $\deg f_\Gamma = n$ and $\deg f_\Delta \leq s$, we get that $\Gamma \cup \Delta$ is P-independent if and only if $\deg((f_\Delta, h)_r) = 0$ and Δ is P-independent. Since the irreducible factors of f_Δ and f_Γ are all linear one can conclude that $\Gamma \cup \Delta$ is P-independent if and only if $V(f_\Delta) \cap V(f_\Gamma) = \emptyset$ and Δ is P-independent. In other words $\Delta \cup \Gamma$ is independent if and only if $\overline{\Delta} \cap V(h) = \emptyset$ and Δ is P-independent. Statement (3) of the theorem shows that these last two conditions are equivalent to $\mathrm{rk}\,(\phi_h(\Delta)) = \mathrm{rk}\,(\Delta) = s$. Since one always has $\mathrm{rk}\,(\phi_h(\Delta)) \leq \mathrm{rk}\,(\Delta)$ the last statement is equivalent to $\mathrm{rk}\,(\phi_h(\Delta)) = s$, as desired. □

4. **Companion matrices**

In this section we will show that the companion matrices together with pseudo linear transformations give a natural interpretation of some notions related to $R = K[t; S, D]$-modules.

Definition 4.1. Two polynomials $g, h \in R = K[t; S, D]$ are similar if $R/Rg \cong R/Rh$ as left R-modules. This will be denoted by $f \sim g$. $\Delta(f)$ will stand for the set of polynomials similar to f.

Remarks 4.2. a) The notion of similarity can be introduced over a general ring. It is obviously an equivalence relation and in the case of an integral domain we always have $R/Rg \cong R/Rf$ if and only if $R/gR \cong R/fR$ (Cf. [LO], [Co_2]).

b) Let $a, b \in K$, then $t - a \sim t - b$ if and only if a and b are (S, D)-conjugate. Theorem 4.9 will generalize this example and give a description of similarity of polynomials in terms of (S, D)-conjugation.

Lemma 4.3. *Let $f, g, h \in R = K[t; S, D]$ be monic polynomials. Then:*

(1) *There exist uniquely determined monic polynomials $g', h' \in R$ such that $Rg \cap Rh = Rg'h = Rh'g$. We will denote g' and h' by g^h and h^g respectively.*

(2)
$$\frac{R}{Rh^g} \cong \frac{Rg + Rh}{Rh}$$
In particular, if $Rg + Rh = R$ we have $h^g \sim h$ and hence $\deg h^g = \deg h$.

(3)
$$Rfg \cap Rh = \begin{cases} Rfg & \text{if } g \in Rh, \\ (Rf \cap Rh^g)g & \text{if } g \notin Rh. \end{cases}$$

Proof. (1) This is clear.

(2) This is given by a classical isomorphism theorem. Notice also that the map $R/Rh^g \longrightarrow R/Rh : x \mapsto xg$ is easily seen to be well defined and injective. Moreover it is onto when $Rg + Rh = R$.

(3) This is easy to check and is left to the reader. □

Remark 4.4. Let us first notice that if $g = t - a$ and $h = t - b$, $a \neq b$, we have $g^h = t - a^{a-b}$, where, as usual, $a^c = S(c)ac^{-1} + D(c)c^{-1}$ for $c \in K \setminus \{0\}$. More generally, when $h = t - a$ we have $Rg \cap R(t-a) = Rg$ if $g(a) = 0$ and $Rg \cap R(t-a) = R(t - a^{g(a)})g$ if $g(a) \neq 0$. Remark also that, when $h = t - a$, the formula in 4.3(3) above gives back the way of evaluating the product fg at the element $a \in K$.

We collect without proofs some easy facts related to similarity.

Lemma 4.5. *For monic polynomials $f, g, h \in R$, we have:*

(1) $\deg f^g \leq \deg f$.
(2) *If $g - h \in Rf$, then $f^g \sim f^h$.*
(3) $\Delta(f) = \{f^q \mid q \in R,\ Rq + Rf = R \text{ and } \deg q < \deg f\}$.
(4) *$gh \in Rf$ if and only if either $h \in Rf$ or $g \in Rf^r$ where r is the remainder of h right divided by f.*
(5) $(f^g)^h = f^{hg}$.

Proof. We leave the proofs of these statements to the reader (Cf. [LO] for similar facts in the more general frame of 2-firs). □

For a monic polynomial $f(t) = \sum_{i=0}^{n} a_i t^i \in R = K[t; S, D]$, the companion matrix of $f(t)$, denoted by C_f, is the $n \times n$ matrix defined by

$$C_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}.$$

We need also some results on pseudo-linear transformations (abbreviated by PLT or (S,D)-PLT in the sequel). For details on this topic we refer the reader to [L]. Let us recall that for a left K-vector space V, a map $T : V \longrightarrow V$ is an (S,D)-PLT if T is additive and $T(\alpha v) = S(\alpha)T(v) + D(\alpha)v$ for $\alpha \in K$ and $v \in V$. If $dim_K V = n < \infty$ and $\beta = \{e_1, \ldots, e_n\}$ is a K-basis for V, we associate to T a matrix in the usual way: $M_\beta(T) = (a_{ij})$ where $T(e_i) = \sum_{j=1}^n a_{ij}e_j$. On the other hand if A is a matrix in $M_n(K)$ and if K^n stands for the set of row vectors with coefficients in K. One can define the map $T_A : K^n \longrightarrow K^n$ given by $T_A(v) = S(v)A + D(v)$, where the maps S and D have been extended to K^n in an obvious way. T_A is an (S,D)-PLT which defines a left $R = K[t;S,D]$-module structure on K^n via $(\sum_{i=0}^n \alpha_i t^i).v = \sum_{i=0}^n \alpha_i (T_A)^i(v)$ for $v \in K^n$ and $\sum \alpha_i t^i \in K[t;S,D]$. Conversely any structure of left R-module defined on K^n is of this form. Let us denote $e_i := (0, \ldots, 0, 1, 0 \ldots 0)$ the element of K^n with a 1 in position i and zero elsewhere. For a monic polynomial $f \in R$ of degree n, the K-linear map $R/Rf \longrightarrow K^n$ defined by $t^i \mapsto e_{i+1}$, for $i = 0, 1, \ldots, n-1$ induces an R-module structure on K^n that corresponds to T_{C_f} where C_f is the companion matrix defined above. The matrix representing a PLT depends on the K-basis of K^n which is chosen. If two matrices A and B represent the same PLT in different bases, there exists an invertible matrix $P \in GL_n(K)$ such that

$$B := S(P)AP^{-1} + D(P)P^{-1}.$$

This leads to the following definitions.

Definitions 4.6. *(1) $A, B \in M_n(K)$ are (S,D)-similar if there exists an invertible matrix $P \in GL_n(K)$ such that $B = S(P)AP^{-1} + D(P)P^{-1}$.*
(2) A matrix A is (S,D)-diagonalizable (resp. triangularizable) if it is (S,D)-similar to a diagonal (resp. triangular) matrix.

Throughout the next two sections and independently of the size of the matrix involved, we will denote by U a matrix having zeros everywhere but a 1 in the bottom left corner. When different such matrices

appear in the same statement we will just use the notation $U_1, \ldots, U_n$ for the various instances of this type of matrices.

Lemma 4.7. *Let $f \in R = K[t; S, D]$ be a monic polynomial. Then:*

(1) *All submodules of R/Rf are of the form Rg/Rf, where g is a monic right factor of f.*

(2) *If there exist $a_1, \ldots, a_n \in K$ such that $f(t) = (t - a_n)(t - a_{n-1}) \cdots (t - a_1)$, then the companion matrix C_f is (S, D)-similar to the following one:*

$$\begin{pmatrix} a_1 & 1 & 0 & \ldots & 0 \\ 0 & a_2 & 1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & & a_{n-1} & 1 \\ 0 & & & 0 & a_n \end{pmatrix}$$

(3) *If $f = gh$ where $g, h \in R$ are monic then the companion matrix C_f is (S, D)-similar to the following matrix*

$$\begin{pmatrix} C_h & U \\ 0 & C_g \end{pmatrix}$$

Where the rectangular matrices are of the required sizes.

Proof. (1) This is clear since R is a left principal domain.

(2) Notice first that the set $\{1 + Rf, t - a_1 + Rf, (t - a_2)(t - a_1) + Rf, \ldots, (t - a_{n-1})(t - a_{n-2}) \cdots (t - a_1) + Rf\} \subseteq R/Rf$ is a K-basis of R/Rf. In this K-basis the matrix associated to left multiplication by t on R/Rf is exactly the one displayed in the statement (2). This shows that C_f is (S, D)-similar to this matrix.

(3) Put $l = \deg g$ and $n = \deg h$. It is enough to consider the following K basis of R/Rf:

$1 + Rf, t + Rf, \ldots, t^{n-1} + Rf, h + Rf, th + Rf, \ldots, t^{l-1}h + Rf$.

It is easy to check that in this basis the matrix representing left multiplication by t is exactly the one mentioned in the statement of the lemma. This shows that this matrix is (S, D)-similar to C_f. □

Let us remark that the second statement in the above Lemma 4.7 could also be obtained by using the third one repeatedly.

The following easy lemma will be very useful allowing us to translate $R = K[t; S, D]$-module theoretic notions into matrix related ones. It will be used again in the next section.

Lemma 4.8. *Let ${}_RV$ and ${}_RW$ be left R-modules which are finite dimensional as left K-vector spaces with bases $\mathcal{B}$ and $\mathcal{C}$ respectively. Let*

$\varphi : V \longrightarrow W$ be a left K-linear map and denote

$$P := M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \quad A := M_{\mathcal{B}}^{\mathcal{B}}(t\cdot) \quad \text{and} \quad B := M_{\mathcal{C}}^{\mathcal{C}}(t\cdot)\,.$$

Then φ is a morphism of left R-modules if and only if $AP = S(P)B + D(P)$.

Proof. For a vector $v \in V$ we denote $v_{\mathcal{B}}$ the row in K^n consisting of the coordinates of v in the basis $\mathcal{B}$. We use similar notations in W. The definition of $M_{\mathcal{B}}^{\mathcal{B}}(t\cdot)$ gives: $(t\cdot v)_{\mathcal{B}} = S(v_{\mathcal{B}})A + D(v_{\mathcal{B}})$ and so $\varphi(t\cdot v)_{\mathcal{C}} = S(v_{\mathcal{B}})AP + D(v_{\mathcal{B}})P$. On the other hand, $(t\cdot\varphi(v))_{\mathcal{C}} = S(\varphi(v)_{\mathcal{C}})B + D(\varphi(v)_{\mathcal{C}}) = S(v_{\mathcal{B}}P)B + D(v_{\mathcal{B}}P) = S(v_{\mathcal{B}})(S(P)B + D(P)) + D(v_{\mathcal{B}})P$. Since φ is a morphism of left R-modules if and only if $\varphi \circ t\cdot = t\cdot \circ\varphi$, we obtain the required equality. □

As a first consequence we get the following:

Theorem 4.9. *Two monic polynomials $f, g \in R$ are similar if and only if their companion matrices C_f and C_g are (S, D)-conjugate.*

Proof. Let $\mathcal{B} := \{1 + Rf, t + Rf, \ldots, t^{n-1} + Rf\}$, where $n = \deg f$, be a basis for the left K-vector space R/Rf. Then C_f represents the (S, D)-pseudo linear transformation $t\cdot$ acting on R/Rf i.e. $C_f = M_{\mathcal{B}}^{\mathcal{B}}(t\cdot)$. Similarly C_g represents $t\cdot$ in the appropriate basis $\mathcal{C}$ of R/Rg. Since $f \sim g$ if and only if there exists an isomorphism $R/Rf \overset{\varphi}{\cong} R/Rg$ of left R-modules. Hence the matrix $P := M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ is invertible and the above Lemma 4.8 shows that $f \sim g$ if and only if C_f and C_g are (S, D)-conjugate. □

Proposition 4.10. *Let $g, h \in R = K[t; S, D]$ be two monic polynomials of degree l and n respectively. Put*

$$A := \begin{pmatrix} C_h & U \\ 0 & C_g \end{pmatrix} \quad \text{and} \quad B := \begin{pmatrix} C_h & 0 \\ 0 & C_g \end{pmatrix}$$

where C_g, C_h denote the companion matrices of g and h respectively and U is our standard notation for the unit matrix $e_{n1} \in M_{n\times l}(K)$. Then the following are equivalent:

1. $0 \longrightarrow R/Rg \xrightarrow{\cdot h} R/Rgh \longrightarrow R/Rh \longrightarrow 0$ *splits.*
2. $1 \in Rg + hR$.
3. *There exists a matrix $X \in M_{n\times l}(K)$ such that*
$$\begin{pmatrix} I & S(X) \\ 0 & I \end{pmatrix} A + \begin{pmatrix} 0 & D(X) \\ 0 & 0 \end{pmatrix} = B \begin{pmatrix} I & X \\ 0 & I \end{pmatrix}$$
4. *There exists a matrix $X \in M_{n\times l}(K)$ such that $C_h X - S(X)C_g - D(X) = U$.*

Proof. (1) $\Rightarrow$ (2) By hypothesis there exists a map $\varphi : R/Rgh \longrightarrow R/Rg$ such that $\varphi \circ \cdot h = \mathrm{Id}_{R/Rg}$. Let $y \in R$ be such that $\varphi(1+Rgh) = y + Rg$. We then have $(\varphi \circ \cdot h)(1+Rg) = 1 + Rg$, i.e. $hy - 1 \in Rg$. This gives that there exists $x \in R$ such that $hy + xg = 1$.

(2) $\Rightarrow$ (3) By hypothesis there exist $x, y \in R$ such that $1 = xg + hy$. using the right euclidian division, we may assume that $\deg(y) < \deg(g)$. Define $\varphi : R/Rgh \longrightarrow R/Rh \oplus R/Rg : u + Rgh \mapsto (u + Rh, uy + Rg)$. It is easy to check that this map is a well defined morphism of left R-modules. Let $\mathcal{B} = \{1 + Rgh, t + Rgh, \ldots, t^{n-1} + Rgh, h + Rgh, th + Rgh, \ldots, t^{l-1}h + Rgh\}$ and $\mathcal{C} := \{(1 + Rh, 0), (t + Rh, 0), \ldots, (t^{n-1} + Rh, 0), (0, 1 + Rg), \ldots, (0, t^{l-1} + Rg)\}$ be bases for the left K-vector spaces R/Rgh and $R/Rh \bigoplus R/Rg$, respectively. Since $hy + Rg = 1 + Rg$, it is easy to check that the matrix of φ in these bases is of the form

$$P := M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} I & Y \\ 0 & I \end{pmatrix}$$

(where Y is the $n \times l$ matrix whose rows are given by writing $t^i y + Rg$, $i = 1, \ldots, n-1$, in the basis $t^j + Rg$, $j \in \{0, \ldots, l-1\}$). Remark that we also have $A = M_{\mathcal{B}}^{\mathcal{B}}(t\cdot)$ and $B = M_{\mathcal{C}}^{\mathcal{C}}(t\cdot)$. Since φ is a morphism of left R-modules, Lemma 4.8 implies that $AP = S(P)B + D(P)$ i.e. $S(P^{-1})A + D(P^{-1}) = BP^{-1}$. We then get the desired conclusion with $X := -Y$.

(3) $\Rightarrow$ (1) Let $\mathcal{B}$ and $\mathcal{C}$ be the bases for the K-vector spaces R/Rgh and $R/Rh \bigoplus R/Rg$ defined in the proof of (2) $\Rightarrow$ (3). Let $\varphi : R/Rgh \longrightarrow R/Rh \bigoplus R/Rg$ be the left K-isomorphism map such that

$$P := M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} I & -X \\ 0 & I \end{pmatrix}$$

We have $A = M_{\mathcal{B}}^{\mathcal{B}}(t\cdot)$ and $B = M_{\mathcal{C}}^{\mathcal{C}}(t\cdot)$. Statement (3) implies that $S(P^{-1})A + D(P^{-1}) = BP^{-1}$ i.e. $AP = S(P)B + D(P)$. Lemma 4.8 shows that φ is an homomorphism of left R-modules. Let p denotes the projection $R/Rh \bigoplus R/Rg \longrightarrow R/Rg$. We claim that $p \circ \varphi : R/Rgh \longrightarrow R/Rg$ is a splitting of $\cdot h$. Indeed $(p \circ \varphi \circ .h)(1 + Rg) = p(\varphi(h + Rgh)) = p((0, 1 + Rg)) = 1 + Rg$.

(3) $\Leftrightarrow$ (4) This is left to the reader. □

5. DIAGONALIZATION AND TRIANGULARIZATION

In this section we will briefly consider a generalization of Wedderburn polynomials which will be called fully reducible polynomials. The family of fully reducible polynomials is larger than the Wedderburn one, but they share many properties and, for what we have in mind, the

fully reducible polynomials are not more difficult to handle. They will show better the connection between factorization in R and companion matrices. They were introduced by Ore himself and further studied by P.M. Cohn in the setting of 2-firs ([Co_2]) and more recently by the second and third authors of this paper (again in the setting of 2-firs, Cf. [LO]). The companion matrices of these families of polynomials will lead us naturally to a characterization of diagonalizability of a matrix over a division ring.

Definition 5.1. A monic polynomial $f \in R = K[t; S, D]$ is fully reducible if there exist irreducible polynomials $p_1, \ldots, p_n$ such that $Rf = \bigcap_{i=1}^{n} Rp_i$.

Wedderburn polynomials and monic irreducible polynomials are fully reducible. Notice also that a polynomial $g(t) = (t - a_1) \cdots (t - a_n)$ is fully reducible if and only if it is Wedderburn.

The notion of fully reducible polynomials is symmetric i.e. if $f \in R = K[t; S, D]$ is a monic polynomial and $p_1, p_2, \ldots, p_n$ are irreducible polynomials such that $Rf = \bigcap_{i=1}^{n} Rp_i$ then there exist irreducible polynomials $q_1, \ldots, q_n$ such that $fR = \bigcap_{i=1}^{n} q_i R$. Moreover there exists a permutation $\pi \in S_n$ such that $p_i \sim q_{\pi(i)}$ i.e. $R/Rp_i \cong R/Rq_{\pi(i)}$ (Cf. [LL_4] or [LO]).

Theorem 5.2. *Let $f \in R$ be a monic polynomial of degree l. Then the following are equivalent:*

(1) *f is fully reducible.*
(2) *There exist monic irreducible polynomials $p_1, \ldots, p_n$ such that $Rf = \bigcap_{i=1}^{n} Rp_i$ is an irredundant intersection.*
(3) *There exist monic irreducible polynomials $p_1, \ldots, p_n \in R$ such that the map $\varphi : R/Rf \longrightarrow \bigoplus_{i=1}^{n} R/Rp_i$ given by $\varphi(q + Rf) = (q + Rp_1, \ldots, q + Rp_n)$ is an isomorphism of R-modules.*
(4) *There exist monic irreducible polynomials $p_1, \ldots, p_n \in R$ and an invertible matrix $V \in M_l(K)$ such that*

$$C_f V = S(V)\mathrm{diag}\,(C_{p_1}, \ldots, C_{p_n}) + D(V).$$

(5) *R/Rf is semisimple.*

Proof. (1) $\Leftrightarrow$ (2) is clear by definition.

(2) $\Rightarrow$ (3). The map φ is easily seen to be well defined and injective. Since, for every $j \in \{1, \ldots, n\}$, $Rp_j + (\bigcap_{i \neq j} Rp_i) = R$, Lemma 4.3 and an easy induction on n show that $\deg f = \sum_{i=1}^{n} \deg p_i$. This implies that the $\dim_K(R/Rf) = \dim_K(\bigoplus_i R/Rp_i)$ and we conclude that φ is onto.

(3) $\Longrightarrow$ (2). Composing φ with the natural homomorphism $R\xrightarrow{p}R/Rf$ we obtain an onto R-morphism: $\psi = \varphi \circ p$ such that $\ker\psi = Rf$ and we conclude that $Rf = \bigcap_{i=1}^{n} Rp_i$. The fact the this intersection is irredundant is clear from the equalities: $l = \deg(f) = \dim_K(R/Rf) = \sum_i \dim_K(R/Rp_i) = \sum_i \deg(p_i)$.

(3) $\Rightarrow$ (4). Let $\mathcal{B} = \{t^i + Rf \,|\, i = 0, \ldots, l-1\}$ be a basis for the left K space R/Rf and $\mathcal{C} = \{(0, \ldots, 0, t^j + Rp_i, 0, \ldots, 0) \,|\, i = 1, \ldots, n \text{ and } j = 0, \ldots, n_i - 1\}$, where $n_i = \deg p_i$, be a K-basis for $\oplus_i R/Rp_i$. We have $M_{\mathcal{B}}^{\mathcal{B}}(t\cdot) = C_f$ and $M_{\mathcal{C}}^{\mathcal{C}}(t\cdot) = \operatorname{diag}(C_{p_1}, \ldots, C_{p_n})$. Put $V := M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$. Then V is invertible and since φ is a morphism of left R-modules, Lemma 4.8 yields the required equality.

(4) $\Rightarrow$ (5). It is enough to define the K-linear map $\varphi : R/Rf \longrightarrow \oplus_{i=1}^{n} R/Rp_i$ such that $V = M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ where $\mathcal{B}$ and $\mathcal{C}$ are the bases defined in the proof of the implication (3) $\Rightarrow$ (4). Since V is invertible, this map is bijective. Statement (4) and Lemma 4.8 imply that φ an isomorphism of left R-modules. The simplicity of the left R-modules $R/Rp_1, \ldots, R/Rp_n$ implies that R/Rf is semi-simple.

(5) $\Rightarrow$ (3). This is clear and left to the reader. □

In ([LL$_5$]) (resp. [LO]) several criterion were given for a product of Wedderburn polynomials (resp. fully reducible polynomials) to be again a Wedderburn polynomial (resp. fully reducible). We will give two more criterions in the following theorem. We treat the cases of Wedderburn polynomials and fully reducible polynomials simultaneously. Let us first introduce some technical notations. Let g be a monic polynomial of degree l and suppose g admits a factorization $g = p_r \cdots p_1$, where $p_1, \ldots, p_r$ are monic polynomials of degree $l_1, \ldots, l_r$ respectively. We put:

$$C_g(p_r, \ldots, p_1) = \begin{pmatrix} C_{p_1} & U_1 & 0 & \cdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & C_{p_{r-1}} & U_{r-1} \\ 0 & 0 & 0 & C_{p_r} \end{pmatrix},$$

where for $i = 1, \ldots, r-1$, the matrices $U_i \in M_{n_i \times n_{i+1}}(K)$ have a 1 in the bottom left corner and zero elsewhere. In particular, if $g(t) = (t - a_r) \cdots (t - a_1)$ the above matrix takes a simpler form:

$$C_g(a_r, \ldots, a_1) = \begin{pmatrix} a_1 & 1 & 0 & \cdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & a_{r-1} & 1 \\ 0 & 0 & 0 & a_r \end{pmatrix}.$$

Lemma 5.3. *With the above notation, the companion matrix of g is (S, D)-similar to $C_g(p_r, \dots, p_1)$. More precisely, there exists an invertible lower triangular matrix $Q \in M_{l\times l}(K)$ with 1's on the diagonal such that:*

$$C_g^Q = C_g(p_r, \dots, p_1).$$

Where, as usual, $Cg^Q = S(Q)C_gQ^{-1} + D(Q)Q^{-1}$.

Proof. Let us put $\deg(p_i) = l_i$, $i = 1, \dots, r$. Similarly as in the proof of Lemma 4.7, consider the bases $\mathcal{B}$ and $\mathcal{C}$ of the K-vector space R/Rg defined as follows: $\mathcal{B} := \{1 + Rg, t + Rg, \dots, t^{l_1-1} + Rg, p_1 + Rg, tp_1 + Rg, \dots, t^{l_2-1}p_1 + Rg, p_2p_1 + Rg, tp_2p_1 + Rg, \dots, t^{l-1}p_{r-1}\cdots p_1 + Rg\}$ and $\mathcal{C} := \{1 + Rg, t + Rg, \dots, t^{l-1} + Rg\}$. We have $M_{\mathcal{B}}^{\mathcal{B}}(t\cdot) = C_g(p_r, \dots, p_1)$, $M_{\mathcal{C}}^{\mathcal{C}}(t\cdot) = C_g$ and it is easy to check that the matrix $Q := M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{Id})$ representing the identity map on R/Rg in the bases $\mathcal{B}$ and $\mathcal{C}$ is lower triangular with ones on the diagonal. Since the identity is an R-module map, Lemma 4.8 gives the desired result. □

Theorem 5.4. *Let g, h be fully reducible polynomials (resp. W-polynomials) from R of degree l and n respectively. Then the following are equivalent:*

(1) *gh is a fully reducible (resp. W-) polynomial.*
(2) $1 \in Rg + hR$.
(3) *There exists a matrix $X \in M_{n\times l}(K)$ such that*

$$C_hX - S(X)C_g - D(X) = U,$$

where $U = e_{n1} \in M_{n\times l}(K)$.

(4) *Let $g = p_r \cdots p_1$ and $h = q_s \cdots q_1$ (resp. $p_1 = (t - b_l), \cdots, p_l = t - b_l$ and $q_1 = (t - a_1), \cdots, q_s = t - a_s$)). Then there exists $Y \in M_{n\times l}(K)$ such that*

$$C_h(q_s, \dots, q_1)Y - S(Y)C_g(p_r, \dots, p_1) - D(Y) = U.$$

(resp.

$$C_h(a_n, \dots, a_1)Y - S(Y)C_g(b_l, \dots, b_1) - D(Y) = U.)$$

Proof. (1)⇔(2) This comes from the fact that a monic polynomial $f \in R$ is fully reducible if and only if the left R-module R/Rf is semi simple. In particular, by hypothesis, R/Rg and R/Rh are semi simple modules. With these remarks, Equivalence (1) ⇔ (2) in Proposition 4.10 easily yields the result.

(2)⇔(3) This is exactly the equivalence (2)⇔(4) in Proposition 4.10.

(3)⇔(4) The above Lemma 5.3 shows that there exist lower triangular matrices P, Q with $1'$s on their diagonals such that $C_h^P = C_h(q_s, \dots, q_1)$ and $C_g^Q = C_g(p_r, \dots, p_1)$. From (3) we have $C_h^PPX -$

$D(PX)-S(PX)C_g = S(P)U$. Putting $Z = PX$ we get $C_h(q_s, \ldots, q_1)Z - D(Z) - S(Z)C_g = S(P)U$. Multiplying by Q^{-1} on the right we obtain $C_h(q_s, \ldots, q_1)ZQ^{-1} - (D(Z)Q^{-1} + S(Z)D(Q^{-1})) - S(ZQ^{-1})C_g^Q = S(P)UQ^{-1}$. Defining $Y := ZQ^{-1}$ we finally get that $C_h(q_s, \ldots, q_1)Z - D(Z) - S(Z)C_g(p_r, \ldots, p_1) = S(P)UQ^{-1} = U$, where the last equality comes from the definition of $U = e_{n1}$ and the fact that the matrices P and Q are lower triangular matrices with ones on the diagonal. □

In our previous work Wed1 ([LL$_5$]) we have obtained a few conditions for a product of two W-polynomials to be a W-polynomial. Let us point out that the advantage of the characterization (3) in the above theorem is that there is a finite number of equations to check and that they are directly available from the coefficients of g and h themselves. The characterization (4) is also interesting if one knows in advance a factorization of f and g.

Example 5.5. Let $K = \mathbb{Q}(x)$ be the field of rational fractions in x over the rationals and let R be the Ore extension $R = \mathbb{Q}(x)[t; \mathrm{Id}, \frac{d}{dx}]$. Using the above theorem it is easy to show that, for any $q \in \mathbb{Q}(x)$ and for any $n \in \mathbb{N}$, the polynomials $(t-q)^n \in R$ are W-polynomials. To check this, let us write $(t-q)^n = (t-q)^{n-1}(t-q)$ and $U = (1, 0, \ldots, 0) \in M_{1\times n-1}(\mathbb{Q}(x))$. Part (4) of the theorem, with $g = (t-q)^{n-1}$ and $h = t - q$, shows that we have to find $(y_1, \ldots, y_{n-1}) \in \mathbb{Q}(x)^{n-1}$ such that:

$$\left\{\begin{array}{l} y_1 q + D(y_1) - qy_1 + 1 = 0 \\ y_1 + y_2 q + D(y_2) - qy_2 = 0 \\ y_2 + y_3 q + D(y_3) - qy_3 = 0 \\ \vdots \\ y_{n-2} + y_{n-1} q + D(y_{n-1}) - qy_{n-1} = 0 \end{array}\right.$$

It is then easy to see that the sequence defined by $y_i = (-1)^i \frac{x^i}{i!}$ $(i = 1, \ldots, n-1)$ gives a solution of the above system of equations. We can thus conclude that, for any $n \in \mathbb{N}$, the polynomial $(t-q)^n \in R$ is a W-polynomial.

Example 5.6. Let k be a commutative field of characteristic 0, D a derivation ($S = \mathrm{Id}$) on k. Kolchin (Cf. [Ko]) showed that there exists a field L containing k as a subfield and a derivation $\overline{D}$ over L extending D such that the equation

$$p(x, \overline{D}(x), \ldots, \overline{D}^{(n)}(x)) = 0, \quad n \text{ arbitrary},$$

has a solution $u \in L$ for all $p(X) \in U[X_1, \ldots, X_{n+1}] \setminus L$. Applying this property to the polynomial $X_2 - v$, for $v \in L$, we conclude that

$\overline{D}$ is onto. We claim that all monic polynomials of $R = L[t; \overline{D}]$ are W-polynomials. Let us first show the the irreducible polynomials are of degree at most 1. Indeed, if $p(t) = \sum a_i t^i \in R$ is such that $\deg(p(t)) > 1$, it is easy to verify that the hypothesis made on L implies that there exists $v \in L$ such that $p(v) = \sum a_i N_i(v) = 0$ i.e. $t - v$ divides $p(t)$ on the right. It follows that any monic polynomial $h(t)$ of degree n can be factorized in the form $h(t) = (t - a_n) \dots (t - a_1)$. By induction on the degree we need only show that if $h(t)$ is a W-polynomial, than $(t-b)h(t)$ is also a W-polynomial. Once again using the above Theorem 5.4(4), we must find $(y_1, \dots, y_n) \in L^n$ such that:

$$\begin{pmatrix} a_1 & 1 & 0 & \cdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & a_{n-1} & 1 \\ 0 & 0 & 0 & a_n \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} - \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} b - \begin{pmatrix} D(y_1) \\ D(y_2) \\ \vdots \\ D(y_n) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

In other words we have to solve (for y_i's) the equations

$$a_i y_i - y_i b - D(y_i) = u_i \quad \text{for } 1 \leq i \leq n\,,$$

where $u_i = -y_{i+1}$ for $1 \leq i \leq n-1$ and $u_n = 1$. But solving first for y_n and then for y_{n-1},... it is easy to check that these equations all have solutions thanks to the property of L.

We now come to the diagonalization. As is well known, a matrix $A \in M_n(k)$ over a commutative field k is diagonalizable if and only if its minimal polynomial can be written as a product of distinct linear polynomials in $k[t]$. In other words the minimal polynomial of A must be a W-polynomial. In the next section we will generalize this result and obtain a criterion for the diagonalizability of a matrix with coefficients in a division ring. This will be developed in an "(S, D)" setting.

Let us recall some results and notations from [LL$_1$]. For $\{b_1, \dots, b_n\} \subset K$ we define the Vandermonde matrix:

$$V_n(b_1, \dots, b_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ b_1 & b_2 & \cdots & b_n \\ N_2(b_1) & N_2(b_2) & \cdots & N_2(b_n) \\ \vdots & \vdots & \vdots & \vdots \\ N_{n-1}(b_1) & N_{n-1}(b_2) & \cdots & N_{n-1}(b_n) \end{pmatrix}$$

where, for $a \in K$ and $i \geq 0$, $N_i(a)$ denotes the evaluation of t^i at a. Notice that one has $N_0(a) = 1$ and, using the product formula recalled in (2.1), one gets $N_{i+1}(a) = (tt^i)(a) = \phi_{t^i}(a)t^i(a) = S(N_i(a))a + D(N_i(a))$.

Let us also remark that this matrix appeared already in an hidden form in 5.2. Indeed if, in this theorem, $p_1 = t - b_1, \ldots, p_n = t - b_n$ the matrix V in Theorem 5.2 (4)(Cf. also its proof) is exactly the above Vandermonde matrix. This can be exploited to get the equivalence between (*iii*) and (*iv*) in the following proposition.

Lemma 5.7. *For $\Delta := \{b_1, \ldots, b_n\} \subset K$ the following are equivalent*

i) $\Delta := \{b_1, \ldots, b_n\}$ *is P-independent.*
ii) $\deg f_\Delta = n$.
iii) $Rf_\Delta = \bigcap_{i=1}^n R(t - b_i)$.
iv) *The matrix $V_n(b_1, \ldots, b_n)$ is invertible.*

Proof. (i) $\Leftrightarrow$ (ii) and (ii) $\Leftrightarrow$ (iii) are easy to establish and were proved in [LL_4],[LL_5].

(iii) $\Leftrightarrow$ (iv) This is a simple application of Theorem 5.2; The irreducible polynomials "p_i's" in this theorem are in the present case $p_i = t - b_i$ and, as noticed above, the matrix V appearing in the statement (3) of 5.2 is exactly the Vandermonde matrix $V_n(b_1, \ldots, b_n)$. The rest is clear. □

Since a W-polynomial is of the form f_Δ for some finite subset $\Delta \subset K$, the above lemma also shows the strong relation existing between W-polynomials and Vandermonde matrices. This leads to the following theorem which shows, in particular, that a companion matrix C_f is (S, D)-diagonalizable if and only if f is a W-polynomial.

Theorem 5.8. *Let $f \in R$ be a monic polynomial of degree n. Then the following are equivalent:*

i) *f is a W-polynomial.*
ii) *There exists a P-independent set $B = \{b_1, b_2, \ldots, b_n\} \subset K$ such that $f = f_B$.*
iii) *There exist $\{b_1, b_2, \ldots, b_n\} \subset K$ such that $V = V_n(b_1, b_2, \ldots, b_n)$ is invertible and*

$$C_f V = S(V)\mathrm{diag}\,(b_1, b_2, \ldots, b_n) + D(V)$$

iv) *C_f is (S, D)-diagonalizable.*
v) *The left R-module R/Rf is semi-simple with simple components of dimension 1 over K.*

Proof. These equivalences are special cases of 5.2 using Lemma 5.7. □

Remark 5.9. Let us mention that the statement (v) above is specific to the left R-module R/Rf. In fact, if S is not onto, even right modules such as $R/(t - a)R$ need not be semisimple. Consider for instance the field $K := k(x)$ and the k-endomorphism S given by $S(x) = x^2$.

If $f(t) := t \in R = K[t; S, D]$ then the R-module R/fR is finitely generated but not artinian (it contains the descending chain of right R-modules $xt^nR + tR$ for $n \in \mathbb{N}$) and so can not be semisimple.

For the more general case of a matrix A we will assume that the endomorphism S is an automorphism. Let us recall that, in this case, the ring $R = K[t; S, D]$ is a left and right principal ideal domain. We will need the following definitions:

Definitions 5.10. *For $f, g \in R = K[t; S, D]$ we say that f strongly divides g, and we write $f||g$, if there exists an invariant element $c \in R$ (i.e. $cR = Rc$) such that f divides c on the left and c divides g on the left.*

Notice, in particular, that if $f, g \in R$ are such that $f||g$ then f divides g on both sides i.e. $g \in Rf \cap fR$. It is easy to check that the notion of strong divisibility is left right symmetric.

We can then use the following classical result (Cf. [Co_2]).

Lemma 5.11. *Let R be a principal ideal domain and let A be an $n \times n$ matrix with coefficients from R. Then there exist invertible $n \times n$ matrices P and Q such that the matrix*

$$PAQ = \mathrm{diag}\,(e_1, e_2, \ldots, e_n)$$

where e_i strongly divides e_{i+1}, for $1 \leq i \leq n-1$.

A matrix $A \in M_n(K)$ determines a left $R = K[t; S, D]$-module structure on the space of rows K^n. More precisely this structure is given by $t \cdot \underline{v} = S(\underline{v})A + D(\underline{v})$ (in other words the action of t is given by the map T_A defined in the paragraph before Definition 4.6). We thus have an exact sequence of left R-modules:

$$0 \longrightarrow R^n \xrightarrow{tI-A} R^n \xrightarrow{\varphi} K^n \longrightarrow 0$$

where φ is the left R-morphism sending the unit vectors of $f_i = (0, \ldots, 0, 1, 0 \ldots, 0) \in R^n$ to the unit vectors of K^n. The above lemma shows that there exist matrices $P, Q \in GL_n(R)$ such that $P(tI-A)Q = \mathrm{diag}\,(e_1, e_2, \ldots, e_n)$. Remarking that if $e = 1$ then $R/eR = 0$, we get, after reindexing the e_i's if necessary, an isomorphism of left R-modules

$$ {}_RK^n \cong \bigoplus_{i=1}^{r} \frac{R}{Re_i} \quad \text{for } r \leq n \tag{5.1}$$

The elements $e_1, \ldots, e_r$ in this decomposition are called the invariant factors. They are defined up to similarity. Notice that if two polynomials $f, g \in R$ are similar than f is Wedderburn if and only if g is

Wedderburn. This shows that the statements of our next results are really independent of the representant chosen for e_r. We will thus call e_r "the last invariant factor". We are now ready for the characterization of an (S, D)-diagonalizable matrix. The last invariant factor "e_r" will play a key role in the characterization of (S, D)-diagonalizability and triangulability.

Theorem 5.12. *Let K, S, D be a division ring, an automorphism and a S-derivation of K, respectively. A matrix $A \in M_n(K)$ is (S, D)-diagonalizable if and only if its last invariant factor is a W-polynomial.*

Proof. We use the above notations in particular ${}_RK^n$ is decomposed as in 5.1. Since the action of $t\cdot$ is determined by A on K^n and by the C_{e_i} on R/Re_i it then follows from classical facts (Cf. [L]) that there exists an invertible matrix P such that

$$S(P)AP^{-1} + D(P) = \operatorname{diag}(C_{e_1}, C_{e_2}, \ldots, C_{e_r}) \tag{5.2}$$

It is easy to check that, if the matrices C_{e_i}'s are (S, D)-diagonalizable then the matrix $\operatorname{diag}(C_{e_1}, C_{e_2}, \ldots, C_{e_r})$ is (S, D)-diagonalizable. Conversely: assume that the matrix $\operatorname{diag}(C_{e_1}, C_{e_2}, \ldots, C_{e_r})$ is (S, D)-diagonalizable. This matrix represents the action of $t\cdot$ (left multiplication by t) on ${}_RK^n \cong \bigoplus_{i=1}^r \frac{R}{Re_i}$. Hence there exists a K-basis $\{u_1, u_2, \ldots, u_n\}$ of K^n consisting of eigenvectors for the action of $t\cdot$. We thus have, for $l \in \{1, 2, \ldots, n\}$, $t \cdot u_l = \alpha_l u_l$ for some $\alpha_l \in K$. Decomposing each u_l according to the direct sum $\bigoplus_{i=1}^r \frac{R}{Re_i}$, we can write $u_l = \sum_{j=1}^r u_{l,j}$. It is then easy to check that for all $j = 1, \ldots, r$ and $l = 1, \ldots, n$, the non zero elements u_{lj} are eigenvectors for left multiplication by t. For all $j = 1, \ldots, r$ the set $\{u_{lj} \,|\, l = 1, \ldots, n\}$ is a generating set for R/Re_j from which one can extract a K-basis consisting of eigenvectors for left multiplication by t. This shows that $C_{e_1}, C_{e_2}, \ldots, C_{e_r}$ are (S, D)-diagonalizable. It is now clear that A is (S, D)-diagonalizable if and only if the matrices C_{e_i}'s are (S, D)-diagonalizable. Theorem 5.8 shows that this is the case if and only if the polynomials $e_1, e_2, \ldots, e_r$ are W-polynomials. By Lemma 5.11 we know that e_i divides e_{i+1} the conclusion of the theorem now follows from Corollary 3.5. □

In the special case when $S = \mathrm{Id}$ and $D = 0$, the above theorem was presented during a conference in Caen in 2000 by G. Cauchon. He used the quasi determinants techniques to produce a polynomial and showed that a matrix is diagonalizable if and only if this polynomial has separate zeros (which means Wedderburn in our language). In particular, Cauchon didn't use the Vandermonde matrices and uses a different technique of diagonalization.

Let us now come to triangularization. The expected result holds: a square matrix A is triangularizable if and only if the last invariant factor of A is a product of linear factors. As in the case of diagonalization we will reduce the problem to the case of a companion matrix.

Proposition 5.13. *Let $f \in R = K[t; S, D]$ be a monic polynomial of degree n. The following are equivalent:*

(i) *C_f is (S, D)-triangularizable.*

(ii) *There exists a chain of left R-modules of R/Rf*

$$0 = V_0 \lneqq V_1 \lneqq \cdots \lneqq V_{n-1} \lneqq V_n = R/Rf.$$

(iii) *There exists $g_1, g_2, \ldots, g_{n-1} \in R$ such that*

$$Rf \subsetneq Rg_1 \subsetneq \cdots \subsetneq Rg_{n-1} \subsetneq R.$$

(iv) *f is a product of monic linear polynomials.*

Proof. (i) $\longrightarrow$ (ii) C_f represents the left multiplication $t\cdot : R/Rf \longrightarrow R/Rf$ in the basis $1, t, \ldots, t^{n-1}$. Since C_f is (S, D)-triangularizable one can find $v_1, \ldots, v_n$ a K-basis of R/Rf such that $t \cdot v_i \in Kv_1 + \cdots + Kv_i$. In particular, for any $i = 1, \ldots, n$, the left K-vector space $V_i = Kv_1 + \cdots + Kv_i$ is a left R-module. From this we conclude that these modules satisfy the required property.

(ii) $\longrightarrow$ (iii) Thanks to Lemma 4.7(i), we can find $g_1, \ldots, g_n \in R$ such that $V_i = Rg_i/Rf$. The properties of the V_i's give the required inclusions between the Rg_i's.

(iii) $\longrightarrow$ (iv) Since $\deg f = n$ and the inclusions are strict we must have $\deg g_i = n - i$ for $i = 1, \ldots, n-1$ and we conclude easily.

(iv) $\longrightarrow$ (i) Let us write $f(t) = (t - a_n) \ldots (t - a_1)$. Lemma 4.7 (2) shows that C_f is (S, D)-triangularizable. $\square$

We are now ready to present the general case of the criterion for (upper) triangularization. For a square matrix $A \in M_n(K)$ we denote, as in Theorem 5.12, by $e_1, \ldots, e_r$ the invariant factors of A. Recall that we have $e_1 || e_2 || \cdots || e_r$, which means that there exist invariant polynomials $c_r, \ldots, c_1$ such that $e_i | c_i | e_{i+1}$.

Theorem 5.14. *Let K, S, D be a division ring an automorphism and a S-derivation of K, respectively. Let $A \in M_n(K)$ be a square matrix, then A is (S, D)-triangularizable if and only if the last invariant factor e_r is a product of monic linear polynomials.*

Proof. Assume that e_r is a product of linear polynomials. Since we have $e_1 || e_2 || \cdots || e_r$, the fact that R is a U.F.D. implies that $e_1, \ldots, e_{r-1}$ are also product of linear polynomials. Proposition 5.13 makes it clear

that the matrices C_{e_i} are all triangularizable. Thanks to Equation 5.2 (Cf. the proof of Theorem 5.12), we know that A is similar to $\mathrm{diag}\,(C_{e_1},\ldots,C_{e_r})$ and the result is now clear.

Conversely, assume that $A \in M_n(K)$ is triangularizable. K^n is a left R-module via the action $t\cdot v := S(v)A + D(v)$, $v \in K^n$. Let $v_1,\ldots,v_n$ be a basis of K^n such that, for all $i \in \{1,\ldots,n\}$, $t\cdot v_i = \sum_{j=1}^{i}\alpha_{ij}v_j$. Decomposing each v_i according to the isomorphism 5.1 we get $v_i = \sum_{k=1}^{r} v_{ik}$ and so we obtain on one hand $t\cdot v_i = \sum_{j=1}^{i}\alpha_{ij}v_j = \sum_{k=1}^{r}(\sum_{j=1}^{i}\alpha_{ij}v_{jk})$ and on the other hand we have $t\cdot v_i = t\cdot\sum_{k=1}^{r} v_{ik} = \sum_{k=1}^{r} t\cdot v_{ik}$. Since R/Re_k is stable by the action of $t\cdot$ and the decomposition in 5.1 is direct we get $t\cdot v_{ik} = \sum_{j=1}^{i}\alpha_{ij}v_{jk}$, for $k \in \{1,\ldots,r\}$. Let us now observe that, for $k = 1,\ldots,r$ $\{v_{ik}|\, i = 1,\ldots,n\}$ is a generating set for R/Re_k as left K vector space. It is now easy to check that one can extract a basis B_k from this generating set such that the matrix representing $t\cdot|_{R/Re_k}$ in the basis B_k is triangular. Proposition 5.13 then shows that the e_k's are product of linear polynomials. □

6. EIGENVALUES

In this section we will give some basic facts on eigenvalues of matrices over division rings. We will again assume that S is an automorphism of the division ring K. We have seen in the preceding section (see also the paragraph before Definition 4.6) how to associate with every matrix $A \in M_{n\times n}(K)$ a structure of left R-module on K^n or equivalently how to define a pseudo linear transformation $T_A : K^n \longrightarrow K^n$. Since S is assumed to be an automorphism, the concept defined so far must be symmetric. In the sequel we will denote ${}^nK$ the row matrix space of size $1\times n$ over K and we will use $(v)^T$ for the transpose of the matrix v. The aim of the next lemma is to examine more closely this symmetry.

Lemma 6.1. (1) *$\delta := -DS^{-1}$ is a right S^{-1}-derivation; i.e. $\delta(ab) = \delta(a)S^{-1}(b) + a\delta(b)$ and $R = K[t;S,D]$ is a left and right principal ideal domain. The elements of R can be written in the form $\sum_{i=0}^{n} t^i a_i$ with the commutation rule at $= tS^{-1}(a) - DS^{-1}(a)$ for any $a \in K$.*

(2) *We have $\Delta^{S,D}(a) := \{a^c := S(c)ac^{-1} + D(c)c^{-1}\,|\, c \in K\setminus\{0\}\} = \Delta^{-DS^{-1},S^{-1}}(a) := \{{}^ca := caS^{-1}(c^{-1}) + c(-DS^{-1}(c^{-1}))\,|\, c \in K\setminus\{0\}\}$.*

(3) *If $A \in M_n(K)$, we can define a structure of right R-module on the set ${}^nK$ of columns via $u.t := L_A(u) := AS^{-1}(u) - DS^{-1}(u)$ where $u \in {}^nK$.*

If $A \in M_n(K)$ the left R-module K^n and the right R-module ${}^nK$ induced by A gives rise to the same invariant factors (up to similarity). i.e. $K^n \cong \bigoplus_{i=1}^{r} R/Re_i \Leftrightarrow {}^nK \cong \bigoplus_{i=1}^{r} R/e_iR$.

Proof. (1) This is standard and easy to prove.

(2) It suffices to check that for $c \in K \setminus \{0\}$ we have ${}^c a = a^d$ where $d = S^{-1}(c)$.

(3) Let us compute, for $\alpha \in K$ and $u \in {}^n K$, $L_A(u\alpha) = AS^{-1}(u\alpha) - DS^{-1}(u\alpha) = AS^{-1}(u)S^{-1}(\alpha) - D(S^{-1}(u)S^{-1}(\alpha)) = AS^{-1}(u)S^{-1}(\alpha) - uDS^{-1}(\alpha) - D(S^{-1}(u))S^{-1}(\alpha) = L_A(u)S^{-1}(\alpha) + u(-DS^{-1})(\alpha)$. This shows that $(u\alpha).t = (u.t)S^{-1}(\alpha) + u(-DS^{-1})(\alpha) = u.(tS^{-1}(\alpha) - (DS^{-1})(\alpha)) = u.(\alpha t)$. The rest is clear.

(4) This is due to the fact that the invariant factors are obtained from $tI - A \in M_n(R)$ using elementary transformations on rows and columns and hence depend only on A. □

Definition 6.2. For $A \in M_{n\times n}(K)$, $\alpha, \beta \in K$, $v \in K^n \setminus \{(0, \dots, 0)\}$ and $u \in {}^n K \setminus \{(0, \dots, 0)^T\}$, we say that:

(1) α is a left eigenvalue of A associated to v if

$$T_A(v) = \alpha v$$

.

(2) β is a right eigenvalue of A associated to u if

$$L_A(u) = u\beta$$

We will denote $\mathrm{lspec}(A)$ and $\mathrm{rspec}(A)$ the sets of left and right eigenvalues of a matrix A; $\mathrm{Spec}(A)$ will stand for the union of left and right eigenvalues.

In the next proposition we collect a few elementary properties of the left and right eigenvalues.

Proposition 6.3. *Let A be a matrix in $M_n(K)$. Then,*

(1) $\mathrm{lspec}(A)$, $\mathrm{rspec}(A)$, $\mathrm{Spec}(A)$ *are closed under (S, D)-conjugation.*

(2) *If $P \in GL_n(K)$,*

$$\mathrm{lspec}(A) = \mathrm{lspec}(A^P),\ \mathrm{rspec}(A) = \mathrm{rspec}(A^P),\ \mathrm{Spec}(A) = \mathrm{Spec}(A^P)\,.$$

(3) *Left eigenvectors corresponding to non (S, D)-conjugate left eigenvalues are left linearly independent.*

(4) *Right eigenvectors corresponding to non (S, D)-conjugate right eigenvalues are right linearly independent.*

(5) *If $\alpha \in \mathrm{lspec}(A)$ and $\beta \in \mathrm{rspec}(A)$ are not (S, D)-conjugate and $v = (v_1, \dots, v_n) \in K^n$, $u = (u_1, \dots, u_n)^T \in {}^n K$ are the associated eigenvectors then $v.u := \sum_{i=1}^n v_i u_i = 0$.*

Proof. (1) Assume $\alpha \in \mathrm{lspec}(A)$ and let $v \in K^n$ be an eigenvector for α. We thus have $T_A(v) = \alpha v$. If $\beta \in K \setminus \{0\}$ we have $T_A(\beta v) = S(\beta)T_A(v) + D(\beta)v = (S(\beta)\alpha + D(\beta))v = (\alpha^\beta)\beta v$. This shows that α^β

is also a left eigenvalue and proves that lspec(A) is closed under (S, D)-conjugation. Similarly, if $\lambda \in \text{rspec}(A)$, $u \in {}^nK$ and $\mu \in K \setminus \{0\}$ are such that $L_A(u) = u\lambda$, one can check that $L_A(uS(\mu^{-1})) = uS(\mu^{-1})\lambda^\mu$.

(2) It is easy to verify that for $v \in K^n$ we have $T_{A^P}(v)P = T_A(vP)$. From this one deduces that if $\lambda \in K$ is such that $T_{A^P}(v) = \lambda v$ then $T_A(vP) = \lambda vP$; This shows that lspec$(A^P) \subseteq$ lspec(A). The reverse inclusion follows since $P \in GL_n(K)$. Similar computations lead to rspec$(A) =$ rspec(A^P)

(3), (4) and (5) are easy to prove and can be found in [L], Proposition 4.13. □

As in the case when K is a commutative field and $S = \text{Id}, D = 0$ we will now show that the eigenvalues are exactly the roots of some monic polynomials. In the classical case the last invariant factor is the minimal polynomial. This polynomial is unique. In our case the last invariant factor is only defined up to similarity. In Lemma 6.4 we will compare the roots of similar polynomials. First let us recall that $f, g \in R$ are said to be similar, denoted $f \sim g$, iff $R/Rf \cong R/Rg$ if and only if $R/fR \cong R/gR$. For a polynomial $f \in R = K[t; S, D]$, we continue to denote $V(f)$ the set of its right roots i.e. $V(f) = \{a \in K \mid f \in R(t-a)\}$. Similarly we will denote $V'(f)$ the set of left roots of f i.e. $V'(f) = \{a \in K \mid f \in (t-a)R\}$.

Let us recall that, for $q \in R = K[t; S, D]$ and $x \in K \setminus V(q)$, the map ϕ_q is defined by $\phi_q(x) = x^{q(x)}$.

Lemma 6.4. *Let f, g be similar elements of R and let gamma : $R/Rf \longrightarrow R/Rg$ be an isomorphism of left R-modules defined by $\gamma(1 + Rf) = q + Rg$. Then $V(f) = \phi_q(V(g))$.*

Proof. Since $\gamma(f+Rf) = 0+Rg$, there exists $q' \in R$ such that $fq = q'g$. If $x \in V(g) \cap V(q)$ then $Rg + Rq \subseteq R(t-x)$, this would imply that $(t-x) + Rg$ is not in the image of γ. So if $x \in V(g)$, we have $x \in V(fq) \setminus V(q)$ and the formula 2.1 implies that $\phi_q(x) \in V(f)$. We thus conclude that $\phi_q(V(g)) \subseteq V(f)$. Similarly if $\gamma^{-1}(1 + Rg) = p + Rf$, we must have $\phi_p(V(f)) \subseteq V(g)$. We also have $qp \in 1 + Rf$ and this implies that ϕ_{qp} is the identity on $V(f)$. It is also easy to check that $\phi_{qp} = \phi_q \circ \phi_p$ (Cf. [LL$_5$]). Thus we get:

$$V(f) = \phi_{qp}(V(f)) = \phi_q(\phi_p(V(f))) \subseteq \phi_q(V(g)) \subset V(f)\,.$$

This yields the result. □

Corollary 6.5. *If $f, g \in R = K[t; S, D]$ are similar, then there exist $p, q \in R$ such that $V(g) \cap V(q) = V(f) \cap V(p) = \emptyset$, $V(f) = \{\alpha^{q(\alpha)} \mid \alpha \in V(g)\}$ and $V(g) = \{\beta^{p(\beta)} \mid \beta \in V(f)\}$.*

Of course, there exist similar statements for the left roots using the left analogue of the map ϕ.

We can now give the analogue of the classical fact that roots of the minimal polynomial are exactly the eigenvalues of the matrix.

Proposition 6.6. *Let $A \in M_n(K)$ and $\{e_1, \ldots, e_r\}$ be a matrix and a complete set of invariant factors for A. Denote by $\Delta(e_r)$ the set $\{f \in R \,|\, f \sim e_r\}$, then the following are equivalent:*

i) $\beta \in \mathrm{rspec}(A)$.
ii) *There exists $\gamma \in K \setminus \{0\}$ such that $\beta^\gamma \in V(e_r)$.*
iii) *There exists a polynomial $e'_r \in \Delta(e_r)$ such that $\beta \in V(e'_r)$.*

Similar statements hold for elements of $\mathrm{lspec}(A)$ *and $V'(e_r)$.*

Proof. $(i) \Rightarrow (ii)$ Assume $u \in {}^nK \setminus \{0\}$ is such that $L_A(u) = u\beta$. This also means that while considering ${}^nK$ as a right R-module, $u \cdot (t - \beta) = 0$. According to the decomposition obtained in Lemma 6.1(4), we write $u = (u_1 + e_1R, \ldots, u_r + e_rR)$. Since $u \neq 0$, we get that there exists $i \in \{1, \ldots, r\}$ such that $u_i \notin e_iR \neq 0$ but $u_i(t - \beta) \in e_iR$. We may assume that $\deg(u_i) < \deg(e_i)$ and, comparing degrees, we conclude that there exists an element $\gamma \in K \setminus \{0\}$ such that $u_i(t - \beta) = e_i\gamma$. This leads to $u_iS(\gamma^{-1})(t - \beta^\gamma) = e_i$. Since e_i divides e_r on the right, we do get that $\beta^\gamma \in V(e_r)$.

$(ii) \Rightarrow (iii)$ By the hypothesis there exists $\gamma \in K \setminus \{0\}$ and $g \in R$ such that $g(t - \beta^\gamma) = e_r$. Multiplying by γ on the right, we get $g(t - \beta^\gamma)\gamma = e_r\gamma$ i.e. $gS(\gamma)(t - \beta) = e_r\gamma$. This yields the result since $e'_r := e_r\gamma$ is obviously similar to e_r.

$(iii) \Rightarrow (ii)$ This is clear from Corollary 6.5.

$(ii) \Rightarrow (i)$ Since $\beta^\gamma \in V(e_r)$, we easily get that $\beta^\gamma \in \mathrm{rspec}(A)$ and the fact that $\mathrm{rspec}(A)$ is closed by (S, D) conjugation implies that $\beta \in \mathrm{rspec}(A)$. □

We can now conclude:

Corollary 6.7. *Let A be a matrix in $M_n(K)$ and $\{e_1, \ldots, e_r\}$ be a complete set of invariant factors for A such that $e_1 || e_2 \ldots || e_r$. Then*

(1) $\mathrm{lspec}(A) = \bigcup_{f \in \Delta(e_r)} V'(f)$.
(2) $\mathrm{rspec}(A) = \bigcup_{f \in \Delta(e_r)} V(f)$.

In particular, if $\Gamma_r := \{q \in R \,|\, Rq + Re_r = R \text{ and } \deg q < \deg e_r\}$ then $\mathrm{rspec}(A) = \bigcup_{q \in \Gamma_r} \phi_q(V(e_r))$.

Corollary 6.8. *Let A be a matrix in $M_n(K)$. The number of non (S, D)-conjugate elements in* $\mathrm{Spec}(A)$ *is bounded by* $\deg(e_r)$.

Proof. Notice that if $f \in \Delta(e_r)$, Corollary 6.5 shows that the conjugacy classes intersecting $V(f)$ also intersect $V(e_r)$. Hence the (S, D) conjugacy classes intersecting $\mathrm{rspec}(A)$ also intersect $V(e_r)$. Similarly the (S, D) conjugacy classes intersecting $\mathrm{lspec}(A)$ also intersect $V'(e_r)$. Now, Corollary 3.2 shows that the number of (S, D)-conjugacy classes intersecting $\mathrm{Spec}(A)$ is bounded by $\deg(e_r)$. □

7. G-algebraic sets and G-polynomials

In this section we will restrict our attention to the case when $S = \mathrm{Id}$ and $D = 0$. K will stand for a division ring, G will denote a group of automorphisms of K and $K^G := \{x \in K | \sigma(x) = x \ \forall \sigma \in G\}$.

Definition 7.1. A subset $\Delta \subseteq K$ is G-algebraic if there exists a monic polynomial $f \in K^G[t]$ such that $f(x) = 0$ for all $x \in \Delta$. The monic polynomial in $K^G[t]$ of minimal degree annihilating Δ is denoted $f_{\Delta,G}$. Polynomials of the form $f_{\Delta,G}$ will be called G-polynomials. In particular, if $G = \{\mathrm{Id}\}$ we find back the notion of an algebraic set in the sense defined in Wed1 ([LL_5]).

It will sometimes be useful to denote the unique monic least left common multiple of a set Γ of (monic) polynomials by Γ_ℓ. Of course, every G-algebraic set is algebraic; the next proposition gives characterizations of G-algebraic sets. Let us first recall that a P-basis for an algebraic set $\Delta \subseteq K$ is a minimal subset $\Gamma \subseteq \Delta$ such that $f_\Gamma(\Delta) = 0$.

Proposition 7.2. *With the above notations, the following are equivalent:*

i) Δ *is G-algebraic.*
ii) $\bigcup_{\sigma \in G} \sigma(\Delta)$ *is algebraic.*
iii) Δ *is algebraic and for all $a \in \Delta$, $\{\sigma(a) | \sigma \in G\}$ is algebraic.*
iv) Δ *is algebraic and if $\{a_1, a_2, \ldots, a_n\}$ is a P-basis for Δ then $\{a_i\}$ is G-algebraic for $1 \leq i \leq n$.*
v) *There exists a left common multiple of the set $\{t - \sigma(a) \,|\, \sigma \in G,\ a \in \Delta\}$*

Proof. (i) $\Longrightarrow$ (ii) If $f \in K^G[t]$ is such that $f(\Delta) = 0$ then $f(\Delta^\sigma) = 0$ for all $\sigma \in G$. Hence $f(\bigcup_{\sigma \in G} \sigma(\Delta)) = 0$.
(ii) $\Longrightarrow$ (iii) Since $\Delta \subseteq \bigcup_{\sigma \in G} \sigma(\Delta)$, we have that Δ is algebraic. Similarly for all $a \in \Delta$, $G.a := \{\sigma(a) | \sigma \in G\} \subseteq \bigcup_{\sigma \in G} \sigma(\Delta)$, hence $G.a$ is algebraic and its minimal polynomial is precisely the monic generator of the left ideal $\bigcap_{\sigma \in G} R(t - \sigma(a)) \neq 0$. In other words, $f_{G.a} = \{t - \sigma(a) | \sigma \in G\}_\ell \in K^G[t]$.
(iii) $\Longrightarrow$ (iv) This is obvious.

(iv) $\Longrightarrow$ (v) Let $\{a_1, a_2, \cdots, a_n\}$ be a P-basis for for Δ and define f_i to be the left common multiple of the set $\{t - \sigma(a_i) \mid \sigma \in G\}$. Then $f_i^\sigma = f_i \in K^G[t]$ for all $i \in \{1, 2, \cdots, n\}$. Hence we have $f := \{f_i \mid i = 1, 2, \cdots, n\}_\ell = \{t - \sigma(a) \mid \sigma \in G\ ,\ a \in \{a_1, a_2, \cdots, a_n\}\}_\ell \in K^G[t]$. However $a \in \Delta$ implies that $t - a$ divides on the right $\{t - a_i \mid i \in \{1, 2, \cdots, n\}\}_\ell$ which itself divides f on the right. Since $f \in K^G[t]$ we thus get that f is a left common multiple of the set $\{t - \sigma(a) \mid \sigma \in G\ ,\ a \in \Delta\}$.
(iv) $\Longrightarrow$ (i) This is left to the reader. □

Remarks 7.3. (a) *Of course, if G is a finite group then every algebraic set is G-algebraic.*
(b) *Notice that in the case when K is commutative, a G-algebraic set must be finite.*
(c) *Part (iii) of the above proposition explains why we will be mainly concerned with G-algebraic sets of the form $\{\sigma(a) | \sigma \in G\}$ for some $a \in K$; this set will be denoted by $G.a$.*

Corollary 7.4. *Any G-polynomial $f = f_{\Delta,G}$ factorizes linearly: $f = (t - b_1) \cdots (t - b_n)$ in $K[t]$, where $b_1, \ldots, b_n$ are conjugated to elements in $\bigcup_{\sigma \in G} \sigma(\Delta)$. Moreover any root of f is conjugated to a certain b_i, $1 \leq i \leq n$.*

Proof. These are obvious consequences of the above proposition and of our earlier results in [LL_5]. □

Examples 7.5. (a) Let G be the set of all inner automorphisms of K i.e. $G = \{I_x | \, x \in K^*\}$. Then $K^G = Z(K)$ the center of K. An element is then G-algebraic if it is algebraic over the center $Z(K)$. In particular the above corollary gives back the Wedderburn classical theorem: If an element a of a division ring K is algebraic over the center $Z(K)$ then its minimal polynomial factorizes in $K[t]$ into linear factors of the form $t - b$ where $b \in K$ is conjugate to a.
(b) Let D be a division subring of K and put $L = C_K(D)$ the centralizer of D in K. Then $L = K^G$ for $G = \{I_x | x \in D^*\}$ hence an element $a \in K$ is algebraic over L if and only if it is G-algebraic. In this case, the above corollary shows that its minimal polynomial over L factorizes linearly in $K[t]$. In particular, this conclusion holds if K is a finite dimensional division ring over its center $Z(K)$. Any subdivision ring L such that $Z(K) \subseteq L \subseteq K$ of a finite dimensional division ring K since in this case $L = C_K(C_K(L))$.

Theorem 7.6. *Let G be a group of automorphisms of K, and suppose that $a \in K$ is algebraic over K^G. Define $G_a := \{\sigma \in G \,|\, \sigma(a) \in \Delta(a)\}$, where $\Delta(a) = \{a^x \,|\, x \in K \setminus \{0\}\}$. Then:*

(a) *G_a is a subgroup of G.*
(b) *For any $\sigma, \tau \in G$ we have $\sigma G_a = \tau G_a$ (resp. $G_a\sigma = G_a\tau$) if and only if $\Delta(\sigma(a)) = \Delta(\tau(a))$ (resp. $\Delta(\sigma^{-1}(a)) = \Delta(\tau^{-1}(a))$).*
(c) *G_a is of finite index in G.*
(d) *The decomposition of G into its right cosets modulo G_a corresponds to the decomposition of $G.a$ into conjugacy classes. More precisely if $G = \bigcup_{i=1}^{n} \sigma_i G_a$ is the decomposition of G into its right cosets modulo G_a, then $G.a = \bigcup_{i=1}^{n} \sigma_i(G_a.a)$ is the decomposition of $G.a$ into conjugacy classes.*
(e) *$\mathrm{rk}\,(G.a) = \deg f_{a,G} = (G : G_a)\mathrm{rk}\, G_a.a = (G : G_a)\deg f_{a,G_a} = (G : G_a)\dim_C YC$, where $Y \subseteq K \setminus \{0\}$ is such that $G_a.a = a^Y$ and $C = C^{S,D}(a)$ is the (S, D) centralizer of a. More precisely, if $\{y_1, y_2, \cdots, y_n\}$ is a maximal C-independent set in Y, then $\sigma(a^{y_j})$ is a P-basis for $G.a$.*
(f) *If $G_a = \{\mathrm{Id}\}$, then $G_{in.} := \{\sigma \in G \,|\, \sigma \text{ is inner}\} = \{\mathrm{Id}\}$. Moreover, if σ and τ are different elements in G, then $\sigma(a)$ and $\tau(a)$ belong to different conjugacy classes.*

Proof. (a) This is left to the reader.
(b) Suppose $\sigma G_a = \tau G_a$. We can write $\sigma = \tau g_1$ for some $g_1 \in G_a$. The definition of G_a shows that there exists $x_1 \in K$ such that $g_1(a) = a^{x_1}$. For $y \in K$ we then have $\sigma(a)^y = \tau(g_1(a))^y = \tau(a^{x_1})^y = (\tau(a)^{\tau(x_1)})^y = \tau(a)^{y\tau(x_1)}$. This shows that $\Delta(\sigma(a)) \subseteq \Delta(\tau(a))$. The reverse inclusion is proved similarly.
The proof of sufficiency of the condition, as well as the proof of the analogue left-right statements, are left to the reader.
(c) Since $G.a$ is algebraic, it can only intersects a finite number of conjugacy classes i.e. the number of conjugacy classes of the form $\Delta(\sigma(a))$ where $\sigma \in G$ is finite. Part b) above yields the thesis.
(d) This is easily deduced from b) above.
(e) This is a direct consequence of d) above using results from [LL$_2$].
(f) Theses are easy consequences of definitions. □

Let us remark that the subgroup G_a contains the subgroup G_{int} of all the inner automorphisms.

Example 7.7. The condition $(G : G_a) < \infty$ is not sufficient for a to be G-algebraic: for instance if $G = G_{int}$, then $K^G = Z(K)$, the center of K and $G = G_a$ for any $a \in K$ but of course a is not necessarily algebraic over $Z(K)$.

Before giving necessary and sufficient conditions for a to be G-algebraic let us recall that a subset of a conjugacy class $\Delta(a)$, say a^Y, is algebraic if and only if the right $C(a)$-vector space $YC(a)$ generated

by Y over the centralizer of a is finite dimensional. (Cf. Proposition 4.2 in [LL$_2$])

Proposition 7.8. *Let a be an element of K and Y a subset of $K \setminus \{0\}$ such that $G_a.a = \{a^y \mid y \in Y\}$. Then a is G-algebraic if and only if the right $C(a)$-vector space generated by Y is finite dimensionnal and $(G : G_a) < \infty$.*

Proof. If $G.a$ is algebraic, we have seen in Theorem 7.6 that $(G : G_a) < \infty$. On the other hand, since $G_a.a \subseteq G.a$, it is clear that $G_a.a$ is an algebraic subset contained in $\Delta(a)$. This implies that the $C(a)$-right vector space generated by Y is finite dimensional.
Conversely, suppose that $(G : G_a) < \infty$ and let $\sigma_1, \ldots, \sigma_l$ be such that $G = \bigcup_{i=1}^{l} \sigma_i G_a$. Then $G.a = \bigcup_{i=1}^{l} \sigma_i G_a.a = \bigcup_{i=1}^{l} \sigma_i(a)^{\sigma_i(Y)}$ is the decomposition of $G.a$ into conjugacy classes. It is easy to check that, for any $i = 1, \ldots, l$, $\dim_{C(a)} YC(a) = \dim_{C(\sigma_i(a))}(\sigma_i(Y)C(\sigma_i(a))$. Since $\dim_{C(a)} YC(a) < \infty$, we conclude that the subsets $\sigma_i G_a.a$ are algebraic for $i = 1, \ldots, l$. From this and the decomposition of $G.a$ given above we get the result. □

We will end this section with some results about the irreducibility of a G-polynomial. First let us notice that a G-polynomial is not always irreducible:

Example 7.9. Let $K = \mathbb{H}$, denote the real quaternions and $G = \{\mathrm{Id}, \mathrm{In(i)}\}$, where In(i) stands for the inner automorphism induced by i. Clearly, $K^G = \mathbb{C}$. Consider $a = j$, $G.a = \{j, j^i\}$ is algebraic with minimal polynomial $t^2 + 1 \in \mathbb{C}[t]$. Since $t^2 + 1 = (t + i)(t - i)$ we conclude that the G-polynomial $t^2 + 1$ is reducible in $K^G[t]$.

Let us recall, from our earlier work, the following definition:

Definition 7.10. An algebraic set $\Delta \subseteq K$ is said to be full if $V(f_\Delta) = \Delta$.

Proposition 7.11. *Let $a \in K$ be a G-algebraic element such that $\Delta := G.a$ is full then f_Δ is irreducible in $K^G[t]$.*

Proof. Assume $f_\Delta = gh$ in $K^G[t]$. If $\deg h > 0$ then, since f_Δ is a W-polynomial, we get that $V(h) \neq \emptyset$. Now if $x \in V(h)$, then $x \in V(f_\Delta) = \Delta$, where the last equality comes from the hypothesis that $G.a$ is full. Since $h \in K^G[t]$ we have, for any $\sigma \in G$, $0 = \sigma(h(x)) = h(\sigma(x))$. We thus get that $h(G.x) = 0$. Now writing $x = \tau(a)$ for some τ in G, we easily get that $G.x = G.a = \Delta$ and hence, $h(\Delta) = 0$. This shows that $h = f_\Delta$. □

Remark 7.12. The above sufficient condition for irreducibility in $K^G[t]$ of a minimal polynomial of a G-algebraic set is not necessary, i.e. a G-algebraic set Δ such that f_Δ is irreducible in $K^G[t]$ is not necessarily full. Indeed, consider $K = \mathbb{H}_\mathbb{Q}$ the quaternions over the rational numbers, $G = \{\mathrm{Id}, Int(i)\}$, $K^G = \mathbb{Q}(i)$ and $a = i + j$. Then $G.a = \{i + j, i - j\}$ is algebraic. $f_{G.a} \in \mathbb{Q}(i)[t]$ has degree 2 and $V(f_{G.a}) = \{(i + j)^{\lambda+i\mu} \mid \lambda, \mu \in C_\mathbb{H}(i + j)\}$. This shows that $G.a$ is not full. Now, if $f_{G.a}$ has a root in $\mathbb{Q}(i)$ then there exists $x \in \mathbb{H}_\mathbb{Q}$ such that $(i + j)^x \in \mathbb{Q}(i)$. Let us write $(i + j)^x = \alpha + i\beta$ with $\alpha, \beta \in \mathbb{Q}$. Taking traces on both sides of this equation, we get $\alpha = 0$ and looking at norms we then conclude that $\beta^2 = 2$. Since this last relation is impossible we can conclude that $f_{G.a}$ is irreducible in $\mathbb{Q}(i)$.

The above proposition and Theorem 7.6 immediately leads to the following:

Corollary 7.13. *Assume the group G_a is trivial: $G_a = \{1\}$ then $\Delta = G.a$ is full and f_Δ is irreducible in $K^G[t]$.*

In the same spirit, let us mention the following necessary and sufficient condition for irreducibility of the minimal G-polynomial associated to a G-algebraic set:

Proposition 7.14. *Let $a \in K$ and $\Delta = G.a$ be algebraic. Then f_Δ is irreducible in $K^G[t]$ if and only if for any $b \in K$ such that $f_\Delta(b) = 0$ we have $f_\Delta = f_{G.b}$.*

Proof. Assume $f_\Delta(b) = 0$ then $f_\Delta(G.b) = 0$ and hence $f_{G.b}$ divides on the right f_Δ in $K^G[t]$. Moreover, since f_Δ is irreducible, we get that $f_{G.b} = f_\Delta$.
Conversely, assume $f_\Delta = gh$ in $K^G[t]$ with h monic and $\deg h \geq 1$. Then there exists $x \in \Delta = G.a$ such that $h(x) = 0$ and so $h(\Delta) = 0$ which shows that $h = f_\Delta$. □

Acknoweldgement

We would like to thank the referee for a very careful reading leading to substantial improvements of the presentation of the paper.

References

[A1] A. A. Albert: *A determination of all normal algebras in 16 units*, Trans. Amer Math. Soc. **32**(1929), 253-260.

[A2] A. A. Albert: *On ordered algebras*, Bull. A.M.S. **45**(1940), 521-522.

[Am] S. A. Amitsur: *A generalization of a theorem on differential equations*, Bull. A.M.S. **54**(1948), 937-941.

[Co_1] P. M. Cohn: *The range of derivations on a skew field and the equation* $ax - xb = c$, J. Indian Math. Soc. **37**(1973), 1-9.

[Co_2] P. M. Cohn: *Free Rings and Their Relations*, 2nd Edition, London Math. Soc. Monograph No. 19, Academic Press, London/New York, 1985.

[Co_3] 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*, to appear in J. Algebra and its Applications.

[GGRW] I. Gelfand, S. Gelfand, V. Retakh and R.L. Wilson: *Quasideterminants*, Advances in Math. **193** (2005), 56-141.

[GR] I. Gelfand and V. Retakh: *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**, (2001), 493-523.

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

[Ja_1] N. Jacobson: *The Theory of Rings*, Math. Surveys, No. 2, Amer. Math. Soc., Providence, R.I., 1943.

[Ja_2] N. Jacobson: *The equation* $x' \equiv xd - dx = b$, Bull. A.M.S. **50**(1944), 902-905.

[Ja_3] N. Jacobson: *Finite-Dimensional Division Algebras over Fields,* Springer-Verlag, Berlin-Heidelberg-New York, 1996.

[Jo] R. E. Johnson: *On the equation* $\chi\alpha = \gamma\chi + \beta$ *over an algebraic division ring*, Bull. A.M.S. **50**(1944), 202-207.

[Ko] E. R. Kolchin: *Galois theory of differential fields*, Amer. J. Math. **75** (1953), 753-824.

[La_1] T. Y. Lam: *A general theory of Vandermonde matrices*, Expositiones Mathematicae **4**(1986), 193-215.

[La_2] T. Y. Lam: *A First Course in Noncommutative Rings*, Graduate Texts in Math., Vol. **131**, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

[La_3] T. Y. Lam: *Exercises in Classical Ring Theory*, Problem Books in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1995.

[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_4] T. Y. Lam and A. Leroy: *Principal one-sided ideals in Ore polynomial rings,* in *Algebra and Its Applications* (D.V. Huynh, S.K. Jain and S.R. López-Permouth, eds.), Contemp. Math. **259**, pp. 333-352, Amer. Math. Soc., Providence, R.I., 2000.

[LL_5] T. Y. Lam and A. Leroy: *Wedderburn polynomials over division rings,* I, Journal of Pure and Applied Algebra, **186** (2004), 43-76.

[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.

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

[Ro_1] L. H. Rowen: *Wedderburn's method and algebraic elements in simple artinian rings*, Contemp. Math. **124**(1991), 179-202.

[Ro_2] L. H. Rowen: *Polynomials over division rings and their applications*, in "Ring Theory, Granville, Ohio, 1992" (S. K. Jain and S. T. Rizvi, eds.), pp. 287-301, World Scientific Publ. Co., Singapore-Hong Kong, 1993.

[RS_1] L. H. Rowen and Y. Segev: *The finite quotients of the multiplicative group of a division algebra of degree* 3 *are solvable*, Israel J. Math. **111**(1999), 373-380.

[RS_2] L. H. Rowen and Y. Segev: *The multiplicative group of a division algebra of degree* 5 *and Wedderburn's factorization theorem*, in *Algebra and Its Applications* (D.V. Huynh, S.K. Jain and S.R. López-Permouth, eds.), Contemp. Math. **259**, pp. 475-486. Amer. Math. Soc., Providence, R.I., 2000.

[Se] Y. Segev: *Some applications of Wedderburn's factorization theorem*, Bull. Austral. Math. Soc. **59**(1999), 105-110.

[Tr] J. Treur: *Separate zeros and Galois extensions of skew fields*, J. Algebra **120**(1989), 392-405.

[We] J. H. M. Wedderburn: *On division algebras*, Trans. A.M.S. **22**(1921), 129-135.

Department of Mathematics, University of California, Berkeley, CA 94720

E-mail address: lam@math.berkeley.edu

Department of Mathematics, Université d'Artois, 62307 Lens = Cedex, France

E-mail address: leroy@euler.univ-artois.fr

Institut de Mathématique, Université de Mons-Hainaut, B-7000 Mons, Belgique.

E-mail address: ozturk@umh.ac.be