De l'irréductibilité des polynômes de différentielles à une variable et à coefficients sur un corps différentiel

Alain **W**azner

Introduction.

Un des intérêts des connexions est qu'elles permettent par le lemme du vecteur cyclique de ramener l'étude d'un polynôme d'une algèbre non commutative à celle d'un opérateur particulier d'ordre 1 : une connexion différentielle. Par analogie avec les algèbres commutatives de matrices, l'étude des applications linéaires et de la réduction d'endomorphismes est connectée à celle des polynômes les caractérisant. Pour des applications linéaires sur un corps la théorie des diviseurs élémentaires permet, grâce aux notions d'espaces cycliques ou stables, la factorisation de polynômes en polynômes irréductibles. Le but est, dans cet article, pour les connexions sur des corps différentiels de traduire certaines notions propres aux polynômes d'endomorphismes linéaires sur des corps.

Généralités sur les anneaux non commutatifs unitaires.

Dans cette section A sera un anneau unitaire, non nécessairement commutatif, $\mathcal{U}_A$ sera son groupe des inversibles et dans tout l'article on obtiendra les mêmes énoncés en remplaçant *gauche* ou son abréviation par *droite* ou son abréviation et en renversant les produits.

Diviseurs, p.g.c.d., p.p.c.m., éléments irréductibles.

Définition : soit $a \in A$, on dit que $b \in A$ est un diviseur de A *à gauche* si $a \in (b)_g$, où $(b)_g$ est l'idéal *à gauche* engendré par b. Autrement dit, si $\exists c \in A$ tel que $a = cb$ ce qu'on écrira $b_{|g}a$.

Définitions :

- si $E \subset A$ alors un p.g.c.d. *à gauche* des éléments de E, s'il en existe, est un élément $d \in A$ tel que $\forall e \in E,\ d_{|g}e$ et $\big(\forall e \in E,\ c_{|g}e\big) \Rightarrow c_{|g}d$.
- Si E est une partie **finie** de A alors un p.p.c.m. *à gauche* des éléments de E, s'il en existe, est un élément $p \in A$ tel que $\forall e \in E,\ e_{|g}p$ et $\big(\forall e \in E,\ e_{|g}q\big) \Rightarrow p_{|g}q$.
- Un idéal *à gauche* est un sous-groupe additif de A stable pour la multiplication *à gauche* par tout élément de A.
- Un idéal *à gauche* $I \subset A$ est de type fini *à gauche* s'il est engendré par un nombre fini d'éléments de A.
- Un anneau A est nœthérien *à gauche* si tout idéal *à gauche* I de A est de type fini.
- Un idéal *à gauche* I de A est dit monogène si et seulement $(\exists i \in A)\ I = \{ai / a \in A\}$.

- Un anneau A est principal *à gauche* si tout idéal *à gauche* I de A est monogène.
- Un anneau A est gradué euclidien *à gauche* si
  - il est intègre.
  - Il existe un stathme euclidien : une application $\nu : A\backslash\{0\} \to \mathbb{N}$ telle que $(\forall a, b \in A\backslash\{0\}), (\exists! q, r \in A)$ *avec* $a = qb + r$ *et* $(r = 0$ *ou* $\nu(r) < \nu(b))$. r, q sont appelés le *reste* et le *quotient* de la *division euclidienne à gauche* de a par b.
  - $(\forall p, q \in A)\ \nu(pq) = \nu(qp) = \nu(p) + \nu(q)$
- Tout anneau gradué euclidien *à gauche* est principal *à gauche*.
- Dans un anneau A gradué euclidien *à gauche* un élément a sera dit irréductible *à gauche* si et seulement si l'idéal $(a)_g$ est propre et maximal pour l'ordre de l'inclusion.

Propriété :

- soit A un anneau nœthérien *à gauche* alors

  (1) Tout idéal de A *à gauche* est de type fini.

  (2) Toute suite croissante d'idéaux de A *à gauche* est stationnaire.

  (3) Tout ensemble d'idéaux de A *à gauche* a un élément maximal pour l'inclusion.

- Tout anneau principal *à gauche* est nœthérien *à gauche*.
- Tout anneau A euclidien *à gauche*. est principal *à gauche*.
- Tout élément irréductible d'un anneau unitaire gradué euclidien *à gauche* n'est pas le produit de deux éléments de $A\backslash\mathcal{U}_A$ où $\mathcal{U}_A$ est le groupe multiplicatif des inversibles de A.
- Dans un anneau unitaire gradué euclidien *à gauche* qui n'est pas un corps il existe des éléments irréductibles et tout élément qui n'est pas inversible est divisible *à gauche* par un élément irréductible *à gauche*.

Preuves :

- soit A un anneau nœthérien *à gauche*.

(1)⇒ (2) : soit $I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$ une suite croissante d'idéaux de A *à gauche* alors la réunion $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A *à gauche* engendré par k éléments $a_1, \ldots, a_k \in I$ qui sont tous dans I_N pour un $N \in \mathbb{N}$. On a alors : $I = I_N$ et la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire à partir du rang N.

(2)⇒ (3) : soit E un ensemble d'idéaux de A *à gauche*. Si E n'a pas délément maximal alors on construit une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux de

A *à gauche* en choisissant I_0 dans E et, I_n étant choisi, $I_{n+1} \in E$ tel que $I_n \subsetneq I_{n+1}$. La suite $(I_n)_{n\in\mathbb{N}}$ n'est pas stationnaire et contredit (2).

(3)$\Rightarrow$ (1) : soit I un idéal *à gauche* de A et E l'ensemble des idéaux contenus dans I et qui sont de type fini. E n'est pas vide puisqu'il contient $\{0\}$, il a donc un élément maximal J dont nous prouvons que c'est I. Soit $a \in I$ si $a \notin J$ alors $J + (a)_g$ est contenu dans I et J n'est pas maximal puisque $J \subsetneq J + (a)_g$: ce qui est contradictoire.

- Tout idéal d'un anneau A principal *à gauche* est monogène donc de type fini.

- Si I est un idéal de A et $i \in I$ tel que $\nu(i)$ soit minimal. Soit $a \in I$ on effectue la division euclidienne *à gauche* de a par i : $a = qi + r$ avec $r = 0$ ou $\nu(r) < \nu(i)$. $r = 0$ puisque $\nu(i)$ est minimal. Il suit que $I = (i)_g$.

- Soit A un anneau unitaire gradué euclidien *à gauche*. De $1 \times 1 = 1$ nous déduisons que $\nu(1)+\nu(1) = \nu(1)$ soit $\nu(1) = 0$. Si $u \in \mathcal{U}_A$ de $u \times u^{-1} = 1$ nous déduisons que $\nu(u) + \nu(u^{-1}) = 0$ soit $\nu(u) = \nu(u^{-1}) = 0$ puisque ν est à valeurs dans $\mathbb{N}$. Soit $a = b \times c$ avec $b, c \notin \mathcal{U}_A$ alors $(a)_g \subset (c)_g$ et

$\nu(a) = \nu(b) + \nu(c)$ et puisque $\nu(c) > 0$ et $\nu(b) > 0$ c'est que $\nu(a) < \nu(c)$; la division euclidienne *à gauche* de c par a s'écrit alors $c = 0 \times a + c$ et comme son reste c n'est pas 0 c'est que $c \notin (a)_g$: l'idéal $(a)_g$ n'est donc pas maximal et a n'est pas irréductible. Soit $a \in A\backslash\{0\}$ alors soit il est irréductible, auquel cas il est divisible par un irréductible car divisible par lui-même, soit $a = b_1 a_1$ avec $b_1, a_1 \notin \mathcal{U}_A$, soit a_1 est irréductible auquel cas a est divisible par un irréductible soit $a_1 = b_2 a_2$ (et donc $a = b_1 b_2 a_2$) avec $b_2, a_2 \notin \mathcal{U}_A \ldots$, on construit ainsi un ensemble E, indexé par $\mathbb{N}$, d'idéaux $(a_i)_g \subset (a)_g$. E a un élément maximal a_n qui divise a, a_n n'est pas produit de deux éléments $b_n, c_n \notin \mathcal{U}_A$ car on aurait alors $(b_n)_g \subset (a)_g$ et $(a_n)_g$ non maximal dans E, a_n est donc un diviseur irréductible de a.

Propriété : si A est un anneau gradué euclidien *à gauche* alors :

(i) si $E \subset A$, l'ensemble des p.g.c.d. *à gauche* de E est l'ensemble des $a \in A\backslash\{0\}$ tels que $\sum_{e\in E}(e)_g = (a)_g$.

(ii) L'ensemble des p.p.c.m. *à gauche* de $(a_1, \ldots, a_n)$ est l'ensemble des $a \in A\backslash\{0\}$ tels que $\cap_{i=1}^{n}(a_i)_g = (a)_g$.

Preuve :

(i) **tout générateur de $\sum_{e\in E}(e)_g$ est un p.g.c.d. de E:**
soit $E \subset A$ alors $\sum_{e\in E}(e)_g$ est l'ensemble des sommes $\sum_{i=1}^{n} a_i e_i$ où $a_i \in A$ et $e_i \in E$; Cet ensemble est un idéal *à gauche* : $(\exists a \in A) \sum_{e\in E}(e)_g = (a)_g$. On a donc

$$(\forall (a_1, \ldots, a_n) \in A^n, \forall (e_1, \ldots, e_n) \in E^n)$$

$$\exists c \in A,\ \sum_{i=1}^{n} a_i e_i = ca$$

En particulier pour $n = 1$ $a_1 = a = 1$ on a $(\forall e \in E), \exists c \in A,\ e = ca$ ce qui équivaut à $(\forall e \in E), a_{|g} e$.
De $\sum_{e\in E}(e)_g = (a)_g$, il suit que $a \in \sum_{e\in E}(e)_g$ et donc

$$\exists (\alpha_1, \ldots, \alpha_n) \in A^n, \exists (e_1^*, \ldots, e_n^*) \in E^n,$$

$$a = \sum_{i=1}^{n} \alpha_i e_i^*$$

Soit d tel que $\forall e \in E,\ d_{|g} e$ alors

$$\forall e \in E, \exists \alpha(e) \in A\ e = \alpha(e) d$$

puis

$$\exists (\alpha(e_1^*), \ldots, \alpha(e_n^*)) \in E^n, \forall i \in \{1, \ldots, n\},$$

$$e_i^* = \alpha(e_i^*)d$$

On a alors

$$a = \sum_{i=1}^{n} \alpha_i e_i^* = \sum_{i=1}^{n} \alpha_i \alpha(e_i^*) d = \left(\sum_{i=1}^{n} \alpha_i \alpha(e_i^*) \right) d$$

donc $d_{|g} a$ et a est un p.g.c.d. de E.

Tout p.g.c.d. de E est un générateur de $\sum_{e \in E}(e)_g$:

nous distinguons deux cas :

- E est un ensemble fini $\{e_1, \ldots, e_n\}$. Soit d un diviseur commun de $e_1, \ldots, e_n$ alors $\forall i \in \{1, \ldots, n\}$, $(e_i)_g \subset (d)_g$. En particulier si m est un p.g.c.d. de E, $\forall i \in \{1, \ldots, n\}$, $(e_i)_g \subset (m)_g$ ce qui entraîne $\sum_{i=1}^{n}(e_i)_g \subset (m)_g$. Mais, d'après ce qui précède, $\sum_{i=1}^{n}(e_i)_g \subset (m')_g$ où m' est un p.g.c.d. de E, on a donc $(m')_g \subset (m)_g$. Ceci étant vrai pour tout m', m p.g.c.d. de E, on peut dans les propositions qui précèdent, échanger m et m' et donc $(m')_g \subset (m')_g$ soit

$$(m)_g = (m')_g = \sum_{i=1}^{n}(e_i)_g$$

- E est un ensemble infini alors l'ensemble des sommes finies d'idéaux *à gauche* à générateur dans E est un ensemble d'idéaux de A

à gauche, anneau nœthérien *à gauche*, il admet un élément maximal $\sum_{i=1}^{n}(e_i)_g$. Si m est un p.g.c.d. *à gauche* de E alors m divise *à gauche* chaque e_i et donc $\sum_{i=1}^{n}(e_i)_g \subset (m)_g$, mais comme $\sum_{i=1}^{n}(e_i)_g$ est maximal $\sum_{i=1}^{n}(e_i)_g = (m)_g$. Si $(f_1, \ldots, f_p)$ est un p-uplet quelquonque d'éléments de E alors m, qui est un p.g.c.d. de E, divise *à gauche* chaque f_j et donc $\sum_{i=1}^{p}(f_j)_g \subset (m)_g$: ceci prouve que pour tout m p.g.c.d. de E *à gauche* l'ensemble des sommes finies d'idéaux générés par un élément de E a pour élément maximum $(m)_g = \sum_{i=1}^{n}(e_i)_g$. Tout générateur de cet élément maximum, donc tout p.g.c.d. *à gauche* de E est un générateur de $\sum_{e\in E}(e)_g$ qui est l'idéal des sommes finies d'idéaux *à gauche* à générateurs dans E.

(ii) Nous montrons d'abord que $\forall P, Q \in A\backslash\{0\}$ $(P)_g \cap (Q)_g \neq (0)_g$ en montrant le
lemme : $\forall P, Q, R \in A\backslash\{0\}$,

- Si $(P)_g \cap (Q)_g = (0)_g$ alors $(PR)_g \cap (QR)_g = (0)_g$
- Si $(P)_g \cap (Q)_g \neq (0)_g$ alors il existe au moins un p.p.c.m. de $\{P, Q\}$, notons le $P \wedge_g Q$ et il existe au moins un p.p.c.m. de $\{PR, QR\}$, notons le $PR \wedge_g QR$, on a de plus :

$$(\exists u \in \mathcal{U}_A), (P \wedge_g Q)R = v(PR \wedge_g QR).$$

Preuve : si $(P)_g \cap (Q)_g = (0)_g$ alors :
$HP = KQ = 0 \Rightarrow HP = KQ = 0$ et comme $P, Q \in A\backslash\{0\}$ ceci équivaut à :

$$HP = KQ = 0 \Rightarrow H = K = 0$$

Soient à présent $H, K \in A$ tels que $HPR = KQR$ alors $(HP - KQ)R = 0$. Mais $R \neq 0$ et A intègre entraînent alors $HP = KQ$ qui entraîne $H = K = 0$.
Si $(P)_g \cap (Q)_g \neq (0)_g$ alors :
soit $P \wedge_g Q$ un p.p.c.m. de $\{P, Q\}$, $\exists H, K \in A\backslash\{0\}$ tel que $P \wedge_g Q = HP = KQ$. On en déduit :

$$(\forall R \in A\backslash\{0\}),\ (P \wedge_g Q)R = HPR = KQR.$$

Il suit $(P \wedge Q)_g R \in (PR)_g \cap (QR)_g$: il existe donc un p.p.c.m. de $\{PR, QR\}$, notons le $PR \wedge_g QR$.

$$(\exists v \in A\backslash\{0\}),\ (P \wedge_g Q)R = v(PR \wedge_g QR)$$

Mais $PR \wedge_g QR \in (PR)_g \cap (QR)_g$, donc

$$(\exists H', K' \in A\backslash\{0\}),\ PR \wedge_g QR = H'PR = K'QR$$

puis $H'P = K'Q \in (P)_g \cap (Q)_g$. On a alors

$$(\exists u \in A\backslash\{0\}),\ H'P = K'Q = u(P \wedge_g Q)$$

puis

$$(\exists u \in A\backslash\{0\}),\ PR \wedge_g QR = H'PR = K'QR = u(P \wedge_g Q)R$$

$\exists v, u \in A\backslash\{0\}$ avec $\left\{ \begin{array}{ll} (P \wedge_g Q)R & = v(PR \wedge_g QR) \\ PR \wedge_g QR & = u(P \wedge_g Q)R \end{array} \right.$

donc $\left\{ \begin{array}{ll} (P \wedge_g Q)R & = vu(P \wedge_g Q)R \\ PR \wedge_g QR & = uv(PR \wedge_g QR) \end{array} \right.$ soit

$$\left\{ \begin{array}{ll} (1 - vu)(P \wedge_g Q)R & = 0 \\ (1 - uv)(PR \wedge_g QR) & = 0 \end{array} \right.$$

Mais A est intègre donc $\left\{ \begin{array}{ll} (1 - vu) & = 0 \\ (1 - uv) & = 0 \end{array} \right.$ soit $v, u \in \mathcal{U}_A$ CQFD!

Nous pouvons à présent montrer par récurrence que

$$(a_1, \ldots, a_n) \in (A\{0\})^n \Rightarrow \cap_{i=0}^{n} (a_i)_g \neq (0)_g$$

il suffit, pour cela, de montrer que :

$$(a, b) \in (A\{0\})^2 \Rightarrow (a)_g \cap (b)_g \neq (0)_g$$

Si a ou b sont des unités alors $(a)_g \cap (b)_g$ est $(b)_g \neq (0)_g$ ou $(a)_g \neq (0)_g$ suivant que a ou b est une unité. Si ni a ni b ne sont des unités alors nous supposons que $(a)_g \cap (b)_g = (0)_g$. Posons $\left\{ \begin{array}{ll} a & = a'(a \vee_g b) \\ b & = b'(a \vee_g b) \end{array} \right.$, où $a \vee_g b$ est un p.g.c.d. de a et b, alors

$$(0)_g = (a)_g \cap (b)_g = \left(a'(a \vee_g b)\right)_g \cap \left(b'(a \vee_g b)\right)_g$$

– **Supposons** $(a')_g \cap (b')_g \neq (0)_g$ **:** alors il existe un p.p.c.m. de $\{a', b'\}$ et, par le

lemme qui précède, un p.p.c.m. de $\{a'(a \vee_g b), b'(a \vee_g b)\}$ que nous notons $a' \wedge_g b'$ et $a \wedge_g b$ et

$$\exists u \in \mathcal{U}_A,\ (a' \wedge_g b')(a \vee_g b) = u(a \wedge_g b)$$

on en déduit que

$$((a' \wedge_g b')(a \vee_g b))_g = ((a \wedge_g b))_g = (a)_g \cap (b)_g = (0)_g$$

ceci entraîne que $(a' \wedge_g b')(a \vee_g b) = 0$ et donc, puisque $a' \wedge_g b' \neq 0$, $a \vee_g b = 0$ qui entraîne $a = b = 0$: ce qui est contradictoire.

– **Supposons** $(a')_g \cap (b')_g = (0)_g$ **:**

$$(0)_g = (a'(a \vee_g b))_g \cap (b'(a \vee_g b))_g = (a)_g \cap (b)_g$$

de sorte que

$$(a \vee_g b)_g = (a)_g + (b)_g = (a)_g \oplus (b)_g$$

Soient $f, g \in A$ tels que $a \vee_g b = fa + gb$ alors $(a \vee_g b)_g = (fa)_g + (gb)_g = (a)_g \oplus (b)_g$ entraîne que $f, g \in \mathcal{U}_A$.
De $(a)_g \oplus (b)_g = (fa + gb)_g = (fa)_g + (gb)_g$ il suit que $f, g \in \mathcal{U}_A$.
De

$$\begin{aligned}
(a \vee_g b)_g &= (a)_g \oplus (b)_g \\
(a \vee_g b)_g &= (a'(fa + gb))_g + (b'(fa + gb))_g \\
(a \vee_g b)_g &= ((a' + b')fa)_g + ((a' + b')gb)_g
\end{aligned}$$

il suit que $(a'+b')f \in \mathcal{U}_A$ ce qui entraîne que $a'+b' \in \mathcal{U}_A$ puis $(a')_g + (b')_g = A$ soit $(\forall x \in A)\exists H, K \in A,\ x = Ha' + Kb'$.
Nous prouvons à présent l'assertion

$$(\exists x \notin (a)_g) \wedge (Fx = Ga') \Rightarrow F = G = 0$$

Soient $H, K \in A$ tels que $x = Ha' + Kb'$ alors $Fx = Ga'$ entraîne que $(G - FH)a' = FKb'$ et comme $(a')_g \cap (b')_g = (0)_g$ $FK = G - FH = 0$, A est intègre : $(F = 0) \vee (K = 0)$. Si $K = 0$ alors $x \in (a')_g$. *Si nous choisissons* $x \notin (a')_g$ *alors* $K \neq 0$, donc $F = 0$ et puisque $Ga' = Fx$ et $a' \neq 0$ il suit $G = F = 0$.
Nous concluons : l'assertion

$$(\exists x \notin (a)_g) \wedge (Fx = Ga') \Rightarrow F = G = 0$$

équivaut à l'assertion

$$(\forall x \notin (a')_g)(a')_g \cap (x)_g = (0)_g$$

$1 \notin (a')_g$ (sinon $a \in \mathcal{U}_A$) donc $(0)_g = (a')_g \cap (1)_g = (a')_g$ ce qui contredit que $a' \neq 0$.

Modules *à gauche* et dérivations sur un anneau commutatif unitaire.

Modules *à gauche* et espaces vectoriels.

Soit $(A, +, \times)$ un anneau commutatif unitaire et un groupe commutatif noté, *au risque de la confusion sur le* $+$, $(M, +)$ on appelle opération externe de A sur M , *notée plus simplement* . , toute application $._A$ de $A \times M$ dans M et on dit que $(M, +, .)$ est un A-module *à gauche* si les propriétés qui suivent sont vérifiées :

- distributivité sur M

$$a.(x + y) = a.x + a.y, \ \forall a \in A \forall x, y \in M$$

- Distributivité sur A

$$(a + b).x = a.x + b.x, \ \forall a, b \in A \forall x \in M$$

- $(a \times b).x = a.(b.x), \ \forall a, b \in A, \forall x \in M$
- $1.x = x, \forall x \in M$

Si A est *un corps* alors on dit que $(M, +, .)$ est un A-espace vectoriel.

Exemples :

- les ensembles $\mathbb{Z}/n\mathbb{Z}$ sont des $\mathbb{Z}$-modules à gauche.

- L'ensemble des vecteurs du plan euclidien, des fonctions d'un domaine I dans $\mathbb{R}$ sont des $\mathbb{R}$-espaces vectoriels.

Dérivations sur un anneau commutatif unitaire.

Soit $(A, +, \times)$ un anneau commutatif unitaire et D un morphisme du groupe $(A, +)$, *qui n'est ni l'identité ni le morphisme nul* alors on dit que D est une dérivation s'il vérifie **l'identité de Leinitz**

$$\boxed{D(a \times b) = D(a) \times b + a \times D(b),\ \forall a, b \in A}$$

de laquelle se déduit **la formule de Leinitz**

$$\boxed{\forall n \in \mathbb{N}, \forall a, b \in A}$$

$$\boxed{D^n(a \times b) = \sum_{k=0}^{n} C_n^k D^{n-k}(a) \times D^k(b)}$$

Exemple :

si A est l'anneau des fonctions infiniment dérivables d'un domaine I dans $\mathbb{R}$ le morphisme qui à une fonction associe sa dérivée est une dérivation.

L'anneau des constantes A_D.

Si D est une dérivation sur un anneau de caractéristique c alors l'ensemble $\{x \in A | D(x) = 0\}$ est

un anneau de caractéristique c appelé anneau des constantes et noté A_D.

Exemple : si A est l'anneau des fonctions $\mathcal{C}^\infty$ d'un domaine I dans $\mathbb{R}$ et D la dérivation usuelle alors l'anneau des constantes est $\mathbb{R}$.

Preuve : A_D, noyau d'une application additive est un groupe abélien, c'est aussi le noyau d'un dem-groupe multiplicatif par l'identité de Leibnitz c'est un anneau de même caractéristique que A puisque $1_A \in A_D$ est l'unité de A_D.

L'exemple de l'anneau des polynômes différentiels $K[D]$.

Si K est un corps, $K[X]$ son anneau des polynômes, D est la dérivation des polynômes à coefficients sur K et D^i la composée i-ème de D avec elle-même alors on appelle anneau des polynômes différentiels, l'anneau noté $K[D]$ des morphismes $\sum_{i=0}^{n} a_i D^i$ avec $a_i \in K[X]$ et muni des opérations d'addition et de composition. Cet anneau est gradué euclidien si on choisit le stathme euclidien ν par $\nu\left(\sum_{i=0}^{n} a_i D^i\right) = n$ si $a_n \neq 0$ et $\nu(0) = 0$. Son corps des constantes est K. La structure d'anneau non commutatif gradué euclidien de $K[D]$ s'enrichit en celle d'algèbre, *doublement non -commutative*, par la donnée de la multiplication externe . définie par

$$. \ : \ \begin{cases} K[X] \times K[X][D] & \to & K[X][D] \\ (a, P) & \mapsto & aD^0 \times P \end{cases}$$

On a les

Propriétés :

(i) la famille $(D^n)_{n\in\mathbb{N}}$ est une famille-base de l'espace vectoriel $(K[X][D], +, .)$.

(ii) L'anneau $(K[X][D], +, \times)$ est gradué euclidien *à gauche* et *à droite*.

(iii) $\mathcal{U}_{K[X][D]}$ est l'ensemble des opérateurs non nuls de degré (c'est ν) 0 de $K[X][D]$. Ce groupe est isomorphe à $K\backslash\{0\}$.

Nous laissons aux lecteurs le soin d'en faire la preuve qui est technique mais sans grande difficulté.
On a la

Propriété : si $a_n \neq 0$ alors les morphismes $\sum_{i=0}^{n} a_i D^i$ sont des applications K-linéaires de $K[X]$ dans $K[X]$ dont les noyaux sont des K-espaces vectoriels de dimension au plus n.

Preuve : par récurrence sur n.
Si $n = 0$ alors l'équation $L(s) = 0$ a pour solution $\{0\}$ espace vectoriel de dimension 0.
Si la propriété est vraie à l'ordre $n-1$ et si $L = \sum_{i=0}^{n} a_i D^i$ avec $a_n \neq 0$ alors soit *l'équation différentielle* $L(s) = 0$ n'a pas de solution sur $K[X]$, auquel cas l'espace vectoriel des solutions

est de dimension 0, soit elle a une solution non nulle $s_0 \in K[X]$, nous effectuons alors le *changement d'inconnue* $s = s_0 u$. Par la **formule de Leibnitz** on voit que $L(s_0 u) = H(u)$ où $H = \sum_{i=1}^{n} b_i D^i$ et $b_n = a_n$ de sorte que $H(u) = J(D(u))$ où $J = \sum_{0}^{n-1} b_{i+1} D^i$. L'équation $H(u) = 0$ est équivallente au système :

$$\begin{cases} J(v) &= 0 \\ D(u) &= v \end{cases}$$

Nous appliquons à J l'hypothèse de récurrence : le K-espace vectoriel V des solutions de $J(v) = 0$ est au plus de dimension $n-1$. Si E est le K-espace vectoriel $D^{-1}(V)$ et p la projection canonique $E \to E/Ker(D) = E/K$ alors il existe un isomorphisme

$$i \ : \ E/K \to D(E) = D(D^{-1}(V)) \subset V$$

tel que $i \circ p = D$.
E/K est isomorphe à $D(E)$ K-espace vectoriel de dimension finie au plus $n-1$ et comme K est espace vectoriel sur lui-même de dimension 1, E est un K-espace vectoriel de dimension au plus égale à n.
Le K-espace vectoriel des solutions de $H(u) = 0$ est de dimension au plus n et, comme toute solution de $L(s) = 0$ s'exprime par $s = s_0 u$, où $s_0 \neq 0$ et u est solution de $H(u) = 0$, le K-espace vecto-

riel des solutions de $L(s) = 0$ est de dimension au plus n.

Deux algorithmes de division euclidienne dans $K[X](D)$.

Pour un polynôme différentiel dans $K[X][D]$ le degré, soit le plus grand indice de ses coefficients non nuls, est un stathme euclidien dont nous nous servons pour construire des algorithmes de division euclidienne *à gauche et à droite*.
Pour la division euclidienne *à gauche* de $a = \sum_{i=0}^{deg(a)} a_i D^i$ par $b = \sum_{i=0}^{deg(b)} b_i D^i$ nous considérons les trois suites stationnaires $(r_n)_{n\in\mathbb{N}}$, $(q_n)_{n\in\mathbb{N}}$, $(\varepsilon_n)_{n\in\mathbb{N}}$ où $\begin{cases} \varepsilon_0 &= 0 \\ q_0 &= 0 \\ r_0 &= a \end{cases}$

$$\begin{cases} \varepsilon_n &= Max(0, deg(r_{n-1}) - deg(b)) \\ q_n &= q_{n-1} + \varepsilon_n \frac{r^*_{n-1}}{b_{deg(b)}} D^{\varepsilon_n} b \\ r_n &= r_{n-1} - q_n b \end{cases}$$

où r^*_{n-1} est le coefficient dominant de r_n.
Pour la division euclidienne *à droite* de $a = \sum_{i=0}^{deg(a)} a_i D^i$ par $b = \sum_{i=0}^{deg(b)} b_i D^i$ nous considérons les trois suites stationnaires

$(r_n)_{n\in\mathbb{N}},\ (q_n)_{n\in\mathbb{N}},\ (\varepsilon_n)_{n\in\mathbb{N}}$ où $\left\{\begin{array}{lcl}\varepsilon_0 &=& 0\\ q_0 &=& 0\\ r_0 &=& a\end{array}\right.$

$$\left\{\begin{array}{lcl}\varepsilon_n &=& Max(0, deg(r_{n-1}) - deg(b))\\ q_n &=& q_{n-1} + b\varepsilon_n \frac{r^*_{n-1}}{b_{deg(b)}} D^{\varepsilon_n}\\ r_n &=& r_{n-1} - bq_n\end{array}\right.$$

où r^*_{n-1} est le coefficient dominant de r_n.
Ces suites sont stationnaires à partir de l'indice $i^* = Max(0, deg(a) - deg(b))$: ces deux algorithmes sont de complexité polynomiale.

Algorithmes pour les p.g.c.d. *à gauche et à droite* d'un nombre fini de polynômes de $K[X][D]$.

Nous pouvons alors choisir pour algorithmes ceux des divisions euclidiennes, tels qu'ils sont enseignés au lycée pour les entiers, le stathme euclidien étant le degré et les produits s'effectuant *à gauche ou à droite.*

Des connexions modulaires ou vectorielles à une variable.

Définitions :

si D est une dérivation sur un anneau commutatif unitaire $(A, +, \times)$ à valeurs dans un A-module $(M, +, .)$ une connexion modulaire de dérivation D sera une application ∇_D, et plus simplement

∇, additive de M dans M qui *satisfait l'identité dite de Leibnitz* :

$$\forall (x,a) \in M \times A \ \nabla(a.x) = a.\nabla(x) + D(a).x$$

∇ sera dite vectorielle si A est un corps et M un espace vectoriel. *Sauf dans l'exemple qui suit, dans tout ce qui suit les espaces vectoriels considérés seront de dimension finie et on appellera triplet (K, D, E) la donnée d'un corps K, d'une dérivation D sur K et d'un espace vectoriel E de dimension finie sur K.*

Un exemple :

soit l'anneau $K[X][D]$ alors l'application

$$\nabla \ : \ \left\{ \begin{array}{lll} K[X][D] & \rightarrow & K[X][D] \\ P & \mapsto & D \times P \end{array} \right.$$

est une connection vectorielle de dérivation D telle que, pour tout idéal *à gauche* de $K[X][D]$ de générateur $i \in I$: $D(I) \subset I \Rightarrow \nabla(I) \subset I$.
Preuve : si $I = (i)_g$ alors $\forall x \in K[X]$ $D(x.i) = D(x).i + x.D(i) \in (i)_g$

Matrice d'une connexion vectorielle et formule de changement de base.

Dans cette partie ∇ est une connexion de dérivation D sur un K-espace vectoriel V de dimension n.

Matrice d'une connexion vectorielle.

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de V on appelle matrice de ∇ dans la base $\mathcal{B}$ la matrice dont les vecteurs colonnes sont les coordonnées des vecteurs $(\nabla(e_1), \ldots, \nabla(e_n))$ dans la base $\mathcal{B}$, c'est une matrice de $M_n(K)$ que l'on note $(\nabla)_{\mathcal{B}}$.

Formule de changement de base.

Soient $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ nous posons $P_{\mathcal{B},\mathcal{B}'}$ la matrice des coordonnées des vecteurs de $\mathcal{B}$ exprimées dans la base $\mathcal{B}'$.
Si $P_{\mathcal{B},\mathcal{B}'} = (P_{i,j})_{1 \leq i,j \leq 1}$ alors

$$\begin{cases} e_1 &= P_{1,1}.e'_1 + P_{2,1}.e'_2 + \cdots + P_{n,1}.e'_n \\ e_2 &= P_{1,2}.e'_1 + P_{2,2}.e'_2 + \cdots + P_{n,2}.e'_n \\ \vdots & \vdots \quad \vdots \\ e_n &= P_{1,n}.e'_1 + P_{2,n}.e'_2 + \cdots + P_{n,n}.e'_n \end{cases}$$

$$\begin{cases} \nabla(e_1) &= P_{1,1}.\nabla(e'_1) + P_{2,1}.\nabla(e'_2) + \cdots + P_{n,1}.\nabla(e'_n) \\ &+ D(P_{1,1}).e'_1 + D(P_{2,1}).e'_2 + \cdots + D(P_{n,1}).e'_n \\ \nabla(e_2) &= P_{1,2}.\nabla(e'_1) + (P_{2,2}.\nabla(e'_2) + \cdots + P_{n,2}.\nabla(e'_n) \\ &+ D(P_{1,2}).e'_1 + D(P_{2,2}).e'_2 + \cdots + D(P_{n,2}).e'_n \\ \vdots & \vdots \quad \vdots \\ \nabla(e_n) &= P_{1,n}.\nabla(e'_1) + P_{2,n}.\nabla(e'_2) + \cdots + P_{n,n}.\nabla(e'_n) \\ &+ D(P_{1,n}).e'_1 + D(P_{2,n}).e'_2 + \cdots + D(P_{n,n}).e'_n \end{cases}$$

ce qui donne la relation

$$\boxed{P_{\mathcal{B},\mathcal{B}'} \times (\nabla)_{\mathcal{B}} = (\nabla)_{\mathcal{B}'} \times P_{\mathcal{B},\mathcal{B}'} + D(P_{\mathcal{B},\mathcal{B}'})}$$

Vecteurs cycliques.

Dans cette partie E est un K-espace vectoriel de dimension n, D une dérivation sur K et ∇ une connexion vectorielle.

Définition : un vecteur $y \in E$ est cyclique (pour ∇) si et seulement si la famille $y,\ \nabla(y),\ \ldots,\ \nabla^{n-1}(y))$ est une famille libre dans E. Autrement écrit : si et seulement si $(y,\ \nabla(y),\ \ldots,\ \nabla^{n-1}(y)))$ *est une base* de E. Dans ce cas E est dit *cyclique pour* ∇.

Interprétation. Si E possède un vecteur cyclique alors E est *stable* pour ∇ (autrement écrit $\nabla(E) \subset E$). On peut écrire cette tautologie : « Tout vecteur est cyclique pour l'espace vectoriel engendré par la suite des puissances de ∇ appliquées à ce vecteur ». Ce qui suit essaie de répondre aux questions :

- existe-t-il un vecteur cyclique pour tout l'espace E?
- Tout espace stable pour ∇ (qui contient son image par ∇) est-il cyclique?
- Existe-t-il d'autres espaces stables que l'espace de départ E?

Quelques propriétés des vecteurs cycliques. **Définitions et lemme :** on appelle *ordre cyclique* d'un vecteur la dimension de l'espace vectoriel engendré par la suite des puissances de ∇ appliquées à ce vecteur et *espace caractéristique stable* de ce vecteur cet espace vectoriel engendré et on le note $Escars(\nabla, y)$. On appelle *base caractéristique* de ce vecteur la base extraite des premiers vecteurs indépendants de la suite des puissances de ∇ appliquées à ce vecteur. La matrice d'une connexion vectorielle dans une base caractéristique est *compagnon*.

Preuve : pour une base caractéristique de cardinal k il y a un vecteur y pour lequel la base-suite $y,\ \nabla(y),\ \ldots,\ \nabla^{k-1}$ est indépendante et $\nabla^k(y)$ est lié par une relation

$$\nabla^k(y) = c_{n-1}.\nabla^{k-1} + \cdots + c_1.\nabla(y) + c_0.y$$

L'espace vectoriel engendré par la base-uplet $(y,\ \nabla(y),\ \ldots,\ \nabla^{k-1})$ est stable pour ∇ et la matrice de ∇ par rapport à cette base vient naturellement, c'est la matrice compagnon

$$\begin{pmatrix} 0 & \ldots & 0 & -c_0 \\ 1 & \ddots & 0 & -c_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \ldots & 1 & -c_{k-1} \end{pmatrix}$$

Définitions d'une transformée et d'une connexion associées aux espaces caractéristiques stables.

La connexion dérivation. **Lemme et définition :** sur l'anneau $K[D]$ l'application

$$D_\times \ : \ \left\{ \begin{array}{lll} K(D] & \to & K[D] \\ P & \mapsto & D \times P \end{array} \right.$$

est une connexion que nous appelons *la connexion dérivation.*

Preuve : la proposition « $D_\times$ est une connection» se déduit de l'identité de Leibnitz.

La transformée dérivante en un vecteur $y \in E$. **Lemme et définition :** si $y \in E$ est cyclique d'ordre cyclique k alors la partie $\left\{y, \ldots, \nabla^{k-1}(y)\right\}$ est une base de son espace caractéristique stable et nous appellons transformée dérivante en y l'application linéaire bijective qui transforme la base caractéristique en la base $(1, D, \ldots, D^{k-1})$. On note cet isomorphisme $Dante(\nabla, y)$.

Le polynôme différentiel caractéristique d'un vecteur $y \in E$. **Définition :** à tout vecteur $y \in E$ d'ordre cyclique k on peut associer le polynôme différentiel unique $D^k - \sum_{i=1}^{k-1} a_i D^i$ si la relation de dépendance de $y, \ldots, \nabla^{k-1}(y), \nabla^k(y)$ est la relation $(\nabla^k - \sum_{i=1}^{k-1} a_i \nabla^i)(y) = 0$. On l'appelle le polynôme différentiel caractéristique de y et on le note $\kappa(\nabla, y)$.

La connexion dérivation du quotient de $K[D]$ par l'idéal caractéristique d'un vecteur $y \in E$ **lemme et définition :** soit $y \in E$ d'ordre cyclique k, $p(\nabla, y)$ la projection canonique $E \overset{p(\nabla,y)}{\rightarrow} E/(\kappa(\nabla, y))_g$ alors il existe une unique connexion notée $D_\times(\nabla, y)$, on l'appelle *la connexion dérivation caractéristique en y* qui rende commutatif le shéma qui suit :

$$\begin{array}{ccc} Escars(\nabla, y) & \xrightarrow{\nabla} & Escars(\nabla, y) \\ \downarrow Dante(\nabla,y) & & \downarrow Dante(\nabla,y) \\ K[D] & \xrightarrow{D_\times} & K[D] \\ \downarrow p(\nabla,y) & & \downarrow p(\nabla,y) \\ K[D]/(\kappa(\nabla, y))_g & \xrightarrow{D_\times(\nabla,y)} & K[D]/(\kappa(\nabla, y))_g \end{array}$$

Preuve : la commutativité des quatres flêches de la partie supérieure du shéma est une conséquence directe des définitions qui précèdent. Soit à présent $P,\ P'$ tels que $P - P' \in (\kappa(\nabla, y))_g$ alors $\exists(Q,\ Q',\ R) \begin{cases} P &= Q \times \kappa(\nabla, y) + R \\ P' &= Q' \times \kappa(\nabla, y) + R \end{cases}$ soit $\begin{cases} D \times P &= D \times Q \times \kappa(\nabla, y) + D \times R \\ D \times P' &= D \times Q' \times \kappa(\nabla, y) + D \times R \end{cases}$ qui entraîne que

$$(D \times P - D \times P') = (D \times Q - D \times Q') \times \kappa(\nabla, y)$$

tous les représentants de la classe de P appartiennent à la classe de $D \times P$ ce qui induit sur

$K[D]/(\kappa(\nabla,y))_g$ une application unique, notée $D_\times(\nabla,y)$ qui a la classe de $P \in K[D]$ associe la classe de $D \times P \in K[D]$. Comme la classe de la somme $P+Q$ est la somme des classes de P et Q et comme l'application $D_\times$ est additive : $D_\times(\nabla,y)$ est additive. Si $a \in K$ alors de $\begin{cases} P &= Q \times \kappa(\nabla,y) + R \\ P' &= Q' \times \kappa(\nabla,y) + R \end{cases}$ on déduit que

$$\begin{cases} D \times a.P &= D \times a.Q \times \kappa(\nabla,y) + (a.D + D(a)) \times R \\ D \times a.P' &= D \times a.Q' \times \kappa(\nabla,y) + (a.D + D(a)) \times R \end{cases}$$

ce qui prouve que $D_\times(\nabla,y)$ vérifie bien l'identité de Leibnitz : c'est donc une connexion. La commutativité des quatre flêches de la partie inférieure du shéma résulte alors de la stabilité sur toutes les classes de l'application $P \overset{D_\times}{\mapsto} D \times P$.

L'isomorphisme de cast d'une connexion en un vecteur $y \in E$:

lemme et définition : la composée $p(\nabla,y) \circ Dante(\nabla,y)$ est un isomorphisme linéaire de $K[D]$ dans
$K[D]/(\kappa(\nabla,y))_g$ appelé isomorphisme de cast et on le notera $Caste(\nabla,y)$.

Preuve : posons

$$p(\nabla,y) \circ Dante(\nabla,y) = Caste(\nabla,y)$$

alors l'application linéaire $Caste$ est un isomorphisme car il transforme la base caractéristique du vecteur y de $Escars(\nabla,y)$ en la base caractéristi-

que de $K[D]/(\kappa(\nabla, y))$.
Nous en déduisons *la commutativité du shéma de cast*

$$\begin{array}{ccc} Escars(\nabla, y) & \xrightarrow{\nabla} & Escars(\nabla, y) \\ \downarrow Caste(\nabla,y) & & \downarrow Caste(\nabla,y) \\ K[D]/(\kappa(\nabla, y))_g & \xrightarrow{D_\times(\nabla,y))} & K[D]/(\kappa(\nabla, y))_g \end{array}$$

Des polynômes de connexions vectorielles.

Définition de polynômes d'une application, d'une connexion, sur un triplet (K, D, E)**.**

On se donne un triplet (K, D, E) et une application f de E dans E et un polynôme $P = \sum_{i=0}^{k} a_i D^i \in K[D]$, le polynôme $P(f)$ sera défini comme l'application de E dans E telle que $x \mapsto \sum_{i=0}^{k} a_i f^i(x)$ où $f^0 = Id$ et si $i \geq 1$ alors $f^i = f \circ f^{i-1}$. Cette définition s'applique en particulier aux connexions ∇ de E dans E.

Shéma de cast et shéma de projection.

Pour tout triplet (K, D, E) et tout polynôme $P \in K[D]$ on a le shéma commutatif :

$$\begin{array}{ccc} Escars(\nabla, y) & \xrightarrow{P(\nabla)} & Escars(\nabla, y) \\ \downarrow{\scriptstyle Caste(\nabla,y)} & & \downarrow{\scriptstyle Caste(\nabla,y)} \\ K[D]/(\kappa(\nabla, y))_g & \xrightarrow{P(D_\times(\nabla,y))} & K[D]/(\kappa(\nabla, y))_g \\ \uparrow{\scriptstyle p(\nabla,y)} & & \uparrow{\scriptstyle p(\nabla,y)} \\ K[D] & \xrightarrow{P(D_\times)} & K[D] \end{array}$$

Preuve : la commutativité du shéma de cast

$$\begin{array}{ccc} Escars(\nabla, y) & \xrightarrow{\nabla} & Escars(\nabla, y) \\ \downarrow{\scriptstyle Caste(\nabla,y)} & & \downarrow{\scriptstyle Caste(\nabla,y)} \\ K[D]/(\kappa(\nabla, y))_g & \xrightarrow{D_\times(\nabla,y)} & K[D]/(\kappa(\nabla, y))_g \end{array}$$

se formalise par

$$Caste(\nabla, y) \circ \nabla = D_\times(\nabla, y) \circ Caste(\nabla, y)$$

soit

$$\nabla = Caste(\nabla, y)^{-1} \circ D_\times(\nabla, y) \circ Caste(\nabla, y)$$

qui, par composition itérés et combinaison linéaire, devient $\forall P \in K[D]$

$$P(\nabla) = Caste(\nabla, y)^{-1} \circ P(D_\times(\nabla, y)) \circ Caste(\nabla, y)$$

et prouve la commutativité du shéma supérieur. Par l'utilisation du shéma d'axiomes de substitu-

tion la commutativité du shéma inférieur se déduit du shéma de projection

$$\begin{array}{ccc} K[D]/(\kappa(\nabla,y))_g & \xrightarrow{D_\times(\nabla,y)} & K[D]/(\kappa(\nabla,y))_g \\ \uparrow{\scriptstyle p(\nabla,y)} & & \uparrow{\scriptstyle p(\nabla,y)} \\ K[D] & \xrightarrow{D_\times} & K[D] \end{array}$$

Polynômes de connexion et idéaux annulateurs d'un vecteur.

Lemme : si y est un vecteur d'un triplet (K, D, E) alors $\forall x \in Escars(\nabla, y),\ \forall P \in K[D]$,

$$P(\nabla)(x) = Caste(\nabla, y)^{-1} \circ p(\nabla, y)\,(P.Dante(\nabla, y))$$

Preuve : comme $Caste(\nabla, y)^{-1} \circ p(\nabla, y)$ est une application K-linéaire de $K[D]$ dans $Escars(\nabla, y)$ il suffit de montrer que

$$Caste(\nabla, y)^{-1} \circ p(\nabla, y)\left(D^i.Dante(\nabla, y)\right) = \nabla^i$$

pour toutes les valeurs entières de i ce que nous faisons par récurrence sur i : y est d'ordre k alors nous pouvons écrire $x = \sum_{j=0}^{k-1} c_j \nabla^j(y)$ puis

$$\begin{array}{rcl} Dante(\nabla, y) & = & \sum_{j=0}^{k-1} c_j D^j \\ p(\nabla, y)\,(Dante(\nabla, y)) & = & \sum_{j=0}^{k-1} c_j D^j \\ Caste^{-1}(\nabla, y) \circ p(\nabla, y)\,(Dante(\nabla, y)) & = & \sum_{j=0}^{k-1} c_j Caste^{-1}(\nabla, y)\,(D^j) \\ & = & \sum_{j=0}^{k-1} c_j \nabla^i(y) = x \end{array}$$

ce qui montre le lemme pour $i = 0$. Supposons à présent que

$$Caste(\nabla, y)^{-1} \circ p(\nabla, y)\left(D^i.Dante(\nabla, y)\right) = \nabla^i$$

alors :

$$\begin{array}{rcl}
\nabla^{i+1}(x) & = & Caste(\nabla,y)^{-1}\circ D\times_{\nabla,y}\circ p(\nabla,y)\left(D^{i}Dante(\nabla,y)(x)\right)\\
car\ \nabla^{i} & = & Caste(\nabla,y)^{-1}\circ D\times_{\nabla,y}\circ Caste(\nabla,y)\\
 & = & Caste(\nabla,y)^{-1}\circ p(\nabla,y)\circ D\times(Dante(\nabla,y))\\
car\ D\times_{\nabla,y}\circ p(\nabla,y) & = & p(\nabla,y)\circ D\times\\
 & = & Caste(\nabla,y)^{-1}\circ\left(D.D^{i}.Dante(\nabla,y)\right)\\
 & = & Caste(\nabla,y)^{-1}\circ\left(D^{i+1}.Dante(\nabla,y)\right)
\end{array}$$

Lemme : si y est un vecteur d'un triplet (K, D, E) alors l'ensemble des polynômes de connexion annulateurs de $x \in E$ est un idéal de $K[D]$ *à gauche.*

Preuve : si y annule $P, P' \in K[D]$ alors $\forall Q \in K[D]$ il annule $-P,\ P+P',\ QP$.

Le lemme du transporteur

s'énonce : si A est un anneau euclidien gradué *à gauche*, $L, f \in A\backslash\{0\}$ alors l'ensemble $\{P \in A|\ P \times f \in (L)_g\}$ est un *idéal à gauche* dont on note $L : f \ll$ un$\gg$ générateur (on remarquera que $L : f$ est un *groupe multiplicatif*). On a alors la double égalité :

$$\boxed{(L:f)_g f = (f:L)_g L = (L)_g \cap (f)_g}$$

Si $f,\ L$ sont premiers entre eux *à gauche* alors l'idéal $(L\ :\ f)_g$ n'est pas nécessairement $K[D]$ contrairement au cas des idéaux sur les anneaux gradués euclidiens commutatif (par exemple $K[X]$)