Factorisation de polynômes de différentielles à coefficients sur un corps de dimension infinie sur ses constantes

Alain Wazner

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 linéaire d'ordre 1. 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 caractéristiques ou des polynômes minimaux. 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 dont le corps des constantes n'est pas algébriquement clos de traduire certaines notions propres aux polynômes d'endomorphismes linéaires sur des corps. Les informaticiens savent obtenir l'algèbre calculable des endomorphismes linéaires qui commutent avec une connexion en se donnant les solutions rationnelles en M de $DM = PM - MP$, M et P étant des matrices d'ordre n sur un corps, D étant une dérivation : nous définirons dans ce qui suit le sens de ces termes.

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* $\mathcal{I}$ de A est dit *monogène* si et seulement $(\exists i \in A)\ \mathcal{I} = \{ai/a \in A\}$
- Un anneau A est principal si tout idéal $\mathcal{I}$ de A est monogène.
- Un anneau A est gradué euclidien si :
  - Il est intègre.
  - Il existe un stathme euclidien : une application $\nu \quad : \quad A\backslash\{0\} \rightarrow \mathbb{N}$ 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 est principal.

Propriété : Dans un anneau A gradué euclidien à gauche un élément a sera dit irréductible si et seulement si l'idéal $(a)_g$ est propre et maximal pour l'ordre de l'inclusion. Dans un anneau A gradué euclidien à gauche et qui n'est pas un corps il existe des éléments irréductibles et tout élément qui n'est pas inversible est divisible par un irréductible.

Preuves :

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

- Si $\mathcal{I}$ est un idéal de A et $i \in \mathcal{I}$ tel que $\nu(i)$ soit minimal. Soit $a \in \mathcal{I}$ on effectue la division euclidienne à gauche de a par i : $a = iq + r$ avec $\nu(r) = 0$ ou $\nu(r) < \nu(i)$. $\nu(r) = 0$ puisque $\nu(i)$ est minimal. Il suit que $\mathcal{I} = (i)_g$.
- $(a)_g \subset (b)_g \Leftrightarrow b_{|g}a$:
  $(a)_g \subset (b)_g \Leftrightarrow \{za/z \in A\} \subset \{zb/z \in A\}$
  $a \in (a)_g \Rightarrow (\exists z \in A),\ a = zb \Rightarrow b_{|g}a$.
  $b_{|g}a \Rightarrow (\exists z \in A),\ a = zb \Rightarrow \{xa/x \in A\} \subset \{xzb/x \in A\} \Rightarrow (a)_g \subset (b)_g$.
- Sans utilisation de l'axiome du choix, l'assertion $(\exists a \in A)\nu(a) = Min_{P \in A}\nu(P)$ est vraie. $(\forall b \in A), (\exists! q, r)(a = qb + r) \wedge (\nu(r) < \nu(a))$, comme $\nu(a)$ est minimal nous en déduisons que $r = 0$ soit $b_{|g}a$ soit $(a)_g \subset (b)_g$.

Propriété : Si A est un anneau gradué euclidien à gauche alors :

(1) 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 $\sum_{e \in E}(e)_g = (a)_g$.

(2) 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 :

(1) **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

$$\exists(\alpha(e_1^*),\dots,\alpha(e_n^*))\in E^n,\forall i\in\{1,\dots,n\},$$
$$e_i^*=\alpha(e_i^*)d$$

On a alors

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

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 $\sum_{e\in E}(e)_g$:

Soit d un p.g.c.d. de E alors

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

On a $\forall(e_1,\dots,e_n)\in E^n,\forall(\alpha_1,\dots,\alpha_n)\in A^n$, $\sum_{i=1}^n\alpha_ie_i=\left(\sum_{i=1}^n\alpha_i\alpha(e_i)\right)d$ ce qui entraîne $\sum_{i=1}^n\alpha_ie_i\in(d)_g$. On a donc $\sum_{e\in E}(e)_g\subset(d)_g$.

Soit c tel que $\sum_{e\in E}(e)_g=(c)_g$ alors $(c)_g\subset(d)_g$ et $\exists\alpha\in A$ tel que $c=\alpha d$.

c est un diviseur commun à tout $e\in E$ et comme d est un p.g.c.d. c divise d. Il existe donc α, β dans A tels que $\begin{cases} c = & \alpha d \\ d = & \beta c \end{cases}$

$$\begin{cases} c = & \alpha d \\ d = & \beta c \end{cases} \Leftrightarrow \begin{cases} c = & \alpha\beta c \\ d = & \beta\alpha d \end{cases}$$

$$\Leftrightarrow \begin{cases} c(1-\alpha\beta) = & 0 \\ d(1-\beta\alpha) = & 0 \end{cases}$$

A est intègre cela entraîne $\begin{cases} 1-\alpha\beta = & 0 \\ 1-\beta\alpha = & 0 \end{cases}$ soit $\alpha\beta = \beta\alpha = 1$ soit $\begin{cases} \alpha \in \mathcal{U}_A \\ \beta \in \mathcal{U}_A \end{cases}$. De $d = \beta c$ avec $\beta \in \mathcal{U}_A$ il suit que $(c)_g = (d)_g$.

(2) **Supposons $(a)_g \cap (b)_g \neq (0)_g$ et posons $(a)_g \cap (b)_g = (m)_g$ alors $m \neq 0$.**

- **m est un p.p.c.m. de a et b :**
  $m \in (a)_g$ et $m \in (b)_g$ donc pour tout élément e de $\{a, b\}$ $e_{|g}m$.
  Si q est tel que tout élément e de $\{a, b\}$ $e_{|g}q$ alors $q \in (a)_g$ et $q \in (b)_g$ donc $q \in (m)_g = (a)_g \cap (b)_g$ et $m_{|g}q$.
- **Tout générateur de $(m)_g$ est un p.p.c.m. de $\{a, b\}$:**
  Soit M un générateur de $(m)_g$ alors puisque $(m)_g = (a)_g \cap (b)_g$: $a_{|g}M$ et $b_{|g}M$.
  Soit $q \in A$ tel que $a_{|g}q$ et $b_{|g}q$ alors $q \in (a)_g \cap (b)_g = (M)_g$ donc $M_{|g}q$.

Supposons $(a)_g \cap (b)_g = (0)_g$ **:**
Nous montrons le
Lemme : Si A est un anneau gradué euclidien à gauche alors $\forall P, Q, R \in A$:

(i) Si $(P)_g \cap (Q)_g = (0)_g$ alors

$$(PR)_g \cap (QR)_g = (0)_g$$

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

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

Preuve :

(i) 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 $H = K = 0$.

(ii) 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 $PR \wedge_g QR$.

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

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

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

puis

$$(\exists v \in A\backslash\{0\}),$$

$$PR \wedge_g QR = H'PR = K'QR = v(P \wedge_g Q)R$$

$\exists u, v \in A\backslash\{0\}$ avec

$$\begin{cases} (P \wedge_g Q)R & = u(PR \wedge_g QR) \\ PR \wedge_g QR & = v(P \wedge_g Q)R \end{cases}$$

donc $\begin{cases} (P \wedge_g Q)R & = uv(P \wedge_g Q)R \\ PR \wedge_g QR & = vu(PR \wedge_g QR) \end{cases}$

soit $\begin{cases} (1-uv)(P \wedge_g Q)R & = 0 \\ (1-vu)(PR \wedge_g QR) & = 0 \end{cases}$ Mais A est intègre donc $\begin{cases} (1-uv) & = 0 \\ (1-vu) & = 0 \end{cases}$ soit $u, v \in \mathcal{U}_A$ 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 $\begin{cases} a & = a'(a \vee_g b) \\ b & = b'(a \vee_g b) \end{cases}$ où $a \vee_g b$ est un p.g.c.d. de a et b, alors

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

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

$$\begin{aligned} ((a' \wedge_g b')(a \vee_g b))_g &= (a \wedge_g b))_g \\ &= (a)_g \cap (b)_g = (0)_g \end{aligned}$$

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

$$\begin{aligned} (0)_g &= (a'(a \vee_g b))_g \cap (b'(a \vee_g b))_g \\ &= (a)_g \cap (b)_g \end{aligned}$$

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 $(a \vee_g b)_g = (fa)_g + (gb)_g = (a)_g \oplus (b)_g$. 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 $a' \neq 0$.

Si $a_1, \ldots, a_n \in A \backslash \{0\}$ alors l'assertion démontrée

$$(a \neq 0) \wedge (b \neq 0) \Rightarrow (a \wedge_g b)_g = (a)_g \cap (b)_g$$

permet une récurrence qui montre que l'ensemble des p.p.c.m. de $\{a_1, \ldots, a_n\}$ est l'ensemble des générateurs de $\bigcap_{i=1}^{n}(a_i)_g$.

Sur les dérivations sur les anneaux commutatifs

Définitions

Soit $(A, +, \times)$ un anneau commutatif unitaire et $(M, +)$ un groupe commutatif

Si de plus M est muni d'une loi externe $\times$ de $A \times M$ dans M vérifiant, pour tous éléments a et b de A et x, y de M :

(1) $a \times (x + y) = a \times x + a \times y$

(2) $(a + b) \times x = a \times x + b \times x$

(3) $(a \times b) \times x = a \times (b \times x)$

(4) $1 \times x = x$

Nota :*On prendra garde de ce que le + sur A n'est pas le + sur M, il en est de même du $\times$ sur A et du $\times$ sur M. La différence fondamentale entre module et espace vectoriel vient de ce que l'opération externe de multiplication ne peut-être inversée comme c'est le cas d'un espace vectoriel sur un corps. On peut dire qu'un A-module M est un espace vectoriel sur lequel* *on a* ***oublié*** *la possibilité d'inversion, c'est les modules sont importants en théorie algébrique des nombres.*

Une dérivation D d'un anneau commutatif $(A, +, \times)$ à valeurs dans un A-module $(M, +, \times)$ est une application additive de A dans M qui satisfait l'identité de Leibniz :

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

Définition : Si D est une dérivation sur un anneau de caractéristique c alors l'ensemble $\{x \in A / D(x) = 0\}$ est un anneau dont la caractéristique est celle de A. On l'appelle l'anneau des constantes et on pourra le noter A_D.

Preuve : A_D est le noyau d'une application additive, c'est un groupe additif, c'est aussi le noyau d'un demi-groupe. multiplicatif par l'identité de Leibnitz. A et A_D ont même caractéristique puisque $1 \in A_D$.

Quelques exemples

Un exemple linéaire

Le paradoxe des rames, c'est qu'elles ne sont pas linéaires, **Jérôme K. Jérôme**, *citation*

apocryphe
Si K est un corps de caractéristique 0, $K[X]$ son anneau des polynômes, D est la dérivation des polynômes, D^i la dérivation i-ème, avec $D^0 = Id$ alors l'anneau des polynômes $\sum_{i=0}^{n} a_i D^i$ est gradué si on choisit $\nu\left(\sum_{i=0}^{n} a_i D^i\right)$ comme le grand entier i tel que $a_i \neq 0$ et $\nu(0) = 0$. On note cet anneau $K[X][D]$, son corps des constantes est K. Si $P, Q \in K[X][D]$ alors $P \times Q \overset{déf}{=} P \circ Q$. $K[X][D]$ est euclidien par la formule du binôme

$$a_i D^i \times b_j D^j = \sum_{k=0}^{i} C_i^k a_i D^k(b_j) D^{i-k+j}$$

La structure de $K[X][D]$ peut s'enrichir d'une opération externe $K[X] \times K[X][D] \dot{\rightarrow} K[X][D]$ par

$$a.P(D) \overset{déf}{=} aD^0 \times P(D)$$

L'algèbre $(K[X][D], +, \times, .)$ est doublement non-commutative.

Propriété :

(i) La famille $(D^n)_{n\in\mathbb{N}}$ est une famille-base des espaces vectoriel $K[X][D]$.

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

(iii) $\mathcal{U}_{K[X][D]}$ est l'ensemble des opérateurs de degré 0 à coefficient sur K, il est isomorphe à $K\backslash\{0\}$.

Preuve :

(i) Nous montrons le

Lemme : $L = \sum_{i=0}^{n} a_i D^i$ avec $a_n \neq 0$ est K-linéaire, son noyau est un K-espace vectoriel de dimension au plus égale à n.

Preuve : Si $n = 0$ alors $L(s) = a_0 s$. L'équation $L(s) = 0$ a pour ensemble de solutions $\{0\}$ espace vectoriel de dimension 0. Si $L = \sum_{i=0}^{n} a_i D^i$, avec $a_n \neq 0$ et $n > 0$, soit l'équation $L(s) = 0$ n'a pas de solution non nulle, auquel cas son ensemble de solutions est $\{0\}$ espace vectoriel de dimension 0, soit l'équation $L(s) = 0$ possède une solution non nulle s_0 : nous effectuons alors le changement d'inconnue $s = s_0 u$. Par la formule du binôme

$$D^n(xy) = \sum_{i=0}^{n} C_n^i D^i(x) D^{n-i}(y)$$

on voit que $L(s_0 u) = H(u)$, avec $H = \sum_{i=0}^{n} b_i D^i$ avec $b_n = a_n$, $b_0 = L(s_0) = 0$, de sorte que $H(u) = J(D(u))$ où $J = \sum_{i=0}^{n-1} b_{i+1} D^i$.

L'équation $H(u) = 0$ est équivalente au système :

$$\left\{ \begin{array}{l} J(v) = 0 \\ D(u) = v \end{array} \right.$$

Nous appliquons l'hypothèse de récurrence pour J : le K-espace vectoriel V des solutions de $J(v) = 0$ est de dimension au plus $n - 1$, si E

est l'espace vectoriel $D^{-1}(V)$, p la projection canonique $E \to E/ker(D) = E/K$, 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 $D(E)$ espace vectoriel de dimension finie au plus $n-1$, comme K est un espace vectoriel sur lui-même de dimension 1, E est donc un espace vectoriel de dimension finie au plus égale à n sur K.
L'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 $s = s_0 u$ avec $s_0 \neq 0$ et u solution de $H(u) = 0$, l'espace vectoriel des solutions de $L(s) = 0$ est de dimension au plus égale à n.
La famille $(D)_{n\in\mathbb{N}}$ est une partie libre de $K[X][D]$: Supposons qu'une combinaison linéaire finie de cette famille est nulle alors un opérateur $L = \sum_{i=0}^{n} a_i D^i$ avec $(a_0, \ldots, a_n) \neq (0, \ldots, 0) \in K[X]^n$ est nul. Ce qui revient à dire que $K[X]$ est inclus dans l'espace vectoriel des solutions de $L(u) = 0$; hors un tel opérateur a au plus n solutions K-linéairement indépendantes et le K-espace vectoriel $K[X]$ est de dimension infinie : il y a contradiction et la famille $(D)_{n\in\mathbb{N}}$ est une

partie libre de $K[X][D]$. Cette famille est par définition
génératrice de $K[X][D]$: c'en est donc une base.

(ii) Soit $L = \sum_{i=0}^{n} a_i D^i$ avec $a_n \neq 0$, on pose $deg(L) = n$: deg est un stathme euclidien. Nous considérons la formule du binôme

$$a_i D^i \times b_j D^j = \sum_{k=0}^{i} C_i^k a_i D^k(b_j) D^{i-k+j}$$

et nous en servons pour construire les divisions euclidiennes. Posant $b = \sum_{i=0}^{deg(b)} b_i D^i$ nous considérons les trois suites $(r_n)_{n\in\mathbb{N}}$, $(q_n)_{n\in\mathbb{N}}$, $(\varepsilon_n)_{n\in\mathbb{N}}$ où $\begin{cases} \varepsilon_0 &= 0 \\ q_0 &= 0 \\ r_0 &= a \end{cases}$ et
$\begin{cases} \varepsilon_n &= Max(0, deg(r_{n-1}) - deg(b)) \\ q_n &= q_{n-1} + \varepsilon_n \frac{r_{n-1}*}{b_{deg(b)}} D^{\varepsilon_n} b \\ r_n &= r_{n-1} - q_n b \end{cases}$ où $r_{n-1}*$ est le coefficient dominant de r_{n-1}. Pour la division euclidienne à droite nous considérons les trois suites $(r_n)_{n\in\mathbb{N}}$, $(q_n)_{n\in\mathbb{N}}$, $(\varepsilon_n)_{n\in\mathbb{N}}$ où
$\begin{cases} \varepsilon_0 &= 0 \\ q_0 &= 0 \\ r_0 &= a \end{cases}$ et

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

est le coefficient dominant de r_{n-1}. Ces suites sont stationnaires à partir de l'indice $i^* = Max(0, deg(a) - deg(b))$ où r_{i^*}, q_{i^*} sont le reste et le quotient de la division à gauche (Resp. à droite) de a par b. Ceci prouve que $K[X][D]$ est euclidien gradué à gauche (Resp. à droite).

(iii) Soit $a \in K[X][D]$ inversible alors $\exists b \in K[X][D],\ ab = ba = 1$ ceci entraîne que $deg(a) + deg(b) = 0$ soit $a, b \in K[X]$ et comme a est inversible dans $K[X]$ c'est que $a \in K\backslash\{0\}$. Réciproquement si $a \in K\backslash\{0\}$ alors a est inversible d'inverse a^{-1}.
On pourra alors écrire **le** p.g.c.d. et **le** p.p.c.m. à gauche (Resp. à droite) en choisissant 1 pour coefficient dominant du coefficient dominant du terme de plus haut degré d'un opérateur de $K[X][D]$.

Les p.g.c.d. se programment alors formellement par l'algorithme des divisions euclidiennes comme on le pratique au collège avec les entiers.

Sur les connexions modulaires et vectorielles

De quoi s'agit-il?

Définition Si D est une dérivation sur un anneau commutatif unitaire $(A, +, \times)$ à valeurs dans un A-module $(M, +, \times, .)$ alors une connexion ∇ de dérivation D est une application de M vers M telle que :

(1) $\forall x, y \in M,\ \nabla(x + y) = \nabla(x) + \nabla(y)$ (additivité)

(2) $\forall (x, a) \in M \times A$,

$$\nabla(ax) = a.\nabla(x) + D(a).x$$

(identité de Leibnitz)

Nota : Cette notion n'est pas à proprement parler géométrique, toute géométrie ne pouvant se fonder sans algèbre, elle permettra une qualification locale des singularités d' équations différentielles.

Un exemple linéaire

Si $E = K[X][D]$ alors l'application $\nabla : \begin{cases} K[X][D] & \to K[X][D] \\ P & \mapsto D \times P \end{cases}$ est une connexion modulaire telle que pour tout idéal à gauche I $D(i) \subset (i)_g \Rightarrow \nabla(I) \subset I$.
Preuve : si $I = (i)_g$ alors $\forall x \in K[X][D]$ $D(xi) = x \times D(i) + D(x) \times i \subset (i)_g$.
L'identité de Leibnitz permet aussi de démontrer que pour toute connexion modulaire ∇ et tout idéal à gauche I de générateur i :

$$D(i) \subset (i)_g \Rightarrow \nabla(I) \subset I$$

Un cas particulier d'anneau sous-jacent et de connexion

Un corps est un cas particulier d'anneau et dans tout ce qui suit A sera un corps de caractéristique 0 muni d'une dérivation sur lui-même et de dimension infinie sur ces constantes, des exemples de tels anneaux A sont donnés par $A = K(X)$ ou $A = K((X))$ muni de la dérivation $\frac{d}{dX}$. On ne considérera les connexions, dites **connexions vectorielles**, ∇ de dérivation D que comme application d'un espace vectoriel V de dimension n sur A vers lui-même.

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

Matrice d'une connexion vectorielle Soit $\mathcal{B} = (e_1, \ \ldots, \ e_n)$ une base du A-espace vectoriel V et ∇ une connexion vectorielle de dérivation D alors

$$\begin{array}{rcl} \nabla\left(\sum_{j=1}^{n} x_j.e_j\right) & = & \sum_{j=1}^{n} (x_j.\nabla(e_j) + D(x_j).e_i) \\ & = & \sum_{j=1}^{n} x_j.\nabla(e_j) + \left(\sum_{j=1}^{n} D(x_j).e_j\right) \\ & = & L\left(\sum_{j=1}^{n} x_j.e_j\right) + (\sum_{i=1}^{n} D(x_i).e_i) \end{array}$$

où L est la matrice $(\nabla(e_j)_i)_{1\leq i\leq n, \ 1\leq i\leq n} \overset{déf}{=} (\nabla)_{\mathcal{B}}$ dont les éléments $L_{i,j}$ de ligne d'indice i et de colonne d'indice j sont $\nabla(e_j)_i$.

Formule de changement de base Soit $\mathcal{B}' = (f_1, \ \ldots, \ f_n)$ une autre base du A-espace vectoriel V alors

$$\begin{array}{rcl} \sum_{j=1}^{n} x_j.e_j & = & \sum_{j=1}^{n} y_j.f_j \\ \nabla\left(\sum_{j=1}^{n} x_j.e_j\right) & = & \nabla\left(\sum_{j=1}^{n} y_j.f_j\right) \end{array}$$

Les vecteurs $L\left(\sum_{j=1}^{n} x_j.e_j\right) + \sum_{i=1}^{n} D(x_i).e_i$ et $M\left(\sum_{j=1}^{n} y_j.f_j\right) + \sum_{i=1}^{n} D(y_i).f_i$ sont égaux et nous avons la relation $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P_{\mathcal{B},\mathcal{B}'} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

Soit $1 \leq j \leq n$ alors le vecteur f_j a, pour coordonnées dans le base $\mathcal{B}'$, le vecteur F_j de coefficient nul sur toutes les lignes sauf la i-ème où il vaut 1. La formule de changement de coordonnées $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P_{\mathcal{B},\mathcal{B}'} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ indique que f_j a, pour coordonnées dans le base $\mathcal{B}$, le j-ème vecteur-colonne $P_{\mathcal{B},\mathcal{B}'}(.,j)$ de $P_{\mathcal{B},\mathcal{B}'}$, le vecteur $M.f_j$ est alors le vecteur $L.P_{\mathcal{B},\mathcal{B}'}(.,j) + D\left(P_{\mathcal{B},\mathcal{B}'}(.,j)\right)$. Ceci étant vrai pour tout j : la matrice des coordonnées, dans la base $\mathcal{B}$, de la suite de vecteurs $(M.f_1, \ \ldots, \ M.f_n)$, est la matrice $LP_{\mathcal{B},\mathcal{B}'} + D\left(P_{\mathcal{B},\mathcal{B}'}\right)$. La formule de changement de coordonnées de base fait alors que la matrice des coordonnées, dans la base $\mathcal{B}'$, de la suite de vecteurs $(M.f_1, \ \ldots, \ M.f_n)$, est la matrice $P^{-1}_{\mathcal{B},\mathcal{B}'}LP_{\mathcal{B},\mathcal{B}'} + P^{-1}_{\mathcal{B},\mathcal{B}'}D\left(P_{\mathcal{B},\mathcal{B}'}\right)$. On obtient alors la formule de changement de base :

$$(\nabla)_{\mathcal{B}'} = P^{-1}_{\mathcal{B},\mathcal{B}'}(\nabla)_{\mathcal{B}}P_{\mathcal{B},\mathcal{B}'} + P^{-1}_{\mathcal{B},\mathcal{B}'}D\left(P_{\mathcal{B},\mathcal{B}'}\right)$$

vecteurs cycliques d'une connexion vectorielle

Définitions

Soit E un espace vectoriel muni d'une connexion vectorielle ∇, $y \in E$ sera dit cyclique pour ∇ si l'espace vectoriel engendré par la famille $\mathcal{F}(\nabla, y) = \left(\nabla^i(y)\right)_{i\in\mathbb{N}}$ est de dimension finie. On appellera cette dimension l'ordre du vecteur cyclique et $V(\nabla, y)$ l'espace vectoriel engendré par la famille $\mathcal{F}(\nabla, y)$. Pour une espace vectoriel V on dira que V est cyclique pour ∇ s'il existe $y \in V$

tel que $V = V(\nabla, y)$. Pour tout espace vectoriel cyclique pour ∇, $\nabla(V) \subset V$: c'est à dire que tout espace vectoriel V cyclique pour ∇ est stable pour ∇.

Quelques propriétés des vecteurs cycliques

Lemme : Pour toute connexion vectorielle ∇ de dérivation D, l'ordre $o(\nabla, y)$ d'un vecteur y cyclique pour ∇ est égal à la dimension de $V(\nabla, y)$ et dans la base $\mathcal{B} = \big(y, \ \ldots, \nabla^{o(\nabla,y)-1}\big)$ la matrice $(\nabla)_{\mathcal{B}}$ est compagnon.

Preuve : $\mathcal{B}$ est une famille libre de $V(\nabla, y)$ par définition de l'ordre de y et $\big(y, \ \ldots, \nabla^{o(\nabla,y)}\big)$ n'en est pas une : il existe $(c_0, \ \ldots, \ c_{o(\nabla,y)})$ non tous nuls tels que $\sum_{k=0}^{o(\nabla,y)} c_k \nabla^k(y) = 0$. $c_{o(\nabla,y)}$ n'est pas nul (s'il l'était l'ordre de y serait strictement plus petit que $o(\nabla, y)$), il suit que $\nabla^{o(V(\nabla,y))} = -\sum_{k=0}^{o(\nabla,y)-1} \frac{c_k}{c_{o(\nabla,y)}} \nabla^k$ et

$$(\nabla)_{\mathcal{B}} = \begin{pmatrix} 0 & \ldots & 0 & -\frac{c_0}{c_{o(\nabla,y)}} \\ 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \ldots & 1 & -\frac{c_{o(\nabla,y)-1}}{c_{o(\nabla,y)}} \end{pmatrix}.$$

Pour finir on prouve, par récurrence sur k, que la famille $\mathcal{B}_k = \big(y, \ \ldots, \ \nabla^{o(\nabla)+k}(y)\big)$ n'est pas libre : ceci est prouvé pour $k = 0$ et une relation de dépendance $\sum_{j=0}^{o(\nabla)+k} \lambda_{j,k} \nabla^j(y) = 0$ entraîne l'égalité $\sum_{j=0}^{o(\nabla)+k} \nabla \left(\lambda_{j,k}\nabla^j(y)\right) = 0$ qui est la relation de dépendance

$$\sum_{j=0}^{o(\nabla)+k} D(\lambda_{j,k})\nabla^j(y) + \sum_{j=0}^{o(\nabla)+k} \lambda_{j,k}\nabla^{j+1}(y) = 0$$

s'appliquant à $\mathcal{B}_{k+1}$.

Lemme Soient E un K-espace vectoriel muni d'une connexion ∇ de dérivation D sur K, y_0 un vecteur cyclique d'ordre k, si $0 \leq i \leq k-1$ alors $y_i = \nabla^i(y_0)$, nous appelons f_{∇,y_0} l'application linéaire de $V(\nabla, y_0)$ vers $K[D]$ telle que $f_{\nabla,y_0}(y_i) = D^i$, $D\times$ la connexion : $\begin{array}{ccc} K[D] & \to & K[D] \\ P & \mapsto & DP \end{array}$, L_{∇,y_0} l'opérateur $D^k - \sum_{i=0}^{k-1} c_i D^i$ si $f_{\nabla,y_0}(y_k) = \sum_{i=0}^{k-1} c_i y_1$, p_{∇,y_0} la projection canonique de $K[D]$ sur $K[D]/(L_{\nabla,y_0})_g$ où $(L_{\nabla,y_0})_g$ est l'idéal à gauche engendré par L_{∇,y_0} alors il existe une unique connexion $D\times_{\nabla,y_0}$ de $K[D]/(L_{\nabla,y_0})_g$ qui rende le shéma suivant commutatif :

$$\begin{array}{ccc} V(\nabla, y_0) & \xrightarrow{\nabla} & V(\nabla, y_0) \\ \downarrow{\scriptstyle f_{\nabla,y_0}} & & \downarrow{\scriptstyle f_{\nabla,y_0}} \\ K[D] & \xrightarrow{D\times} & K[D] \\ \downarrow{\scriptstyle p_{\nabla,y_0}} & & \downarrow{\scriptstyle p_{\nabla,y_0}} \\ K[D]/(L_{\nabla,y_0})_g & \xrightarrow{D\times_{\nabla,y_0}} & K[D]/(L_{\nabla,y_0})_g \end{array}$$

Preuve : Si $P - P' \in (L_{\nabla,y_0})_g$ alors $\left\{\begin{array}{rcl} P & = & QL_{\nabla,y_0} + R \\ P' & = & Q'L_{\nabla,y_0} + R \end{array}\right.$

puis $\left\{\begin{array}{rcl} DP & = & DQL_{\nabla,y_0} + DR \\ DP' & = & DQ'L_{\nabla,y_0} + DR \end{array}\right.$ donc $DP - DP' = (DQ - DQ')L_{\nabla,y_0} \in (L_{\nabla,y_0})_g$, tous les représentants de la classe de P appartiennent à la classe de DP. Ceci induit sur $K[D]/(L_{\nabla,y_0})_g$ une application unique $D\times_{\nabla,y_0}$: celle qui à la classe de $P \in K[D]$ associe la classe de DP. Comme la classe de la somme $P+Q$ est la somme des classes de P et Q et comme $D_\times$ est additive, $D\times_{\nabla,y_0}$ est additive. Si $\left\{\begin{array}{rcl} P & = & QL_{\nabla,y_0} + R \\ P' & = & Q'L_{\nabla,y_0} + R \end{array}\right.$ et $a \in K$ alors $\left\{\begin{array}{rcl} DaP & = & DaQL_{\nabla,y_0} + aDR + D(a)R \\ DaP' & = & DaQ'L_{\nabla,y_0} + aDR + D(a)R \end{array}\right.$

soit $\left\{\begin{array}{rcl} DaP & = & DaQL_{\nabla,y_0} + (aD + D(a))R \\ DaP' & = & DaQ'L_{\nabla,y_0} + (aD + D(a))R \end{array}\right.$

prouve que $D\times_{\nabla,y_0}$ vérifie bien l'identité de Leibnitz.

De plus il découle aisément de la définition de $D\times_{\nabla,y_0}$ que $D\times_{\nabla,y_0}$ et p_{∇,y_0} commutent : ce qui rend le deuxième shéma commutatif.

Explicitons à présent $D\times_{\nabla,y_0} \circ p_{\nabla,y_0}$: soient $P \in K[D]$ et R le reste de la division euclidienne de P par L_{∇,y_0}, son degré est alors au plus $o(\nabla,y_0)-1$, alors $R = \sum_{i=0}^{o(\nabla,y_0)-1} r_i D^i$ et DP est dans la classe de

$$DR = \sum_{i=0}^{o(\nabla,y_0)-1} D(r_i)D^i + \sum_{i=0}^{o(\nabla,y_0)-1} r_iD^{i+1}$$

Soit à présent $v = \sum_{i=0}^{o(\nabla,y_0)-1} r_iy_i \in V(\nabla, y_0)$ alors $f_{\nabla,y_0} = \sum_{i=0}^{o(\nabla,y_0)-1} r_iD^i$ et $D \times_{\nabla,y_0} \circ p_{\nabla,y_0} \circ f_{\nabla,y_0}(v)$, est la classe de

$$\sum_{i=0}^{o(\nabla,y_0)-1} D(r_i)D^i + \sum_{i=0}^{o(\nabla,y_0)-1} r_iD^{i+1} = D(R)$$

On a aussi

$$\nabla(v) = \sum_{i=0}^{o(\nabla,y_0)-1} D(r_i)y_i + \sum_{i=0}^{o(\nabla,y_0)-1} r_i\nabla(y_i)$$

et sachant que

$$\begin{cases} \nabla(y_i) & = \; y_{i+1} \; si \; i < o(\nabla, y_0) - 1 \\ \nabla(y_{o(\nabla,y_0)-1}) & = \; \nabla^{o(\nabla,y_0)}(y_0) = \sum_{i=0}^{o(\nabla,y_0)-1} c_iy_i \end{cases}$$

on obtient

$$\nabla(v) = \sum_{i=0}^{o(\nabla,y_0)-1} D(r_i)y_i + \sum_{i=0}^{o(\nabla,y_0)-2} r_iy_{i+1} + r_{o(\nabla,y_0)-1} \sum_{i=0}^{o(\nabla,y_0)-1} c_iy_i$$

puis que $p_{\nabla,y_0} \circ f_{\nabla,y_0} \circ \nabla(v)$ est la classe de

$$\sum_{i=0}^{o(\nabla,y_0)-1} D(r_i)D^i + \sum_{i=0}^{o(\nabla,y_0)-1} r_iD^{i+1} + r_{o(\nabla,y_0)-1} \sum_{i=0}^{o(\nabla,y_0)-1} c_iD^i$$

Ceci rend le premier shéma commutatif.
Soit à présent $\phi_{\nabla,y_0} = p_{\nabla,y_0} \circ f_{\nabla,y_0}$ alors ϕ_{∇,y_0}

est K-linéaire comme composée d'applications K-linéaires et, transforme la base $(y_0,\ \ldots,\ \nabla^{o(\nabla,y_0)-1}(y))$ en la base : la famille des classes de $(1,\ D,\ \ldots,\ D^{o(\nabla,y_0)-1})$ c'est donc un isomorphisme. On a la

Propriété : Si D est une dérivation du corps K, E un K-espace vectoriel, ∇ une connexion vectorielle sur E, de dérivation D, y_0 un vecteur cyclique d'ordre $o(\nabla, y_0)$ pour ∇, $L_{\nabla,y_0} = D^{o(\nabla)} - \sum_{i=0}^{o(\nabla,y_0)-1} c_i D^i$ si $\nabla^{o(\nabla)}(y_0) = \sum_{i=0}^{o(\nabla,y_0)-1} c_i \nabla^i(y_0)$; alors il existe un isomorphisme $\phi_{\nabla,y_0}\ :\ V(\nabla, y_0) \to K[D]/(L_{\nabla,y_0})_g$ et une connexion $D\times_{\nabla,y_0}$ qui rendent le shéma suivant commutatif :

$$\begin{array}{ccc}
V(\nabla, y_0) & \xrightarrow{\nabla} & V(\nabla, y_0) \\
\Big\downarrow \phi_{\nabla,y_0} & & \Big\downarrow \phi_{\nabla,y_0} \\
K[D]/(L_{\nabla,y_0})_g & \xrightarrow{D\times_{\nabla,y_0}} & K[D]/(L_{\nabla,y_0})_g
\end{array}$$

Polynômes de connexions vectorielles

Définitions et propriétés

Définitions

Soient E un K-espace vectoriel sur un corps K, D une dérivation sur K, f une application de E dans E et $P = \sum_{i=0}^{n} a_i D^i \in K[D]$ on pose $P(f) = \sum_{i=0}^{n} a_i f^i$ avec, $f_0 = Id_E$ et si $i > 0$

alors $f^i = f \circ f^{i-1}$: on peut alors définir une application $\theta_E \; : \left\{ \begin{array}{ccc} K[D] \times E^E & \to & E^E \\ (P, f) & \mapsto & P(f) \end{array} \right.$ qui est K-linéaire par rapport à la variable P et telle que pour un f donné l'ensemble $\theta_E(K[D], f)$ peut-être muni d'une structure d'algèbre (en général non-commutative) en posant $P(f)Q(f) = PQ(f)$, on l'appelle l'algèbre des polynômes de f.
Exemple : Si $f = \nabla$ une connexion sur le K-espace vectoriel E de dérivation D sur K alors $\theta_E(K[D], \nabla)$ définit l'algèbre des polynômes de ∇.

$P \in K[D]$ est dit **irréductible** s'il n'est pas le produit de deux éléments de $K[D] \backslash \mathcal{U}_{K[D]} = K[D] \backslash K$.
Exemples Tous les $P \in K[D]$ de degré 1.

Propriétés :

Si y est cyclique d'ordre k pour ∇, connexion vectorielle sur E espace vectoriel de corps K de dérivation D alors, si $p_{\nabla,y}$ est la projection de $K[D]$ sur $K[D]/(L_{\nabla,y})_g$, $\phi_{\nabla,y}$ l'isomorphisme de $V(\nabla, y)$ vers $K[D]/(L_{\nabla,y})_g$, alors pour tout polynôme, le shéma qui suit est commutatif :

$$\begin{tikzcd} V(\nabla,y) \arrow[r, "P(\nabla)"] \arrow[d, "\phi_{\nabla,y}"] & V(\nabla,y) \arrow[d, "\phi(\nabla,y)"] \\ K[D]/(L_{\nabla,y})_g \arrow[r, "P(D\times_{\nabla,y})"] & K[D]/(L_{\nabla,y})_g \\ K[D] \arrow[r, "P(D\times)"] \arrow[u, "p_{\nabla,y}"] & K[D] \arrow[u, "p_{\nabla,y}"] \end{tikzcd}$$

Preuve : la commutativité du shéma

$$\begin{tikzcd} V(\nabla,y) \arrow[r, "\nabla"] \arrow[d, "\phi_{\nabla,y}"] & V(\nabla,y) \arrow[d, "\phi_{\nabla,y}"] \\ K[D]/(L_{\nabla,y})_g \arrow[r, "D\times_{\nabla,y}"] & K[D]/(L_{\nabla,y})_g \end{tikzcd}$$

donne $\nabla = \phi^{-1}_{\nabla,y} \circ D \times_{\nabla,y} \circ \phi_{\nabla,y}$ qui, par compositions itérées et combinaison linéaire, devient

$$\forall P \in K[X],\ P(\nabla) = \phi^{-1}_{\nabla,y} \circ P(D\times_{\nabla,y}) \circ \phi_{\nabla,y}$$

rend commutatif le shéma :

$$\begin{tikzcd} V(\nabla,y) \arrow[r, "P(\nabla)"] \arrow[d, "\phi_{\nabla,y}"] & V(\nabla,y) \arrow[d, "\phi_{\nabla,y}"] \\ K[D]/(L_{\nabla,y})_g \arrow[r, "P(D\times_{\nabla,y})"] & K[D]/(L_{\nabla,y})_g \end{tikzcd}$$

La commutativité du shéma

$$\begin{array}{ccc} K[D] & \xrightarrow{D\times} & K[D] \\ \big\downarrow{\scriptstyle p_{\nabla,y_0}} & & \big\downarrow{\scriptstyle p_{\nabla,y_0}} \\ K[D]/(L_{\nabla,y})_g & \xrightarrow{D\times_{\nabla,y}} & K[D]/(L_{\nabla,y})_g \end{array}$$

donne $p_{\nabla,y} \circ D_\times = D \times_{\nabla,y} \circ p_{\nabla,y}$ qui, après composition avec le projecteur $p_{\nabla,y}$ devient

$$D_\times = p_{\nabla,y} \circ D \times_{\nabla,y} \circ p_{\nabla,y}$$

qui, par compositions itérées et combinaison linéaire, devient

$$\forall P \in K[X],\ P\left(D_\times\right) = p_{\nabla,y} \circ P\left(D\times_{\nabla,y}\right) \circ p_{\nabla,y}$$

qui, après composition avec le projecteur $p_{\nabla,y}$ devient

$$\forall P \in K[X],\ p_{\nabla,y} \circ P\left(D_\times\right) = P\left(D\times_{\nabla,y}\right) \circ p_{\nabla,y}$$

rend commutatif le shéma :

$$\begin{array}{ccc} K[D]/(L_{\nabla,y})_g & \xrightarrow{P(D\times_{\nabla,y})} & K[D]/(L_{\nabla,y})_g \\ \big\uparrow{\scriptstyle p_{\nabla,y}} & & \big\uparrow{\scriptstyle p_{\nabla,y}} \\ K[D] & \xrightarrow{P(D\times)} & K[D] \end{array}$$

Polynômes de connection vectorielle annulateurs d'un vecteur, idéaux annulateurs d'un vecteur

Dans tout ce qui suit nous adopterons le vocabulaire suivant : K est un corps de caractéristique

0, D une dérivation sur le corps K, E est un K-espace vectoriel, ∇ une connection de E dans E associée à la dérivation D, y est cyclique d'ordre k pour ∇ si et seulement si le K-espace vectoriel engendré par $\left(\nabla^i(y)\right)_{i\in\mathbb{N}}$ est de dimension k, la famille finie $\left(y,\ \ldots,\ \nabla^{k-1}(y)\right)$ en engendre l'espace vectoriel stable $V(\nabla, y)$ tout en en étant une base. Si $\nabla^k(y) = \sum_{i=0}^{k-1} \nabla^i(y)$ alors on pose $L_{\nabla,y} = D^k - \sum_{i=0}^{k-1} D^k$, la dérivation D définie sur $K[D]$ passe au quotient à gauche sur $K[D]/(L_{\nabla,y})_g$ en $\dot{D}$ avec $\dot{D}(P + (L_{\nabla,y})_g) = D\left((P(mod)_g L_{\nabla,y}\right)$ où $P(mod)_g L_{\nabla,y}$ est le reste de la division euclidienne à gauche de P par $L_{\nabla,y}$, $f_{\nabla,y}$ est l'application linéaire injective de $V(\nabla, y)$ vers $K[D]$ telle que $0 \leq i \leq k-1 \Rightarrow f_{\nabla,y}\left(\nabla^i(y)\right) = D^i$, $p_{\nabla,y}$ est la projection linéaire du K-espace vectoriel $K[D]$ sur le K-espace vectoriel $K[D]/(L_{\nabla,y})_g$, $\phi_{\nabla,y}$ est l'isomorphisme K-linéaire de $V(\nabla, y)$ vers $K[D]/(L_{\nabla,y})_g$ tel que

$$\forall 0 \leq i \leq k-1,\ \phi_{\nabla,y}\left(\nabla^i(y)\right) = \dot{D}^i$$

Polynômes de connection annulateurs d'un vecteur

Lemme : Soit $y \in E$, cyclique d'ordre K pour ∇ alors

$$\forall x \in V(\nabla, y),\ \forall P \in K[D],\ P(\nabla)(x) = \phi_{\nabla,y}^{-1} \circ p_{\nabla,y}\left(P f_{\nabla,y}(x)\right)$$

Preuve : Comme $\phi_{\nabla,y}^{-1} \circ p_{\nabla,y}$ est une application

K-linéaire, il suffit de montrer que :

$\forall x \in V(\nabla, y),\ \forall i \in \mathbb{N},\ \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(D^i f_{\nabla,y}(x)\right)$

Ce que nous faisons par récurrence sur i : y est cyclique d'ordre k alors on peut écrire $x = \sum_{j=0}^{k-1} c_j \nabla^j(y)$ puis :

$$\begin{aligned}
f_{\nabla,y}(x) &= \sum_{j=0}^{k-1} c_j D^j \\
p_{\nabla,y}\left(f_{\nabla,y}(x)\right) &= \sum_{j=0}^{k-1} c_j \dot{D}^j \\
\phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(f_{\nabla,y}(x)\right) &= \sum_{j=0}^{k-1} c_j \phi^{-1}_{\nabla,y}\left(\dot{D}^j\right) \\
&= \sum_{j=0}^{k-1} c_j \nabla^j(y) = x
\end{aligned}$$

ce qui montre le lemme pour $i = 0$.
Supposons à présent que $\phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(D^i f_{\nabla,y}(x)\right)$ alors :

$$\begin{aligned}
\nabla^{i+1}(x) &= \phi^{-1}_{\nabla,y} \circ D \times_{\nabla,y} \circ p_{\nabla,y}\left(D^i f_{\nabla,y}(x)\right) \\
car\ \nabla &= \phi^{-1}_{\nabla,y} \circ D \times_{\nabla,y} \circ \phi_{\nabla,y} \\
&= \phi^{-1}_{\nabla,y} \circ p_{\nabla,y} \circ D \times \left(D^i f_{\nabla,y}(x)\right) \\
car\ D \times_{\nabla,y} \circ p_{\nabla,y} &= p_{\nabla,y} \circ D \times \\
&= \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(D D^i f_{\nabla,y}(x)\right) \\
&= \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(D^{i+1} f_{\nabla,y}(x)\right)
\end{aligned}$$

Définition : Soit $z \in E$, on dit que $P \in K[D]$ est annulateur de z relativement à la connexion ∇ si et seulement si $P(\nabla)(z) = 0$. Pour $z \in E$ l'ensemble des polynômes annulateurs de z relativement à ∇ est un idéal à gauche de $K[D]$.
On vérifie facilement, si P et P' sont des polynômes annulateurs de z, qu'alors $P + P'$, $-P$, QP avec $Q \in K[D]$ sont encore des polynômes annulateurs de z : l'ensemble des polynômes annulateurs de z relativement à la connexion ∇ est donc un idéal à gauche de $K[D]$. D'autre part, du lemme précédent, on déduit la
Propriété : Si $z \in V(\nabla, y)$ alors $P \in K[D]$ est un polynôme annulateur de z relativement à ∇ si et seulement si $L_{\nabla,y}$ divise $Pf_{\nabla,y}$, en particulier si $z = y$ l'ensemble des polynômes annulateurs de y relativement à ∇ est l'idéal à gauche $(L_{\nabla,y})_g$. $L_{\nabla,y}$ est donc le polynôme annulateur de y relativement à ∇ de degré minimum.
Lemme du transport Soit A un anneau euclidien gradué à gauche, soient $f,\ L \in A\backslash\{0\}$ l'ensemble des $P \in A$ tels que $Pf \in (L)_g$ est un idéal dont on note $L : f$ un générateur, on a alors les égalités

$$\begin{cases} (L:f)_g f &= (L)_g \cap (f)_g \\ (f:L)_g L &= (L)_g \cap (f)_g \end{cases}$$

Dans le cas où f et L sont premiers entre eux à

gauche l'idéal $(L : f)_g$ n'est pas nécessairement $(L)_g$ contrairement au cas d'un anneau commutatif euclidien gradué.
Preuve : $I = \{P \in A / Pf \in (L)_g\}$ est un idéal à gauche dont nous appelons $L : f$ un générateur. Un élément de I est un Pf tel qu'il existe $Q \in A$, tel que $Pf = QL$: Pf est un multiple commun de f et L on a donc $If \subset (L)_g \cap (f)_g$. Un élément de $(L)_g \cap (f)_g$ est un Pf tel que $P \in A$ et $Pf \in (L)_g$: c'est Pf où $P \in I$, ce qui donne $(L)_g \cap (f)_g \subset If$. On a donc $If = (L)g \cap (f)_g$ ce qui entraîne $(L : f)_g f = (L)_g \cap (f)_g$ puis, en permutant L et f, $(L : f)_g L = (L)_g \cap (f)_g$.
Lemme du vecteur cyclique : Soit $y \in E$ cyclique d'ordre k pour ∇ et soit $z \in V(\nabla, y)$ alors

- L'idéal annulateur de y relativement à ∇ est l'idéal $(L_{\nabla,y})_g$.
- L'idéal annulateur de z relativement à ∇ est l'idéal $(L_{\nabla,y} : f_{\nabla,y}(z))_g$. Comme c'est aussi l'idéal $(L_{\nabla,z})_g$ on a alors

$$(L_{\nabla,z})_g = (L_{\nabla,y} : f_{\nabla,y}(z))_g$$

Preuve : Soit $z \in V(\nabla, y)$ alors $\forall P \in K[D]$ alors $\forall P \in K[D]$, $P(\nabla)(z) = \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}(Pf_{\nabla,y})$

Comme $\phi_{\nabla,y}$ est un isomorphisme :

$$\begin{aligned} P(\nabla)(z)=0 &\iff p_{\nabla,y}\left(Pf_{\nabla,y}\right)=0 \\ &\iff Pf_{\nabla,y}\in\left(L_{\nabla,y}\right)_g \\ &\iff P\in\left(L_{\nabla,y}:f_{\nabla,y}(z)\right)_g \end{aligned}$$

Si $z\in V(\nabla,y)$ alors $\left(L_{\nabla,y}:f_{\nabla,y}(z)\right)_g$ est l'idéal annulateur de z relativement à ∇, comme cet idéal est aussi $\left(L_{\nabla,z}\right)_g$ on a donc

$$\left(L_{\nabla,z}\right)_g=\left(L_{\nabla,y}:f_{\nabla,y}(z)\right)_g$$

Etude d'une connexion sur un sous-espace cyclique $V(\nabla,y)$

Dans cette partie y est cyclique d'ordre k pour la connexion ∇ et $z\in V(\nabla,y)$

Si $f_{\nabla,y}(z)\vee_g L_{\nabla,y}=1$

Alors $\exists P,Q\in K[D],\ Pf_{\nabla,y}(z)+QL_{\nabla,y}=1$ et appliquant $\phi^{-1}_{\nabla,y}\circ p_{\nabla,y}$ à cette égalité on obtient $P(\nabla)(z)=y$ dont on déduit que

$$\boxed{V(\nabla,z)=V(\nabla,y)}$$

Preuve : ∇ est stable sur $V(\nabla,y)$ donc

$$\begin{aligned} z\in V(\nabla,y) &\Rightarrow \forall i\in\mathbb{N},\ \nabla^i(z)\in V(\nabla,y) \\ &\Rightarrow V(\nabla,z)\subset V(\nabla,y) \end{aligned}$$

∇ étant stable sur $V(\nabla,z)$ on a

$$\forall i\in\mathbb{N},\ \nabla^i(z)\in V(\nabla,z)$$

puis par combinaison linéaire à coefficients sur K, on a $\forall Q \in K[D],\ Q(\nabla)(z) \in V(\nabla, z)$. En particulier pour Q variant dans la famille $\left(D^i P\right)_{i\in\mathbb{N}}$ on obtient $\forall i \in \mathbb{N},\ \nabla^i\left(P(\nabla)(z)\right) \in V(\nabla, z)$ soit $\forall i \in \mathbb{N},\ \nabla^i(y) \in V(\nabla, z)$ qui entraîne que $V(\nabla, y) \subset V(\nabla, z)$
Nous savons que $P(\nabla)(z) = \phi_{\nabla,z}^{-1} \circ p_{\nabla,z}\left(P f_{\nabla,z}(z)\right)$ si on remarque que $f_{\nabla,z}(z) = 1$ et si on effectue la division euclidienne de P par $L_{\nabla,z}$, soit $P = RL_{\nabla,z} + P'$ avec $deg(P') < deg\left(L_{\nabla,z}\right) = k$, on obtient alors

$$\begin{aligned} y = P(\nabla)(z) &= \phi_{\nabla,z}^{-1}\left(p_{\nabla,z}(RL_{\nabla,z}) + p_{\nabla,z}(P')\right) \\ &= \phi_{\nabla,z}^{-1}\left(_{\nabla,z}(P')\right) \\ &= \phi_{\nabla,z}^{-1} \circ p_{\nabla,z}\left(P' f_{\nabla,z}(z)\right) = P'(\nabla)(z) \end{aligned}$$

Mais $P'(\nabla)(z) = y$ s'écrit aussi

$$\phi_{\nabla,y}^{-1} \circ p_{\nabla,y}\left(P' f_{\nabla,y}\right) = \phi_{\nabla,y}^{-1} \circ p_{\nabla,y}(1)$$

soit $\phi_{\nabla,y}^{-1} \circ p_{\nabla,y}\left(P' f_{\nabla,y}(z) - 1\right) = 0$
soit $p_{\nabla,y}\left(P' f_{\nabla,y}(z) - 1\right) = 0$
soit $P' f_{\nabla,y}(z) - 1 = -Q' L_{\nabla,y}$
soit $P' f_{\nabla,y}(z) + Q' L_{\nabla,y} = 1$.
Comme $deg\left(f_{\nabla,y}(z)\right) = deg\left(L_{\nabla,y}\right) = k > 0$ et $deg(P') < k$, cette égalité entraîne

$$\exists P', Q' \in K[D],$$

$$\begin{aligned} (deg(P') < deg\left(L_{\nabla,y}\right)) &\vee\ (deg(Q') < deg\left(f_{\nabla,y}\right)) \\ &\vee\ (P' f_{\nabla,y}(z) + Q' L_{\nabla,y} = 1) \end{aligned}$$

Ce lemme se généralise à tout $L,\ f \in K[D]\backslash K$ par le

Théorème *de Bezout avec limitation des degrés*
Si $f,\ L \in K[D]\backslash K$ vérifient $f \vee_g L = 1$ alors $\exists P,\ Q \in K[D]$ avec $deg(Q) < deg(f)$, $deg(P) < deg(L)$ et $Pf + QL = 1$.

Preuve : On ne perd rien à la généralité de la démonstration si on suppose que $deg(L) = max(deg(L), deg(f)) = k > 0$, on distingue alors deux cas :

(i) $deg(L) > deg(f)$: si $a_k \in K\backslash\{0\}$ est le coefficient de D^k dans L alors $f \vee_g L = f \vee_g a_k^{-1}L = 1$ et on peut écrire $a_n^{-1}L = D^k - \sum_{i=0}^{k-1} c_i D^i$ et $f = \sum_{i=0}^{k-1} b_i D^i$ où les b_i ne sont pas tous nuls. Soit $\mathcal{B} = (e_1,\ \ldots,\ e_k)$ la base canonique de K^k et ∇ la connexion dont la matrice dans $\mathcal{B}$ est la matrice compagnon de dernière colonne $\begin{pmatrix} c_0 \\ \vdots \\ c_{k-1} \end{pmatrix}$ alors e_1 est cyclique d'ordre k pour ∇, $L_{\nabla,e_1} = a_n^{-1}L$ et $f_{\nabla,e_1}\left(\sum_{i=0}^{k-1} b_i e_{i+1}\right) = f$. Nous appliquons le lemme précédent : $\exists P',\ Q' \in K[D],\ P'f + Q'a_k^{-1}L = 1$ et $deg(P') < deg(a_n^{-1}L)$ et $deg(Q') < deg(f)$; le théorème vient alors en posant $P = P'$ et $Q = Q'a_k^{-1}$.

(ii) $deg(L) = deg(f)$: nous posons $L = \sum_{i=0}^{k} a_i D^i$ et $f = \sum_{i=0}^{k} b_i D^i$ avec $a_k \neq 0$, $b_k \neq 0$ et nous considérons R le reste de la division euclidienne à gauche de f par L alors, l'algorithme de calcul de p.g.c.d par divisions euclidiennes indique que $1 = f \vee_g L = R \vee_g L$ il existe donc $P',\ Q' \in K[D]$ avec $deg(Q') < deg(R)$ et $deg(P') < deg(L)$ tels que $P'R + Q'L = 1$. Mais $f = aL + R$ avec $a \in K \backslash \{0\}$, il vient $R = f - aL$ puis $P'f + (Q' - P'a)L = 1$. On pose $P = P'$ et $Q = Q' - P'a$ alors, $deg(P) < deg(L)$ et $deg(Q) < deg(L) = deg(F)$ (puisque $deg(a) = 0$) et $Pf + QL = 1$.

Corollaire : Si $f, L \in K[D] \backslash K$ vérifient $f \vee_g L = d$ alors $\exists P, Q \in K[D]$ avec $deg(Q) < deg(f) - deg(d)$ et $deg(P) < deg(L) - deg(d)$ tels que $Pf + QL = d$.
Preuve : Posons $f = f'd$ et $L = l'd$ alors $f' \vee_g L' = 1$ donc $\exists P',\ Q' \in K[D]$ avec $deg(Q) < deg(f') = deg(f) - deg(d)$ et $deg(P) < deg(L') = deg(L) - deg(d)$ et $Pf' + QL' = 1$.

$$Pf' + QL' = 1 \Rightarrow Pf'd + QL'd = Pf + QL = d$$

Nous pouvons alors énoncer le

Corollaire des degrés : $\forall P, Q \in K[D]$

$deg\,(P \vee_g Q) + deg\,(P \wedge_g Q) = deg(P) + deg(Q)$

Preuve : on ne perd rien à la généralité du raisonnement si on suppose que $deg(P) \geq deg(Q)$.

- si $P \vee_g Q = 1$
  - si $deg(P) > deg(Q)$ alors, si on pose $k = deg(P)$ et si $a_k \in K\backslash\{0\}$ est le coefficient dominant de P, on peut écrire

$$\begin{cases} P \wedge_g Q &=& a_k^{-1} P \wedge_g Q \\ P \vee_g Q &=& a_k^{-1} P \vee_g Q = 1 \\ a_k^{-1} P &=& D^k - \sum_{i=0}^{k-1} c_i D^i \\ Q &=& \sum_{i=0}^{k-1} b_i D^i \end{cases}$$

Soit $\mathcal{B} = (e_1, \ \ldots, \ e_k)$ la base canonique de K^n et ∇ la connexion dont la matrice dans la base $\mathcal{B}$ est la matrice compagnon de dernière colonne le vecteur $\begin{pmatrix} c_0 \\ \ldots \\ c_k \end{pmatrix}$ alors e_1 est cyclique pour ∇, $L_{\nabla, e_1} = a_k^{-1} P$ et $f_{\nabla, e_1}\left(\sum_{i=0}^{k-1} b_i e_{i+1}\right) = Q$. Si nous posons $z = \sum_{i=0}^{k-1} b_i e_{i+1}$ alors, d'après le lemme du transport, $\exists a \in K[D]\backslash \{0\}$

$$L_{\nabla, z} f_{\nabla, e_1}(z) = a f_{\nabla, e_1}(z) \wedge_g L_{\nabla, e_1}$$

On a alors

$$
\begin{aligned}
deg\,(af_{\nabla,e_1}(z) \wedge_g L_{\nabla,e_1}) &= deg\,(P \wedge_g Q) \\
&= deg\,(L_{\nabla,z} f_{\nabla,e_1}(z)) \\
&= deg\,(L_{\nabla,z}) + deg\,(f_{\nabla,e_1}(z)) \\
&= deg(P) + deg(Q) \\
&= deg(P) + deg(Q) \\
&\quad -deg\,(P \vee_g Q)
\end{aligned}
$$

qui donne le corollaire.

- si $deg(P) = deg(Q)$ alors on pose $k = deg(P)$, le corollaire des degrés étant trivial si $k = 0$, on suppose que $k > 0$ et on pose $a_k \neq 0$, $b_k \neq 0$ les coefficients dominants de P, Q, $L = a_k^{-1}P$ et $f = b_k^{-1}Q$. Puisque ces polynômes sont unitaires, la division euclidienne à gauche de L par f donne $L = f + R$ avec $deg(R) < k$. Les *tautologies* $\forall P$,

$$
\begin{aligned}
Pf = PL - PR &\Leftrightarrow PR = PL - Pf \\
&\Leftrightarrow PL = PR + Pf
\end{aligned}
$$

se spécialisent sur $K[D]$ en les égalités ensemblistes $(L : f)_g = (L : R)_g$ et $(f : L)_g = (f : R)_g$. Le lemme du transport, appliqué à L et f, s'écrit

$$\begin{aligned}(L)_g \cap (f)_g &= (L:f)_g f \\ &= (L:R)_g f \\ &= (f:L)_g L \\ &= (f:R)_g L\end{aligned}$$

Remarquons que R est à la fois le reste de la division de L par f et de f par L. L'algorithme des divisions euclidiennes à gauche donne à la fois $\begin{cases} 1 = L \vee_g f = f \vee_g R \\ 1 = f \vee_g L = L \vee_g R \end{cases}$
De $deg(R) < deg(L)$ et $L \vee_g R = 1$ on déduit, d'après l'item qui précède, la suite d'égalités équivalentes

$$\begin{aligned}
deg((L:R)R) + deg(L \vee_g R) &= deg(R) + deg(L) \\
deg((L:f)R) + deg(L \vee_g f) &= deg(R) + deg(L) \\
deg(L:f) + deg(R) + deg(L \vee_g f) &= deg(R) + deg(L) \\
deg(L:f) + deg(f) + deg(L \vee_g f) &= deg(L) + deg(f) \\
deg(L \wedge_g f) + deg(L \vee_g f) &= deg(L) + deg(f)
\end{aligned}$$

Nous concluons en prouvant l'égalité $(P:Q)_g = (P':Q')_g$:

$$\begin{aligned}
(P':Q')_g &= \{\mathcal{P} \in K[D] / \ \mathcal{P}Q' \in (P')_g\} \\
&= \{\mathcal{P} \in K[D], \ \exists \mathcal{Q} \in K[D] / \mathcal{P}Q' = \mathcal{Q}P'\} \\
&= \{\mathcal{P} \in K[D], \ \exists \mathcal{Q} \in K[D] / \mathcal{P}Q'd = \mathcal{Q}Pd'\} \\
&= \{\mathcal{P} \in K[D], \ \exists \mathcal{Q} \in K[D] / \mathcal{P}Q = \mathcal{Q}P\} \\
&= \{\mathcal{P} \in K[D] / \ \mathcal{P}Q \in (P)_g\} \\
&= (P:Q)_g
\end{aligned}$$

Si $f_{\nabla,y}(z) \vee_g L_{\nabla,y} = d \neq 1$

Soit $\xi = \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}(d) \in V(\nabla, y)$ **alors** ξ **est cyclique pour** ∇ **d'ordre** $k - deg(d)$ **et donc** $V(\nabla, \xi) \subsetneq V(\nabla, y)$

Preuve : Si $f_{\nabla,y}(z) \vee_g L_{\nabla,y} = d \neq 1$ alors

$$\exists P, Q \in K[D] \left\{ \begin{array}{lcl} d & = & P f_{\nabla,y}(z) + Q L_{\nabla,y} \\ deg(P) & < & deg\left(L_{\nabla,y}\right) - deg(d) \\ deq(Q) & < & deg\left(f_{\nabla,y}\right) - deg(d) \end{array} \right.$$

Soit ξ l'image de d par $\phi^{-1}_{\nabla,y} \circ p_{\nabla,y}$ alors $\xi = P_{\nabla}(z)$. Comme $deg(d) \leq f_{\nabla,z} \leq k-1$, on peut écrire $d = \sum_{i=0}^{k-1} d_i D^i$ puis

$$\xi = \sum_{i=0}^{k-1} d_i \phi^{-1}_{\nabla,y} \circ p_{\nabla,y}\left(D^i\right) = \sum_{i=0}^{k-1} d_i \nabla^i(y)$$

puis $f_{\nabla,y}(\xi) = \sum_{i=0}^{k-1} d_i D^i = d$. $\mathcal{P} \in K[D]$ est annulateur de ξ relativement à ∇ si et seulement si $\mathcal{P} f_{\nabla,y}(\xi) \in \left(L_{\nabla,y}\right)_g$ c'est à dire si et seulement si il appartient à l'idéal $\left(L_{\nabla,y} : d\right)_g$: le polynôme annulateur de ξ relativement à ∇ de degré minimum est $L_{\nabla,y} : d$ dont le degré est déterminé par la relation

$$\left(\left(L_{\nabla,y} : d\right) d\right)_g = \left(L_{\nabla,y}\right)_g \cap (d)_g = \left(L_{\nabla,y}\right)_g$$

qui donne $deg(d) + deg\left(L_{\nabla,y} : d\right) = k$ soit $deg\left(L_{\nabla,y} : d\right) = k - deg(d)$ qui est l'ordre de ξ.

Si $L_{\nabla,y}$ est irréductible

Lemme : Soit $P \in K[D]$ alors P est irréductible si et seulement si

$$\forall Q \in P[D]\ deg(Q) < deg(P) \Rightarrow P \vee_g Q = 1$$

Preuve :

- Si P n'est pas irréductible : $\exists R,\ Q \in K[D] \backslash K\ P = QR$, on a alors $0 < deg(R) < deg(P)$ et $R \vee_g P = aR$ avec $a \in K \backslash \{0\}$ soit $R \vee_g P \neq 1$
- Si

  $$\exists Q \in P[D]\,(deg(Q) < deg(P)) \wedge (P \vee_g Q \neq 1)$$

  alors $R = deg(P \vee_g Q) > 0$ et c'est un diviseur à gauche de P donc $\exists \mathcal{Q} \in K[D],\ P = \mathcal{Q}R$, $deg(\mathcal{Q}) > 0$ puisque $deg(R) < deg(P)$. P, le produit de deux éléments de $K[D] \backslash K$, n'est donc pas irréductible.

Théorème Si y et cyclique d'ordre k et $L_{\nabla,y}$ est irréductible alors

- $\forall z \in V(\nabla, y)$, z est cyclique d'ordre k (et donc $V(\nabla, y) = V(\nabla, z)$).
- $\forall z \in V(\nabla, y)$, $L_{\nabla,z}$ est irréductible.

Preuve :

- Soit $z \in V(\nabla, y)$ alors

$$deg\,(f_{\nabla,y}(z)) \leq k-1 < k = deg(L_{\nabla,y})$$

  $L_{\nabla,y}$ est irréductible donc $f_{\nabla,y}(z) \vee_g L_{\nabla,y} = 1$ ce qui entraîne, d'après ce qui précède, $V(\nabla, z) = V(\nabla, y)$ et donc $dim\,(V(\nabla, z)) = k$ ce qui est équivalent à z cyclique d'ordre k.

- Supposons que $L_{\nabla,z}$ ne soit pas irréductible alors $\exists L', d \in K[D]\backslash K,\ L_{\nabla,z} = L'd$. Posons $d = \sum_{i=0}^{deg(d)} d_i D^i$ et $\omega = \sum_{i=0}^{deg(d)} d_i \nabla^i(z)$ alors $f_{\nabla,z}(\omega) = d$, on a alors $f_{\nabla,z}(\omega) \vee_g L_{\nabla,z} = d$. D'après ce qui précède si $\xi = \phi_{\nabla,z}^{-1} \circ p_{\nabla,z}(d)$ alors

$$dim(V(\nabla, \xi)) = dim(V(\nabla, z)) - deg(d) < dim(V(\nabla, z)) = k$$

  mais, comme $\xi \in V(\nabla, y)$ on a $dim(V(\nabla, \xi)) = k$ ce qui est contradictoire.

Sous-espaces vectoriels stables de $V(\nabla, y)$

Idéaux associés aux sous-espaces stables de $V(\nabla, y)$

Propriété : Un sous-espace vectoriel V d'un K-espace vectoriel E muni d'une connexion vectorielle ∇ est stable pour ∇ si et seulement si $V(\nabla) \subset V$. On a la propriété :

- Soit $y \in E$ et I un idéal à gauche de $K[D]$ alors l'ensemble $I(y) = \{P(\nabla)(y)/y \in I\}$ est un sous-espace vectoriel stable pour ∇.
- Si V est un sous-espace vectoriel de E stable pour ∇ et s'il existe $y \in E$ tel que $V \subset V(\nabla, y)$ alors il existe I un idéal à gauche de $K[D]$ tel que $V = I(y)$.

Preuve :

- Soient $x, z \in I(y)$, $\lambda, \mu \in K$ alors $\exists P, Q \in I$, $x = P(\nabla)(y)$ $z = Q(\nabla)(y)$ et on a :
  - $0 \in I$ donc $0 = 0(\nabla)(y) \in I(y)$
  -
  $$\begin{aligned} \lambda x + \mu y &= (\lambda P(\nabla)(y) + \mu Q(\nabla)(y)) \\ &= (\lambda P + \mu Q)(\nabla)(y) \end{aligned}$$
  I est un idéal donc $\lambda P + \mu Q \in I$ et donc $\lambda x + \mu y \in I(y)$: ce qui achève de montrer que I est un K-espace vectoriel.
  - I est un idéal donc
  $$P \in I \Rightarrow DP \in I \Rightarrow \nabla\left(P(\nabla(y))\right) = \nabla(x) \in I(y)$$
  ceci étant vrai pour tout x prouve que $I(y)$ est stable pour ∇.
- Soit V un sous-espace vectoriel de E tel que $V \subset V(\nabla, y)$ et
$$I = \{P \in K[D]/P(\nabla)(y) \in V\}$$

alors $0 \in I$ puisque $V \ni 0 = 0(\nabla)(y)$, si $P, Q \in I$ alors

$$(P+Q)(\nabla)(y) = P(\nabla)(y) + Q(\nabla)(y) \in V$$

puisque $P(\nabla)(y) \in V$ et $Q(\nabla)(y) \in V$ prouve que $P+Q \in I$,

$$(-P)(\nabla)(y) = -P(\nabla)(y) \in V$$

puisque $P(\nabla)(y) \in V$ et $P(\nabla)(y) \in V$ prouve que $-P \in I$ et $\forall R \in K[D]$

$$(R.P)(\nabla)(y) = R(\nabla)\left(P(\nabla)(y)\right) \in V$$

puisque $P(\nabla)(y) \in V$ et V stable pour ∇ prouve que $R.P \in I$: ceci prouve que I est un idéal. Nous prouvons à présent que $V = I(y)$: $I(y)$ est un sous-espace vectoriel de $V(\nabla, y)$ stable pour ∇ et, par construction, $\forall P \in I(y)$, $P(\nabla)(y) \in V$. On a donc $I(y) \subset V$. $\forall z \in V$, $z \in V(\nabla, y)$, donc $\exists P_z$, $z = P_z(\nabla)(y)$ donc $z \in I(y)$: ceci étant vrai pour tout z dans V on a $V \subset I(y)$.

Lemme : Soient F, G deux sous-espaces vectoriels de E, on suppose que

$$(\exists y \in E)\ F, G \subset V(\nabla, y)$$

alors si I et J sont des idéaux à gauche de $K[D]$ tels que $F = I(y)$ et $G = J(y)$ alors $F + G = (I+J)(y)$.

Preuve : Soit $z \in F + G$ alors $z = w + x$ avec $w \in F = I(y)$ et $x \in G = J(y)$, donc $(\exists (P, Q) \in I \times J),\ (w, x) = (P(\nabla)(y), Q(\nabla)(y))$. On a alors $z = (P + Q)\,(\nabla)(y)$ avec $P+Q \in I+J$ soit $z \in (I + J)\,(y)$.
Si $z \in (I + J)(y)$ alors $z = (P + Q)(\nabla)(y)$ avec $(P, Q) \in I \times J$, soit $z = w + x$ où $w = P(\nabla)(y) \in F$ et $x = Q(\nabla)(y) \in G$.
Lemme : Soient y cyclique d'ordre k pour ∇, E, F deux espaces vectoriels tels que $E,\ F \subset V(\nabla, y)$ alors, si I et J sont des idéaux à gauche de $K[D]$ tels que $E = I(y)$ et $F = J(y)$, $E = F$ si et seulement si $\left\{ \begin{array}{lcl} I & \subset & J + (L_{\nabla,y})_g \\ J & \subset & I + (L_{\nabla,y})_g \end{array} \right.$
Preuve : On montre que

$$E \subset F \Rightarrow I \subset J + (L_{\nabla,y})_g$$

Chacune des propositions est équivalente à celle qui la précède :

- $\forall x \in E,\ x \in F$
- $\forall P \in I, \exists Q \in J,\ P(\nabla)(y) = Q(\nabla)(y)$
- $\forall P \in I, \exists Q \in J, R \in K[D],\ P = Q + RL_{\nabla,y}$
- $I \subset J + (L_{\nabla,y})_g$

et en permutant E et F, I et J, chacune des propositions suivantes est équivalente à celle qui la précède :

- $\forall x \in F,\ x \in E$
- $\forall P \in J, \exists Q \in I,\ Q(\nabla)(y) = P(\nabla)(y)$

- $\forall P \in J, \exists Q \in I, R \in K[D],\ Q = P + RL_{\nabla,y}$
- $J \subset I + \left(L_{\nabla,y}\right)_g$

Définition et propriété : Soit E un espace vectoriel de dimension finie stable pour ∇, un sous-espace vectoriel M de E non réduit à $\{0\}$ est dit minimal s'il est minimal pour l'inclusion dans l'ensemble des sous-espaces vectoriels de E stables pour ∇ et non réduits à $\{0\}$. Pour E, stable et de dimension finie, il existe des sous-espaces vectoriels stables et minimaux non réduits à $\{0\}$.
Les assertions suivantes sont équivalentes :

(i) M est un sous-espace vectoriel de E stable et minimum non réduit à $\{0\}$.

(ii) $\forall z \in M \backslash \{0\}, M = V(\nabla, z)$ et $L_{\nabla,z}$ est irréductible.

(iii) $\exists z \in M \backslash \{0\}, M = V(\nabla, z)$ et $L_{\nabla,z}$ est irréductible.

Preuve : L'ensemble des suites $(V_i)_i$ -nécessairement finies d'au plus $dim(E)$ termes- de sous-espaces vectoriels stables pour ∇ : $(V_i)_i = (V(\nabla, y_i))_i$ avec $y_i \in E \backslash \{0\}$, strictement décroissantes pour l'inclusion n'est pas vide car il contient la suite à un seul terme $V_0 = V(\nabla, y_0)$ avec $y_0 \in E\backslash\{0\}$. Considérons une suite $(W_i)_i$ à $k \leq dim(E)$ termes pour laquelle la longueur- i.e. le nombre de termes de la suite- est le maximum de la longueur de telles suites $(V_i)_i$, alors W_k est un sous-espace vectoriel de E stable et non réduit à $\{0\}$ et nous prouvons que W_k est minimal : dans le cas contraire, il existe $y_{k+1} \in E\backslash\{0\}$ tel que $W_{k+1} = V(\nabla, y_k) \subset W_k$ et k n'est pas le maximum.

Nous prouvons par l'absurde que $(i) \Rightarrow (ii)$: supposons (i) et $\exists z \in M,\ L_{\nabla,z}$ non irréductible alors d'après la contraposée du théorème de la page 44 il existe dans M un vecteur w cyclique non nul d'ordre plus $l < k$ le sous-espace vectoriel de M de base $(w, \ldots,\ \nabla^{l-1}(w))$ est stable pour ∇ de dimension $l < k = dim(M)$ et M n'est pas minimal.

$(ii) \Rightarrow (iii)$ parce que M n'est pas réduit à 0.

Nous prouvons par l'absurde que $(iii) \Rightarrow (i)$: supposons (iii) et M non stable ou non minimum. D'après le théorème de la page 44 tout vecteur z non nul de M est cyclique d'ordre $deg\,(L_{\nabla,z})$ et l'ensemble des espaces vectoriels $\{V(\nabla, z)/z \in M\}$ est un singleton $\{N\}$ stable pour ∇ avec $N \subset M$. Si $N = M$ comme M n'est pas minimal il existe un sous espace vectoriel stable minimal de M de dimension strictement plus petite que M qui ne peut-être que N ce qui contredit que $N = M$. Si $N \neq M$ alors si on remarque que, par définition de N- puisque $\forall z,\ z \in V(\nabla, z)$- N contient M ce qui contredit $N \subset M$ et $N \neq M$. Par impossibilité du tiers exclus entre $N = M$ et $N \neq M$ M est stable minimum.

Lemme : Soit V un espace vectoriel de dimension finie différente de 1 sur K supposé de dimension non finie sur son corps des constantes, si V est stable minimal pour une connexion ∇ non nilpotente alors l'ensemble $\{L_{\nabla,u}/u \in V\}$ n'est pas fini.

Preuve : Supposons que l'ensemble $\{L_{\nabla,u}/u \in V\}$ soit fini et égal à $\{L_1,\ \ldots,\ L_s\}$ alors si $P = L_1 \wedge_g \cdots \wedge_g L_s$ on a

$$\forall u \in V,\ P(\nabla)(u) = 0$$

et en particulier :

$$\forall \lambda \in K,\ \forall u \in V,\ P(\nabla)(\lambda u) = 0$$

Soit ϕ l'homomorphisme d'anneau de $\mathbb{Z}$ vers K tel que si $n > 0$ alors $\phi(n) = \underbrace{1 + \cdots + 1}_{n\ fois}$ alors on pose pour des entiers n, k tels que $n \geq k \geq 0$ $\mathbf{C}_n^k = \phi\left(C_n^k\right)$. Par application de ϕ : indépendamment de la caractéristique de K la proposition qui suit est vraie :

$$(\forall k, n \in \mathbb{N}),\ k+1 \leq n \Rightarrow \mathbf{C}_{n+1}^{k+1} = \mathbf{C}_n^k + \mathbf{C}_n^{k+1}$$

Grâce à elle on peut obtenir, par récurrence sur k, la proposition :

$$(\forall k \in \mathbb{N}),\ (\lambda \in K) \wedge (u \in V) \Rightarrow \nabla^k(\lambda u) = \sum_{j=0}^{k} \mathbf{C}_k^j D^j(\lambda) \nabla^{k-j}(u)$$

Pour $j \in \mathbb{N}$ et $P \in K[D]$ nous notons $P^{(j)}$ l'image de P par l'application linéaire définie sur la base $\left(D^k\right)_{k \in \mathbb{N}}$ par $(D^k)^{(j)} = 0$ si $j \geq k$ et $(D^k)^{(j)} = \mathbf{C}_k^j D^{k-j}$ si $j \leq k$ alors on a la proposition :

$$(\forall k \in \mathbb{N}),\ (\lambda \in K) \wedge (u \in V) \Rightarrow \nabla^k(\lambda u) = \sum_{j=0}^{k} D^j(\lambda) (D^k)^{(j)}(\nabla)(u)$$

puis par linéarité on a la proposition : $(\forall k \in \mathbb{N})$,

$$(\lambda \in K) \wedge (u \in V) \Rightarrow P(\nabla)(\lambda u) = \sum_{j=0}^{deg(P)} D^j(\lambda) P^{(j)}(\nabla)(u)$$

Pour $P = L_1 \wedge_g \cdots \wedge_g L_s$, et comme $\forall u \in V$, $P(\nabla)(u) = 0$, on obtient

$$\forall \lambda \in K,\ \forall u \in V,\ P(\nabla)(\lambda u) = \sum_{j=1}^{deg(P)} D^j(\lambda) P^{(j)}(\nabla)(u)$$

Si $L_1 \wedge_g \cdots \wedge_g L_s = \sum_{k=0}^{deg(P)} a_k D^k$ on a : si $j > deg(P)$ alors $P^{(j)} = 0$ sinon

$P^{(j)} = \sum_{k=j}^{deg(P)} \mathbf{C}_k^j a_k D^{k-j}$, de sorte que

$$\forall \lambda \in K,\ \forall u \in V,\ 0 = P(\nabla)(\lambda u) = \sum_{j=1}^{deg(P)} D^j(\lambda) \sum_{k=j}^{deg(P)} \mathbf{C}_k^j a_k \nabla^{k-j}(u)$$

$$\forall \lambda \in K,\ \forall u \in V,\ 0 = \sum_{j=1}^{deg(P)} \sum_{k=j}^{deg(P)} D^j(\lambda) \mathbf{C}_k^j a_k \nabla^{k-j}(u)$$

On pose $l = k - j$ on a alors

$$\forall \lambda \in K,\ \forall u \in V,\ 0 = \sum_{l=0}^{deg(P)-1} \sum_{k=l+1}^{deg(P)} D^{k-l}(\lambda) \mathbf{C}_k^{k-l} a_k \nabla^l(u)$$

$$\forall \lambda \in K,\ \forall u \in V,\ 0 = \sum_{l=0}^{deg(P)-1} \left(P^{(l)}(\lambda) - a_l \right) \nabla^l(u)$$

Quelque soit le choix de $\lambda \in K$ le polynôme $\sum_{l=0}^{deg(P)-1} \left(P^{(l)}(\lambda) - a_l \right) D^l$ annule tout u dans V, il annule en particulier les $u \in V$ tels que $L_{\nabla,u} = L_i$ pour $i = 1, \ldots, s$. Pour $i = 1,\ \ldots,\ s$ c'est un multiple de L_i et donc de $P = L_1 \wedge_g \cdots \wedge_g L_s$. Mais puisque ce polynôme est de degré $deg(P) - 1 < deg(P)$ il est nul et on a

$$\forall \lambda \in K,\ \forall l \in \{0, \ldots, deg(P)-1\},\ P(l)(\lambda) - a_l = 0$$

soit

$$\forall \lambda \in K,\ \forall l \in \{0, \ldots, deg(P) - 1\},\ P(l)(\lambda) = a_l$$

En remarquant que $P^{(l)}(\lambda+\lambda) = P^{(l)}(\lambda)+P^{(l)}(\lambda)$ pour tout $\lambda \in K$ on obtient, indépendamment de la caractéristique de K, $a_l = a_l+a_l$, et donc $a_l = 0$, pour $k = 0, \ldots, \deg(P)-1$. P qui est unitaire est donc égal à $D^{deg(P)}$. Comme $P(\nabla)(u) = 0, \ \forall u \in V$ on a $\nabla^{deg(P)}(u) = 0, \ \forall u \in V$: la connexion est nilpotente.

Lemme du sous-recouvrement stable : Soient $y \in E$ et V un sous-espace vectoriel de $V(\nabla, y)$ stable pour ∇, p_V la projection canonique de
$V(\nabla, y)$ sur $V(\nabla, y)/V$ alors il n'existe qu'une connexion ∇/V vers $V(\nabla, y)/V$ qui rende commutatif les shémas :

$$\begin{array}{ccc} V(\nabla, y) & \xrightarrow{\nabla} & V(\nabla, y) \\ \downarrow{\scriptstyle p_V} & & \downarrow{\scriptstyle p_V} \\ V(\nabla, y)/V & \xrightarrow{\nabla/V} & V(\nabla, y)/V \end{array}$$

$\forall P \in K[D]$:

$$\begin{array}{ccc} V(\nabla, y) & \xrightarrow{P(\nabla)} & V(\nabla, y) \\ \downarrow{\scriptstyle p_V} & & \downarrow{\scriptstyle p_V} \\ V(\nabla, y)/V & \xrightarrow{P(\nabla/V)} & V(\nabla, y)/V \end{array}$$

Preuve : Soient $x, \ z \in V(\nabla, y)$, si $x - z \in V$

alors $\nabla(x-z) \in V$ soit $\nabla(x) - \nabla(z) \in V$: il existe donc une seule application ∇/V de $V(\nabla, y)/V$ vers $V(\nabla, y)/V$ qui rende le premier shéma commutatif : c'est l'application qui à la classe de x *modulo* V, notée x/V, associe la classe de $\nabla(x)$ *modulo* V : $\nabla/V(x/V)$. Cette application est une connexion vectorielle : soient $x,\ z \in V(\nabla, y)$ alors $\nabla(x+z) - \nabla(x) - \nabla(z) = 0 \in V$ ce qui prouve que ∇/V est additive. Soient $x,\ a \in V(\nabla, y) \times K$ alors $\nabla(ax) - a\nabla(x) - D(a)x = 0 \in V$ ce qui prouve que $\nabla/V(ax) - a\nabla/V(x) - D(a)x = 0$. Nous *déduisons par combinaison linéaire*

$$\forall P \in K[D],\ p_V \circ P(\nabla) = P(\nabla/V) \circ p_V$$

de $\forall n \in \mathbb{N},\ p_V \circ \nabla^n = (\nabla/V)^n \circ p_V$ qui se montre par une récurrence élémentaire. Cette assertion est vraie pour $n = 0,\ 1$, supposons la vraie pour $n \in \mathbb{N}$ alors :

$$\begin{aligned} p_V \circ \nabla^{n+1} &= p_V \circ \nabla^n \circ \nabla \\ &= (\nabla/V)^n \circ p_V \circ \nabla \\ &= (\nabla/V)^n \circ \nabla/V \circ p_V \\ &= (\nabla/V)^{n+1} \circ p_V \end{aligned}$$

Du lemme du sous-recouvrement stable se déduit cette relation aux cousines : pour tout vecteur cyclique y d'ordre fini k relativement à une connexion vectorielle ∇, le polynôme annula-

teur $L_{\nabla/V,y/V}$ de sa projection canonique sur un sous-espace vectoriel stable V divise à gauche le polynôme annulateur du vecteur cyclique et si le sous-espace vectoriel V est stable minimum alors le polynôme annulateur $L_{\nabla/V,y/V}$ est irréductible, la connexion vectorielle sur ce sous-espace est alors qualifiée de connexion irréductible. Soient y cyclique pour ∇ et $V \subset V(\nabla, y)$ stable

$$\exists P \in K[D],\ P[\nabla](y) = 0$$
$$\Downarrow$$
$$0 = p_V \circ P(\nabla)(y) = P(\nabla/V)(y/V) = 0$$

Nous en déduisons, sur les idéaux annulateurs de y et y/V, $\left(L_{\nabla/V,y/V}\right)_g \subset \left(L_{\nabla,y}\right)_g$ soit $\exists H_y \in K[D],\ L_{\nabla,y} = H_y L_{\nabla,y/V}$. Supposons à présent que $V \subsetneq V(\nabla, y)$, alors $L_{\nabla,y/V}(y/V) = 0$ équivaut à $v = L_{\nabla/V,V}(y) \in V\backslash\{0\}$ -v n'est pas nul en raison du fait que

$$dim(V(\nabla, y)/V) = deg(L_{\nabla/y/V}) < deg(L_{\nabla,y}) = dim(V(\nabla, y))$$

et l'égalité $L_{\nabla,y}(\nabla)(y) = 0$ devient l'égalité $H_y(\nabla)(v) = 0$ qui entraîne $H_y \in (L_{\nabla,v})_g$. Mais comme l'idéal $(L_{\nabla,y})_g$ est principal et $deg(H_y) = deg(L_{\nabla,vV})$: $\exists a \in K\{0\}$, $H_y = aL_{\nabla,v}$. L'égalité $L_{\nabla,y} = H_y L_{\nabla,y/V}$ devient $L_{\nabla,y} = aL_{\nabla,v}L_{\nabla/y,y/V}$ et puisque $L_{\nabla,y}$, $L_{\nabla,v}$,

$L_{\nabla/y,y/V}$ sont unitaires elle devient

$$L_{\nabla,y} = L_{\nabla,v} L_{\nabla/y,y/V}$$

Nous en déduisons le

Lemme : Soit E un K-espace vectoriel et une connexion vectorielle ∇ sur E relative à la dérivation D sur K, si $\exists z \in E\backslash\{0\}$ et un sous-espace vectoriel V de E stable minimum pour ∇ tel que $V \subsetneq E$ et $E = V \oplus V(\nabla, z)$ alors, si $y = z + v$ où $v \in V\backslash\{0\}$ alors

- $L_{\nabla,y} = L_{\nabla,z} \wedge_g L_{\nabla,v}$
- – Soit $L_{\nabla,z} \vee_g L_{\nabla,v} \neq 1$ et $L_{\nabla,y} = L_{\nabla,z}$.
  – Soit $L_{\nabla,z} \vee_g L_{\nabla,v} = 1$ et $E = V(\nabla, y)$.

Preuve : Si $y = z + v$ alors si P est un polynôme annulateur de y relativement à ∇ alors $0 = P(\nabla)(y) = P(\nabla)(z) + P(\nabla)(v)$ et comme $P(\nabla)(v) \in V$ et $P(\nabla)(z)$ sont dans deux sous-espaces vectoriels supplémentaire alors $P \in (L_{\nabla,z})_g$ et $P \in (L_{\nabla,v})_g$ donc $P \in (L_{\nabla,z} \wedge_g L_{\nabla,v})_g$. En particulier $L_{\nabla,y} \in (L_{\nabla,z} \wedge_g L_{\nabla,v})_g$: donc $L_{\nabla,z} \wedge_g L_{\nabla,v}$ divise à gauche $L_{\nabla,y}$. Soit à présent un polynome $P \in (L_{\nabla,z} \wedge_g L_{\nabla,v})_g$: P est multiple à gauche de $L_{\nabla,z}$ donc $P(\nabla)(z) = 0$, P est multiple à gauche de $L_{\nabla,v}$ donc $P(\nabla)(v) = 0$, il suit que $P(\nabla)(y) = P(\nabla)(z) + P(\nabla)(v) = 0$ donc $L_{\nabla,y}$ divise à gauche P. Ceci prouve que les idéaux $(L_{\nabla,y})_g$ et $(L_{\nabla,z} \wedge_g L_{\nabla,v})_g$ sont égaux, on

a donc l'égalité de leur représentant unitaire soit $L_{\nabla,y} = L_{\nabla,z} \wedge_g L_{\nabla,v}$.
Si $L_{\nabla,z} \vee_g L_{\nabla,v} = 1$ alors, par le corollaire des degrés,

$$\begin{aligned} deg(L_{\nabla,y}) &= deg(L_{\nabla,z}) + deg(L_{\nabla,v}) \\ &= dim(V) + dim(V(\nabla, z)) + dim(V) \\ &= dim(E) \end{aligned}$$

ce qui prouve que $E = V(\nabla, y)$ puisque $V(\nabla, y) \subset E$.
Si $L_{\nabla,z} \vee_g L_{\nabla,v} = d \neq 1$ alors $d \notin K$ est diviseur de $L_{\nabla,v}$ irréductible : c'est $L_{\nabla,v}$. $L_{\nabla,v}$ est un diviseur de $L_{\nabla,z}$, on a donc $L_{\nabla,z} = \mathcal{P} L_{\nabla,v}$ puis

$$\begin{aligned} L_{\nabla,z}(\nabla)(y) &= L_{\nabla,z}(\nabla)(z) + \mathcal{P} L_{\nabla,v}(\nabla)(v) \\ &= 0 + 0 = 0 \end{aligned}$$

$L_{\nabla,y}$ divise à gauche $L_{\nabla,z}$. Soit à présent $\mathcal{Q} \in K[D]$ tel que $\mathcal{Q}(\nabla)(y) = 0$ alors $\mathcal{Q}$ divise $L_{\nabla,z} \wedge_g L_{\nabla,v} = L_{\nabla,z}$.
Lemme d'Euclide irréductible : Soient $P,\ P_1,\ P_2 \in K[D]$ irréductibles et unitaires, si P divise à gauche $P_1 \wedge_g P_2$ alors $P = P_1$ ou $P = P_2$.
Preuve : Sans perte de généralité nous supposerons que $deg(P_1) = n_1 \geq n_2 = deg(P_2)$.

- Si $P_1 = P_2$ alors $P_1 \wedge_g P_2 = P_1 = P_2$ et si P divise à gauche $P_1 \wedge_g P_2$ il divise à gauche P_1 et P_2 et donc il divise à gauche P_1 ou P_2.
- Si $P_1 \neq P_2$ alors $P_1 \vee_g P_2 = 1$, pour $i = 1,\ 2$

on pose $P_i = \sum_{i=0}^{n_i} a_{j,i} D^i$ avec $a_{n_i} \neq 0$ et C_i la matrice compagnon de $M_{n_i}(K)$ dont la dernière colonne est le vecteur $\begin{pmatrix} -\frac{a_{0,i}}{a_{n_i,i}} \\ \vdots \\ -\frac{a_{n_i-1,i}}{a_{n_i,i}} \end{pmatrix}$, ∇ la connexion relative à la dérivation D et dont la matrice de exprimée dans la base canonique de $K^{n_1+n_2}$ est $diag\,(C_1,\ C_2)$. Les vecteurs e_1 et e_{n_1+1} sont cycliques pour ∇ d'ordres n_1 et n_2, de polynômes annulateurs de degré minimum P_1 et P_2. Parce que ces polynômes sont irréductibles $V(\nabla, e_1)$ et $V(\nabla, e_{n_1}+1)$ sont des espaces vectoriels stables pour ∇ minimaux tels que

$$K^{n_1+n_2} = V(\nabla, e_1) \oplus V(\nabla, e_{n_1+1})$$

et d'après le lemme qui précède $K^{n_1+n_2} = V(\nabla, e_1 + e_{n_1+1})$ et le polynôme annulateur de degré minimum de $e_1 + e_{n_1+1}$ est $P_1 \wedge_g P_2$. Posons $P_1 \wedge_g P_2 = \phi P$ alors, par projection sur $V(\nabla, e_1)$ et sur $V(\nabla, e_{n_1}+1)$

$$\phi P(\nabla)(e_1 + e_{n_1+1}) = 0$$
$$\Downarrow$$
$$(\phi P(\nabla)(e_1) = 0) \wedge (\phi P(\nabla)(e_{n_1}+1) = 0)$$

– Si $P(\nabla)(e_1) = 0$ ou $P(\nabla)(e_{n_1}+1) = 0$ alors P_1 ou P_2 divise P et comme $P,\ P_1,\ P_2$ sont irréductibles et unitaires $P_1 = P$ ou

$P_2 = P$.

- Si $P(\nabla)(e_1) \neq 0$ et $P(\nabla)(e_{n_1+1}) \neq 0$ alors ϕ est un polynôme annulateur pour ∇ de $v_1 = P(\nabla)(e_1) \neq 0$ *dans le sous-espace vectoriel stable minimum* $V(\nabla, e_1)$ et $v_2 = P(\nabla)(e_{n_1+1}) \neq 0$ *dans le sous-espace vectoriel stable minimum* $V(\nabla, e_{n_1} + 1)$, on en déduit que $deg(\phi) \geq n_1$ et, de $deg(P) = deg(P_1) + deg(P_2)$, que $deg(P) \leq n_2$.
  - $*$ Si $deg(P) < n_2$ alors, si $v_2 = P(\nabla)(e_{n_1}+1) \in V(\nabla, e_{n_1}+1)\backslash\{0\}$, le polynôme P est égal à $f_{\nabla, e_{n_1+1}}(v)$ et l'annulateur $P_2 : P$ de v est de degré n_2 puisque $V(\nabla, e_{n_1} + 1)$ est un espace vectoriel stable minimum, on en déduit :

$$\exists k \in K[D],\ \phi = k(P_2 : P)$$

Il vient alors

$$P_1 \wedge_g P_2 = k(P_2 : P)P = k(P_2 \wedge_g P)$$

et comme $P_1,\ P_2,\ P$ sont premiers entre eux deux à deux, il vient $deg(P) + deg(k) = n_2$ soit $deg(k) < n_2$. k est un polynôme non nul annulateur de $w_1 = (P_2 : P)P(\nabla)(e_1) \in V(\nabla, e_1)$ et de
$w_2 = (P_2 : P)P(\nabla)(e_{n_1+1}) \in V(\nabla, e_{n_1+1})$.

· Si ni w_1 ni w_2 n'est nul, alors d'après le lemme qui précède w_1+w_2 est cyclique pour ∇ d'ordre n_1+n_2 ce qui contredit que $k(\nabla)(w_1+w_2)=0$ avec $k\neq 0$ et $deg(k)<n_1+n_2$.

· Si $w_1 = 0$ alors, puisque $deg(P) < n_2 \leq n_1$, le vecteur $v_1 = P(\nabla)(e_1)$ est d'après le lemme qui précède cyclique dans $V(\nabla, e_1)$, il est annulé par le polynôme $P_2 : P$ de degré n_2 ce qui est impossible puisque $n_2 < dim(V(\nabla, e_1)) = n_1$.

· Si $w_2 = 0$ alors, puisque $deg(P) < n_2 \leq n_1$, le vecteur $v_1 = P(\nabla)(e_1)$ est d'après le lemme qui précède cyclique dans $V(\nabla, e_1)$, $w_1 = (P_2 : P)(\nabla)(v_1)$ est encore cyclique dans $V(\nabla, e_1)$ puisque $deg(P_2 : P) = n_2 < n_1$, w_1 est annullé par $k(\nabla)$ ce qui est impossible puisque $deg(k) < n_2 \leq n_1$.

$*$ Si $deg(P) = n_2$ alors $deg(\phi) = n_1$: $V(\nabla, e_1)$ et $V(\nabla, e_{n_1+1})$ étant stables minimums de dimension n_1 et n_2 les ensembles

$$\mathcal{B}_1 = \{\nabla^k(v_1)/0 \leq k \leq n_1 - 1\}$$

et

$$\mathcal{B}_2 = \{\nabla^k(v_2)/0 \leq k \leq n_2 - 1\}$$

sont des parties basiques de $V(\nabla, e_1)$ et $V(\nabla, e_{n_1+1})$. On appelle g l'application linéaire de $V(\nabla, e_1)$ dans $V(\nabla, e_{n_1+1})$ telle que $g(\nabla^k(v_1)) = \nabla^k(v_2)$ pour $k = 0, \ldots, n_1$: cette application est injective. Comme g est une application linéaire de $V(\nabla, e_1)$ dans $V(\nabla, e_{n_1+1})$ et ∇ une connexion vectorielle stable sur $V(\nabla, e_{n_1} + 1)$ l'application linéaire $L = g \circ \nabla - \nabla \circ g$ définie sur $V(\nabla, e_1)$ est à image dans $V(\nabla, e_{n_1} + 1)$, nous l'explicitons par son image de la base $\mathcal{B}_1$. Si $k < n_1 + 1$ alors $L\left(\nabla^k(v_k)\right) = 0$, sinon en posant $\phi = D^{n_1} - \sum_{k=0}^{n_1-1} \phi_k D^k$ on voit que $\nabla^{n_1}(v_1) = \sum_{k=0}^{n_1-1} \phi_k \nabla^k(v_1)$ ce qui donne

$$\begin{aligned} g\left(\nabla^{n_1}(v_1)\right) &= \sum_{k=0}^{n_1-1} \phi_k \nabla^k(v_2) \\ &= \nabla^{n_1}(v_2) - \phi(\nabla)(v_2) \end{aligned}$$

Mais $\phi(\nabla)(v_2) = \phi P(\nabla)(e_{n_1+1}) = 0$, cela donne $g\left(\nabla^{n_1}(v_1)\right) = \nabla^{n_1}(v_2)$ soit $L\left(\nabla^{n_1-1}(v_1)\right) = 0$: L est donc l'application nulle. Il vient $g \circ \nabla = \nabla \circ g$ puis, par récurrence, $\forall k \in \mathbb{N},\ g \circ \nabla^k = \nabla^k \circ g$ et enfin, par combinaison linéaire

$\forall \mathcal{Q} \in K[D],\ g \circ \mathcal{Q}(\nabla) = \mathcal{Q}(\nabla) \circ g$. Pour $\mathcal{Q} = L_{\nabla, v_2}$ et appliquée à v_1 cette égalité devient $0 = L_{\nabla, v_2}(\nabla)(v_1)$. Comme v_1 est cyclique d'ordre $n_1 \geq n_2$, cette égalité prouve que $n_1 = n_2$. L_{∇, v_1} et L_{∇, v_2} sont alors deux polynômes annulateurs unitaires de degré n_1 de v_1, ils sont égaux; Et sachant que $P_1 = L_{\nabla, e_1}$ et $P_2 = L_{\nabla, e_2}$ on a $P_1 = P_2$ qui est exclus par hypothèse.

Théorème de décomposition des espaces cycliques Soit y un vecteur cyclique d'ordre k alors il existe $s \in \mathbb{N}$ et $V_1, \ \ldots, \ V_s$ sous-espaces vectoriels stables minimaux de $V(\nabla, y)$ tels que $V(\nabla, y) = \bigoplus_{i=0}^{s} V_s$.

Preuve : Si $V(\nabla, y)$ est stable minimum alors on pose $V(\nabla, y) = V_1$ et le théorème est démontré sinon, il existe un sous-espace vectoriel stable minimum $V_1 \subsetneq V(\nabla, y)$ et un supplémentaire W_1 de V_1 tel que $V(\nabla, y) = V_1 \bigoplus W_1$. Pour $t \in \mathbb{N}$ on appelle $\mathcal{P}(t)$ l'assertion $W = \bigoplus_{i=0}^{t} V_i \bigoplus W_t$, avec V_i sous-espaces vectoriels stables minimaux de $V(\nabla, y)$ et W_t sous espace vectoriel de $V(\nabla, y)$ égal à $\{0\}$ ou non stable-minimum et on montre que $W_t \neq \{0\} \Rightarrow (\mathcal{P}(t) \Rightarrow \mathcal{P}(t+1))$. Si $V(\nabla, y)$ n'est pas stable-minimum alors $\mathcal{P}(1)$ est vraie; Supposons que pour $t \in \mathbb{N}$ $\mathcal{P}(t)$ est vraie avec

$W_t \neq \{0\}$ alors

- Si W_t est stable minimum pour ∇, on pose alors $V_{t+1} = W_t$ et $\mathcal{P}(t+1)$ est vraie (avec $W_{t+1} = \{0\}$).
- Si W_t n'est pas stable minimum pour ∇ alors il existe un sous-espace vectoriel $V_{t+1} \subsetneq W_t$ stable minimum pour ∇ dont nous appelons W_{t+1} un supplémentaire (nécessairement non réduit à $\{0\}$). On a $V(\nabla, y) = \bigoplus_{i=0}^{t+1} V_i \bigoplus W_{t+1}$ avec $W_{t+1} \neq \{0\}$

Cette récurence permet de construire une suite de sous-espaces vectoriels $(W_t)_{t\in\mathbb{N}}$ décroissante pour l'inclusion et telle que

- $V(\nabla, y) = \bigoplus_{i=0}^{t} V_i \bigoplus W_t$ avec V_i sous-espaces vectoriels de $V(\nabla, y)$ stables minimaux pour ∇.
- $W_t \neq \{0\} \Rightarrow W_{t+1} \subsetneq W_t$

Par finitude de la dimension de $V(\nabla, y)$ la suite de sous-espaces vectoriels $W_t \subset V(\nabla, y)$ est de dimension strictement décroissante tant que $W_t \neq \{0\}$: il existe donc un plus petit rang t_0 de la suite pour lequel $W_{t_0} = \{0\}$ on pose $s = t_0$ et on a $\mathcal{P}(s)$ soit $V(\nabla, y) = \bigoplus_{i=0}^{s} V_i$ avec V_i sous-espaces vectoriels stables minimaux de $V(\nabla, y)$.

Lemme complet d'Euclide comme corollaire de l'additivité des degrés du p.p.c.m.

de polynômes irréductibles : Soient $L_1, \ \ldots, \ L_s \in K[D]$ irréductibles et deux à deux distincts alors

$$deg\,(L_1 \wedge_g \cdots \wedge_g L_s) = \sum_{i=1}^{s} deg(L_i)$$

et si $L \in K[D]$, unitaire et irréductible divise à gauche $L_1 \wedge_g \cdots \wedge_g L_s$ alors $\exists i \in \{1, \ \ldots, \ s\}$ tel que $L = L_i$.

Preuve : L'assertion suivante est vraie $\mathcal{P}(2) \ : \ \forall a_1, b_1 \in K[D]$,

$$\begin{array}{rcl} deg(a_1 \wedge_g a_2) & = & deg(a_1) + deg(a_2) - deg(a_1 \vee_g a_2) \\ & \leq & deg(a_1) + deg(a_2) \end{array}$$

puis nous prouvons que

$$\begin{array}{ccc} \mathcal{P}(s) & : & deg(a_1 \wedge_g \cdots \wedge_g a_s) \leq \sum_{i=1}^{s} deg(a_i) \\ \Downarrow & & \\ \mathcal{P}(s+1) & : & deg(a_1 \wedge_g \cdots \wedge_g a_{s+1}) \leq \sum_{i=1}^{s+1} deg(a_i) \end{array}$$

Si $\mathcal{P}(s)$ est vraie alors

$$\begin{array}{rcl} deg(a_1 \wedge_g \cdots \wedge_g a_{s+1}) & = & deg\,((a_1 \wedge_g \cdots \wedge_g a_s) \wedge_g a_{s+1}) \\ & = & deg\,(a_1 \wedge_g \cdots \wedge_g a_s) + deg(a_{s+1}) \\ & & -deg\,((a_1 \wedge_g \cdots \wedge_g a_s) \vee_g a_{s+1}) \\ & \leq & deg\,(a_1 \wedge_g \cdots \wedge_g a_s) + deg(a_{s+1}) \\ & \leq & \sum_{i=1}^{s} deg(a_i) + deg(a_{s+1}) \\ & \leq & \sum_{i=1}^{s+1} deg(a_i) \ : \ \mathcal{P}(s+1) \end{array}$$

est vraie.
A partir des polynômes L_i nous allons définir des indices, des matrices, des espaces vectoriels et des connexions vectorielles :

- Pour $i = 1, \ldots, s$ nous posons $L_i = D^{deg(L_i)} - \sum_{j=0}^{deg(L_i)-1} b_{i,j} D^j$ et C_i la matrice compagnon d'ordre $deg(L_i)$ de dernier vecteur colonne égal à $\begin{pmatrix} b_{i,0} \\ \vdots \\ b_{i,deg(L_i)-1} \end{pmatrix}$.
- Pour r tel que $1 \leq r \leq s$ nous posons $K_r = K^{deg(L_1)+\cdots+deg(L_r)}$ et nous appelons ∇_r la connexion dont la matrice, exprimée dans la base canonique de K_r $\mathcal{B}_r = \left(e_1, \ldots, e_{deg(L1)+\cdots+deg(L_r)}\right)$, est $diag(C_1, \ldots, C_r)$.
- Pour $j \in \{1 , \ldots, r\}$ nous posons : si $j > 1$ alors $\sigma(j) = 1 + \sum_{k=1}^{j-1} deg(L_k)$ si $j = 1$ alors $\sigma(j) = 1$.

Par construction et pour $1 \leq r \leq s$ et $1 \leq j \leq r$:

- L_j est le polynôme annulateur de degré minimum de $e_{\sigma(j)}$ relativement à ∇_r.
- $V_j = V\left(\nabla_r, e_{\sigma(j)}\right)$ est un espace vectoriel stable-minimum de dimension $deg(L_j)$ relativement à ∇_r.

- $(e_{\sigma(j)}, e_{\sigma(j)+1}, \ldots, e_{\sigma(j)+deg(L_j)+1})$ est une base de V_j. Le théorème de complétion des bases prouve alors que $K_r = \bigoplus_{j=1}^{r} V_j$.

Nous prouvons alors par récurrence sur r la propriété $\mathcal{P}(r)$:

- $deg(L_1 \wedge_g \cdots \wedge_g L_r) = deg(L_1) + \cdots + deg(L_r)$
- Si $L \in K[D]$ irréductible divise $L_1 \wedge_g \cdots \wedge_g L_r$ alors $\exists j \in \{1, \ldots, r\}$ tel que $L = L_j$.

$\mathcal{P}(1)$ et $\mathcal{P}(r)$ sont déjà établies nous prouvons alors que $\mathcal{P}(r) \Rightarrow \mathcal{P}(r+1)$ par l'absurde en supposant que $\mathcal{P}(r)$ soit vraie et $\mathcal{P}(r+1)$ fausse soit

$$deg(L_1 \wedge_g \cdots \wedge_g L_{r+1}) < deg(L_1) + \cdots + deg(L_{r+1})$$

ou il existe L irréductible différent de L_1 et ... L_{r+1} qui divise $L_1 \wedge \cdots \wedge_g L_{r+1}$. Nous distinguons deux cas :

- Si

  $$deg(L_1 \wedge_g \cdots \wedge_g L_{r+1}) < deg(L_1) + \cdots + deg(L_{r+1})$$

  alors : puisque

  $$L_1 \wedge_g \cdots \wedge_g L_r = (L_1 \wedge_g \cdots \wedge_g L_r) \wedge_g L_{r+1}$$

  et $deg(L_1 \wedge_g \cdots \wedge_g L_r) = \sum_{i=1}^{r} L_i$ et $\forall a, b \in K[D]$,

  $$deg(a \wedge_g b) = deg(a) + deg(b) - deg(a \vee_g b)$$

c'est que $deg\left((L_1 \wedge_g \cdots \wedge_g L_r) \vee_g L_{r+1}\right) > 0$ et donc $(L_1 \wedge_g \cdots \wedge_g L_r) \vee_g L_{r+1} = d_{r+1} \neq 1$.

Posons (1) $\begin{cases} \mathcal{P} d_{r+1} = L_1 \wedge_g \cdots \wedge_g L_r \\ \mathcal{Q} d_{r+1} = L_{r+1} \end{cases}$ alors *par le lemme du transport*

$\exists \phi,\ \psi \in K[D]$, (2) $\begin{cases} \mathcal{P} &= \phi(L_1 \wedge_g \cdots \wedge_g L_r)(L_r : d_{r+1}) \\ \mathcal{Q} &= \psi(L_{r+1} : d_{r+1}) \end{cases}$

En mesurant les degrés de chaque terme de chaque équation du système (1) on a

$$\begin{cases} deg(\mathcal{P}) &= \sum_{i=1}^{n} deg(L_i) - deg(d_{r+1}) \\ deg(\mathcal{Q}) &= deg(L_{r+1}) - deg(d_{r+1}) \end{cases}$$

et en mesurant ceux de chaque terme de chaque équation du système (2) on a

$$(3) \begin{cases} deg(\phi) &= -deg(d_{r+1}) - deg(L_r : d_{r+1}) \\ deg(\psi) &= deg(L_{r+1}) - deg(d_{r+1}) - deg(L_r : d_{r+1}) \end{cases}$$

Puisque le degré d'un polynôme non nul est positif ou nul le système (3) est équivalent à

$$\begin{cases} 0 = deg(\phi) &= deg(d_{r+1}) = deg(L_r : d_{r+1}) \\ deg(\psi) &= deg(L_{r+1}) \end{cases}$$

En remarquant que $\mathcal{P},\ \mathcal{Q},\ \phi,\ \psi$ sont unitaires il vient $1 = \phi = d_{r+1} = L_r : d_{r+1}$ et ce qui contredit que $d_{r+1} \neq 1$.

- Si il existe L irréductible différent de L_1 et ... L_{r+1} qui divise $L_1 \wedge \cdots \wedge_g L_{r+1}$ alors d'après l'item précédent $d_{r+1} = 1$ et l'égalité

$deg(L_1 \wedge_g \cdots \wedge_g L_{s+1}) = \sum_{i=1}^{r+1} deg(L_i)$ est vraie, nous introduisons alors la connexion ∇_{r+1} de matrice $diag(C_1, \ldots, C_{r+1})$ sur la base canonique de $K_{r+1} = K^{deg(L_1)+\cdots+deg(L_{r+1})}$. On a la décomposition $K_{r+1} = \bigoplus_{j=1}^{r+1} V(\nabla_{r+1}, e_{\sigma(j)})$ et si nous posons $L_1 \wedge \cdots \wedge_g L_{r+1} = \phi_{r+1} L$ alors $y_{r+1} = \sum_{i=1}^{r+1} e_{\sigma(i)}$ admet pour polynôme annulateur relativement à ∇_{r+1} de degré minimum $L_1 \wedge \cdots \wedge_g L_{r+1}$ dont le degré est *précisemment* $dim(K_{r+1})$: on a donc $V(\nabla_{r+1}, y_{r+1}) = K_{r+1}$. Soit $\xi = L(\nabla_{r+1})(y_{r+1})$ alors $f_{\nabla_{r+1}, y_{r+1}}(\xi) = L$ et $L_{\nabla_{r+1},\xi} = L_{\nabla_{r+1},\xi} : L = \phi_{r+1}$. On a la décomposition $\xi = \sum_{j=1}^{r+1} \xi_j$ avec $\xi_j = L(\nabla_{r+1})(e_{\sigma(j)}) \in V_j = V(\nabla_{r+1}, e_{\sigma(j)})$ et nous allons distinguer deux cas :

- Si les ξ_j ne sont pas tous non nuls alors, pour toute valeur j telle que $\xi_j = 0$ on a $L(\nabla_{r+1})(e_{\sigma(j)}) = 0$, L_j le polynôme annulateur de $e_{\sigma(j)}$ relativement à ∇_{r+1} divise L et comme ces deux polynômes sont irréductibles et unitaires, ils sont égaux. Il n'y a donc qu'un seul j tel que $\xi_j = 0$ et pour cette valeur de j $L = L_j$.
- Si tous les ξ_j sont non nuls alors, puisque $\forall j \in \{1, \ldots, r+1\}$ $V(\nabla_{r+1}, e_{\sigma(j)})$ est stable minimum, et que $\xi_j \in V(\nabla_{r+1}, e_{\sigma(j)}) \backslash \{0\}$

$\exists L_1^*, \ \ldots, \ L_{r+1}^* \in K[D]$ avec $\forall j, \ deg(L_j^*) = deg(L_j)$ et L_j^* est le polynôme annulateur de ξ_j de degré minimum L divise à gauche $L_1 \wedge_g \cdots \wedge_g L_{r+1}$ donc

$$L_1 \wedge_g \cdots \wedge_g L_{r+1} = \Psi L$$

avec $deg(\Psi) < \sum_{i=1}^{r+1} deg(L_i)$. Cette égalité de polynômes prise en $\nabla_{r+1}(e_{\sigma(j)})$ entraîne que

$$\forall j \in \{1, \ \ldots, \ r+1\}, \ \Psi(\nabla_{r+1})(\xi_j) = 0$$

Ψ est un multiple du p.p.c.m. de $L_1^*, \ \ldots, \ L_{r+1}^*$ et a donc pour degré *au moins* $\sum_{i=1}^{r+1} deg(L_i^*) = \sum_{i=1}^{r+1} deg(L_i)$ ce qui est contradictoire.

Corollaire : Soit $L_1, \ \ldots, \ L_r$ des polynômes irréductibles de $K[D]$, non nécessairement distincts, si L irréductible divise à gauche $L_1 \wedge_g \cdots \wedge_g L_r$ alors L est associé à l'un des polynômes de l'ensemble $\{L_i / \ 1 \leq i \leq r\}$.

Preuve : Soit $L_{\sigma(1)}, \ \ldots, \ L_{\sigma(s)}$ avec $s \leq r$ l'ensemble $\{L_i / \ 1 \leq i \leq r\}$ alors

$$L_{\sigma(1)} \wedge_g \cdots \wedge_g L_{\sigma(s)} = L_1 \wedge_g \cdots \wedge_g L_r$$

Pour $P \in K[D]$ nous appelons P^* l'unique polynôme unitaire tel que $(L)_g = (L^*)_g$ alors, si L divise à gauche $L_1 \wedge_g \cdots \wedge_g L_r$ on a

$$(L)_g \subset \cap_{j=1}^r (L_j)_g = \cap_{i=1}^s (L_\sigma(i))_g$$

soit $(L^*)_g \subset \cap_{i=1}^s (L_{\sigma(s)})_g = \cap_{i=1}^s (L^*_{\sigma(s)})_g$: Le polynôme irréductible unitaire L^* divise à gauche $L^*_{\sigma(1)} \wedge_g \cdots \wedge_g L^*_{\sigma(s)}$ donc pour un $i \in \{1, \ldots, s\}$ $L^* = L^*_{\sigma(i)}$ ce qui prouve que pour un $j \in \{1, \ldots, r\}$ $L = L_j$.

Propriétés arithmétiques de $K[D]$

Dans un anneau principal intègre et commutatif, les éléments irréductibles sont premiers, et tout élément se décompose comme produit d'éléments premiers, dans $K[D]$ anneau non commutatif et euclidien gradué la notion usuelle d'élément premier doit fait intervenir une notion de produit non commutatif, nous remplacerons avantageusement la notion d'élément premier au sens d'un produit non commutatif par celle d'élément premier au sens d'un p.p.c.m. à gauche. Dans tout ce qui suit E sera un espace vectoriel de dimension finie stable pour une connexion vectorielle ∇ non nilpotente et on aura donc $E = V(\nabla, y)$.

Représentation par des idéaux vectoriels d'espaces vectoriels cycliques stables pour une connexion vectorielle non nilpotente

Lemme d'existence de vecteur cyclique :
Si F est un sous-espace vectoriel de E stable pour

∇ alors il existe un vecteur cyclique pour ∇ (soit $\exists z \in F,\ F = V(\nabla, z)$).

Preuve : Suivant le lemme du décomposition des espaces vectoriels cycliques $\exists s \in \mathbb{N},\ E = \bigoplus_{i=1}^{s} V_i$ où $V_1,\ \ldots,\ V_s$ sont des sous-espaces vectoriels stables minimimaux tels que $E = \bigoplus_{i=1}^{s} V_i$.

$$F = F \cap E = F \cap \bigoplus_{i=0}^{s} V_i = \bigoplus_{i=0}^{s} (F \cap V_i)$$

- Si $\exists i \in \{1,\ \ldots, s\}/V_i = F$: alors, d'après ce qui précède, tout $z \in F \backslash \{0\}$ est cyclique dans F.

- Sinon : on pose $\forall i \in \{1,\ \ldots, s\}$, $W_i = F \cap V_i$ alors les $W_i \neq \{0\}$ sont des sous-espaces vectoriels de F stables pour ∇ comme intersection d'espaces vectoriels stables pour ∇. Ils sont stables minimaux dans F : $\forall i \in \{1,\ \ldots, s\}$ si G_i est un sous-espace vectoriel de $F \cap V_i$ stable pour ∇ alors c'est un sous-espace vectoriel stable de V_i stable minimum : c'est donc V_i ou $\{0\}$ mais comme $F \cap V_i \subsetneq V_i$ cela ne peut être V_i c'est donc $\{0\}$ et $\{0\} \neq W_i = F \cap V_i$ est un sous-espace vectoriel stable minimum dans F. Comme ∇ est une connexion non nilpotente nous pouvons choisir $w_1,\ \ldots,\ w_s$ dans $W_1,\ \ldots,\ W_s$ de façon à ce que les polynômes irréductibles

L_{∇,w_1}, ..., L_{∇,w_s} soient deux à deux distincts, avec ce choix le vecteur $z = w_1 + \cdots + w_s$ est un vecteur cyclique dans F. En effet si

$$P(\nabla)(z) = P(\nabla)(w_1) + \cdots + P(\nabla)(w_s) = 0$$

alors $\forall i \in \{1, \ldots, s\}$ $P(\nabla)(w_i) = 0$, donc $P \in (L_{\nabla,w_i})_g$, $\forall i \in \{1, \ldots, s\}$ soit $P \in \left(L_{\nabla,w_1} \wedge_g \cdots \wedge_g L_{\nabla,w_s}\right)_g$ et $L_{\nabla,w_1} \wedge_g \cdots \wedge_g L_{\nabla,w_s}$ est le polynôme annulateur de plus petit degré de z *dont le degré* $\sum_{i=0}^{s} deg(L_{\nabla,w_i}) = \sum_{i=0}^{s} dim(W_i) = dim(F)$ *est précisément la dimension de* F.

Arithmétique des p.g.c.d. et des p.p.c.m. des polynômes de $K[D]$

Corollaire de représentation des sous-espaces vectoriels stables de $V(\nabla, y)$: Soit F un sous-espace vectoriel de $E = V(\nabla, y)$ alors il existe un unique idéal à gauche I de $K[D]$ tel que $V = I(y)$ et $\left(L_{\nabla,y}\right)_g \subset I$.

Preuve :

- Existence : Soit z un vecteur cyclique pour F alors si $d = f_{\nabla,y}(z) \vee_g L_{\nabla,y}$ et $\xi = d(\nabla)(y)$ nous savons que $L_{\nabla,y} = L_{\nabla,\xi} d$. Cette égalité entraîne $V(\nabla, \xi) = K[D](\xi)(d)_g(y)$ et $(L_{\nabla,y})_g \subset (d)_g$. Nous posons $f_{\nabla,y}(z) = f \times d$ alors, si $k = dim(E)$, f est un polynôme de degré au plus $k - deg(d) - 1$ tel que $f(\nabla)(\xi) = z$, sachant que

$$dim\,(V(\nabla,\xi)) = deg\,(L_{\nabla,\xi}) = k - deg(d)$$

c'est que $z \in V(\nabla,\xi)$ et $f = f_{\nabla,\xi}(z)$. On a alors

$$d = f_{\nabla,y}(z) \vee_g L_{\nabla,y} = f_{\nabla,\xi}(z) d \vee_g L_{\nabla,\xi} d = (f_{\nabla,\xi(z)\vee_g L_{\nabla,\xi}})d$$

ce qui donne $f_{\nabla,\xi}(z) \vee_g L_{\nabla,\xi} = 1$, nous savons alors que, puisque $z \in V(\nabla,\xi)$ on a $V(\nabla,\xi) = V(\nabla,z) = F$. On a donc $F = (d)_g(y)$ où $(L_{\nabla,y})_g \subset (d)_g$: ce qui montre l'existence de I.

- Si I et J sont deux idéaux de $K[D]$ tels que $F = I(y) = J(y)$ nous savons alors, d'après le lemme de la page 46, que $I + (L_{\nabla,y})_g = J + (L_{\nabla,y})_g$; Si de plus $(L_{\nabla,y})_g \subset I$ et $(L_{\nabla,y})_g \subset J$ alors $I + (L_{\nabla,y})_g = J + (L_{\nabla,y})_g$ devient $I = J$: ce qui prouve l'unicité de I.

L'application Φ qui à un idéal I tel que $(L_{\nabla,y})_g \subset I$ associe $I(y)$ (sous-espace vectoriel de E stable pour ∇) est :

- *une bijection additive (i.e. telle que $\Phi(I+J) = \Phi(I) + \Phi(J)$) de l'ensemble des idéaux de $K[D]$ contenant $(L_{\nabla,y})_g$ vers l'ensemble des sous-espaces vectoriels de E stables pour ∇,*

- *croissante pour l'inclusion (des idéaux).*

Par l'action de Φ^{-1} et des résultats qui précèdent nous en déduisons le

Corollaire de factorialité simple de $K[D]$ au sens des p.p.c.m. : si la caractéristique de K supposé de dimension infinie sur K_D son corps des constantes est telle que toute connexion vectorielle sur un espace vectoriel de dimension finie n'est pas nilpotente alors si un polynôme P de $K[D]$ admet une décomposition, en un produit d'un élément $a \in K$ et du p.p.c.m. à gauche de r éléments irréductibles $P_1^*, \ldots, P_s^*$ de $K[D]$ alors s'il admet une autre décomposition telle que si

$$P = a \times P_1^* \wedge_g \cdots \wedge_g P_s^* = b \times L_1 \wedge_g \cdots \wedge_g L_r$$

alors $a = b$ et $\{P_i^* | 1 \leq s \leq r\} = \{L_j | 1 \leq j \leq r\}$.

Preuve : Ce résultat est déjà prouvé si on note que $\{P_i^* | 1 \leq s \leq r\}$ et $\{L_j^* | 1 \leq j \leq r\}$ sont les ensembles formés par les *valeurs des suites finies* $P_1^*, \ldots, P_s^*$ et $L_1, \ldots, L_r$.

De la factorialité simple vers la factorialité semi-simple de $K[D]$

Il s'agit ici de traduire en termes d'opérateurs de $K[D]$ la propriété de décomposition unique des entiers en produit de *puissances finies* de nombres premiers (décomposition semi-simple) en place de décomposition unique de *certains* entiers en pro-

duit fini de nombres premiers distincts (décomposition simple), et par là même de donner en terme d'opérateurs de $K[D]$ un sens à opérateur puissance finie d'un opérateur irréductible.
(A Suivre...)