Philippe Robba

Lemme de Hensel pour les opérateurs différentiels

Groupe de travail d'analyse ultramétrique, tome 2 (1974-1975), exp. nº 16, p. 1-11
<http://www.numdam.org/item?id=GAU_1974-1975__2__A14_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, P. ROBBA)
2e année, 1974/75, n° 16, 11 p.
21 avril 1975

LEMME DE HENSEL POUR LES OPÉRATEURS DIFFÉRENTIELS

par Philippe ROBBA

(d'après un travail en commun avec B. DWORK)

Nous reprenons les notations de l'exposé [2]. Nous supposerons encore que le corps résiduel de K est de caractéristique $p \neq 0$.

1. Introduction.

1.0. A propos de notre étude de la factorisation des opérateurs différentiels et du prolongement analytique des coefficients des opérateurs factorisants [2], nous nous posions la question de savoir s'il était possible d'obtenir des informations concernant les classes résiduelles où il y a prolongement à partir d'une simple étude des opérateurs différentiels dans le corps résiduel.

Nous avons obtenu, dans certains cas particuliers, une réponse positive à cette question. A notre surprise il est alors apparu que les conditions dans lesquelles on pouvait obtenir de telles informations pouvaient s'interpréter comme une adaptation des conditions d'application du lemme de Hensel classique sur les polynômes.

La question se posait alors de savoir s'il existait une démonstration purement algébrique de nos résultats n'utilisant pas la théorie des équations différentielles p-adiques. Pour l'instant cette question n'a pas reçu de réponse complète, mais nous indiquerons un cas particulier où la démonstration classique pour les polynômes se transpose sans difficulté au cas des polynômes différentiels.

1.1. Soit K un corps de caractéristique zéro, complet pour une valuation ultramétrique. Nous noterons $\mathfrak{U}$ son anneau de valuation, et $\overline{K}$ le corps résiduel de K.

Soit $P \in \mathfrak{U}[X]$. Par passage au corps résiduel, il lui correspond $\overline{P} \in \overline{K}[X]$. Le lemme de Hensel nous dit que si $\overline{P}$ admet une factorisation dans $\overline{K}[X]$: $\overline{P} = Q^* R^*$, et si Q^* et R^* sont premiers entre eux, alors P se factorise dans $\mathfrak{U}[X]$, $P = QR$, avec de plus $\overline{Q} = Q^*$ et $\overline{R} = R^*$.

1.2. Muni de la norme de Gauss, E est un corps valué complet ultramétrique. Comme $E_0 = K(X)$ est dense dans E, le corps résiduel de E coïncide avec celui de E_0, et s'identifie donc à $\overline{K}(X)$. Nous noterons $\mathfrak{B}$ l'anneau de valuation de E.

Soit alors $L \in \mathfrak{B}[D]$ d'ordre $n + m$, et supposons que son image $\overline{L} \in \overline{E}[D] = \overline{\mathfrak{D}}$ se factorise dans $\overline{\mathfrak{D}}$, $\overline{L} = N^* M^*$, avec ordre $M^* = m$ (et donc ordre $N^* \leq n$).

Notons $\overline{\mathcal{O}}_k$ l'espace des polynômes différentiels à coefficients dans $\overline{E}$ d'ordre $\leq k$. Nous montrerons que si

$$(*)\quad \left\{\begin{array}{l}\text{l'application } \overline{L}_{N^*,M^*} : (P,Q) \longmapsto PM^* + N^* Q \\ \qquad\qquad \text{de } \overline{\mathcal{O}}_{n-1} \times \overline{\mathcal{O}}_{m-1} \text{ dans } \overline{\mathcal{O}}_{n+m-1} \text{ est injective,}\end{array}\right.$$

alors L se factorise dans $\mathcal{E}[D]$, $L = NM$, avec ordre $M = m$ et de plus $\overline{N} = N^*$ et $\overline{M} = M^*$.

1.3. Observons d'abord que nos hypothèses sont une transcription appropriée au cas des opérateurs différentiels des hypothèses du lemme de Hensel. Dans le cas commutatif, la condition (*) équivaut à dire que M^* et N^* sont premiers entre eux. Précisément, soient N^* et M^* appartenant à $\overline{K}[X]$. Soit L_{N^*,M^*} l'application

$$(P , Q) \longmapsto PM^* + N^* Q$$

de $\overline{K}_{n-1}[X] \times \overline{K}_{m-1}[X]$ dans $\overline{K}_{n+m-1}[X]$ avec $m =$ ordre M^*, $n \geq$ ordre N^*. Alors M^* et N^* sont premiers entre eux si, et seulement si, L_{N^*,M^*} est injective.

En effet, comme $\dim \overline{K}_{n+m-1}[X] = n + m = \dim(\overline{K}_{n-1}(X) \times \overline{K}_{m-1}(X))$, L_{N^*,M^*} est injective si, et seulement si, L_{N^*,M^*} est surjective.

Alors si L_{N^*,M^*} est surjective, $1 \in \operatorname{Im}(L_{N^*,M^*})$, et donc $(N^* , M^*) = 1$.

Maintenant, si $(N^* , M^*) = 1$, soient $U , V \in \overline{K}[X]$ tels que $UM^* + VN^* = 1$. Si $R \in K_{n+m-1}[X]$, soit $RV = SM^* + Q$, $\deg Q < m = \deg M^*$, et $P=RU - SN^*$. On voit que

$$PM^* + QN^* = RUM^* + SM^* N^* + RVN^* - SM^* N^* = R$$

et par des considérations sur le degré, on voit que $\deg P \leq n - 1$. Donc L_{N^*,M^*} est surjective.

1.4. Si on suppose que les coefficients de L sont non seulement dans E, mais sont des éléments analytiques sur une union de classes résiduelles A, on peut alors choisir N et M avec leurs coefficients éléments analytiques sur un sous-ensemble admissible (et même superadmissible) B de A, c'est-à-dire que B contient presque toutes les classes résiduelles de A.

Comme pour démontrer ce lemme de Hensel pour les opérateurs différentiels, on montrera qu'on est dans les conditions d'applications du théorème 2.6 de [2], cette précision n'est en fait qu'une conséquence immédiate de ce théorème 2.6. Mais ce qui est intéressant, c'est que, dans ce cas particulier, on va pouvoir déterminer explicitement, par des considérations portant sur les opérateurs M^* et N^*, les classes résiduelles où les coefficients de M et N se prolongent.

Nous illustrerons cette procédure avec l'opérateur de Monsky dont une étude détaillée a été faite dans [3].

1.5. Nous indiquerons dans le cas particulier où l'on prend $M^* = \overline{L}$ (c'est-à-dire dans le cas où ordre $\overline{L} <$ ordre L, ce qui est le cas de l'opérateur de Monsky) une démonstration plus directe et qui coïncide avec la démonstration classique du lemme de Hensel pour les polynômes (cf. §5).

1.6. Nous aurons besoin de certains résultats concernant les équations différentielles en caractéristique $p \neq 0$. Nous avons regroupé tous ces résultats dans un appendice. Comme ces résultats, bien que simples, semblent difficilement accessibles dans la littérature, nous y avons inclus certains résultats qui ne nous serviront pas pour cet exposé.

1.7. On obtiendra en particulier le résultat suivant (corollaire A.4) :

Considérons $\overline{K}(X)$ comme espace vectoriel sur $\overline{K}(X^p)$ (ce point de vue est motivé par le fait que si $u \in \overline{K}(X^p)$, alors $Du = 0$ puisque caract. $\overline{K} = p$). Soit $\overline{L} \in \overline{K}(X)[D]$. Alors il existe $M^* \in \overline{K}(X)[D]$, unitaire, tel que $\operatorname{Ker} \overline{L} = \operatorname{Ker} M^*$, et que la dimension (sur $\overline{K}(X^p)$) de $\operatorname{Ker} M^*$ coïncide avec l'ordre de M^*. On a bien sûr $\overline{L} = N^* M^*$ pour un certain $N^* \in \overline{K}(X)[D]$.

Il serait important, par exemple pour l'étude du noyau borné de l'opérateur L, de savoir si la conjecture suivante est satisfaite.

Conjecture. - Soit $L \in E[D]$. Soit $\overline{L}$ son image dans $\overline{K}(X)[D]$. Soit $\overline{L} = N^* M^*$ la factorisation que l'on vient de définir. Il existe N, M appartenant à $E[D]$, M unitaire, tels que $L = NM$. De plus, si L a ses coefficients éléments analytiques sur une union de classes résiduelles A, les coefficients de M et N se prolongent dans presque toutes les classes résiduelles de A.

2. Un lemme préparatoire.

2.1. Rappelons quelques notations du paragraphe 2.5 de [2].

L'ensemble A est une union de classes résiduelles de Ω.

On considère le polynôme à coefficients dans $(H(A))^n$ de degré total ≤ 2

$$F(x\ ;\ Y_0, Y_1, \dots, Y_{S-1}) = \sum_k C_k(x) \prod_{i=0}^{S-1} \prod_{j=1}^{n} Y_{ij}^{k_{ij}},$$

où $C_k(x) = (C_{k1}(x), \dots, C_{kn}(x)) \in H(A)^n$, où Y_i $0 \leq i \leq S-1$, est un n-uplet $Y_i = (Y_{i1}, \dots, Y_{in})$, et où la sommation porte sur les $S \times n$ matrices k à coefficients entiers ≥ 0 avec $|k| = \sum_{i,j} k_{ij} \leq 2$.

Le développement taylorien de F au voisinage de $Y \in \Omega^{nS}$ s'écrit

$$F(x\ ;\ Y_0+Z_0, \dots, Y_{S-1}+Z_{S-1})$$
$$= F(x\ ;\ Y_0, \dots, Y_{S-1}) + L(x\ ;\ Y_0, \dots, Y_{S-1}\ ;\ Z_0, \dots, Z_{S-1}) + \phi(x\ ;\ Z_0, \dots, Z_{S-1})$$

où L est linéaire en $Z_0 \dots Z_{S-1}$ et ϕ est quadratique en $Z_0, \dots, Z_{S-1}$.

On considère alors le système différentiel non linéaire en $Y = (Y_1, \dots, Y_n)$

(2.1.1) $$F(x\ ,\ Y\ ,\ Y'\ ,\ \dots\ ,\ Y^{(S-1)}) = 0\ ,$$

et à chaque $Y \in E^n$ on associe l'opérateur différentiel linéaire (tangent à F)

(2.1.2) $L_Y : Z=(Z_1,\dots,Z_n) \longmapsto L_Y(Z)=L(x\ ;\ Y,Y',\dots,Y^{(S-1)},Z,\dots,Z^{(s-1)})$.

Si alors on suppose que les coefficients $C_k(x)$ de F appartiennent à $\mathfrak{B}^n$ (c'est-à-dire $\forall\ k\ ,\ i\ ,\ |C_{ki}| \leq 1$), l'équation différentielle (2.1.1) peut être réduite dans le corps résiduel en envoyant C_k dans $\overline{C}_k$, on obtient :

(2.1.3) $$\overline{F}(x\ ;\ Y\ ,\ Y'\ ,\ \dots\ ,\ Y^{(S-1)}) = 0\ .$$

De même, si on choisit $Y^* \in \overline{E}^n$, on peut considérer l'opérateur différentiel tangent réduit

(2.1.4) $\overline{L}_{Y^*} : Z=(Z_1,\dots,Z_n) \longmapsto \overline{L}_{Y^*}(Z)=\overline{L}(x\ ;\ Y^*,Y^{*\prime},\dots,Y^{*(S-1)},Z,\dots,Z^{(S-1)})$.

2.2. LEMME. - <u>Soit</u> F <u>satisfaisant aux conditions du paragraphe</u> 2.1. <u>Soit</u> $Y^* \in \overline{E}^n$ <u>une solution de l'équation réduite</u> (2.1.3). <u>Supposons, de plus, que l'opérateur tangent réduit</u> $\overline{L}_{Y^*}$ <u>est injectif dans</u> $\overline{E}^n$. <u>Alors il existe un relèvement unique</u> Y <u>de</u> Y^* <u>(c'est-à-dire que</u> $\overline{Y} = Y^*$) <u>dans</u> E^n <u>solution de l'équation</u> (2.1.1). <u>De plus,</u> Y <u>satisfait les hypothèses du théorème</u> 2.6 <u>de</u> [2] <u>et, par conséquent,</u> $Y \in H(B)^n$, <u>où</u> B <u>est un sous-ensemble super admissible de</u> A .

<u>Démonstration.</u> - Comme $\overline{L}_{Y^*}$ est injectif dans $\overline{E}^n$, en vertu du corollaire A8, il existe une $n \times n$ matrice Q^* à coefficients dans $\overline{\mathfrak{D}}$ telle que

(2.2.1) $$Q^*\,\overline{L}_{Y^*} = I$$

(où l'on considère Q^* et $\overline{L}_{Y^*}$ comme endomorphismes de $\overline{E}^n$).

Soit η un relèvement quelconque de Y^* dans E_0 , et Q une $n \times n$ matrice à coefficients dans $E_0[D]$ relèvement de Q^* . On peut supposer que η et Q n'ont de singularités que dans les classes résiduelles qui sont des singularités de Y^* et Q^* .

L'équation (2.2.1) nous donne alors

(2.2.2) $$\|QL_\eta - I\|_{E^n} \leq \|QL_\eta - I\|_{(W_t^n,0)^n} < 1\ .$$

Ce qui entraîne que QL_η , et donc L_η , est inversible dans E^n (cf. [1] §4.10, et le théorème 1.4 de [2]) et même dans $H(B)^n$, où B est un sous-ensemble admissible de A contenant toutes les classes résiduelles de A où ni η ni Q n'ont de singularités.

Montrons que

(2.2.3) $$\|L_\eta^{-1}\|_{E^n} = 1\ .$$

On a d'une part $1 = \|I\| = \|L_\eta^{-1}\,L_\eta\| \leq \|L_\eta^{-1}\|$. D'autre part, si $\|L_\eta^{-1}\| > 1$, il existe $u \in E^n$, $|u| = 1$ tel que $|L_\eta\,u| > 1$, et on obtient par réduction $\overline{u} \neq 0$ et $\overline{L}_{Y^*}\,\overline{u} = 0$ ce qui contredit l'injectivité de $\overline{L}_{Y^*}$.

Si $g = F(x\ ;\ \eta\ ,\ \eta'\ ,\ \ldots\ ,\ \eta^{(S-1)})$, comme Y^* satisfait l'équation (2.1.3), on a $|g|_{E^n} < 1$. Choisissons ω avec $|g| < \omega < 1$, et posons

$$U = \{Z \in E^n\ ;\ \ |Z| \leq \omega\}\ .$$

On vérifie alors, comme dans la démonstration du théorème 2.6 de [2], que l'application

$$\varphi\ :\ \ Z \longmapsto -\ L_\eta^{-1}(g + \psi(Z))$$

est une contraction de U dans lui-même, et donc a un unique point fixe Z_0 . Il est alors clair que $Y = \eta + Z_0$ est un relèvement de Y^* qui satisfait l'équation (2.1.1).

Si alors Y_1 est un autre relèvement de Y^* satisfaisant (2.1.1), $Z_1 = Y_1 - \eta$ est aussi un point fixe de φ , et comme $|Z_1| < 1$, on peut choisir λ avec $|Z_1| < \lambda < 1$, le point fixe de φ dans U étant unique $Z_1 = Z_0$ et $Y_1 = Y$.

3. Lemme de Hensel pour les opérateurs différentiels.

Rappelons que $\overline{\mathcal{D}}_k$ a été défini au paragraphe 1.2, et désigne l'espace des éléments de $\overline{\mathcal{D}}$ d'ordre $\leq k$.

THÉORÈME.

(i) Soit $L \in \mathcal{B}[D]$, d'ordre $n + m$. Supposons que son image $\overline{L}$ dans $\overline{\mathcal{D}}$ se factorise sous la forme

$$\overline{L} = N^*\ M^*\ , \tag{3.1}$$

où M^* est unitaire et d'ordre m . Soit L_{N^*,M^*} l'application

$$(P\ ,\ Q) \longmapsto PM^* + N^*\ Q \tag{3.2}$$

de $\overline{\mathcal{D}}_{n-1} \times \overline{\mathcal{D}}_{m-1}$ dans $\overline{\mathcal{D}}_{n+m-1}$. Si cette application est injective, il existe un relèvement unique M de M^* , unitaire d'ordre m , qui divise L à droite. On a donc

$$L = NM\ , \tag{3.3}$$

et N est un relèvement de N d'ordre n .

(ii) Sous les hypothèses de (i), si de plus $L \in H(A)[D]$, où A est une union de classes résiduelles, alors N et M appartiennent à $H(B)[D]$ où B est un sous-ensemble super admissible de A .

(iii) $\overline{\mathcal{D}}_{n-1} \times \overline{\mathcal{D}}_{m-1}$ et $\overline{\mathcal{D}}_{n+m-1}$ s'identifient de façon évidente avec $\overline{E}^{n+m}$. En vertu du corollaire A.8, l'endomorphisme différentiel L_{N^*,M^*} de $\overline{E}^{n+m}$ possède un inverse Q qui est un endomorphisme différentiel. Alors sous les hypothèses de (ii), on peut ajouter que B contient toutes les classes résiduelles de A qui ne sont pas des singularités pour les coefficients de Q , de M^* ou de N^* .

Démonstration. - L'équation (3.3) peut s'interpréter comme une équation différentielle non linéaire sur les coefficients (d'ordre $\leq n-1$ et d'ordre $\leq m-1$ respectivement) de N et M, et (3.1) est l'équation réduite. Alors $\overline{L}_{N^*,M^*}$ est l'opérateur tangentiel réduit.

Alors (i) et (ii) résultent du lemme 2.2, et (iii) résulte des remarques que l'on a faites au début de la démonstration du lemme 2.2 sur le relèvement de Q et de Y^*.

4. Exemples.

4.1. Nous indiquons quelques cas simples où la condition (*) est (ou n'est pas) satisfaite. Il pourra être intéressant de comparer les théorèmes 3.2 et 3.4 de [2] avec la proposition suivante.

PROPOSITION. - Soient m et n des entiers, et soient M^* et N^* des éléments de $\overline{\mathfrak{D}}$ d'ordre m, resp. $\leq n$. L'application L_{N^*,M^*}, définie par (3.2),

(i) n'est pas injective si $\operatorname{Ker} N^* \neq \{0\}$ et $\dim_{\overline{K}(X^P)} \operatorname{Ker} M^* = \text{ordre } M^* = m$,

(ii) est injective si $\operatorname{Ker} N^* = \{0\}$ et $\dim \operatorname{Ker} M^* = m$,

(iii) est injective si N^* est d'ordre zéro.

Démonstration.

(i) Soit $u_1 \dots u_m$ une base de $\operatorname{Ker} M^*$, et soit $v \neq 0 \in \operatorname{Ker} N^*$. Comme le wronskien de $u_1 \dots u_m$ n'est pas nul, il existe un polynôme différentiel Q d'ordre $\leq m-1$ tel que

$$Qu_i = 0 \,, \quad 1 \leq i \leq m-1$$

$$Qu_m = v \,.$$

Il est alors clair que $\operatorname{Ker} M^* \subset \operatorname{Ker} - N^* Q$, et donc, en vertu du lemme A.3 et du corollaire A.6, M^* divise à droite $-N^* Q$, ce qui montre que l'application $\overline{L}_{N^*,M^*}$ n'est pas injective.

(ii) Supposons qu'il existe $P \in \overline{\mathfrak{D}}_{n-1}$ et $Q \in \overline{\mathfrak{D}}_{m-1}$ tels que $PM^* + N^* Q = 0$. Comme $\dim \operatorname{Ker} Q \leq \text{ordre } Q < m = \dim \operatorname{Ker} M^*$, il existe $u \in \overline{E}$ tel que $M^* u = 0$ et $Qu \neq 0$. On voit alors que $Qu \in \operatorname{Ker} N^*$ ce qui contredit l'hypothèse.

(iii) Si P et Q sont non nuls, on a ordre $N^* Q < m \leq$ ordre PM^*, et on ne peut donc avoir $PM^* + N^* Q = 0$.

4.2. PROPOSITION. - Soit A une union de classes résiduelles, et soit $L \in H(A)[D] \cap \mathfrak{B}[D]$, d'ordre $n+m$. Supposons que son image $\overline{L}$ dans $\overline{\mathfrak{D}}$ soit unitaire d'ordre m. Alors L se factorise dans $H(A)[D]$, $L = NM$, avec M unitaire et $\overline{M} = \overline{L}$.

Démonstration. - En vertu de la proposition 4.1 (iii), on est dans les conditions d'application du théorème 3 avec $N^* = 1$, $M^* = \overline{L}$. Il suffit, en vertu du théorème 3, (iii), de déterminer les singularités de l'application inverse de $\overline{L}_{N^*,M^*}$. Or $\overline{L}_{N^*,M^*}$ est de la forme

$$(P , Q) \longmapsto PM^* + Q ,$$

et l'application inverse

$$S = PM^* + Q \longmapsto (P , Q) ,$$

correspond à la division de S par M^* . Comme M^* est unitaire, les singularités de cette application sont celles de M^* , et donc ne sont pas dans A .

4.3. Exemple : Dans [3], nous avons fait une étude extensive de l'opérateur de Monsky.

$$L = \frac{px}{1-x} D^2 + D - \frac{c}{1-x} .$$

Nous pouvons appliquer la proposition 4.2 avec $A = \complement D(1 , 1^-)$.

Il existe donc $\eta \in H(D(1 , 1^-))$, tel que

$$\overline{\eta} = \frac{c}{1-x}$$

et

$$L = (\frac{px}{1-x} D + 1 + \frac{px}{1-x} \eta)(D - \eta) .$$

Remarquons que dans [3] on obtenait des précisions supplémentaires sur η (à savoir $\eta = \frac{c}{1-x} + \frac{V'}{V}$ avec $V \in H(\complement D(1 , r^+))$, $r < 1$) ce qui était essentiel pour l'étude faite en [3], §4.3 et seq.

5. Démonstration algébrique du lemme de Hensel, dans un cas particulier.

Nous allons donner une démonstration algébrique de la proposition 4.2 calquée sur la démonstration correspondante du lemme de Hensel pour les polynômes.

5.1. Pour $L \in \mathcal{O} = E[D]$, $L = \sum c_m D^m$, on pose $|L| = \max_m |c_m|$.

LEMME. - Soient $L \in \mathcal{O}$ et M unitaire de $\mathcal{O}$ avec $|M| = 1$. Soient N et R de $\mathcal{O}$ tels que

$$L = NM + R , \quad \text{ordre } R < \text{ordre } M .$$

Alors $|L| = \max(|N| , |R|)$.

Démonstration. - Elle est évidente.

5.2. Démonstration algébrique de la proposition 4.2.

Soit M , un relèvement unitaire de $\overline{L}$, d'ordre m , dans $H(A)[D]$.

On définit M_n N_n et R_n par induction sur n , grâce aux formules

$L = N_n M_n + R_n$, ordre $R_n <$ ordre M_n ,

$M_{n+1} = M_n + R_n$.

Il est clair que M_n est unitaire d'ordre m et donc pour tout n , M_n N_n et R_n appartiennent à $H(A)$.

De plus, comme $\overline{L} = \overline{M}_1$, on a $\overline{N}_1 = 1$ et $\overline{R}_1 = 0$, soit $|N_1 - 1| < 1$ et $|R_1| < 1$. Posons $\lambda = \max(|N_1 - 1| , |R_1|)$.

Par application du lemme 5.1, on démontre alors facilement par induction sur n que

(5.2.1) $$|N_n - 1| \leqslant \lambda ,$$

(5.2.2) $$|R_n| \leqslant \lambda^n ,$$

(5.2.3) $$|N_{n+1} - N_n| \leqslant \lambda^n .$$

Alors (5.2.2) montre que $R_n \longrightarrow 0$ et que M_n converge vers une limite M , unitaire d'ordre m , et (5.2.3) montre que N_n converge vers une limite N . On a alors à la limite

$$L = \lim_n (N_n M_n + R_n) = NM .$$

Appendice : Opérateurs différentiels en caractéristique p

A.1. On note $\overline{K}$ le corps résiduel de K , $\overline{E} = \overline{K}(X)$, $\overline{\mathcal{D}} = \overline{E}[D]$ l'anneau des opérateurs différentiels à coefficients dans $\overline{E}$.

Comme $\overline{K}$ est de caractéristique p , les éléments u de $\overline{E}$ tels que $Du = 0$ sont précisément les éléments de $\overline{K}(X^p)$. Les éléments de $\overline{\mathcal{D}}$ agissent donc comme opérateurs linéaires sur $\overline{E}$, considéré comme espace vectoriel sur $\overline{K}(X^p)$ (mais on n'identifiera pas $\overline{\mathcal{D}}$ avec un sous-espace de $L(\overline{E} , \overline{E})$).

L'opérateur D^p annihile $\overline{E}$ et se trouve dans le centre de $\overline{\mathcal{D}}$.

L'anneau $\overline{\mathcal{D}}$ possède un algorithme de division euclidienne à gauche et à droite, il en résulte que les idéaux à gauche sont principaux.

Une base de $\overline{K}(X)$ (espace vectoriel sur $\overline{K}(X^p)$) est formée des polynômes $1 , X , \ldots , X^{p-1}$. (Si $u \in \overline{K}[X]$ la décomposition de u suivant cette base est évidente ; si $u = v/w$, v et $w \in \overline{K}[X]$, alors $w^p \in \overline{K}[X^p]$, et donc

$$u = (1/w^p) w^{p-1} v$$

se décompose aussi suivant cette base). On a donc $\dim_{\overline{K}(X^p)} \overline{E} = p$.

A.2. Si $u_1 \ldots u_m$ appartient à $\overline{E}$, alors $u_1 \ldots u_m$ sont linéairement indépendants au-dessus de $\overline{K}(X^p)$ si, et seulement si, leur wronskien n'est pas nul (ceci est lié au fait que le noyau de D dans $\overline{E}$ est $\overline{K}(X^p)$; on peut utiliser ce résultat pour démontrer que la dimension de $\overline{E}$ au-dessus de $\overline{K}(X^p)$ est p .). Il en résulte que si $L \in \overline{\mathcal{D}}$ est d'ordre m, alors $\operatorname{Ker} L$, son noyau dans $\overline{E}$, est de dimension, au-dessus de $\overline{K}(X^p)$, au plus m.

A.3. LEMME. - *Soit* $L \in \overline{\mathcal{D}}$, *d'ordre* m. *Alors*

$$\dim_{\overline{K}(X^p)} \operatorname{Ker} L = m$$

si, et seulement si, D^p *appartient à l'idéal* $\overline{\mathcal{D}}L$.

Démonstration. - Soient A, $B \in \overline{\mathcal{D}}$, avec ordre $B \leq m - 1$, tels que

$$D^p = AL + B .$$

Comme D^p annihile E, $\operatorname{Ker} L \subset \operatorname{Ker} B$. Il résulte donc de A.2 que, si $\dim \operatorname{Ker} L = m$, $B = 0$.

Réciproquement, si $B=0$, alors AL annihile $\overline{E}$, donc $\operatorname{Im} L \subset \operatorname{Ker} A$. Alors

$$\dim \operatorname{Im} L \leq \text{ordre } A = p - m ,$$

donc $\dim \operatorname{Ker} L \geq m$, et on a l'égalité en vertu de A.2.

A.4. COROLLAIRE. - *Soit* M *le générateur (unitaire) de l'idéal à gauche engendré par* D^p *et* L, *c'est-à-dire que*

$$\overline{\mathcal{D}}D^p + \overline{\mathcal{D}}L = \overline{\mathcal{D}}M .$$

Alors

$$\operatorname{Ker} L = \operatorname{Ker} M ,$$

et la dimension du noyau de M *coïncide avec l'ordre de* M.

Démonstration. - Comme $D^p \in \overline{\mathcal{D}}M$, $\dim \operatorname{Ker} M = \text{ordre } M$. Comme L est un multiple à gauche de M, $\operatorname{Ker} M \subset \operatorname{Ker} L$. Comme il existe A, $B \in \overline{\mathcal{D}}$ tels que $AD^p + BL = M$, $\operatorname{Ker} L \subset \operatorname{Ker} M$.

A.5. COROLLAIRE. - *Si* $\operatorname{Ker} L = \{0\}$, *alors*

$$\overline{\mathcal{D}}D^p + \overline{\mathcal{D}}L = \overline{\mathcal{D}} ,$$

et réciproquement.

A.6. COROLLAIRE. - *Soient* L, $N \in \overline{\mathcal{D}}$. *Alors* $\operatorname{Ker} L \subset \operatorname{Ker} N$ *si, et seulement si,* $N \in \overline{\mathcal{D}}D^p + \overline{\mathcal{D}}L$.

Démonstration. - Soit M le générateur de l'idéal $\overline{\mathcal{D}}D^p + \overline{\mathcal{D}}L$. Si $N = BM$, alors $\operatorname{Ker} N \supset \operatorname{Ker} M = \operatorname{Ker} L$.

Réciproquement, soient A, $B \in \overline{\mathcal{D}}$, ordre $B \leq m - 1$, tels que $N = AM + B$. Alors $\operatorname{Ker} N \supset \operatorname{Ker} L = \operatorname{Ker} M$ implique que $\operatorname{Ker} B$ contient $\operatorname{Ker} M$, il résulte alors de A.2 que $B = 0$.

A.7. Soit maintenant L une $n \times n$ matrice à coefficients dans $\overline{\mathcal{D}}$. Alors L

agit sur $\overline{E}^n$, espace vectoriel sur $\overline{K}(X^p)$.

LEMME. – <u>Si L est injectif en tant qu'endomorphisme de $\overline{E}^n$, alors il existe deux $n \times n$ matrices, Q et H , à coefficients dans $\overline{\mathfrak{D}}$, telles que</u>

$$QL + HD^p = I .$$

<u>Démonstration</u>. – En vertu du théorème de l'annexe de [2], il existe deux $n \times n$ matrices inversibles U et V , à coefficients dans $\overline{\mathfrak{D}}$, telles que VLU soit une matrice diagonale de coefficients $\varepsilon_1 \dots \varepsilon_n$ (remarquons qu'on ne peut pas supposer que les ε_j sont tous, sauf un, égaux à 0 ou 1 , car $\overline{E}$ étant de caractéristique non nulle, $\overline{\mathfrak{D}}$ n'est pas simple). Par hypothèse L est injectif et donc chaque ε_j est injectif dans $\overline{E}$. Alors, en vertu du corollaire A.5 il existe A_j et $B_j \in \overline{\mathfrak{D}}$ tels que

$$A_j \, \varepsilon_j + B_j \, D^p = 1 , \quad 1 \leq j \leq n .$$

Soient alors A et B les matrices diagonales dont les termes diagonaux sont respectivement $(A_1 , \dots , A_n)$ et $(B_1 , \dots , B_n)$. On a donc

$$AVLU + BD^p = I .$$

Multiplions cette équation à gauche par U , et à droite par U^{-1} , et posons $Q = UAV$ et $H = UBU^{-1}$. On obtient ainsi la formule annoncée dans le lemme.

A.8. COROLLAIRE. – <u>Un endomorphisme différentiel injectif de $\overline{E}^n$ a un inverse qui est aussi un endomorphisme différentiel.</u>

(Par endomorphisme différentiel de $\overline{E}^n$, on veut dire un endomorphisme de $\overline{E}^n$, en tant que $\overline{K}(X^p)$ espace vectoriel, défini par une $n \times n$ matrice à coefficients dans $\overline{\mathfrak{D}}$.)

A.9. Au lieu d'étudier l'action d'un élément de $\overline{\mathfrak{D}}$ sur $\overline{E} = \overline{K}(X)$, on aurait pu le faire agir sur $\overline{K}((X))$. Les éléments de $\overline{K}((X))$ annihilés par D sont précisément les éléments de $\overline{K}((X^p))$. On montre comme en A.1 que $\overline{K}((X))$ est un espace vectoriel sur $\overline{K}((X^p))$ de dimension p , et que $(1 , X , \dots , X^{p-1})$ forme une base de cet espace. On a donc

$$\overline{K}((X)) = \overline{K}(X) \otimes_{\overline{K}(X^p)} \overline{K}((X^p)) .$$

Cette remarque nous permet de ramener l'étude d'un opérateur différentiel dans $K((X))$ à son étude dans $K(X)$. En effet, si $L \in \overline{\mathfrak{D}}$, il lui correspond un endomorphisme L_1 de $\overline{K}(X)$ et un endomorphisme L_2 de $\overline{K}((X))$, et l'on a

$$L_2 = L_1 \otimes_{\overline{K}(X^p)} 1_{\overline{K}((X^p))}$$

et donc

$$\operatorname{Ker} L_2 = \operatorname{Ker} L_1 \otimes \overline{K}((X^p)) .$$

Comme tout élément de $\overline{K}(X)$ est le produit d'un polynôme par un élément de $\overline{K}(X^p)$, le noyau de L dans $\overline{K}(X)$ possède une base formée de polynômes. Le noyau de L dans $\overline{K}((X))$ possède donc aussi une base formée de polynômes.

On peut, en particulier, appliquer ces résultats à $\overline{K}[[X]]$. On voit donc que toute série formelle solution de L est une combinaison linéaire à coefficients dans $K((X^p))$ de solutions polynômes de L (On ne peut malheureusement pas affirmer que ce soit une combinaison à coefficients dans $K[[X^p]]$, sauf bien sûr si la dimension sur $\overline{K}(X^p)$ du noyau de L dans $\overline{K}(X)$ est 1).

BIBLIOGRAPHIE

[1] ROBBA (P.). - On the index of p-adic differential operators, I, Annals of Math., t. 101, 1975, p. 280-316.

[2] ROBBA (P.). - Factorisation d'un opérateur différentiel, Groupe d'étude d'Analyse ultramétrique, 2e année, 1974/75, n° 2, 16 p.

[3] ROBBA (P.). - Factorisation d'un opérateur différentiel. Applications, Groupe d'étude d'Analyse ultramétrique, 2e année, 1974/75, n° 10, 6 p.

(Texte reçu le 2 juin 1975)

Philippe ROBBA
138 rue Nationale
75013 PARIS