Séminaire Dubreil.
Algèbre et théorie
des nombres

J.-C. Herz

Idéaux différentiels

Séminaire Dubreil. Algèbre et théorie des nombres, tome 5-6 (1951-1953), exp. nº 5, p. 1-10
<http://www.numdam.org/item?id=SD_1951-1953__5-6__A5_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
THÉORIE DES IDÉAUX
Années 1951-1953
-:-:-:-

V. IDÉAUX DIFFÉRENTIELS

par J.-G. HERZ

Les idéaux différentiels ont été introduits par RAUDENBUSH [4], en 1933, spécialement en vue de la théorie algébrique des systèmes d'équations différentielles créée par RITT [5].

1. Anneaux différentiels.

Un anneau différentiel est un anneau commutatif $\mathfrak{A}$ muni d'une application dans lui-même, appelée dérivation, telle que, a' désignant le dérivé de l'élément a, on ait

$$(a + b)' = a' + b'$$

et

$$(ab)' = a'b + ab'$$

THÉORÈME. - " Un anneau d'intégrité différentiel $\mathfrak{A}$ peut-être plongé dans un corps différentiel". En effet, si l'on définit sur les couples (a , b), éléments du corps $\mathfrak{K}$ des quotients de $\mathfrak{A}$, la dérivation

$$(a , b)' = (a'b - ab' , b^2)$$

il est aisé de voir que $\mathfrak{K}$ est un corps différentiel contenant $\mathfrak{A}$.

a. Idéaux. - Soit $\mathfrak{B}$ une partie de $\mathfrak{A}$. La relation $a - b \in \mathfrak{B}$ entre les éléments a et b de $\mathfrak{A}$ est une relation d'équivalence si et seulement si $\mathfrak{B}$ est un sous-module de $\mathfrak{A}$. Elle est alors régulière pour l'addition, et les classes d'équivalence forment un module $\mathfrak{A}/\mathfrak{B}$.

Elle est régulière pour la dérivation si et seulement si $\mathfrak{B}$ est un sous-module différentiel de $\mathfrak{A}$. $\mathfrak{A}/\mathfrak{B}$ est alors un module différentiel.

Elle est régulière pour la multiplication si et seulement si $\mathfrak{B}$ est un idéal de $\mathfrak{A}$. $\mathfrak{A}/\mathfrak{B}$ est alors un anneau. Ces deux dernières conditions font de $\mathfrak{B}$ un idéal différentiel de $\mathfrak{A}$.

Tout diviseur de zéro de $\mathfrak{A}/\mathfrak{B}$ est nilpotent si et seulement si l'idéal $\mathfrak{B}$ est primaire.

$\mathfrak{A}/\mathfrak{B}$ est sans élément nilpotent si et seulement si $\mathfrak{B}$ est <u>semi-premier</u> [3].

$\mathfrak{A}/\mathfrak{B}$ est un anneau d'intégrité si et seulement si $\mathfrak{B}$ est premier. Un idéal primaire semi-premier est premier, et réciproquement. $\mathfrak{A}/\mathfrak{B}$ est un corps si et seulement si $\mathfrak{B}$ est un idéal sans diviseurs.

b. <u>Anneau de polynômes différentiels</u>. - Si l'on adjoint à un corps différentiel $\mathfrak{F}$ les indéterminées y_{ij} $(i = 1, 2, \ldots, n$, j entier ≥ 0 quelconque) on obtient un anneau différentiel $\mathfrak{A} = \mathfrak{F}\{y_1, y_2, \ldots, y_n\}$ avec $y'_{ij} = y_{i,j+1}$; $y_i = y_{i0}$ est appelée indéterminée, y_{ij} la j-ième dérivée de y_i. Dans la suite, $\mathfrak{F}$ sera supposé de <u>caractèristique nulle</u> [6].

2. <u>Idéaux parfaits</u>.

Un idéal <u>parfait</u> est un idéal différentiel semi-premier.

Un idéal $\mathfrak{B}$ est semi-premier si et seulement si

$$a^p \in \mathfrak{B} \longrightarrow a \in \mathfrak{B} \qquad (p \text{ entier } > 0)$$

ou encore

$$\mathfrak{B} = \text{radical } \mathfrak{B} .$$

THÉORÈME 1. - <u>Si $\mathfrak{p}$ est un idéal parfait,</u> $ab \in \mathfrak{p} \longrightarrow a'b \in \mathfrak{p}$.

En effet, $\mathfrak{p}$ contient $(ab)' = a'b + ab'$, donc $a'^2 b^2 + ab\,a'b'$, donc $a'^2 b^2$, donc $a'b$.

COROLLAIRE 1. - <u>Si $\mathfrak{p}$ est parfait,</u>

$$ab \in \mathfrak{p} \longrightarrow a^{(i)}\, b^{(j)} \in \mathfrak{p} \qquad [4]$$

COROLLAIRE 2. - <u>Si $\mathfrak{p}$ est parfait et $\mathfrak{M} \subseteq \mathfrak{A}$, $\mathfrak{p} : \mathfrak{M}$ est un idéal parfait</u> [1].

a. <u>Calcul des idéaux</u>. - Soit $\mathfrak{B}$ une partie de $\mathfrak{A}$. L'intersection de tous les idéaux ordinaires contenant $\mathfrak{B}$ est l'idéal $(\mathfrak{B})$. L'intersection de tous les idéaux différentiels contenant $\mathfrak{B}$ est un idéal différentiel, noté $[\mathfrak{B}]$. L'intersection de tous les idéaux parfaits contenant $\mathfrak{B}$ est un idéal parfait, noté $\{\mathfrak{B}\}$.

$[\mathfrak{B}]$ est l'ensemble des sommes finies $\sum \lambda_{ij}\, b_i^{(j)}$ où $b_i \in \mathfrak{B}$ et $\lambda_{ij} \in \mathfrak{A} \cup C$, C étant l'anneau des entiers.

$\{\mathcal{B}\}$ est la réunion d'une suite non décroissante d'idéaux différentiels $\mathcal{B}_i$, avec $\mathcal{B}_0 = [\mathcal{B}]$, $\mathcal{B}_i = [\text{rad } \mathcal{B}_{i-1}]$ [4].

$\{\mathcal{B}\}$ est aussi la réunion des idéaux semi-premiers $\mathcal{C}_i$ avec $\mathcal{C}_1 = \text{rad } [\mathcal{C}]$, $\mathcal{C}_i = \text{rad } [\mathcal{C}_{i-1}]$ [2].

On a

$$\mathcal{B} \subseteq \mathcal{C} \rightarrow (\mathcal{B}) \subseteq (\mathcal{C}) \rightarrow [\mathcal{B}] \subseteq [\mathcal{C}] \rightarrow \{\mathcal{B}\} \subseteq \{\mathcal{C}\}$$

$$(\mathcal{B}) + (\mathcal{C}) = (\mathcal{B} \cup \mathcal{C})$$

$$[\mathcal{B}] + [\mathcal{C}] = [\mathcal{B} \cup \mathcal{C}]$$

$$\{\mathcal{B}\} + \{\mathcal{C}\} \subseteq \{\mathcal{B} \cup \mathcal{C}\}$$

$$(\mathcal{B}\mathcal{C}) \subseteq (\mathcal{B}) \cap (\mathcal{C})$$

$$[\mathcal{B}\mathcal{C}] \subseteq [\mathcal{B}] \cap [\mathcal{C}]$$

$$\{\mathcal{B}\mathcal{C}\} \subseteq \{\mathcal{B}\} \cap \{\mathcal{C}\}$$

$$[\mathcal{B}].[\mathcal{C}] \subseteq \{\mathcal{B}\mathcal{C}\} \quad \text{(en vertu du corollaire 1)}$$

b. Cas où $\mathcal{A}$ contient le corps r des rationnels.

LEMME. - Si $\mathcal{A} \supseteq r$ et $a^p \in [\mathcal{B}]$, on a $a'^{2p-1} \in [\mathcal{B}]$.

En effet $\frac{1}{p}(p\, a^{p-1} a') \in \mathcal{B}$, donc aussi $(p-1)\; a^{p-2} a'^2 + a^{p-1} a''$, donc aussi $a^{p-2} a'^2$, et par récurrence $a'^{2p-1} \in \mathcal{B}$.

THÉORÈME 2. - $\{\mathcal{B}\}$ est le radical de $[\mathcal{B}]$.

COROLLAIRE 3. - $\{\mathcal{B}\mathcal{C}\} = \{\mathcal{B}\} \cap \{\mathcal{C}\}$.

Montrons l'inclusion du second membre dans le premier : si $a \in \{\mathcal{B}\} \cap \{\mathcal{C}\}$, $a^p \in [\mathcal{B}]$, $a^q \in [\mathcal{C}]$, donc $a^{p+q} \in [\mathcal{B}][\mathcal{C}] \subseteq \{\mathcal{B}\mathcal{C}\}$, et $a \in \{\mathcal{B}\mathcal{C}\}$.

COROLLAIRE 4. - $\{\mathcal{A} \cup \mathcal{B}\mathcal{C}\} = \{\mathcal{A} \cup \mathcal{B}\} \cap \{\mathcal{A} \cup \mathcal{C}\}$ [4].

En effet

$$(\mathcal{A} \cup \mathcal{B}\mathcal{C}) \subseteq (\mathcal{A} \cup \mathcal{B}) ,$$

donc

$$\{\mathfrak{A} \cup \mathfrak{B}\mathfrak{C}\} \subseteq \{\mathfrak{A} \cup \mathfrak{B}\}$$

Inversement,

$$\{\mathfrak{A} \cup \mathfrak{B}\} \cap \{\mathfrak{A} \cup \mathfrak{C}\} = \{\mathfrak{A}^2 \cup \mathfrak{A}\mathfrak{B} \cup \mathfrak{A}\mathfrak{C} \cup \mathfrak{B}\mathfrak{C}\}$$

(corollaire 3), et

$$(\mathfrak{A}^2 \cup \mathfrak{A}\mathfrak{B} \cup \mathfrak{A}\mathfrak{C} \cup \mathfrak{B}\mathfrak{C} \subseteq (\mathfrak{A} \cup \mathfrak{B}\mathfrak{C}) .$$

Donc

$$\{\mathfrak{A} \cup \mathfrak{B}\} \cup \{\mathfrak{A} \cup \mathfrak{C}\} \subseteq \{\mathfrak{A} \cup \mathfrak{B}\mathfrak{C}\}$$

GÉNÉRALISATION.

$$\left\{ \prod_1^p \mathfrak{A}_i \cup \prod_1^q \mathfrak{B}_j \right\} = \bigcap_{\substack{i=1 \\ j=1}}^{\substack{i=p \\ j=q}} \{\mathfrak{A}_i \cup \mathfrak{B}_j\}$$

3. Axiome de la base.

REMARQUE. - Dans l'anneau de polynômes différentiels à une indéterminée $\mathfrak{F}\{y\}$, l'axiome de la base n'est pas vérifiée. En effet le système infini des polynômes A_1, A_2, ..., A_p, ... où $A_i = y_{i-1}\, y_i$ n'est pas contenu dans l'idéal différentiel engendré par un sous-système fini.

Un axiome plus faible est cependant rempli par les anneaux de polynômes différentiels sur un corps de caractéristique nulle.

DÉFINITION. - On dit que Φ est une base (finie) de Σ si $\Phi \subset \Sigma \subset \{\Phi\}$. Si Σ a une base, $\{\Sigma\}$ a une base, et réciproquement [4]. On voit, comme dans la théorie ordinaire des idéaux, que l'axiome de la base est équivalent à l'axiome des chaînes d'idéaux parfaits, qui entraîne pour tout idéal parfait Σ l'existence d'une décomposition

$$\Sigma = \Sigma_1 \cap \Sigma_2 \cap \ldots \cap \Sigma_p$$

en idéaux parfaits indécomposables en idéaux parfaits (plus brièvement "indécomposables").

Tout idéal premier est irréductible, et a fortiori indécomposable. Réciproquement, THÉORÈME 3. - Si $\mathfrak{A} \ni \Gamma$, tout idéal parfait indécomposable est premier.

En effet, si Σ n'est pas premier, il existe $a \notin \Sigma$, $b \notin \Sigma$ tels que $ab \in \Sigma$, et

$$\Sigma = \{\Sigma \cup ab\} = \{\Sigma \cup a\} \cap \{\Sigma \cup b\}$$

corollaire 4), donc Σ n'est pas indécomposable.

On a dans ce cas une décomposition en idéaux premiers. Elle est unique si l'on supprime les diviseurs premiers surabondants. Les diviseurs restants sont appelés diviseurs premiers essentiels.

THÉORÈME 4. - Tout système de polynômes différentiels sur un corps de caractéristique nulle a une base.

La démonstration de ce théorème de la base sera donnée en appendice.

4. Théorème des zéros.

Soit $\mathfrak{A} = \mathfrak{F}\{y_1 \dots y_n\}$ un anneau de polynômes différentiels sur un corps $\mathfrak{F}$ de caractéristique nulle.

On appelle zéro d'un polynôme de A l'ensemble η de n éléments $\eta_1, \dots, \eta_n$ d'un surcorps différentiel $\mathfrak{F}_1$ de $\mathfrak{F}$ tels que, si l'on remplace y_{ij} par $\eta_i^{(j)}$ dans A, l'élément de $\mathfrak{F}_1$ obtenu soit nul, ce qu'on note $A(\eta_1, \dots, \eta_n) = 0$ ou $A(\eta) = 0$

Un zéro commun à tous les polynômes d'un système Σ est appelé zéro de Σ

THÉORÈME 5. - Tout idéal premier Σ distinct de $\mathfrak{A}$ a un zéro.

En effet, l'idéal Σ, étant distinct de $\mathfrak{A} = (1)$, n'a en commun avec $\mathfrak{F}$ que l'élément 0, donc l'homomorphisme canonique qui applique $\mathfrak{A}$ sur $\bar{\mathfrak{A}} = \mathfrak{A}/\Sigma$ est un isomorphisme pour $\mathfrak{F}$. D'autre part, Σ étant premier, $\bar{\mathfrak{A}}$ possède un corps des quotients (paragraphe 1) $\mathfrak{F}_1$, qui est par suite un surcorps de $\mathfrak{F}$. Si $\bar{G}$ est l'homomorphe d'un polynôme $G \in \mathfrak{A}$, on a $\bar{G} = G(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n)$. Donc

1° $\eta = (\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n)$ est un zéro de Σ, et le théorème est démontré.

2° Tout polynôme s'annulant en η appartient à Σ. η est appelé zéro générique de Σ. Si l'on appelle V l'ensemble des zéros de Σ (variété de Σ), $G(\eta) = 0$ entraîne $G(V) = 0$.

THÉORÈME 6.(théorème des zéros). - Si un polynôme $\mathcal{G}$ est annulé par tout zéro du système $F_1, F_2, \dots, F_r$, $\mathcal{G}$ appartient à l'idéal $\{F_1, F_2, \dots, F_r\}$

En effet, si $\Omega = \{F_1, F_2, \dots, F_r\}$ est $\mathcal{U}$, la conclusion est vérifiée.

Si $\Omega \neq \mathcal{U}$, Ω est l'intersection de p idéaux premiers différentiels $\Sigma_1, \Sigma_2, \dots, \Sigma_p$ distincts de $\mathcal{U}$. Soit $\eta_{(i)}$ un zéro générique de Σ_i ; $F_j \in \Sigma_i$ quel que soit j, donc $\mathcal{G}(\eta_{(i)}) = 0$, donc $\mathcal{G} \in \Sigma_i$. Donc $\mathcal{G} \in \Omega$, ce qu'il fallait démontrer.

Ω étant le radical de $[F_1, F_2, \dots, F_r]$, la conclusion s'exprime encore ainsi : une certaine puissance de $\mathcal{G}$ est une combinaison linéaire (dont les coefficients sont des polynômes différentiels) des F_i et de leurs dérivées.

REMARQUE. - Réciproquement, si $\mathcal{G} \in \{F_1, \dots, F_r\}$, $\mathcal{G}$ est évidemment annulé par tout zéro du système $F_1, \dots, F_2$. Plus généralement, $\mathcal{G}$ appartient à un idéal parfait Ω si et seulement si tout zéro de Ω est un zéro de $\mathcal{G}$. Il y a donc une correspondance biunivoque entre idéaux parfaits et variétés.

APPENDICE

Démonstration du théorème de la base (théorème 4) [6].

5. Comparaisons des polynômes différentiels.

On appelle ordre d'un polynôme A relativement à une indéterminée y_k le plus grand indice j tel que y_{kj} apparaisse effectivement dans A. Si A ne contient aucune y_{ki}, il sera dit d'ordre 0 par rapport à y_k.

On appelle classe d'un polynôme A le plus grand indice k tel que y_k ou une de ses dérivées apparaisse effectivement dans A.

Si $A \in \mathcal{F}$, A sera dit de classe zéro.

On dit que A_1 est (de rang) inférieur à (celui de) A_2 relativement à y_k soit si l'ordre de A_1 pour y_k est inférieur à celui de A_2, soit si A_1 et A_2 ont même ordre q pour y_k et si le degré de A_1 pour y_{kq} est inférieur à celui de A_2. On dit que A_1 est inférieur à A_2 soit si la classe de A_1 est inférieure à celle de A_2, soit si A_1 et A_2 ont même classe p et si A_1 est inférieur à A_2 pour y_p. Notations $A_1 < A_2/y_k$,

$A_1 < A_2$.

Si A_1 n'est pas inférieur à A_2 , ni A_2 à A_1 , A_1 et A_2 sont dits <u>de même rang</u>. Notation $A_1 \bar{\sim} A_2$.

A_2 est dit <u>réduit</u> pour A_1 , si A_1 est de classe de $p > 0$ et $A_2 < A_1/y_p$.
r polynômes $A_1\ A_2 \ldots A_r$ pris dans cet ordre constituant une <u>chaîne</u>, soit si $r = 1$ et $A_1 \neq 0$, soit si les classes des A_i sont positives et croissantes, chacun d'eux étant réduit pour tous ses précécesseurs. Une chaîne a au plus n termes.

$\Phi_1 = A_1 , A_2 , \ldots , A_r$ est dite <u>inférieure</u> à $\Phi_2 = B_1 , B_2 , \ldots , B_s$ soit si $A_i = B_i$ pour tout $i \leq q$ et $A_{q+1} < B_{q+1}$, soit si $r > s$ et $A_i \bar{\sim} B_i$ pour tout $i \leq s$.

REMARQUE importante. - Dans un système $\sum$ de polynômes, il existe un polynôme de rang minimum ; il existe une chaîne ; il existe une chaîne de rang minimum. Une telle chaîne est appelée <u>chaîne caractéristique</u> de $\sum$.

Un système $\sum_1$ sera dit <u>inférieur</u> à un système $\sum_2$ si toute chaîne caractéristique de $\sum_1$ est inférieure à toute chaîne caractéristique de $\sum_2$.

Un polynôme B est dit <u>réduit</u> pour la chaîne Φ s'il est réduit pour tout terme de la chaîne.

THÉORÈME 7. - Φ, <u>chaîne de</u> $\sum$, <u>est caractéristique si et seulement si aucun polynôme non nul de</u> $\sum$ <u>n'est réduit pour</u> Φ .

$(\Phi = A_1 , A_2 , \ldots , A_r)$.

Supposons $F \neq 0$, $\in \sum$, et réduit pour Φ . Supposons la classe de F supérieure à celle de A_j et non à celle de A_{j+1} . Le système $A_1 , A_2 , \ldots , A_j$; F est une chaîne inférieure à Φ , donc Φ n'est pas caractéristique.

Supposons Φ non caractéristique, et $\Phi > \Psi = B_1 , B_2 , \ldots , B_s$. Si $A_i \bar{\sim} B_i$ pour tout $i \leq q$ et $A_{q+1} > B_{q+1}$, on prendre $F = B_{q+1}$. Si $r < s$ et $A_i \bar{\sim} B_i$ tout $i \leq r$, on prendra $F = B_{r+1}$.

6. <u>Algorithme de réduction</u>.

Si A est un polynôme de classe $p > 0$, d'odre q pour y_p , de degré m pour y_{pq} , on appelle : séparant de A , le polynôme

$$S = \frac{\partial A}{\partial y_{pq}} \quad ,$$

initial de A , le polynôme I coefficient de y_{pq}^n dans A .

THÉORÈME 8. - <u>Φ étant la chaîne</u> $A_1 , A_2 , \ldots , A_r$ <u>(A_1 de classe > 0)</u> <u>S_i et I_i étant le séparant et l'initial de A_i , et $\mathcal{G}$ étant un polynôme quelconque, il existe un polynôme R réduit pour Φ et des entiers non négatifs</u> $s_1 , s_2 , \ldots , s_r , t_1 , t_2 , \ldots , t_r$ <u>tels que</u>

$$S_1^{s_1} S_2^{s_2} \ldots S_r^{s_r} I_1^{t_1} I_2^{t_2} \ldots I_r^{t_r} \mathcal{G} \equiv R(\Phi) .$$

DÉMONSTRATION. - <u>Supposons d'abord</u> $r = 1$. On a :

$$A = Iy_{pq}^n + B \quad \text{avec} \quad \text{ord } I/y_p < q \quad \text{et} \quad B < A$$

$$A^{(h)} = Sy_{p,q+h} + C \quad \text{avec} \quad S < A \quad \text{et} \quad \text{ord } C/y_p < q + h .$$

Supposons $\mathcal{G}$ d'ordre $q + k > q$ pour y_p . On a

$$\mathcal{G} = Dy_{p,q+k} + E \quad \text{avec} \quad D < \mathcal{G} \text{ et ord } E/y_p < q + k$$

d'où

$$S \mathcal{G} \equiv \mathcal{G}_1 \ (A^{(k)}) \quad \text{avec} \quad \mathcal{G}_1 < \mathcal{G} .$$

D'où en répétant l'opération,

$$S^u \mathcal{G} \equiv \mathcal{G}_u \ (A^{(k)}) \quad \text{avec} \quad \text{ord } \mathcal{G}_1 < \text{ord } \mathcal{G}/y_p$$

et ensuite

$$S^s \mathcal{G} \equiv H(A^{(k)} , A^{(k-1)} , \ldots , A'' , A') \quad \text{avec} \quad \text{ord } H/y_p \leq q .$$

Si H est d'ordre q pour y_p , on aura, par simple division

$$I^t H \equiv R(A) \quad \text{avec degré} \quad R/y_{pq} < m \text{ , donc } R \text{ réduit pour } A .$$

En définitive, $S^s I^t \mathcal{G} \equiv R[A]$.

Remarquons que $R \leq \mathcal{G}/y_p$, pour $p' > p$.

<u>Supposons</u> $r > 1$. On a

$$S_r^{s_r} I_r^{t_r} \mathcal{G} \equiv R_r[A_r] , \quad R_r \text{ réduit pour } A_r ,$$

$$S_{n-1}^{s_{r-1}} I_{r-1}^{t_{r-1}} R_r \equiv R_{r-1}[A_{r-1}] , \quad R_{r-1} \text{ réduit pour } A_{r-1},$$

ainsi que pour A_r d'après la remarque précédente.

De proche en proche, nous trouvons bien

$$S_1^{s_1} S_a^{s_a} \dots S_r^{s_r} I_1^{t_1} I_2^{t_2} \dots I_r^{t_r} \equiv R[\Phi] \,, \quad R \text{ réduit pour } \Phi \,.$$

R est appelé <u>reste</u> de $\mathcal{G}$ relativement à la chaîne Φ .

7. <u>Théorème de la base.</u>

Supposons que le théorème soit faux. Il existerait alors, d'après la remarque du paragraphe 5, un système Σ sans base tel que tout système Σ' inférieur à Σ ait une base. Soit

(1) $$A_1 \,, A_2 \,, \dots \,, A_r$$

une chaîne caractéristique de Σ, S_i et I_i la séparant et l'initial de A_i .

Le système Ω formé par les termes de (1) et les restes relatifs à (1) des autres éléments de Σ a une base. En effet, si tous les restes sont nuls, (1) est une base. Si un reste n'est pas nul, (1) n'est pas caractéristique pour Ω (théorème 7) et Ω, inférieur à Σ, a une base. Soient

$$\Psi = A_1 \,, A_2 \,, \dots \,, A_n \,, R_1 \,, \dots \,, R_s$$

cette base, B_j le polynôme de Σ dont R_j est le reste.

Le système $\Sigma \cup S_i$ a une base, car S_i est réduit pour (1) ; de même pour le système $\Sigma \cup I_i$. On peut donner à $\Sigma \cup S_i$ et $\Sigma \cup I_i$ les bases $\Phi \cup S_i$ et $\Phi \cup I_i$, où Φ , indépendant de i , contient les A_k et les B_j et est inclus dans Σ . Remarquons que $\Psi \subset [\Phi]$. En effet $R_i \equiv B_i H_i[A_1 \,, \dots \,, A_r]$ (théorème 8), donc $R_i \in [A_1 \,, A_2 \,, \dots \,, A_r \,, B_i] \subseteq [\Phi]$.

Montrons que, contrairement à l'hypothèse, Φ est une base de Σ .

Soit $A \in \Sigma$, distinct des A_k . Il y correspond un élément R de Ω avec

$$S_1^{s_1} S_2^{s_2} \dots S_r^{s_r} I_1^{t_1} I_2^{t_2} \dots I_r^{t_r} A = H A \equiv R[A_1 \,, \dots \,, A_r] \,.$$

On a

$$A \in \Sigma \subseteq \{\Sigma \cup H\} = \bigcap_i \{\Sigma \cup S_i\} \; \bigcap_i \{\Sigma \cup I_i\} = \bigcap_i \{\Phi \cup S_i\} \; \bigcap_i \{\Psi \cup I_i\} = \{\Phi \cup H\}$$

(d'après le corollaire A), donc p étant un certain entier positif,

$$A^p \in [\Phi] + [H] \,, \text{ d'où } A^{p+1} \in [\Phi] A + [H] A \subseteq \{\Phi\} + \{H A\} \,.$$

Or $H A \equiv R[\psi]$ et $R \in \Omega \subseteq \{\psi\}$, donc $\{HA\} \subseteq \{\psi\} \subseteq \{\Phi\}$, d'où $A^{p+1} \in \{\Phi\}$ et $A \in \{\Phi\}$.

Cette contradiction montre que le théorème est vrai.

BIBLIOGRAPHIE

[1] KOLCHIN (E. R.). - On the exponents of differential ideals, Annals of Math., Series 2, t. 42, 1941, p. 740-777.

[2] KOLCHIN (E. R.). - On the basis theorem for differential systems, Trans. Amer. math. Soc., t. 52, 1942, p. 115-127.

[3] KRULL (Wolfgang). - Idealtheorie in Ringen ohne Endlichkeitsbedingung, Math. Annalen, t. 101, 1929, p. 729-744.

[4] RAUDENBUSH (H. W.). - Ideal theory and algebraic differential equations, Trans. Amer. math. Soc., t. 36, 1934, p. 361-368.

[5] RITT (Joseph F.). - Differential equations from the algebraic standpoint. - New-York, American mathematical Society, 1932 (Amer. math. Soc. Colloquium Publications, n° 14).

[6] RITT (Joseph F.). - Differential algebra. - New-York, American mathematical Society, 1950 (Amer. math. Soc. Colloquium Publications, n° 33).