

# 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. n° 5,  
p. 1-10

[http://www.numdam.org/item?id=SD\\_1951-1953\\_\\_5-6\\_\\_A5\\_0](http://www.numdam.org/item?id=SD_1951-1953__5-6__A5_0)

© Séminaire Dubreil. Algèbre et théorie des nombres  
(Secrétariat mathématique, Paris), 1951-1953, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## 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  $\mathcal{A}$  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

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

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

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

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

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

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

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

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

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

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

b. Anneau de polynômes différentiels. - Si l'on adjoint à un corps différentiel  $\mathcal{K}$  les indéterminées  $y_{ij}$  ( $i = 1, 2, \dots, n$ ,  $j$  entier  $\geq 0$  quelconque) on obtient un anneau différentiel  $\mathcal{A} = \mathcal{K}\{y_1, y_2, \dots, y_n\}$  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,  $\mathcal{K}$  sera supposé de caractéristique nulle [6].

## 2. Idéaux parfaits.

Un idéal parfait est un idéal différentiel semi-premier.

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

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

ou encore

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

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

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. - Si  $\mathfrak{p}$  est parfait,

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

COROLLAIRE 2. - Si  $\mathfrak{p}$  est parfait et  $\mathcal{B} \subseteq \mathcal{A}$ ,  $\mathfrak{p} : \mathcal{B}$  est un idéal parfait [1].

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

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

$\mathcal{C}$  étant l'anneau des entiers.

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

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

On a

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

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

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

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

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

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

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

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

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

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

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

THÉOREME 2. -  $\{\mathfrak{B}\}$  est le radical de  $[\mathfrak{B}]$ .

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

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

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

En effet

$$(\mathfrak{B} \cup \mathfrak{C}) \subseteq (\mathfrak{B} \cup \mathfrak{B}) ,$$

donc

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

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

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

Donc

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

GÉNÉRALISATION.

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

### 3. Axiome de la base.

REMARQUE. - Dans l'anneau de polynômes différentiels à une indéterminée  $\{ y \}$ , l'axiome de la base n'est pas vérifiée. En effet le système infini des polynômes  $A_1, A_2, \dots, A_p, \dots$  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.

DEFINITION. - On dit que  $\Phi$  est une base (finie) de  $\Sigma$  si  $\Phi \subset \Sigma$  et  $\Sigma = \langle \Phi \rangle$ .

Si  $\Sigma$  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  $\Sigma$  l'existence d'une décomposition

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

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

Tout idéal premier est irréductible, et a fortiori indécomposable. Réciproquement,

THÉOREME 3. - Si  $\mathcal{O} \neq \Gamma$ , tout idéal parfait indécomposable est premier.

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

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

corollaire 4), donc  $\Sigma$  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.

THÉOREME 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  $\mathcal{O} = \mathbb{k}\{y_1 \dots y_n\}$  un anneau de polynômes différentiels sur un corps  $\mathbb{k}$  de caractéristique nulle.

On appelle zéro d'un polynôme de  $\mathbb{k}$  l'ensemble  $\eta$  de  $n$  éléments  $\eta_1, \dots, \eta_n$  d'un surcorps différentiel  $\mathbb{k}_1$  de  $\mathbb{k}$  tels que, si l'on remplace  $y_{ij}$  par  $\eta_i^{(j)}$  dans  $\mathbb{k}$ , l'élément de  $\mathbb{k}_1$  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  $\Sigma$  est appelé zéro de  $\Sigma$

THÉOREME 5. - Tout idéal premier  $\Sigma$  distinct de  $\mathcal{O}$  a un zéro.

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

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

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

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

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

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

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

REMARQUE. - Réciproquement, si  $G \in \{F_1, \dots, F_r\}$ ,  $G$  est évidemment annulé par tout zéro du système  $F_1, \dots, F_r$ . Plus généralement,  $G$  appartient à un idéal parfait  $\Omega$  si et seulement si tout zéro de  $\Omega$  est un zéro de  $G$ . 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 de même rang. Notation  $A_1 \bar{\sim} A_2$ .

$A_2$  est dit réduit pour  $A_1$ , si  $A_1$  est de classe de  $p > 0$  et  $A_2 < A_1/y_p$ .  
 $r$  polynômes  $A_1, A_2, \dots, A_r$  pris dans cet ordre constituant une chaîne, 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 précédents. Une chaîne a au plus  $n$  termes.

$\bar{\Phi}_1 = A_1, A_2, \dots, A_r$  est dite inférieure à  $\bar{\Phi}_2 = B_1, B_2, \dots, B_s$  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  $\Sigma$  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 chaîne caractéristique de  $\Sigma$ .

Un système  $\Sigma_1$  sera dit inférieur à un système  $\Sigma_2$  si toute chaîne caractéristique de  $\Sigma_1$  est inférieure à toute chaîne caractéristique de  $\Sigma_2$ .

Un polynôme  $B$  est dit réduit pour la chaîne  $\bar{\Phi}$  s'il est réduit pour tout terme de la chaîne.

THÉORÈME 7. -  $\bar{\Phi}$ , chaîne de  $\Sigma$ , est caractéristique si et seulement si aucun polynôme non nul de  $\Sigma$  n'est réduit pour  $\bar{\Phi}$ .

$$(\bar{\Phi} = A_1, A_2, \dots, A_r) .$$

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

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

## 6. Algorithme de réduction.

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

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



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

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

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

DEMONSTRATION. - Supposons d'abord  $r = 1$ . On a :

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

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

Supposons  $G$  d'ordre  $q + k > q$  pour  $y_p$ . On a

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

d'où

$$S G \equiv G_1 (A^{(k)}) \text{ avec } G_1 < G.$$

D'où en répétant l'opération,

$$S^u G \equiv G_u (A^{(k)}) \text{ avec } \text{ord } G_u < \text{ord } G/y_p$$

et ensuite

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

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

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

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

Remarquons que  $R \equiv G/y_p$ , pour  $p' > p$ .

Supposons  $r > 1$ . On a

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

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

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 reste de  $\mathcal{G}$  relativement à la chaîne  $\Phi$ .

### 7. Théorème de la base.

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

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

une chaîne caractéristique de  $\sum$ ,  $S_i$  et  $I_i$  la séparant et l'initial de  $A_i$ .

Le système  $\Omega$  formé par les termes de (1) et les restes relatifs à (1) des autres éléments de  $\sum$  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  $\Omega$  (théorème 7) et  $\Omega$ , inférieur à  $\sum$ , a une base. Soient

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

cette base,  $B_j$  le polynôme de  $\sum$  dont  $R_j$  est le reste.

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

Montrons que, contrairement à l'hypothèse,  $\Phi$  est une base de  $\sum$ .

Soit  $A \in \sum$ , distinct des  $A_k$ . Il y correspond un élément  $R$  de  $\Omega$  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

$$A \in \sum \subset \left\{ \sum \cup H \right\} = \bigcap_i \left\{ \sum \cup S_i \right\} \bigcap_i \left\{ \sum \cup I_i \right\} = \bigcap_i \left\{ \Phi \cup S_i \right\} \bigcap_i \left\{ \bar{\Phi} \cup I_i \right\} = \left\{ \Phi \cup H \right\}$$

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

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

Or  $HA \equiv R[\Psi]$  et  $R \in \mathcal{D} \subseteq \{\Psi\}$ , donc  $\{HA\} \subseteq \{4\} \subseteq \{1\}$ , 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).
-