Séminaire Dubreil.
Algèbre et théorie
des nombres

Michel Lazard

## Valuations de polynômes et de séries formelles

*Séminaire Dubreil. Algèbre et théorie des nombres*, tome 16, n° 2 (1962-1963), exp. n° 23, p. 1-14

<http://www.numdam.org/item?id=SD_1962-1963__16_2_A9_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
16e année, 1962/63, n° 23



6 mai 1963

# VALUATIONS DE POLYNÔMES ET DE SÉRIES FORMELLES

par Michel LAZARD

## 1. Corps valués et polynômes.

(1.1) Une valuation $v$ d'un corps commutatif $k$ est une application $v : k \to \underset{\sim}{R} \cup \{+\infty\}$ qui vérifie les axiomes suivants. Pour tous $x , y \in k$ ,

$$x = 0 \iff v(x) = +\infty \ ;$$

$$v(x - y) \geqslant \min (v(x) , v(y)) \ ;$$

$$v(xy) = v(x) + v(y) \ .$$

(1.2) A partir d'un corps valué $k$ , nous construisons comme suit le corps résiduel $\overline{k}$ : soient $\Omega$ et $I$ l'ensemble des $x \in k$ qui vérifient respectivement $v(x) \geqslant 0$ et $v(x) > 0$ ; les axiomes (1.1) montrent que $\Omega$ est un sous-anneau de $k$ , et $I$ un idéal maximal de $\Omega$ . Le corps $\overline{k}$ est, par définition, le quotient $\Omega/I$ .

(1.3) Nous voulons pouvoir parler de l'ensemble des polynômes à coefficients dans un anneau $\Omega$ (associatif, commutatif et unitaire). Il s'agit des polynômes ordinaires, en un nombre fini quelconque de lettres.

Pour chaque entier $n \in \underset{\sim}{N}$ , nous prenons les $n$ "lettres" $x_{n,i}$ $(1 \leqslant i \leqslant n)$ , et nous construisons l'anneau de polynômes

(1.3.1) $$A^n(\Omega) = \Omega[x_{n,1} , \dots , x_{n,n}] \ .$$

Les ensembles $A^n(\Omega)$ sont disjoints ; leur réunion (pour $n \in \underset{\sim}{N}$ ) sera notée $\underset{\sim}{A}(\Omega)$ . Un élément $f \in A^n(\Omega)$ s'écrit univoquement comme une somme finie de monômes

(1.3.2) $$f = \sum_{\alpha \in \underset{\sim}{N}^n} c_\alpha X^\alpha \ ,$$

où $\alpha = (\alpha_1 , \dots , \alpha_n)$ , $X^\alpha = x_{n,1}^{\alpha_1} \dots x_{n,n}^{\alpha_n}$ et $c_\alpha \in \Omega$ . L'ensemble des monômes de multidegré $\alpha$ , c'est-à-dire de la forme $c_\alpha X^\alpha$ , sera noté $A^n_\alpha(\Omega)$ . Nous noterons $P_\alpha f$ le monôme $c_\alpha X^\alpha$ de la décomposition (1.3.2) de $f$ .

Lorsqu'il n'y aura pas d'ambiguïté, nous allègerons l'écriture en supprimant la référence à $\Omega$ . L'anneau $A^0(\Omega)$ des "polynômes en zéro lettre" se réduit à $\Omega$ . Il sera plus simple d'écrire $x$ (resp. $x$ et $y$ ) au lieu de $x_{1,1}$ (resp. $x_{2,1}$ et $x_{2,2}$ ).

(1.4) Nous savons composer les polynômes à coefficients dans un même anneau $\Omega$ . Soient $\underset{\sim}{A} = \underset{\sim}{A}(\Omega)$ , $f \in A^n$ , $g_1 , \dots , g_n \in A^m$ . Nous notons $f(g_1 , \dots , g_n) \in A^m$ le polynôme composé, c'est-à-dire l'image de $f$ par l'homomorphisme $\varphi : A^n \to A^m$ défini par les relations $\varphi(x_{n,i}) = g_i$ $(1 \leqslant i \leqslant n)$ .

(1.5) Enfin si $\Omega$ est un sous-anneau (resp. un quotient) de l'anneau $\Omega'$ , chaque $A^n(\Omega)$ s'identifie à un sous-anneau (resp. à un quotient) de $A^n(\Omega')$ .

## 2. Valuations des polynômes.

(2.1) Soit $k$ un corps valué (1.1). Formons l'ensemble $\underset{\sim}{A} = \underset{\sim}{A}(k)$ . Pour tout $n \in \underset{\sim}{N}$ et tout $f \in A^n$ , écrit sous la forme (1.3.2), nous posons

$$w_0(f) = \inf_{\alpha \in \underset{\sim}{N}^n} v(c_\alpha) , \tag{2.1.1}$$

et nous appelons $w_0(f)$ la valuation banale de $f$ . Si $\Omega$ désigne l'anneau de valuation de $k$ (1.2), nous pouvons écrire

$$f = cf' , \quad \text{avec} \quad c \in k , \quad v(c) = w_0(f) \tag{2.1.2}$$

et

$$f' \in A^n(\Omega) \subset A^n \quad (1.5) ,$$

et $w_0(f)$ est le plus grand nombre réel auquel correspondent un $c$ et un $f'$ vérifiant (2.1.2).

(2.2) La valuation banale $w_0$ vérifie les propriétés suivantes, que nous écrivons en remplaçant $w_0$ par $w$ ,

(V1) $\forall \ n \in \underset{\sim}{N} , \ \forall \ f \in A^n , \quad f = 0 \iff w(f) = + \infty .$

(V2) $\forall \ n \in \underset{\sim}{N} , \ \forall \ f , g \in A^n , \quad w(f + g) \geqslant \min (w(f) , w(g)) .$

(V3) $\forall \ n \in \underset{\sim}{N} , \ \forall \ \lambda \in k , \ \forall \ f \in A^n , \quad w(\lambda f) = v(\lambda) + w(f) .$

(V4) $\forall \ n \in \underset{\sim}{N} , \ \forall \ f \in A^n , \quad w(f) = \inf_{\alpha \in \underset{\sim}{N}^n} w(P_\alpha f) .$

(V5) $\forall \ m , n \in \underset{\sim}{N} , \ \forall \ \alpha = (\alpha_1 , \dots , \alpha_n) \in \underset{\sim}{N}^n , \ \forall \ f \in A^n_\alpha ,$
$\forall \ g_1 , \dots , g_n \in A^m ,$

$$w(f(g_1 , \dots , g_n)) \geqslant w(f) + \sum_{1 \leqslant i \leqslant n} \alpha_i \, w(g_i)$$

(V6) $\forall \ n \in \underset{\sim}{N} , \ \forall \ i \ \text{(avec } 1 \leqslant i \leqslant n \text{)}, \quad w(x_{n,i}) = 0 .$

Pour vérifier la propriété (V5) il est commode de définir $w_0$ par (2.1.2). Toutes les autres propriétés résultent immédiatement de (2.1.1), et des propriétés de la valuation v de k (1.1).

(2.3) Définition. - Nous appellerons valuation de $\underset{\sim}{A}$ une application $w : \underset{\sim}{A} \to \underset{\sim}{R} \cup \{+\infty\}$ qui vérifie les propriétés (V1) à (V6) de (2.2.1).

(2.4) Soit a un élément non nul de k. Nous définissons une application $f \rightsquigarrow \tilde{f}$ de $\underset{\sim}{A}$ sur lui-même en posant (pour tout $n \in \underset{\sim}{N}$ et tout $f \in A^n$)

$$\tilde{f} = a^{-1} f(ax_{n,1}, \ldots, ax_{n,n}) . \quad (2.4.1)$$

Si nous interprétons les polynômes f comme des fonctions qui définissent des transformations de points donnés par leurs coordonnées, la transformation $f \rightsquigarrow \tilde{f}$ correspond à un changement de coordonnées très simple : une homothétie de rapport $a^{-1}$. Remarquons que les éléments de $A^0$ (= k) ne sont pas invariants : ils sont multipliés par $a^{-1}$. Par contre les $x_{n,i}$ sont invariants.

L'application $f \rightsquigarrow \tilde{f}$ vérifie les propriétés suivantes ;

(2.4.2) elle est k-linéaire : $\widetilde{(\lambda f + \mu g)} = \lambda\tilde{f} + \mu\tilde{g}$ ;

(2.4.3) elle respecte les degrés : $\widetilde{P_\alpha f} = P_\alpha \tilde{f}$ ;

(2.4.4) elle est compatible avec la composition : si $h = f(g_1, \ldots, g_n)$

$$\tilde{h} = \tilde{f}(\tilde{g}_1, \ldots, \tilde{g}_n) ;$$

(2.4.5) si $f \in A^n_\alpha$, $\tilde{f} = a^{|\alpha|-1} f$, où $|\alpha| = \alpha_1 + \ldots + \alpha_n$ est le degré total du monôme f.

(2.5) Conservons les notations de (2.4), et donnons une valuation w de $\underset{\sim}{A}$ (2.3). Pour tout $f \in \underset{\sim}{A}$, posons

$$\tilde{w}(f) = w(\tilde{f}) . \quad (2.5.1)$$

L'application $\tilde{w}$ est encore une valuation de $\underset{\sim}{A}$ ; cela résulte de la définition des valuations par les axiomes V (2.2) et des propriétés (2.4.2), (2.4.3), (2.4.4).

Nous pouvons calculer $\tilde{w}(f)$ pour un élément homogène f au moyen de la formule (2.4.5) et de l'axiome (V3). Nous obtenons

$$\tilde{w}(f) = w(f) + (|\alpha| - 1)\, v(a) , \quad \text{pour } f \in A^n_\alpha . \quad (2.5.2)$$

L'axiome (V4) montre que la relation précédente suffit à calculer $\tilde{w}(f)$ pour un f quelconque, et que $\tilde{w}(f)$ ne dépend que de f, de w, et de v(a).

(2.6) Les valuations $w_\pi$ .

(2.6.1) LEMME. - Soient $k$ un corps valué et $\pi$ un nombre réel. Il existe une extension valuée $k'$ de $k$ et un élément $a \in k'$, tel que $v(a) = \pi$ .

Preuve. - Nous prendrons $k' = k(a)$ où $a$ est transcendant sur $k$ . Formons d'abord l'anneau de polynômes $k[a]$ . Si $x = \sum_{n=0}^{\infty} c_n a^n$ est un polynôme $(c_n \in k)$, nous posons $\overline{v}(x) = \inf_n (v(c_n) + n\pi)$ . La fonction $\overline{v}$ vérifie les axiomes (1.1) sur $k[a]$ , sa restriction à $k$ est $v$ , et $\overline{v}(a) = \pi$ . Il existe un prolongement unique de $\overline{v}$ à $k(a)$ , corps des fractions de $k[a]$ qui soit une valuation. Nous notons encore $v$ ce prolongement.

(2.6.2) PROPOSITION. - Soient $k$ un corps valué, $\pi$ un nombre réel, $\underset{\sim}{A} = \underset{\sim}{A}(k)$ comme en (1.3), $w_0$ la valuation banale de $\underset{\sim}{A}$ comme en (2.1). Il existe une valuation de $\underset{\sim}{A}$ et une seule, notée $w_\pi$ , qui possède la propriété suivante :

(2.6.3) $\forall\ n \in \underset{\sim}{N}$ , $\forall\ \alpha \in \mathbf{N}^n$ , $\forall\ f \in \underset{\sim}{A}^n_\alpha$ , $\quad w_\pi(f) = w_0(f) + (|\alpha| - 1)\pi$ .

Preuve. - L'unicité de la valuation $w_\pi$ est une conséquence de l'axiome (V4). S'il existe dans $k$ un élément $a$ vérifiant $v(a) = \pi$ , nous avons montré en (2.5) l'existence de $w_\pi$ (cf. (2.5.2)). Sinon nous appliquons le lemme (2.6.1) et nous construisons une extension valuée $k'$ de $k$ qui contient l'élément $a$ cherché. Nous avons l'inclusion évidente (1.5)

$$\underset{\sim}{A} = \underset{\sim}{A}(k) \subset \underset{\sim}{A}(k') \ ;$$

la valuation banale de $\underset{\sim}{A}(k')$ induit sur $\underset{\sim}{A}(k)$ sa valuation banale ; nous pouvons donc désigner sans danger les valuations par la lettre $w_0$ . La valuation $w_\pi$ est alors définie sur $\underset{\sim}{A}(k')$ , et sa restriction à $\underset{\sim}{A}$ (que nous notons encore $w_\pi$ ) possède les propriétés voulues.

(2.6.4) Remarque. - La proposition (2.6.2) reste valable si l'on remplace la valuation banale $w_0$ dont nous sommes partis par une valuation $w$ quelconque. Dans le cas où $k$ contient un élément de valuation $\pi$ , la démonstration est la même. Sinon on peut montrer qu'une valuation quelconque $w$ de $\underset{\sim}{A}(k)$ se prolonge en une valuation de $\underset{\sim}{A}(k')$ et se ramener ainsi au cas précédent. Mais cette vérification est assez longue, et il est alors préférable de donner une démonstration directe : cf. [1], proposition 1.

(2.7) Exemple. - Soit $p$ un nombre premier. Prenons pour $k$ le corps $\underset{\sim}{Q}$ des rationnels muni de sa valuation $p$-adique, pour laquelle $v(p) = 1$ , et prenons

$\pi = (p-1)^{-1}$ . Les monômes $n^{-1}x^n$ sont des éléments de $\Lambda^1 = \Lambda^1(\underset{\sim}{Q})$ .

(2.7.1) LEMME. - Pour tout entier $n \geqslant 1$ .

$$w_\pi(n^{-1}x^n) \geqslant 0 ,$$

et l'égalité n'est atteinte que pour $n = 1$ et $n = p$ .

Preuve. - D'après (2.6.3), nous avons

(2.7.2) $\quad w_\pi(n^{-1}x^n) = (n-1)\pi - v(n)$ , avec $\pi = (p-1)^{-1}$ .

Posons $n = n_0 p^k$ , où $k = v(n)$ . Nous obtenons

(2.7.3) $$(n-1)\pi \geqslant (p^k - 1)\pi = \sum_{0 \leqslant i < k} p^i \geqslant k = v(n) ,$$

et l'égalité des membres extrêmes exige $n_0 = 1$ et $k = 0$ ou $1$ .

## 3. Structures résiduelles.

(3.1) Soient $k$ un corps valué et $w$ une valuation (2.3) de $\underset{\sim}{A} = \underset{\sim}{A}(k)$ . Nous avons défini en (1.2) l'anneau de valuation $\Omega$ de $k$ et l'idéal de valuation $I$ ; le corps résiduel $\overline{k}$ est le quotient $\Omega/I$ .

Nous allons donner des définitions et constructions analogues pour $\underset{\sim}{\Lambda}$ . Nous posons

(3.1.1) $$_0\underset{\sim}{\Lambda} = \{f \mid f \in \underset{\sim}{\Lambda} \text{ et } w(f) \geqslant 0\}$$

(3.1.2) $$_{0^+}\underset{\sim}{\Lambda} = \{f \mid f \in \underset{\sim}{\Lambda} \text{ et } w(f) > 0\}$$

(3.1.3) $$_0\Lambda^n = {}_0\underset{\sim}{\Lambda} \cap \Lambda^n ; \qquad {}_0\Lambda^n_\alpha = {}_0\underset{\sim}{\Lambda} \cap \Lambda^n_\alpha \quad (\text{pour } n \in \underset{\sim}{N} , \ \alpha \in \underset{\sim}{N}^n)$$

(3.1.4) $$_{0^+}\Lambda^n = {}_{0^+}\underset{\sim}{\Lambda} \cap \Lambda^n ; \qquad {}_{0^+}\Lambda^n_\alpha = {}_{0^+}\underset{\sim}{\Lambda} \cap \Lambda^n_\alpha .$$

(3.2) Les axiomes (V2) et (V3) de (2.2) montrent que (pour tout $n$ ) $_0\Lambda^n$ et $_{0^+}\Lambda^n$ sont des $\Omega$-modules, avec $_{0^+}\Lambda^n \subset {}_0\Lambda^n$ . De plus, $I.{}_0\Lambda^n \subset {}_{0^+}\Lambda^n$ , ce qui montre que le $\Omega$-module quotient $_0\Lambda^n/{}_{0^+}\Lambda^n$ est un $\overline{k}$-espace vectoriel. Nous le noterons $B^n$ et nous noterons $\rho$ l'épimorphisme canonique de $_0\Lambda^n$ sur $B^n$ . Nous avons donc les suites exactes

(3.2.1) $$0 \to {}_{0^+}\Lambda^n \to {}_0\Lambda^n \xrightarrow{\rho} B^n \to 0 .$$

Nous noterons $\underset{\sim}{B}$ la réunion des $B^n$ (pour $n \in \underset{\sim}{N}$ ), et $\rho$ l'application $\underset{\sim}{A} \to \underset{\sim}{B}$ dont les restrictions aux $\Lambda^n$ sont définies par (3.2.1).

(3.2.2) PROPOSITION. - Pour chaque $n \in \underset{\sim}{N}$, le $\overline{k}$-espace $B^n$ est somme directe des sous-espaces $B^n_\alpha = \rho\, {}_0\Lambda^n_\alpha$ $(\alpha \in \underset{\sim}{N}^n)$. Si $f \in {}_0\Lambda^n$, $g_1, \dots, g_n \in {}_0\Lambda^m$, $h = f(g_1, \dots, g_n)$, alors $h \in {}_0\Lambda^m$ et $\rho h$ ne dépend que de $\rho f$ et des $\rho g_i$, ce qui nous permet de définir la composition des éléments de $\underset{\sim}{B}$ en posant

$$\rho h = \rho f(\rho g_1, \dots, \rho g_n). \tag{3.2.3}$$

Preuve. - L'assertion concernant les $B^n_\alpha$ est une conséquence de (V4), d'après lequel ${}_0\Lambda^n$ (resp. ${}_{0^+}\Lambda^n$) est somme directe des ${}_0\Lambda^n_\alpha$ (resp. ${}_{0^+}\Lambda^n_\alpha$).

Pour établir la fin de notre proposition, nous pouvons supposer $f \in A^n_\alpha$ pour un certain $\alpha$ (d'après (1.3.2) et l'axiome (V4)). L'axiome (V5) nous montre alors que $h \in {}_0\Lambda^m$ et que $\rho h$ dépend seulement de $f$ par l'intermédiaire de $\rho f$.

Pour montrer que $\rho h$ ne dépend de $g_1$ (par exemple) que par l'intermédiaire de $\rho g_1$, introduisons le polynôme $f' \in \Lambda^{n+1}$ défini par

$$f' = f(x_{n+1,1} + x_{n+1,2}, x_{n+1,3}, \dots, x_{n+1,n+1}).$$

Les axiomes (V2), (V5) et (V6) nous montrent que la relation $f \in {}_0\Lambda^n$ implique $f' \in {}_0\Lambda^{n+1}$. Si nous remplaçons $g_1$ par un polynôme $g_1' = g^* + g_1$ où $g^* \in {}_{0^+}\Lambda^m$, le polynôme $h$ se trouve remplacé par $f'(g^*, g_1, \dots, g_n)$ et

$$h' - h = f'(g^*, g_1, \dots, g_n) - f'(0, g_1, \dots, g_n).$$

Or les composantes homogènes non nulles du polynôme

$$f'(x_{n+1,1}, x_{n+1,2}, \dots, x_{n+1,n+1}) - f'(0, x_{n+1,2}, \dots, x_{n+1,n+1})$$

sont de degré strictement positif en $x_{n+1,1}$, et nous déduisons de l'axiome (V5) la relation $h' - h \in {}_{0^+}\Lambda^m$, c'est-à-dire $\rho h = \rho h'$.

(3.3) Exemple. - Reprenons, comme en (2.7) le corps $\underset{\sim}{Q}$ muni de sa valuation p-adique, et une valuation $w_\pi$ de $\underset{\sim}{\Lambda}$, où $\pi$ est l'inverse d'un entier $e \geqslant 1$ (pas nécessairement $p - 1$). L'anneau $\Omega$ est l'anneau $\underset{\sim}{Z}_{(p)}$ des rationnels p-entiers, et $\overline{k}$ est le corps premier $\underset{\sim}{F}_p$.

Soit $\varphi \in B^n$. Nous avons $\varphi = \rho f$, où $f$ est un élément de ${}_0\Lambda^n$, que nous écrivons sous la forme (1.3.2). Seuls importent, pour la détermination de $\varphi$, les monômes $c_\alpha X^\alpha$ tels que $w_\pi(c_\alpha X^\alpha) = 0$. D'après (2.6.3) et (2.1.1), cette relation signifie

$$v(c_\alpha) + \pi(|\alpha| - 1) = 0, \tag{3.3.1}$$

c'est-à-dire

(3.3.2) $$ev(c_\alpha) + |\alpha| - 1 = 0 \ .$$

Nous devons donc avoir

(3.3.3) $$|\alpha| \equiv 1 \pmod{e} \ ,$$

et $c_\alpha$ est de la forme

(3.3.4) $$c_\alpha = p^{-\pi(|\alpha|-1)} \, c'_\alpha$$

où $c'_\alpha$ est un élément inversible de $\underset{\sim}{Z}_{(p)}$ . Notons $c \rightsquigarrow \overline{c}$ l'épimorphisme canonique de $\underset{\sim}{Z}_{(p)}$ sur $\underset{\sim}{F}_p$ . Le polynôme

(3.3.5) $$\sum_\alpha \overline{c'_\alpha} \, X^\alpha \in \Lambda^n(\underset{\sim}{F}_p)$$

ne dépend que de $\varphi$ . Nous le noterons $\sigma\varphi$ . Nous venons de construire une application $\sigma : \underset{\sim}{B} \to \underset{\sim}{\Lambda}(\underset{\sim}{F}_p)$ qui est injective. L'image de $\underset{\sim}{B}$ par $\sigma$ est formée des <u>polynômes à coefficients dans</u> $\underset{\sim}{F}_p$ <u>dont les monômes</u> (non nuls) <u>ont un degré total congru à</u> 1 <u>modulo</u> e . L'application $\sigma$ est $\underset{\sim}{F}_p$-linéaire, et respecte les degrés, c'est-à-dire que $\sigma(B^n_\alpha) \subset \Lambda^n_\alpha(\underset{\sim}{F}_p)$ . De plus $\sigma$ <u>est compatible avec la composition dans</u> $\underset{\sim}{B}$ <u>et dans</u> $\underset{\sim}{\Lambda}(\underset{\sim}{F}_p)$ , c'est-à-dire que

(3.3.6) $$\sigma\circ(\varphi(\gamma_1 \ , \ \cdots \ , \ \gamma_n)) = (\sigma\varphi)(\sigma\gamma_1 \ , \ \cdots \ , \ \sigma\gamma_n) \ ,$$

pour $\varphi \in B^n$ et $\gamma_1 \ , \ \cdots \ , \ \gamma_n \in B^m$ .

Dans le cas où $e > 1$ , remarquons que $B^0 = 0$ , et qu'il n'y a pas d'élément bilinéaire (non nul) dans $B^2$ .

Pour toutes les valuations $w_\pi$ , où $\pi > 0$ , le produit de deux éléments de ${}_0\Lambda^n$ appartient à ${}_0\Lambda^n$ , <u>mais a une image nulle dans</u> $B^n$ .

(3.4) <u>Les</u> $\underset{\sim}{B}$<u>-modules.</u>

Reprenons les notations générales de (3.1) et (3.2). Chaque $\Lambda^n$ peut être considéré comme une structure libre à n générateurs donnés dans la catégorie des k-algèbres associatives, commutatives et unitaires.

Montrons que les $B^n$ sont aussi des structures libres à n générateurs donnés dans une catégorie que nous allons définir.

(3.4.1) <u>Définition.</u> - <u>Un</u> $\underset{\sim}{B}$<u>-module est un ensemble</u> E <u>muni, pour chaque</u> $n \in \underset{\sim}{N}$ , <u>d'une famille d'application de</u> $E^n$ <u>(puissance cartésienne</u> n<u>-ième de</u> E ) <u>dans</u> E <u>en correspondance biunivoque avec les éléments de</u> $B^n$ . <u>L'image dans</u> E <u>de</u> $(a_1 \ , \ \cdots \ , \ a_n) \in E^n$ <u>par l'application associée à</u> $\varphi \in B^n$ <u>est notée</u> $\varphi(a_1 \ , \ \cdots \ , \ a_n)$ . <u>L'axiome suivant doit être vérifié</u> :

soient $m$ , $n \in \underset{\sim}{N}$ , $\varphi \in B^n$ , $\gamma_1$ , ... , $\gamma_n \in B^m$ , $\psi = \varphi(\gamma_1$ , ... , $\gamma_n)$ , $a_1$ , ... , $a_m \in E$ , $b_i = \gamma_i(a_1$ , ... , $a_m)$ ; alors

$$\varphi(b_1 , \dots , b_n) = \psi(a_1 , \dots , a_m) .$$

(3.4.2) Définition. - Soient $E$ et $E'$ deux $\underset{\sim}{B}$-modules. Un morphisme $u : E \to E'$ est une application qui vérifie l'axiome suivant :

soient $n \in \underset{\sim}{N}$ , $\varphi \in B^n$ , $a_1$ , ... , $a_n \in E$ ; alors

$$u(\varphi(a_1 , \dots , a_n)) = \varphi(u(a_1) , \dots , u(a_n)) .$$

La catégorie des $\underset{\sim}{B}$-modules est définie par (3.4.1) et (3.4.2). L'associativité de la composition des polynômes entraîne que chaque $B^n$ est un $\underset{\sim}{B}$-module. Il est aisé de vérifier que $B^n$ est libre pour les générateurs $x_{n,1}$ , ..., $x_{n,m}$. Les $\underset{\sim}{B}$-modules sont des espaces vectoriels sur $\underset{\sim}{F}_p$. Si $\Omega$ est une $\underset{\sim}{F}_p$-algèbre associative, commutative et unitaire, on a une définition naturelle des $(\Omega \otimes \underset{\sim}{B})$-modules, pour laquelle nous renvoyons à [2]. Dans l'exemple étudié en (3.3), un $\underset{\sim}{B}$-module peut être défini (pour $e > 1$ ), par sa structure de $\underset{\sim}{F}_p$-espace vectoriel et par une seule loi de composition $(e + 1)$-aire.

(3.5) Les ${}_\nu B$ .

Conservons les notations de (3.1). Pour tout nombre réel $\nu \geqslant 0$ , notons respectivement ${}_\nu A^n$ et ${}_{\nu^+} A^n$ l'ensemble des éléments $f$ de $A^n$ qui vérifient $w(f) \geqslant \nu$ et $w(f) > \nu$ . Pour $\nu = 0$ , nous retrouvons les définitions de (3.1). Nous voyons comme précédemment que ${}_\nu A^n$ et ${}_{\nu^+} A^n$ sont des $\Omega$-modules, et que leur quotient, que nous noterons ${}_\nu B^n$ , est un $\overline{k}$-espace vectoriel. Nous définissons les applications $\rho_\nu$ par les suites exactes :

$$0 \to {}_{\nu^+} A^n \to {}_\nu A^n \xrightarrow{\rho_\nu} {}_\nu B^n \to 0 . \tag{3.5.1}$$

Les espaces ${}_\nu B^n$ sont, comme précédemment, sommes directes des ${}_\nu B^n_\alpha = \rho_\nu({}_\nu A^n \cap A^n_\alpha)$ . La proposition (3.2.2) admet la généralisation suivante, qui se démontre de même.

(3.5.2) PROPOSITION. - Soient $m$ , $n \in \underset{\sim}{N}$ , $\nu$ , $\nu_1$ , ... , $\nu_n$ des nombres réels $\geqslant 0$ , $\alpha = (\alpha_1 , \dots , \alpha_n) \in \underset{\sim}{N}^n$ , $f \in {}_\nu A^n_\alpha = {}_\nu A^n \cap A^n_\alpha$ , $g_i \in {}_{\nu_i} A^m$ (pour $1 \leqslant i \leqslant n$ ) et $h = f(g_1 , \dots , g_n)$ . Alors $h \in {}_\mu A^m$ , où $\mu = \nu + \sum_{1 \leqslant i \leqslant n} \alpha_i \nu_i$ , et $\rho_\mu h$ ne dépend que de $\rho_\nu f$ et des $\rho_{\nu_i} g_i$ , ce qui nous permet d'écrire

$$\rho_\mu h = \rho_\nu f(\rho_{\nu_1} g_1 , \dots , \rho_{\nu_n} g_n) . \tag{3.5.3}$$

(3.5.4) COROLLAIRE. - Si tous les $\nu_i$ $(1 \leqslant i \leqslant n)$ sont nuls, nous pouvons supposer simplement $f \in {}_{\nu}A^n$ dans l'énoncé (3.5.2).

## 4. Séries formelles.

### (4.1) Extension des résultats précédents aux séries formelles.

Nous noterons $\hat{A}^n(\Omega)$ l'anneau des séries formelles

$$\hat{A}^n(\Omega) = \Omega[[x_{n,1}, \dots, x_{n,n}]] . \tag{4.1.1}$$

Les éléments de $\hat{A}^n(\Omega)$ s'écrivent encore univoquement sous la forme

$$f = \sum_{\alpha \in \underset{\sim}{N}^n} c_\alpha X^\alpha , \tag{4.1.2}$$

mais les $c_\alpha$ sont maintenant des éléments quelconques de $\Omega$. Nous considérons $A^n(\Omega)$ comme un sous-anneau de $\hat{A}^n(\Omega)$. Si nous munissons $\hat{A}^n(\Omega)$ de la topologie usuelle des séries formelles, $\hat{A}(\Omega)$ apparait comme le complété de $A^n(\Omega)$. Comme précédemment, nous supprimons la référence à $\Omega$ quand cela est possible. Nous notons $\underset{\sim}{\hat{A}}$ la réunion des $\hat{A}^n$ $(n \in \underset{\sim}{N})$.

La composition (1.4) se prolonge à $\underset{\sim}{\hat{A}}$ par continuité, mais n'est pas partout définie : si $f \in \hat{A}^n$, $g_1, \dots, g_n \in \hat{A}^m$, nous ne savons définir $f(g_1, \dots, g_n) \in \hat{A}^m$ que si $f$ est un polynôme ou si les termes constants des $g_i$ sont nuls.

Soient $k$ un corps valué, $\underset{\sim}{A} = \underset{\sim}{A}(k)$, $\underset{\sim}{\hat{A}} = \underset{\sim}{\hat{A}}(k)$ et $w$ une valuation de $\underset{\sim}{A}$. Si $f \in \underset{\sim}{\hat{A}}$, donné par le développement (4.1.2), vérifie

$$\inf_{\alpha \in \underset{\sim}{N}^n} w(c_\alpha X^\alpha) > -\infty , \tag{4.1.3}$$

nous posons

$$w(f) = \inf_{\alpha \in \underset{\sim}{N}^n} w(c_\alpha X^\alpha) . \tag{4.1.4}$$

Nous prolongeons ainsi $w$ à une partie $\hat{A}[w]$ de $\hat{A}$, qui dépend de $w$. L'axiome (V4) est vérifié par définition ; il est aisé de voir que les autres axiomes (V) sont satisfaits.

Nous noterons ${}_{\nu}\underset{\sim}{\hat{A}}$ (resp. ${}_{\nu^+}\underset{\sim}{\hat{A}}$) l'ensemble des $f \in \hat{A}[w]$ qui vérifient $w(f) \geqslant \nu$ (resp. $w(f) > \nu$). Ce sont les complétés (pour la topologie des séries

formelles) de $\underset{\nu}{\underset{\sim}{A}}$ et $\underset{\nu^+}{\underset{\sim}{A}}$. De même, le quotient de $\nu\hat{A}^n = \underset{\nu}{\underset{\sim}{\hat{A}}} \cap \hat{A}^n$ par $\nu^+\hat{A}^n = \underset{\nu^+}{\underset{\sim}{\hat{A}}} \cap \hat{A}^n$ s'identifie au complété $\nu\hat{B}^n$ de $\nu B^n$, c'est-à-dire au produit direct des $\nu B_\alpha^n$ dont $\nu B^n$ est la somme directe. Nous appellerons encore $\rho$ l'épimorphisme de $0\hat{A}^n$ sur $\hat{B}^n$ $(= 0\hat{B}^n)$, et, de même, $\rho_\nu$ l'épimorphisme de $\nu\hat{A}^n$ sur $\nu\hat{B}^n = \nu\hat{A}^n / \nu^+\hat{A}^n$.

Les propositions (3.2.2) et (3.5.2) restent valables pour les séries formelles. Il faut, bien entendu, supposer que l'élément $f(g_1, \cdots, g_n)$ est défini dans $\underset{\sim}{\hat{A}}$. Mais si, comme dans l'exemple étudié en (3.3), avec $e > 1$, l'espace $B^0$ se réduit à $0$, nous pouvons toujours supposer que les $g_i$ ont des termes constants nuls ; dans ce cas $\varphi(\gamma_1, \cdots, \gamma_n)$ est défini pour tous $\varphi \in \hat{B}^n$ et tous $\gamma_1, \cdots, \gamma_n \in \hat{B}^m$.

(4.2) Séries réciproques.

Soit $f$ un élément de $\hat{A}^1$, c'est-à-dire une série formelle en une lettre, que nous écrirons $f(x)$. Nous supposons que les termes de degré $< 2$ de $f(x) - x$ sont nuls. Alors il existe une série $g(x) \in \hat{A}^1$ possédant les mêmes propriétés, et déterminée par l'une des relations équivalentes

$$f(g(x)) = x \; ; \qquad g(f(x)) = x \; . \tag{4.2.1}$$

La série $g$ est dite réciproque de $f$. Nous pouvons la calculer par la méthode des approximations successives. Posons

$$f(x) = x - r(x) \; , \tag{4.2.2}$$

où $r(x)$ est de la forme $\sum_{n=2}^{\infty} c_n x^n$. La série $g$ est déterminée par la relation $f(g(x)) = x$, qui s'écrit encore

$$g(x) = x + r(g(x)) \; . \tag{4.2.3}$$

Or, pour calculer les termes de $r(g(x))$ jusqu'au degré $n$, il suffit de connaître ceux de $g$ jusqu'au degré $n-1$. La série $g(x)$ est donc la limite (au sens de la topologie des séries formelles) de la suite $g_n(x)$, définie par

$$g_1(x) = x \; ; \qquad g_{n+1}(x) = x + r(g_n(x)) \; . \tag{4.2.4}$$

Nous en déduisons le résultat suivant.

(4.2.5) LEMME. - *Soit $f \in {}_0\hat{A}^1$ un élément tel que $f - x$ ait ses termes de degré $< 2$ nuls. Alors la série réciproque $g$ appartient aussi à ${}_0\hat{A}^1$, son image $\rho g$ ne dépend que de $\rho f$. Elle est déterminée par l'une des relations équivalentes*

$$\rho f(\rho g) = x \ , \qquad \rho g(\rho f) = x$$

(où x désigne encore l'image $\rho x$ de $x = x_{1,1}$ ). Nous obtenons $\rho g$ par la méthode des approximations successives, comme en (4.2.4).

(4.3) Application au logarithme et à l'exponentielle.

Prenons pour k le corps $\underset{\sim}{Q}$ muni de sa valuation p-adique, et pour valuation w la valuation $w_\pi$ où $\pi = (p-1)^{-1}$ .

Définissons les séries L(x) et e(x) par les formules

$$L(x) = \sum_{n=1}^{\infty} (-1)^{n+1} n^{-1} x^n \ ; \tag{4.3.1}$$

$$e(x) = \sum_{n=1}^{\infty} (n!)^{-1} x^n \ . \tag{4.3.2}$$

Ce sont les séries classiques $\mathrm{Log}(1+x)$ et $e^x - 1$ ; elles sont donc réciproques l'une de l'autre.

(4.3.3) PROPOSITION. - La série L(x) appartient à $_0\hat{A}^1$ et $\rho L(x) = x - \rho u_p(x)$, où

$$u_p(x) = -p^{-1} x^p \ . \tag{4.3.4}$$

Preuve. - Notre assertion ne fait que répéter le lemme (2.7.1).

(4.3.5) PROPOSITION. - La série e(x) appartient à $_0\hat{A}^1$ , et $\rho e(x) = \rho e^*(x)$ , où

$$e^*(x) = \sum_{n=0}^{\infty} u_p^n(x) \ , \tag{4.3.6}$$

$u_p^n(x)$ désignant le n-ième itéré de $u_p(x)$ , c'est-à-dire

$$u_p^n(x) = (-1)^n p^{-\pi(p^n-1)} x^{p^n} \ . \tag{4.3.7}$$

Preuve. - Nous utilisons le lemme (4.2.5) et la proposition (4.3.3). Pour calculer $\rho e(x)$ , nous pouvons remplacer L(x) par $x - u_p(x)$ . Or la relation

$$(x+y)^p = x^p + y^p \ , \tag{4.3.8}$$

valable dans les anneaux associatifs et commutatifs de caractéristique p , entraîne

$$\rho u_p(x+y) = \rho u_p(x) + \rho u_p(y) \ . \tag{4.3.9}$$

Le calcul par approximations successives de la série réciproque de $x - \rho u_p(x)$ est le calcul classique de l'inverse d'un opérateur linéaire de la forme $1 - T$ .

## 5. Polynômes et séries formelles associatives (non commutatives).

(5.1) Rappelons que l'algèbre des polynômes associatifs (non commutatifs) en $n$ lettres et à coefficients dans $\Omega$ est la $\Omega$-algèbre associative (et unitaire) libre engendrée par ces lettres. Si, comme précédemment, les lettres sont notées $x_{n,1}, \dots, x_{n,n}$, les polynômes sont encore des combinaisons linéaires de monômes, mais les monômes $x_{n,i_1}, \dots, x_{n,i_r}$ sont distincts et linéairement indépendants pour toutes les valeurs de $r \in \underset{\sim}{N}$ et toutes les suites d'entiers $i_1, \dots, i_r$ variant indépendamment de $1$ à $n$. Pour chaque

$$\alpha = (\alpha_1, \dots, \alpha_n) \in \underset{\sim}{N}^n ,$$

il existe $|\alpha|!/\Pi_i \alpha_i!$ monômes distincts de multidegré $\alpha$.

(5.2) Modifions désormais nos notations, en appelant $A^n(\Omega)$, ou $A^n$, l'algèbre des polynômes associatifs en $n$ lettres $x_{n,1}, \dots, x_{n,n}$ à coefficients dans $\Omega$. Remarquons que, pour $n = 1$, cela n'entraîne aucune modification, car les polynômes associatifs en une lettre sont aussi commutatifs.

Toutes les considérations des paragraphes 1 à 3, ainsi que de (4.1) et de (4.2) s'étendent sans aucun changement. Dans [1] elles se trouvent exposées directement pour les polynômes et séries formelles associatives.

(5.3) Applications à la série de Hausdorff.

Reprenons les notations de (4.3). Puisque nous n'avons pas modifié les définitions de $A^1$, ${}_0\hat{A}^1$, etc., les propositions (4.3.3) et (4.3.5) restent valables, bien que la preuve de cette dernière utilise l'identité (4.3.8), qui suppose les anneaux commutatifs.

La série de Hausdorff $\Phi(x, y)$ est définie par la relation

$$\Phi(x, y) = \mathrm{Log}(e^x e^y) \tag{5.3.1}$$

c'est-à-dire, en utilisant les séries $L$ et $e$ :

$$\Phi(x, y) = L(e(x) + e(y) + e(x)\, e(y)) . \tag{5.3.2}$$

La série $\Phi$ est un élément de $\hat{A}^2$. Nous avons, (4.3.5), $e(x) \in {}_0\hat{A}^1$, d'où, d'après (3.5.2),

$$e(x)\, e(y) \in {}_{\pi}\hat{A}^2 , \tag{5.3.3}$$

puisque $w(xy) = \pi$.

Rappelons l'identité de Jacobson, qui remplacera la relation (4.3.8). Dans tout anneau associatif, on a la relation

$$(5.3.4) \qquad (x + y)^p = x^p + y^p + \Lambda(x , y) + pR(x , y) ,$$

où $p$ est un nombre premier, $x$ et $y$ deux éléments de l'anneau, $\Lambda$ et $R$ des polynômes associatifs à coefficients entiers, tels que $\Lambda$ soit construit au moyen du crochet de Lie $[u , v] = uv - vu$ (et de l'addition).

Posons

$$(5.3.5) \qquad \theta(x , y) = p^{-1} \Lambda(x , y) .$$

L'identité de Jacobson s'écrit

$$(5.3.6) \qquad u_p(x + y) = u_p(x) + u_p(y) - \theta(x , y) - R(x , y) ,$$

et conduit à

$$(5.3.7) \qquad \rho u_p(x + y) = \rho u_p(x) + \rho u_p(y) - \rho\theta(x , y) .$$

(5.3.8) THÉORÈME. - *La série* $\Phi(x , y)$ *appartient à* $_0\hat{A}^2$ *et*

$$(5.3.9) \qquad \rho\Phi(x , y) = x + y + \rho\theta(\rho e^*(x) , \rho e^*(y)) .$$

Preuve. - Nous savons déjà que $\Phi \in {}_0\hat{A}^2$ . Pour calculer $\rho\Phi$ à partir de (5.3.2), nous pouvons, (3.2.2), remplacer $L(x)$ par $x - u_p(x)$ , $e(x)$ par $e^*(x)$ et $e(x)\, e(y)$ par $0$ (5.3.3). Si nous appliquons (5.3.7), nous obtenons la formule (5.3.9).

Le "commutateur de Hausdorff" $\Psi(x , y)$ est défini par la formule

$$(5.3.10) \qquad \Psi(x , y) = \mathrm{Log}(e^{-x}\, e^{-y}\, e^{x}\, e^{y}) ,$$

c'est-à-dire

$$(5.3.11) \qquad \Psi(x , y) = L((1 + e(-x))(1 + e(-y))(1 + e(x))(1 + e(y)) - 1) .$$

Si on utilise la relation $e(-x) + e(x) + e(-x)\, e(x) = 0$ , on voit que

$$(1 + e(-x))(1 + e(-y))(1 + e(x))(1 + e(y)) - 1$$

se réduit à $e(x)\, e(y) - e(y)\, e(x)$ à condition de négliger les produits d'au moins trois éléments de la forme $e(-x)$ , $e(x)$ , $e(-y)$ , $e(y)$ . Si nous appliquons la proposition (3.5.2), nous parvenons au résultat suivant.

(5.3.12) *La série* $\Psi(x , y)$ *appartient à* $_\pi\hat{A}^2$ , *et*

$$(5.3.13) \qquad \rho_\pi \Psi(x , y) = \rho_\pi[\rho e^*(x) , \rho e^*(y)] ,$$

où $[x , y] = xy - yx \in {}_\pi A^2$ .

(5.4) Toutes les considérations que nous avons développées s'étendent plus généralement aux analyseurs incomplets ou complets au sens de [2]. Les axiomes (V) de (2.2) permettent de définir la valuation d'un analyseur $\underset{\sim}{A}$ sur un corps valué $k$. Les constructions du § 3 conduisent à la définition de l'analyseur résiduel $\underset{\sim}{B}$ de $\underset{\sim}{A}$, et aux espaces ${}_{\nu}B^{n}$.

BIBLIOGRAPHIE

[1] LAZARD (Michel). - Quelques calculs concernant la formule de Hausdorff, Bull. Soc. math. France, t. 91, 1963, p. 435-451.

[2] LAZARD (Michel). - Lois de groupes et analyseurs, Ann. scient. Ec. Norm. Sup., t. 72, 1955, p. 299-400.