ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

JACQUES HELMSTETTER

Systèmes de puissances partiellement divisées

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 9, n° 1 (1982), p. 27-56

<http://www.numdam.org/item?id=ASNSP_1982_4_9_1_27_0>

Systèmes de puissances partiellement divisées.

JACQUES HELMSTETTER

Le but de cet article est de définir et d'étudier des systèmes intermédiaires entre les systèmes de puissances ordinaires et les systèmes de puissances divisées classiques (§§ 1 à 6) et de donner deux applications de cette théorie (§§ 7 à 10), qui peuvent déjà permettre d'en évaluer l'intérêt.

Dans cet article, K est un anneau commutatif unifère; on suppose qu'il existe un nombre entier premier p tel que tous les autres entiers premiers aient une image inversible dans K; en outre on suppose que l'on peut trouver deux entiers r et $s \in \boldsymbol{N}$ et un élément $\varepsilon \in K$ tels que ε^{r+s} soit égal à l'image de p dans K. Ces hypothèses sont vérifiées dans les trois cas suivants. Ou bien K est de caractéristique p (c'est surtout ce cas qui m'intéresse) et ε est nilpotent; soit q le plus petit entier tel que $\varepsilon^q = 0$ (par convention $\varepsilon^0 = 1$; j'accepte le cas où $\varepsilon = 0$ et $q = 1$); q, r et s sont astreints à satisfaire l'inégalité $q \leqslant r + s$. Ou bien K est de caractéristique p^k avec $k \geqslant 2$, et contient une racine $(r + s)$-ième de p. Ou bien encore K est de caractéristique nulle et son unité est contenue dans un sous-anneau isomorphe à $\boldsymbol{Z}_{(p)}[\sqrt[r+s]{p}]$; c'est le sous-anneau de $\boldsymbol{R}$ engendré par $\boldsymbol{Z}$, par les inverses des entiers non divisibles par p, et par $\sqrt[r+s]{p}$. Si l'élément unité de K est contenu dans un sous-anneau isomorphe au corps $\boldsymbol{Q}(\sqrt[r+s]{p})$, tout ce qui suit devient trivial. Une partie importante de ce que je dirai, reste utilisable lorsque plusieurs entiers premiers ne sont pas inversibles dans K, mais pour traiter honnêtement ce cas, il vaudrait mieux utiliser une machinerie plus élaborée.

1. – Préliminaires sur les factorielles.

Pour tout entier $n \in \boldsymbol{N}$, j'appelle $\tau(n)$ l'exposant de la plus grande puissance de p qui divise $n!$; je note $n!^*$ le quotient de $n!$ par $p^{\tau(n)}$; c'est un

Pervenuto alla Redazione il 10 Ottobre 1980 ed in forma definitiva il 14 Febbraio 1981.

entier inversible dans K. Si $(m, n) \in \boldsymbol{N}\times\boldsymbol{N}$, je pose:

$$\sigma(m, n) = \tau(m + n) - \tau(m) - \tau(n)\,, \qquad \varrho(m, n) = \tau(mn) - n\tau(m) - \tau(n)\,;$$

ainsi $\sigma(m, n)$ (resp. $\varrho(m, n)$ lorsque $m \geqslant 1$) est l'exposant de la plus grande puissance de p qui divise

$$\frac{(m + n)!}{m!\,n!} \qquad \left(\text{resp. } \frac{(mn)!}{(m!)^n\,n!} \text{ avec } m \geqslant 1\right).$$

Plus généralement je pose

$$\sigma(n_1, n_2, \ldots, n_k) = \tau(n_1 + \ldots + n_k) - \tau(n_1) - \ldots - \tau(n_k)\,.$$

Soit encore $\chi(n)$ la somme des chiffres de n lorsqu' on l'écrit dans le système de numération de base p; donc $\chi(n) = \sum n_j$ si $n = \sum n_j p^j$ et si $0 \leqslant n_j < p$ pour tout $j \in \boldsymbol{N}$. On peut démontrer que:

$$n = \chi(n) + (p - 1)\,\tau(n)\,, \tag{1}$$

d'où l'on tire

$$\sigma(m, n) = \frac{1}{p - 1}\,(\chi(m) + \chi(n) - \chi(m + n))\,.$$

Cette dernière égalité nous incite à poser:

$$\pi(m, n) = \frac{1}{p - 1}\,(\chi(m)\,\chi(n) - \chi(mn))\,;$$

ainsi σ et π sont des fonctions à valeurs dans $\boldsymbol{N}$, définies sur $\boldsymbol{N}\times\boldsymbol{N}$ et symétriques en leur deux variables. On peut vérifier que:

$$\varrho(m, n) = \pi(m, n) + (\chi(m) - 1)\,\tau(n)\,. \tag{2}$$

Cette égalité montre que, si m n'est égal ni à 0 ni à une puissance de p, alors $\varrho(m, n) \geqslant \tau(n)$ pour tout $n \in \boldsymbol{N}$.

2. – Systèmes de puissances partiellement divisées.

Soit $A = K \oplus A'$ une algèbre commutative augmentée sur K (donc A' est l'idéal d'augmentation), et soient r et $s \in \boldsymbol{N}$ et $\varepsilon \in K$ tels que ε^{r+s} soit

l'image de p dans K. Un système de puissances partiellement divisées sur A de type (r, s) (ou de type $(p; r, s; \varepsilon)$ si l'on veut être plus précis) est une suite d'applications de A' dans A, notées $a \mapsto a^{[n]}$ (avec $n \in \boldsymbol{N}$), vérifiant les six conditions suivantes:

(3a) $\qquad a^{[0]} = 1, \quad a^{[1]} = a \quad \text{et} \quad a^{[n]} \in A' \quad \text{si } n \geqslant 1.$

(3b) $\qquad (\lambda a)^{[n]} = \lambda^n a^{[n]} \quad \text{si } \lambda \in K .$

(3c) $\qquad (a+b)^{[n]} = \sum_{0 \leqslant j \leqslant n} \frac{n!^*}{j!^*(n-j)!^*} \varepsilon^{s\sigma(j,n-j)} a^{[j]} b^{[n-j]} .$

(3d) $\qquad (ab)^{[n]} = \varepsilon^{r\tau(n)} a^{[n]} b^{[n]} .$

(3e) $\qquad a^{[m]} a^{[n]} = \varepsilon^{r\sigma(m,n)} a^{[m+n]} .$

(3f) $\qquad (a^{[m]})^{[n]} = \varepsilon^{r\varrho(m,n)} a^{[mn]} \quad \text{si } m \geqslant 1 .$

Si l'élément unité de K est contenu dans un sous-anneau de K isomorphe au corps $\boldsymbol{Q}(\eta)$, où η est une racine $(r+s)$-ième de p, il existe toujours sur A un et un seul système de puissances partiellement divisées de type $(p; r, s; \eta)$, à savoir:

$$a^{[n]} = \frac{a^n}{\eta^{r\tau(n)}} .$$

Si K est de caractéristique p, soit q l'ordre de l'élément nilpotent ε; on peut imposer à r et s de ne pas être supérieurs à q; en effet si $r > q$ (resp. si $s > q$), un système de type (r, s) est exactement la même chose qu'un système de type (q, s) (resp. (r, q)). En particulier si $\varepsilon = 0$, on peut se limiter aux cas où (r, s) est égal à $(1, 0)$, $(0, 1)$ ou $(1, 1)$.

Si $r = 0$, un système de type $(0, s)$ est la même chose que le système des puissances non divisées: $a^{[n]} = a^n$ pour tout n. Si $s = 0$, la donnée d'un système de type $(r, 0)$ est équivalente à la donnée d'un système de puissances divisées classiques; en effet posons $a^{(n)} = a^{[n]}/n!^*$ pour tout n; les applications $a \mapsto a^{(n)}$ vérifient les six conditions suivantes:

(4a) et (4b) $\qquad$ analogues à (3a) et (3b) .

(4c) $\qquad (a+b)^{(n)} = \sum a^{(j)} b^{(n-j)} .$

(4d) $\qquad (ab)^{(n)} = n!\, a^{(n)} b^{(n)} .$

$$(4e) \qquad a^{(m)}a^{(n)} = \frac{(m+n)!}{m!\,n!}\,a^{(m+n)}.$$

$$(4f) \qquad (a^{(m)})^{(n)} = \frac{(mn)!}{(m!)^n\,n!}\,a^{(mn)} \qquad \text{si } m \geqslant 1.$$

Donc si $s = 0$, je dirai qu'il s'agit d'un système de puissances complètement divisées. Si $r = s$, je dirai qu'il s'agit d'un système de puissances semi-divisées.

Soient r' et s' les quotients de r et s par un diviseur commun d; un système de type $(p; r, s; \varepsilon)$ est aussi un système de type $(p; r', s'; \varepsilon^d)$. Donc si le choix de ε n'est pas imposé, on peut s'arranger pour que r et s soient premiers entre eux; en particulier tout système de puissances semi-divisées peut être considéré comme un système de type $(1, 1)$.

Soit encore $(r'', s'') \in \boldsymbol{N}\times\boldsymbol{N}$ tel que $r''+s''=r+s$ et $r'' \leqslant r$; si A est muni d'un système de puissances de type (r, s) (notées $a \mapsto a^{[n]}$), alors A est aussi muni d'un système de puissances de type (r'', s'') (notées $a \mapsto a^{[n]''}$) si l'on pose

$$a^{[n]''} = \varepsilon^{(r-r'')\tau(n)}\,a^{[n]} \qquad \text{pour tout } n.$$

Enfin si J est un idéal de A contenu dans A', l'algèbre quotient A/J hérite de A son système de puissances partiellement divisées si et seulement si $a^{[n]} \in J$ chaque fois que $a \in J$ et $n \geqslant 1$.

3. – Les foncteurs S_{rs}.

Dorénavant ε sera toujours le même élément de K, choisi une fois pour toutes. Soit M un module sur l'anneau K; je cherche si il existe une algèbre augmentée $S = K \oplus S'$, munie d'un système de puissances de type (r, s), et une application linéaire f de M dans S', telles que soit vérifiée la propriété universelle que voici: quelle que soit l'algèbre $A = K \oplus A'$ munie d'un système de type (r, s) et quelle que soit l'application linéaire φ de M dans A', il existe un et un seul homomorphisme Φ de S dans A, qui respecte leurs systèmes de puissances partiellement divisées, et qui vérifie l'égalité $\varphi = \Phi \circ f$. Si une telle algèbre existe, elle est unique à isomorphisme près, elle sera notée $S_{rs}M = K \oplus S'_{rs}M$, et sera appelée l'algèbre symétrique de type (r, s) construite sur M; s'il faut préciser l'anneau de base, on écrit $S_{rsK}M$.

(5) PROPOSITION. *Il existe une algèbre $S_{rs}M$ vérifiant cette propriété universelle; elle est graduée: $S_{rs}M = \oplus S^n_{rs}M$, avec $S^0_{rs}M = K$; l'application*

$f(M \to S'_{rs}M)$ permet d'identifier $S^1_{rs}M$ avec M. Si M est engendré (comme module sur K) par un sous-ensemble E, alors $S^n_{rs}M$ (où $n \geqslant 1$) est engendré par les produits $e_1^{[n_1]}e_2^{[n_2]}\dots e_k^{[n_k]}$ où $e_1, \dots, e_k$ sont des éléments de E distincts deux à deux, et $n_1, \dots, n_k$ des entiers positifs dont la somme est n. Si M est libre sur K et si E est une base de M, alors $S^n_{sr}M$ est libre sur K et l'ensemble des produits indiqués ci-dessus forme une base de $S^n_{rs}M$.

Voici comment on peut construire cette algèbre $S_{rs}M$. Soit E un sous-ensemble générateur de M; soit $\boldsymbol{Z}[\eta]$ l'anneau obtenu en ajoutant à $\boldsymbol{Z}$ un élément η tel que $\eta^{r+s} = p$; il existe un homomorphisme de $\boldsymbol{Z}[\eta]$ dans K qui envoie η sur ε; soit encore $N = \boldsymbol{Z}[\eta][E]$ le module libre sur $\boldsymbol{Z}[\eta]$ engendré par E; on peut identifier N avec un sous-ensemble de $N_1 = \boldsymbol{Q}(\eta)[E]$, espace vectoriel sur le corps $\boldsymbol{Q}(\eta)$. Construisons son algèbre symétrique SN_1 (sur $\boldsymbol{Q}(\eta)$); cette algèbre SN_1 est trivialement munie d'un système de puissances de type $(p; r, s; \eta)$, à savoir $a^{[n]} = a^n/\eta^{r\tau(n)}$. Soit $S_{rs}N = \boldsymbol{Z}[\eta] \oplus S'_{rs}N$ le sous-module (sur $\boldsymbol{Z}[\eta]$) de SN_1 engendré par 1 et par les produits

$$e_1^{[n_1]}e_2^{[n_2]}\dots e_k^{[n_k]},$$

où $k \geqslant 1$, où $e_2, \dots, e_k$ sont des éléments de E distincts deux à deux, et où $n_1, \dots, n_k$ sont des entiers positifs. On vérifie sans peine que le système de puissances partiellement divisées de SN_1 se transmet par restriction à $S_{rs}N$. Remarquez maintenant que $S_{rs}N$ est libre sur $\boldsymbol{Z}[\eta]$ et admet pour base la famille des générateurs que j'ai indiqués ci-dessus; par suite $(S_{rs}N) \otimes_{\boldsymbol{Z}[\eta]} K$ est une algèbre libre sur K, et on peut lui transmettre le système de puissances partiellement divisées de $S_{rs}N$; en effet tout élément $x \in (S'_{rs}N) \otimes K$ s'écrit de façon unique comme somme de termes tels que $\lambda e_1^{[n_1]}e_2^{[n_2]}\dots e_k^{[n_k]}$, avec $\lambda \in K$, et on définit alors $x^{[n]}$, pour tout $n \in \boldsymbol{N}$, selon les règles qui résultent immédiatement des conditions (3). Par définition de E, il y a une application linéaire (sur K) surjective de $N \otimes_{\boldsymbol{Z}[\eta]} K$ sur M; soit N_0 son noyau; on peut donc identifier M avec $(N \otimes K)/N_0$; soit J l'idéal de $(S_{rs}N) \otimes K$ engendré par les éléments $a^{[n]}$ tels que $a \in N_0$ et $n \geqslant 1$, et soit $S_{rs}M$ le quotient de cette algèbre par cet idéal J; on démontre facilement que $S_{rs}M$ vérifie la propriété universelle qu'on exige d'elle, et les autres propriétés énoncées dans (5).

Il est clair que nous disposons maintenant d'un foncteur S_{rs} de la catégorie des modules sur K dans la catégorie des algèbres sur K munies d'un système de puissances de type (r, s). Si $r = 0$, il coïncide avec le foncteur S; si $s = 0$, il est isomorphe au foncteur Γ qui associe à M l'algèbre à puissances divisées (classiques) ΓM universelle sur M.

Si le couple (r'', s'') est tel que $r'' + s'' = r + s$ et $r'' \leqslant r$, l'algèbre $S_{rs}M$

est aussi munie d'un système de type (r'', s''), et il en résulte un morphisme du foncteur $S_{r''s''}$ vers le foncteur S_{rs}. En particulier si $\varepsilon = 0$, on obtient deux morphismes fonctoriels $S \to S_{11} \to \Gamma$, parce que dans ce cas-là $S_{02} = S_{01} = S$ et $S_{20} = S_{10} = \Gamma$.

Je signale enfin que si l'égalité $\lambda a = 0$ est satisfaite pour un certain couple $(\lambda, a) \in K \times M$, elle n'implique pas que $\lambda a^{[n]} = 0$ pour tout $n \geqslant 1$.

4. – Produits tensoriels.

(6) PROPOSITION. *Si M est un module sur K, et si l'anneau L est une algèbre sur K, alors il existe un isomorphisme de l'algèbre $S_{rsL}(M \otimes_K L)$ sur l'algèbre $(S_{rsK} M) \otimes_K L$ qui envoie tout élément $(a \otimes \lambda)^{[n]}$ (avec $a \in M$, $\lambda \in L$ et $n \in \mathbf{N}$) sur $a^{[n]} \otimes \lambda^n$.*

On peut déduire cette proposition de la construction de l'algèbre $S_{rs} M$ donnée au § 3.

(7) PROPOSITION. *Si $A = K \oplus A'$ est une algèbre sur K munie d'un système de puissances de type (r, s), et si L est une algèbre sur K, alors $A \otimes_K L = L \oplus (A' \otimes L)$ est une algèbre sur L munie d'un système de puissances de type (r, s) compatible avec celui de A.*

En effet à cause de la propriété universelle de $S_{rs} A'$, il existe un homomorphisme Φ de $S_{rs} A'$ sur A qui induit l'application identique sur A et qui respecte les systèmes de puissances partiellement divisées. On en déduit un homomorphisme de $(S_{rs} A') \otimes L$ sur $A \otimes L$; d'où (à cause de (6)) un homorphisme Ψ de $S_{rsL}(A' \otimes L)$ sur $A \otimes L$; le noyau de Ψ est l'image de $(\ker \Phi) \otimes L$ dans $S_{rsL}(A' \otimes L)$; c'est un idéal qui vérifie la propriété qu'il faut, pour que $S_{rsL}(A' \otimes L)/\ker \Psi$ hérite le système de puissances partiellement divisées; or ce quotient est isomorphe à $A \otimes L$.

(8) PROPOSITION. *Si $A = K \oplus A'$ et $B = K \oplus B'$ sont des algèbres sur K, toutes les deux munies d'un système de puissances de type (r, s), l'algèbre $A \otimes B = K \oplus (A' \oplus B' \oplus (A' \otimes B'))$ hérite d'un système de puissances de type (r, s), compatible avec ceux de A et B.*

En effet, d'après (7), en tant qu'algèbre sur A (resp. sur B), $A \otimes B$ reçoit un système de puissances de type (r, s), définies sur l'idéal $B' \oplus (A' \otimes B')$ (resp. sur $A' \oplus (A' \otimes B')$); ces deux systèmes coïncident sur $A' \otimes B'$.

(9) PROPOSITION. *Si M et N sont deux modules sur K, alors $S_{rs}(M \oplus N)$ est isomorphe à $(S_{rs} M) \otimes (S_{rs} N)$.*

Grâce à (9) on peut donner à $S_{rs}M$ une structure de bigèbre; le coproduit δ est l'homomorphisme de $S_{rs}M$ dans $(S_{rs}M)\otimes(S_{rs}M)$ qui provient de l'application diagonale de M dans $M\oplus M$.

5. – Dualité entre les foncteurs S_{rs} et S_{sr}.

Soient M et M' deux modules sur K et soit B une application bilinéaire de $M\times M'$ dans K. Je cherche à définir un produit intérieur qui à deux éléments $x\in S_{rs}M$ et $y\in S_{sr}M'$ associe un élément $i(y)\cdot x\in S_{rs}M$, ou si l'on préfère, $i(x)\cdot y\in S_{sr}M'$. J'exige que ce produit intérieur satisfasse les trois identités suivantes, qui impliquent son unicité:

$$(10a)\qquad \begin{cases} i(b^{[n]})\cdot a^{[m]} = 0 & \text{si } a\in M,\ b\in M' \text{ et } m<n,\\ i(b^{[n]})\cdot a^{[m]} = \dfrac{m!^*}{(m-n)!^*}\,\varepsilon^{s\sigma(n,m-n)}B(a,b)^n\,a^{[m-n]} & \text{si } m\geqslant n. \end{cases}$$

$$(10b)\qquad i(yz)\cdot x = i(y)\cdot\big(i(z)\cdot x\big) \qquad \text{si } x\in S_{rs}M \text{ et } y \text{ et } z\in S_{sr}M'.$$

$$(10c)\qquad i(z)\cdot(xy) = \mu\Big(i\big(\delta(z)\big)\cdot(x\otimes y)\Big) \qquad \text{si } x \text{ et } y\in S_{rs}M \text{ et } z\in S_{sr}M'.$$

Pour la compréhension de (10*c*) (formule de Leibniz), je donne quelques explications: δ est le coproduit qui résulte de l'application diagonale de M' dans $M'\oplus M'$ (voir § 4); si x_1 et $x_2\in S_{rs}M$, et z_1 et $z_2\in S_{sr}M'$, par définition:

$$i(z_1\otimes z_2)\cdot(x_1\otimes x_2) = \big(i(z_1)\cdot x_1\big)\otimes\big(i(z_2)\cdot x_2\big)\ ;$$

enfin μ est l'application de $(S_{rs}M)\otimes(S_{rs}M)$ dans $S_{rs}M$ qui résulte de la structure d'algèbre de $S_{rs}M$.

(11) PROPOSITION. *Il existe une application $(x,y)\mapsto i(y)\cdot x$ qui vérifie les trois propriétés* (10) *ci-dessus; de même il existe une application $(x,y)\mapsto$ $\mapsto i(x)\cdot y$ qui vérifie les trois propriétés analogues. Les produits intérieurs $i(y)\cdot x$ et $i(x)\cdot y$ ont toujours même composante dans $K = S^0_{rs}M =$ $= S^0_{sr}M'$; désignons cette composante par $B(x,y)$; ainsi B est prolongée en une application bilinéaire de $(S_{rs}M)\times(S_{sr}M')$ dans K. Si M et M' sont libres et de rang fini sur K, et si B met M et M' en dualité, alors B met $S^n_{rs}M$ et $S^n_{sr}M'$ en dualité pour tout $n\in\mathbf{N}$.*

DÉMONSTRATION. Soit E (resp. E') un sous-ensemble générateur de M (resp. M'); je reprends les objets N, N_1 et SN_1 que j'ai définis au § 3 à partir de E, et je définis de même N', N'_1 et SN'_1 à partir de E'. En outre j'introduis une famille d'indéterminées $(x_{ee'})$, indexée par les couples $(e,e')\in E\times E'$,

j'introduis l'anneau $A_2 = \boldsymbol{Q}(\eta)[x_{ee'}]$ qui contient toutes les indéterminées $x_{ee'}$, j'introduis encore $N_2 = A_2[E]$, et SN_2 qui est une algèbre libre sur A_2; je définis de même N_2' et SN_2'. Les algèbres SN_2 et SN_2' (qui sont aussi des algèbres sur $\boldsymbol{Q}(\eta)$) sont trivialement munies de systèmes de puissances partiellement divisées de type (r, s) et (s, r) respectivement. Soit C_2 l'application bilinéaire de $N_2 \times N_2'$ dans A_2 telle que $C_2(e, e') = x_{ee'}$ quel que soit $(e, e') \in E \times E'$; grâce à C_2, on peut construire un produit intérieur de $SN_2 \times SN_2'$ dans SN_2, qui vérifie les trois identités (10), à condition d'y remplacer ε par η et B par C_2; je peux aussi construire un produit intérieur à valeurs dans SN_2' et l'on sait que ces deux produits intérieurs ont toujours même composante dans $A_2 = S^0 N_2 = S^0 N_2'$. Revenons au premier produit intérieur, que je préfère maintenant traiter comme une application linéaire de $SN_2 \otimes_{A_2} SN_2'$ dans SN_2, ou encore comme une application de $SN_1 \otimes SN_1 \otimes A_2$ (produit tensoriel sur $\boldsymbol{Q}(\eta)$) dans $SN_1 \otimes A_2$ (idem). Le fait capital à cet endroit de la démonstration est que, si $x \in S_{rs}N$ (sous-algèbre de SN_1 définie au § 3) et si $y \in S_{sr}N'$, alors l'image de $x \otimes y \otimes 1$ dans $SN_1 \otimes A_2$ appartient à la sous-algèbre $S_{rs}N \otimes_{\boldsymbol{Z}[\eta]} \boldsymbol{Z}[\eta][x_{ee'}]$; d'où une application:

$$S_{rs}N \otimes S_{sr}N' \otimes \boldsymbol{Z}[\eta][x_{ee'}] \to S_{rs}N \otimes \boldsymbol{Z}[\eta][x_{ee'}];$$

les produits tensoriels que j'écris sans préciser l'anneau de base se font sur l'anneau $\boldsymbol{Z}[\eta]$. En faisant des produits tensoriels par K (qui est une algèbre sur $\boldsymbol{Z}[\eta]$), j'obtiens une application:

$$(S_{rs}N \otimes K) \otimes_K (S_{rs}N' \otimes K) \otimes_K K[x_{ee'}] \to (S_{rs}N \otimes K) \otimes_K K[x_{ee'}].$$

Je peux faire de K une algèbre sur $K[x_{ee'}]$ grâce à l'homomorphisme de $K[x_{ee'}]$ dans K qui envoie chaque indéterminée $x_{ee'}$ sur $B(e, e')$; en faisant des produits tensoriels par K sur l'anneau $K[x_{ee'}]$, j'obtiens maintenant une application:

$$(S_{rs}N \otimes K) \otimes_K (S_{sr}N' \otimes K) \to S_{rs}N \otimes K;$$

cette application vérifie les trois conditions (10), à condition de remplacer B par l'application bilinéaire C de $(N \otimes K) \times (N' \otimes K)$ dans K induite par B. Je rapelle que $S_{rs}M$ est le quotient de $S_{rs}N \otimes K$ par un certain idéal J que l'on construit à partir du noyau N_0 de l'application $N \otimes K \to M$; de même $S_{rs}M' = (S_{rs}N' \otimes K)/J'$, où J' est l'idéal construit à partir de $N_0' = \ker(N' \otimes K \to M')$; puisque $C(a, b) = 0$ si $a \in N_0$ ou si $b \in N_0'$, on déduit des identités (10) que J et J' vérifient les conditions qu'il faut pour que l'on obtienne à la fin une application de $S_{rs}M \otimes_K S_{sr}M'$ dans $S_{rs}M$.

Si M et M' sont libres et de rang fini, et si B les met en dualité, on peut exiger que E et E' soient des bases duales; c'est-à-dire $B(e, e')$ vaut 1 ou 0

selon que e et e' sont associés ou non; on peut traiter ce cas avec les mêmes méthodes que ci-dessus, mais sans avoir besoin des indéterminées $x_{ee'}$.

La proposition (11) me permet de dire que les foncteurs S_{rs} et S_{sr} sont duaux l'un de l'autre. La dualité bien connue des foncteurs S et Γ est un cas particulier de la dualité entre deux foncteurs S_{rs} et S_{sr}. Un autre cas particulier est la propriété de S_{11} d'être son propre dual.

6. – L'algèbre $S_{rs}^{+}M$ lorsque $r \geqslant s$ et $p \neq 2$.

Si m est un entier pair non nul et si $p \neq 2$, l'égalité (2) nous permet d'écrire $\varrho(m, n) \geqslant \tau(n)$, parce que $\chi(m) \geqslant 2$; si en outre $r \geqslant s$, alors:

$$r\varrho(m, n) - s\tau(n) \geqslant 0 ;$$

cette inégalité sera essentielle dans ce paragraphe.

Soit M un module sur K; l'algèbre $S_{rs}M$ est graduée sur le groupe $\boldsymbol{Z}$, donc aussi sur $\boldsymbol{Z}/2\boldsymbol{Z}$; pour la commodité des notations je remplace le groupe additif $\boldsymbol{Z}/2\boldsymbol{Z}$ par le groupe multiplicatif $\{+, -\}$, et je pose:

$$S_{rs}^{+}M = K \oplus S_{rs}^{2}M \oplus S_{rs}^{4}M \oplus S_{rs}^{6}M \oplus \dots ;$$

ceci est de façon évidente une algèbre augmentée.

(12) PROPOSITION. *Sur l'algèbre $S_{rs}^{+}M = K \oplus S_{rs}^{\prime +}M$ il existe un système de puissances divisées classiques (notées $u \mapsto u^{(n)}$), satisfaisant, en plus des six conditions* (4), *les deux conditions suivantes, dans lesquelles a et $b \in M$:*

si m est pair $\geqslant 2$,

$$(a^{[m]})^{(n)} = \frac{1}{n!^{*}} \varepsilon^{r\varrho(m,n)-s\tau(n)} a^{[mn]} ;$$

si l et m sont impairs,

$$(a^{[l]}b^{[m]})^{(n)} = \frac{1}{n!^{*}} \varepsilon^{r\varrho(l,n)+r\varrho(m,n)+(r-s)\tau(n)} a^{[ln]}b^{[mn]} .$$

DÉMONSTRATION. Rappelons que $S_{rs}M$ est le quotient d'une certaine algèbre $S_{rs}N \otimes K$ par un certain idéal J, et que $S_{rs}N$ est une sous-algèbre d'une certaine algèbre SN_1 sur le corps $\boldsymbol{Q}(\eta)$, où $\eta^{s+r} = p$; cette algèbre SN_1 est donc munie d'un système de puissances complètement divisées de

type $(p; 0, r+s; \eta)$. Grâce à l'inégalité que j'ai indiquée au début de ce paragraphe, on démontre que ce système de puissances de type $(0, r+s)$ respecte la sous-algèbre $S^+_{rs}N$; en outre il vérifie les deux identités analogues à celle écrite dans (12), à condition d'y omettre les facteurs $1/n!^*$. Il se transmet à l'algèbre $S^+_{rs}N \otimes K$, et de là il passe à l'algèbre $S^+_{rs}M$, parce qu'il respecte l'idéal $J \cap (S^+_{rs}N \otimes K)$. Il ne reste plus qu'à associer à ces puissances de type $(0, r+s)$ des puissances divisées classiques (voir § 2); c'est là que s'introduisent les facteurs $1/n!^*$.

Revenons à la situation décrite au § 5: on se donne une application bilinéaire B de $M \times M'$ dans K, et l'on définit un produit intérieur de $(S_{rs}M) \times (S_{sr}M')$ dans $S_{rs}M$; soient $u \in S^2_{rs}M$ et $b \in M'$; puisque $r \geqslant s$ et $p \neq 2$, je peux définir $u^{(m)}$ pour tout $m \in \boldsymbol{N}$ et je me propose de calculer $i(b^{[n]}) \cdot u^{(m)}$ lorsque $2m \geqslant n$. Je pose $a = i(b) \cdot u \in M$ et $\omega = B(a, b) = B(u, b^2) \in K$; j'aurai besoin au § 10 de la formule suivante:

$$(13) \qquad i(b^{[n]}) \cdot u^{(m)} = \sum_{0 \leqslant 2j \leqslant n} \left(\frac{\omega}{2}\right)^j \frac{n!^*}{j!^*(n-2j)!^*} \varepsilon^{\varkappa(j)} a^{[n-2j]} u^{(m-n+j])},$$

$$\text{avec } \varkappa(j) = r\sigma(j, j, n-2j) + (r-s)\tau(j).$$

Pour démontrer rapidement cette formule, il vaut mieux commencer par le cas trivial où K est le corps $\boldsymbol{Q}(\eta)$; dans ce cas on peut démontrer par récurrence sur n que:

$$i\left(\frac{b^n}{n!}\right) \cdot \frac{u^m}{m!} = \sum_{0 \leqslant 2j \leqslant n} \frac{\omega^j}{2^j j!} \frac{a^{n-2j}}{(n-2j)!} \frac{u^{m-n+j}}{(m-n+j)!};$$

on passe ensuite au cas général en refaisant la construction du produit intérieur que j'ai présentée au § 5.

Ayant maintenant défini les foncteurs S_{rs} et indiqué leurs propriétés essentielles, je désire montrer que ces foncteurs méritent notre attention, et dans ce but je vais donner deux applications de ma théorie. La première concerne les foncteurs polynomiaux de Monsieur J. L. Koszul (§ 8); pour en parler j'aurai besoin de quelques résultats techniques que j'expliquerai au § 7. La deuxième application (§ 10) concerne un problème de produit intérieur d'exponentielles, dont les origines seront expliquées au § 9. Les paragraphes 9 et 10 sont indépendants des deux précédents.

7. – L'ensemble $N[z]$ des types de produits généralisés.

Ce paragraphe, essentiellement technique, est seulement nécessaire à la compréhension du § 8. Soit d'abord $A = K \oplus A'$ une quelconque algèbre

sur K munie d'un système de puissances de type (r, s). Soit $a \in A'$, soit $n \in \boldsymbol{N}$ et soit $n = \sum n_j p^j$ son écriture dans le système de numération de base p; on a:

$$a^{[n]} = \prod_{j \geqslant 0} (a^{[p^j]})^{n_j}; \tag{14}$$

cela résulte du fait que les exposants n_j et $[n_j]$ sont synonymes (puisque $n_j < p$), et des égalités suivantes, que l'on peut déduire de (1) et (2):

$$\sigma(n_0, n_1 p, n_2 p^2, \ldots \ldots) = 0\,, \qquad \varrho(p^j, n_j) = \pi(p^j, n_j) = 0\,.$$

On peut donc faire tous les calculs en ne mettant jamais entre crochets d'autres exposants que des puissances de p.

Soit $(n_1, n_2, \ldots, n_k)$ une suite d'exposants (entiers $\geqslant 0$); je lui associe le produit généralisé défini ainsi: c'est l'application qui à toute suite $(a_1, a_2, \ldots, a_k)$ d'éléments de A' associe le produit de toutes les puissances $a_j^{[n_j]}$ $(1 \leqslant j \leqslant k)$; par extension j'appelle aussi produit généralisé la valeur de cette application sur une suite particulière $(a_1, \ldots, a_k)$, que j'appelle alors la suite des facteurs de base. Ecrivons chaque n_j dans le système de numération de base p: $n_j = \sum n_{ij} p^i$; le polynôme $\alpha = \sum_i \left(\sum_j n_{i,j}\right) z^i$ est appelé le type du produit généralisé (ou le type de la suite des exposants); c'est un élément de $\boldsymbol{N}[z]$: $\alpha = \sum \alpha_i z^i$, avec $\alpha_i \in \boldsymbol{N}$ pour tout i; si on transforme l'expression du produit généralisé de telle façon que tous les exposants soient des puissances de p (voir (14)), chaque coefficient α_i est égal au nombre d'exposants égaux à p^i.

Par définition, le degré du produit généralisé (ou de la suite des exposants) est $\sum n_j = \alpha(p)$; j'aurai aussi besoin des degrés tronqués $\alpha(p; j)$ (où $j \in \boldsymbol{N}$), définis ainsi:

$$\alpha(p; j) = \alpha_0 + \alpha_1 p + \ldots + \alpha_j p^j\,.$$

Pour tout $n \in \boldsymbol{N}$, j'appelle $\boldsymbol{N}_n[z]$ l'ensemble des $\alpha \in \boldsymbol{N}[z]$ tels que $\alpha(p) = n$; sur chaque $\boldsymbol{N}_n[z]$ je mets la relation d'ordre suivante: $\alpha \geqslant \beta$ si (par définition) $\alpha(p; j) \geqslant \beta(p; j)$ pour tout $j \geqslant 0$.

Soit maintenant M un module libre de rang fini h sur K et soit $E = (e_1, \ldots, e_h)$ une base de M; il résulte de (5) que $S_{rs}M$ admet pour base la famille E' de tous les produits généralisés dont la suite des facteurs de base est la suite des éléments de E; donc à tout élément $e' \in E'$ est associé un type $\beta \in \boldsymbol{N}[z]$; en particulier à l'unité 1 est associé le type 0; le degré de e' est précisément $\beta(p)$.

Après ces préliminaires, voici le problème dont nous devrons connaitre la solution au § 8. Soit $(m_1, \ldots, m_k)$ une suite d'exposants de type α, soit

(x_{ij}) une famille d'indéterminées telle que $1 \leqslant i \leqslant h$ et $1 \leqslant j \leqslant k$, et soit $P(x_{ij})$ le polynôme obtenu en faisant dans l'algèbre $(S_{rs}M) \otimes K[x_{ij}]$ le produit généralisé que voici:

$$P(x_{ij}) = \prod_{1 \leqslant j \leqslant k} \Big(\sum_{1 \leqslant i \leqslant h} x_{ij}\, e_i \Big)^{[m_j]} ;$$

dans ce polynôme on ne trouve que des monômes $X = \prod_{i,j} x_{ij}^{m_{ij}}$ tels que $\sum_i m_{ij} = m_j$ pour tout j; posons $m'_i = \sum_j m_{ij}$ et soit $e(X)$ le produit des $e_i^{[m'_i]}$; c'est un élément de E' auquel est associé un type β_X; le polynôme $P(x_{ij})$ peut s'écrire ainsi:

$$P(x_{ij}) = \sum_X h(X)\, \varepsilon^{k(X)} X e(X) ,$$

où $h(X)$ est un entier non divisible par p, et que pour cette raison je n'ai pas besoin de connaître, et où seul l'exposant $k(X)$ m'intéresse. En fait la valeur exacte de $k(X)$ ne me sera pas utile, car je n'aurai besoin que des renseignements qui résultent de la seule connaissance des types α et β_X.

Je trouve d'abord que l'image de $k(X)$ dans $\boldsymbol{Z}/(r+s)\boldsymbol{Z}$ ne dépend que de α et β_X. Posons $n = \alpha(p) = \beta_X(p)$; soit $V(\alpha, \beta)$ l'application de $\boldsymbol{N}_n(z) \times \times \boldsymbol{N}_n[z]$ dans $\boldsymbol{Z}$, dont la formule (15) propose deux définitions possibles:

$$V(\alpha, \beta) = \frac{\alpha(1) - \beta(1)}{p-1} = \sum_{j \geqslant 0} \frac{\alpha(p;j) - \beta(p;j)}{p^{j+1}} ; \tag{15}$$

remarquez que l'égalité $\alpha(p) = \beta(p)$ implique que $\alpha(1) - \beta(1)$ est divisible par $p-1$, et que $\alpha(p;j) - \beta(p;j)$ est divisible par p^{j+1}; l'égalité des deux derniers membres de (15) résulte de l'identité

$$\sum_{j \geqslant 0} \frac{1}{p^{j+1}} = \frac{1}{p-1} .$$

Mon premier renseignement sur $k(X)$ est le suivant:

$$k(X) = rV(\alpha, \beta_X) = sV(\beta_X, \alpha) \mod (r+s) . \tag{16}$$

DÉMONSTRATION. Soit (m_{ij}) la suite de longueur hk obtenue en écrivant bout à bout les k suites $(m_{1j}, \ldots, m_{hj})$, et soit γ_X le type de la suite d'exposants (m_{ij}); avec les notations du § 1, on a:

$$\alpha(1) = \sum_j \chi(m_j) , \quad \beta_X(1) = \sum_i \chi(m'_i) \quad \text{et} \quad \gamma_X(1) = \sum_{i,j} \chi(m_{ij}) .$$

A cause de (3*c*) et (3*e*), on a par ailleurs:

$$k(X) = s \sum_j \sigma(m_{1j}, \ldots, m_{hj}) + r \sum_i \sigma(m_{i1}, \ldots, m_{ik}) .$$

Grâce à (1) on obtient une expression de $k(X)$ où figurent les entiers $\chi(m_j)$, $\chi(m_i')$ et $\chi(m_{ij})$; on reconnait alors que:

$$k(X) = \frac{1}{p-1} \left((r+s)\gamma_X(1) - r\beta_X(1) - s\alpha(1)\right) .$$

De là on passe facilement à (16).

Je veux maintenant connaître la valeur minimale de $k(X)$ quand on impose à β_X une valeur donnée.

(17) LEMME. *Soit e' un élément de E' de type $\beta \in \boldsymbol{N}_n[z]$. L'ensemble des monômes X tels que $e(X) = e'$, n'est pas vide, et quand X décrit cet ensemble, la valeur minimale de $k(X)$ est le nombre $\theta(\alpha, \beta)$ défini dans la formule* (18) *ci-dessous.*

Pour définir $\theta(\alpha, \beta)$, j'ai besoin des fonctions « partie positive » et « partie négative », qui à tout $x \in \boldsymbol{Z}$ associent respectivement $x^+ = \sup(0, x)$ et $x^- = -\inf(0, x)$; avec ces notations:

$$\theta(\alpha, \beta) = r \sum_{j \geqslant 0} \left(\frac{\alpha(p;j) - \beta(p;j)}{p^{j+1}} \right)^+ + s \sum \left(\frac{\alpha(p;j) - \beta(p;j)}{p^{j+1}} \right)^- . \tag{18}$$

Il résulte tout de suite de (15) et (18) que:

$$\theta(\alpha, \beta) = rV(\alpha, \beta) = sV(\beta, \alpha) \mod (r+s). \tag{19}$$

Avant de démontrer (17), je vais en tirer quelques conséquences lorsque K est de caractéristique p; puisque $\varepsilon^{r+s} = 0$, on ne s'occupe que des monômes X tels que $k(X) = \theta(\alpha, \beta_X)$. Si il s'agit de puissances non divisées ($r = 0$, $\varepsilon^s = 0$), on ne trouve dans $P(x_{ij})$ que des éléments de E' dont le type est inférieur ou égal à α (pour la relation d'ordre indiquée plus haut); au contraire si il s'agit de puissances complètement divisées ($s = 0$, $\varepsilon^r = 0$), on n'y trouve que des éléments de E' de type supérieur ou égal à α. Si $rs \neq 0$, on ne trouve dans $P(x_{ij})$ que des éléments de E' de type supérieur ou inférieur ou égal à α, et ils sont toujours accompagnés d'une puissance de ε distincte de 1 si leur type est distinct de α; en particulier si $\varepsilon = 0$ et $r = s = 1$, on n'y trouve que des éléments de E' de même type α.

Pour préparer la démonstration de (17) et le paragraphe suivant, je vais dire des choses sur les ensembles finis ordonnés en général, et sur $\boldsymbol{N}_n[z]$ en particulier. Soit d'abord $\mathcal{E}$ un ensemble fini ordonné quelconque; deux éléments de $\mathcal{E}$ sont dits adjacents si l'un est supérieur à l'autre et si il n'existe aucun autre élément compris entre eux deux; une chaîne de longueur l joignant α et β est une suite $(\alpha_0, \alpha_1, \ldots, \alpha_l)$ telle que $\alpha_0 = \alpha$ et $\alpha_l = \beta$, et dans laquelle deux éléments consécutifs sont toujours adjacents.

Soit G le graphe orienté dont les sommets sont les éléments de $\mathcal{E}$ et dont les arêtes (orientées) sont les couples (α, β) où α et β sont adjacents et où $\alpha > \beta$. Si le graphe non orienté sous-jacent à G est connexe, on dit que $\mathcal{E}$ est indécomposable; on peut alors définir une fonction « distance » $d(\alpha, \beta)$: c'est la longueur de la plus courte chaîne joignant α et β. Dans certains cas il existe une fonction « différence de niveau » $V(\alpha, \beta)$ (à valeurs dans $\boldsymbol{Z}$); une telle fonction doit satisfaire les trois conditions suivantes, qui impliquent son unicité lorsque $\mathcal{E}$ est indécomposable:

$V(\alpha, \beta) + V(\beta, \gamma) + V(\gamma, \alpha) = 0$ quels que soient α, β et γ;

si $\alpha > \beta$, alors $V(\alpha, \beta) > 0$;

si α et β sont adjacents, $V(\alpha, \beta) = \pm 1$.

L'existence d'une telle fonction V signifie que, dans tout chaîne, la différence entre le nombre de maillons croissants et le nombre de maillons décroissants ne dépend que des extrémités. Une partie $\mathcal{F}$ de $\mathcal{E}$ est dite fermée si les assertions $\alpha \geqslant \beta$ et $\alpha \in \mathcal{F}$ impliquent toujours $\beta \in \mathcal{F}$; les parties fermées de $\mathcal{E}$ forment un treillis (pour la relation d'ordre de l'inclusion).

L'ensemble ordonné $\boldsymbol{N}_n[z]$ est un treillis; si par exemple α et $\beta \in \boldsymbol{N}_n[z]$, la borne supérieure de α et β est l'élément γ tel que $\gamma(p; j) = \sup(\alpha(p; j), \beta(p; j))$ pour tout j. L'ensemble ordonné $\boldsymbol{N}_n[z]$ est donc indécomposable, et il possède un plus grand et un plus petit élément; le plus grand élément est le polynôme constant n; le plus petit élément est le polynôme $\sum n_j z^j$ tel que $\sum n_j p^j$ soit l'écriture de n dans le système de numération de base p. On passe d'une élément α à un élément adjacent inférieur (resp. adjacent supérieur) en lui ajoutant (resp. retranchant) un polynôme $z^{j+1} - pz^j$ (avec $j \in \boldsymbol{N}$), ce qui est possible chaque fois que $\alpha_j \geqslant p$ (resp. $\alpha_{j+1} \geqslant 1$). La fonction « distance » est celle-ci:

$$d(\alpha, \beta) = \sum_{j \geqslant 0} \left| \frac{\alpha(p; j) - \beta(p; j)}{p^{j+1}} \right| .$$

Il existe une fonction « différence de niveau », c'est précisément la fonction V définie dans (15). Entre les fonctions θ, d et V existe la relation:

$$2\theta = (r + s)\, d + (r - s) V .$$

A cause de (1) la valeur maximale de $V(\alpha, \beta)$, c'est-à-dire la différence de niveau entre le plus grand et le plus petit élément de $\boldsymbol{N}_n[z]$, est égale à $\tau(n)$.

DÉMONSTRATION DE (17). Je reprends les notations introduites dans la démonstration de (16); la valeur de $k(X)$ trouvée là-bas peut encore être écrite ainsi:

$$k(X) = rV(\gamma_X, \beta) + sV(\gamma_X, \alpha) .$$

Remarquez que $\gamma_X \geqslant \alpha$; en effet si m' et m'' sont deux exposants tels que $m' + m'' = m_j$, le type de la suite $(m_1, \ldots, m_{j-1}, m', m'', m_{j+1}, \ldots, m_k)$ est supérieur ou égal à α. De même $\gamma_X \geqslant \beta$. Donc $V(\gamma_X, \alpha)$ et $V(\gamma_X, \beta)$ sont les distances de γ_X à α et β. Si il existe un monôme X tel que $e(X) = e'$ et tel que γ_X soit la borne supérieure de α et β, on peut affirmer, d'une part que $k(X)$ est minimal (si on impose $e(X) = e'$), et d'autre part qu'il a la valeur $\theta(\alpha, \beta)$ indiquée dans (18). Il s'agit donc de construire une suite (m_{ij}) telle que $\sum_i m_{ij} = m_j$ et $\sum_j m_{ij} = m'_i$ (quels que soient i et j), et dont le type γ est la borne supérieure de α et β. On peut procéder ainsi: on décompose les k nombres m_j en sommes de puissances de p, et avec ces puissances de p on fait h paquets dont les sommes sont respectivement les nombres m'_i; on part des décompositions des m_j déterminées par leurs écritures dans le système de numération de base p; ensuite on dresse la liste (par ordre croissant) des entiers $g \in \boldsymbol{N}$ tels que $\alpha(p; g) \neq \beta(p; g)$; si $\alpha(p; g) < \beta(p; g)$, il faut faire apparaitre $p(\beta(p; g) - \alpha(p; g))$ puissances p^g supplémentaires, en décomposant en sommes de puissances p^g quelques puissances de p supérieures à p^g; si au contraire $\alpha(p; g) > \beta(p; g)$, il faut mettre en réserve $p(\alpha(p; g) - \beta(p; g))$ puissances p^g, avec lesquelles on pourra faire apparaitre des puissances de p supérieures à p^g dans ceux des h paquets qui en ont besoin; après toutes ces opérations, chaque m_{ij} est la somme des puissances de p qui proviennent de la décomposition de m_j et qui contribuent ensuite à composer m'_i.

8. – Les foncteurs polynomiaux S^n_{rsq}.

Ici K est un corps infini. Un foncteur polynomial est un foncteur F de la catégorie des espaces vectoriels de dimension finie sur K dans elle-même, vérifiant la propriété suivante: quels que soient U et V dans cette catégorie, l'application de Hom (U, V) dans Hom $(F(U), F(V))$ définie par F est une application polynomiale (d'un espace vectoriel de dimension finie sur K dans un autre). Si quels que soient U et V, elle est homogène de degré n, on dit que F est homogène de degré n. Tout foncteur polynomial est somme

directe de foncteurs polynomiaux homogènes (éventuellement en nombre infini, comme par exemple dans le cas du foncteur « algèbre extérieure »). La théorie des foncteurs polynomiaux fournit des représentations rationnelles des groupes algébriques $GL(U)$; en effet si F est un foncteur polynomial, ce groupe opère dans l'espace vectoriel $F(U)$; si la dimension de U est au moins égale au degré de F, on peut obtenir toutes les propriétés du foncteur F en étudiant l'action de $GL(U)$ dans $F(U)$. On trouvera dans [7] le contexte qui a amené J. L. Koszul à construire la théorie des foncteurs polynomiaux; malheureusement je ne connais pas de publication de lui sur cette théorie.

Si K est de caractéristique nulle, tout foncteur polynomial est somme directe de foncteurs irréductibles, et tout foncteur irréductible de degré n est isomorphe à un sous-foncteur de T^n (puissance tensorielle n-ième); par suite les classes d'isomorphie de foncteurs polynomiaux irréductibles sont en correspondance biunivoque avec les diagrammes de Young. Les choses se passent tout autrement si le corps K a une caractéristique p non nulle; par exemple si $n \geqslant p$, le foncteur S^n n'est ni irréductible, ni même somme directe de sous-foncteurs irréductibles; la même remarque s'applique à Γ^n, et en outre ces deux foncteurs ne sont pas isomorphes. Dans toute la suite de ce paragraphe, K est un corps de caractéristique p; je montrerai que la théorie des foncteurs S^n_{rs} (définis au § 3) fournit des foncteurs polynomiaux différents des foncteurs S^n et Γ^n, et de tous ceux qu'on peut en déduire par les deux opérations élémentaires que voici: faire des quotients de deux sous-foncteurs (le second étant inclus dans le premier), puis faire des sommes directes.

Mais auparavant je voudrais introduire la notion de suite de composition. Soit F un foncteur polynomial de degré n; une suite de composition de F est une suite strictement croissante de sous-foncteurs (polynomiaux), où le premier est égal au foncteur nul, et le dernier à F, et où le quotient de deux sous-foncteurs consécutifs est toujours un foncteur irréductible; ces foncteurs irréductibles s'appellent les facteurs irréductibles de F; plus exactement les facteurs irréductibles sont leurs classes d'isomorphie; les facteurs irréductibles sont les même pour toutes les suites de composition; l'existence de suites de composition (de longueur finie) résulte du fait que tous les sous-foncteurs de F apparaissent lorsqu'on étudie l'action d'un seul groupe $GL(U)$ dans $F(U)$, pourvu que $\dim U \geqslant n$. Dans la suite nous pourrons toujours nous ramener à l'étude de foncteurs F dont tous les facteurs irréductibles sont deux à deux non isomorphes; dans ce cas, si Φ est un facteur irréductible de F, l'intersection de tous les sous-foncteurs dont Φ est un facteur irréductible, est encore un sous-foncteur dont Φ est un facteur irréductible; par définition le sous-foncteur élémentaire associé à Φ

est le plus petit sous-foncteur de F dont Φ est un facteur irréductible. Soit $\mathfrak{E}$ l'ensemble des sous-foncteurs élémentaires de F, ordonné par la relation d'inclusion; puisque tout sous-foncteur de F est la somme des sous-foncteurs élémentaires qu'il contient, le treillis des sous-foncteurs de F est isomorphe au treillis des parties fermées de $\mathfrak{E}$, selon la définition donnée à la fin du § 7; donc ce treillis est fini. Il est clair que la connaissance de l'ensemble ordonné $\mathfrak{E}$ permet de trouver toutes les suites de composition de F.

Définition des foncteurs polynomiaux S^n_{rsq}.

Soient q, r et s trois entiers $\geqslant 0$ tels que $1 \leqslant q \leqslant r+s$; soit K_q l'anneau obtenu en ajoutant à K un élément ε nilpotent d'ordre q:

$$K_q = K \oplus K\varepsilon \oplus K\varepsilon^2 \oplus \ldots \oplus K\varepsilon^{q-1}, \qquad \text{et } \varepsilon^q = 0$$

(en particulier $K_1 = K$); si U est un espace vectoriel de dimension finie sur F, je peux lui associer l'algèbre $S_{rsK_q}(U \otimes K_q)$ sur l'anneau K_q; soit maintenant $n \in \boldsymbol{N}$; si je considère $S^n_{rsK_q}(U \otimes K_q)$ comme un espace vectoriel sur K, j'obtiens un foncteur polynomial de degré n, que je note S^n_{rsq}. Quoique cette définition oblige à « oublier » que $S^n_{rsq}U$ est un module sur K_q, il ne faur pas oublier qu'à tout couple (λ, F) où $\lambda \in K_q$ et où F est un sous-foncteut de S^n_{rsq}, on peut associer un nouveau sous-foncteur λF; il faut donc prévoir que le treillis des sous-foncteurs de S^n_{rsq} peut être infini si $q \geqslant 2$.

On connait tous les foncteurs S^n_{rsq} dès que l'on connait ceux pour lesquels $q = r + s$, et r et s sont premiers entre eux. En effet S^n_{rsq} est isomorphe au quotient de $S^n_{rs(r+s)}$ par $\varepsilon^q S^n_{rs(r+s)}$; en outre si r' et s' sont les quotients de r et s par un diviseur commun d, $S^n_{rs(r+s)}$ est la somme directe de d sous-foncteurs isomorphes à $S^n_{r's'(r'+s')}$; en effet il existe un homomorphisme injectif de $K_{r'+s'}$ dans K_{r+s}, et $S_{rs(r+s)}$ est isomorphe au produit tensoriel sur $K_{r'+s'}$ de K_{r+s} et $S_{r's'(r'+s')}$.

Pour comparer entre eux ces foncteurs S^n_{rsq}, je vais étudier leurs sous-foncteurs, en utilisant les techniques du § 7.

Les sous-foncteurs $S^{(\alpha)}_{rsq}$.

Soient $n \in \boldsymbol{N}$ et $\alpha \in \boldsymbol{N}_n[z]$; j'appelle $S^{(\alpha)}_{rsq}U$ le sous-espace vectoriel de $S^n_{rsq}U$ engendré par tous les produits généralisés de type α dont les facteurs de base sont dans U; autrement dit, $S^{(\alpha)}_{rsq}U$ est engendré par les produits $a_1^{[m_1]} \cdot a_2^{[m_2]} \ldots a_k^{[m_k]}$ où $a_1, \ldots, a_k \in U$, où tous les exposants m_j sont des puissances de p, et où le nombre des exposants égaux à p^i est égal à α_i (pour tout $i \geqslant 0$); ceci implique que $k = \alpha(1)$. On définit ainsi un sous-foncteur $S^{(\alpha)}_{rsq}$ de S^n_{rsq}. Il faut distinguer $S^{(n)}_{rsq}$ de S^n_{rsq}; l'égalité de ces deux foncteurs n'est vraie que si $n < p$ ou si $r = 0$.

Soit $(e_1, e_2, \ldots, e_h)$ une base de U; à cause de (5) on peut lui associer une base E' de $S_{rs}(U \otimes K_q)$ sur K_q, et au § 7 j'ai dit qu'on pouvait associer à tout élément de E' un type $\beta \in \boldsymbol{N}[z]$; l'espace vectoriel $S^n_{rsq}U$ admet pour base (sur K) la famille des $\varepsilon^k e'$, où $0 \leqslant k < q$, et où e' est un élément de E' dont le type est dans $\boldsymbol{N}_n[z]$.

(20) PROPOSITION. *L'espace vectoriel $S^{(\alpha)}_{rsq}U$ admet pour base la famille des $\varepsilon^{\theta(\alpha,\beta)}e'$, où e' est un élément de E' dont le type β est tel que $\theta(\alpha, \beta) < q$.*

Cette proposition (20) est une conséquence immédiate de (16) et (17); je rappelle que le corps K est infini.

(21) PROPOSITION. *Tout sous-foncteur F de S^n_{rsq} est une somme finie de sous-foncteurs tels que $\lambda S^{(\alpha)}_{rsq}$, où $\lambda \in K_q$ et $\alpha \in \boldsymbol{N}_n[z]$.*

DÉMONSTRATION. Supposons que FU contient un élément non nul, et écrivons-le comme combinaison linéaire à coefficients dans K_q d'éléments de E': $\sum \lambda(e')\,e'$. En faisant opérer dans FU le sous-groupe de $GL(U)$ formé par les endomorphismes diagonalisables dans la base $(e_1, \ldots, e_h)$, on trouve que chaque élément $\lambda(e')\,e'$ appartient à FU. Soit $(m_1, \ldots, m_h)$ la suite d'exposants telle que e' soit le produit des $e_i^{[m_i]}$, et soit α son type; en faisant opérer tout le groupe $GL(U)$ dans FU, on trouve que FU contient tous les produits

$$\lambda(e')\,a_1^{[m_1]}a_2^{[m_2]}\ldots a_h^{[m_h]}, \qquad \text{où } a_1, \ldots, a_h \in U.$$

A cause de (16) et (17), FU contient $\lambda(e')\,S^{(\alpha)}_{rsq}U$. Puisqu'il n'existe pas de suite infinie strictement croissante de sous-foncteurs de F, F est une somme finie de sous-foncteurs tels que $\lambda S^{(\alpha)}_{rsq}$.

Les propositions (20) et (21) permettent de construire des suites de composition de S^n_{rsq}; je commence par les cas où $q = 1$; il me suffit alors d'examiner les cas où (r, s) est égal à $(1, 1)$, $(0, 1)$ ou $(1, 0)$; le foncteur S^n_{rs1} est alors égal ou isomorphe respectivement à S^n_{11}, S^n et Γ^n; le sens des notations $S^{(\alpha)}_{11}$, $S^{(\alpha)}$ ou $\Gamma^{(\alpha)}$ est donc évident.

(22) PROPOSITION. *Les sous-foncteurs irréductibles de S^n_{11} sont les sous-foncteurs $S^{(\alpha)}_{rs}$, où $\alpha \in \boldsymbol{N}_n[z]$; ils sont deux à deux non isomorphes, et S^n_{11} est égal à leur somme directe.*

(23) PROPOSITION. *Les facteurs irréductibles de S^n sont (à isomorphie près) les sous-foncteurs irréductibles $S^{(\alpha)}_{11}$ de S^n_{11}; les sous-foncteurs élémentaires de S^n sont les sous-foncteurs $S^{(\alpha)}$; si α et $\beta \in \boldsymbol{N}_n[z]$, l'inclusion $S^{(\alpha)} \supset S^{(\beta)}$ est équivalente à l'inégalité $\alpha \geqslant \beta$. On peut dire les mêmes choses du foncteur Γ^n; la seule différence est que l'inclusion $\Gamma^{(\alpha)} \supset \Gamma^{(\beta)}$ équivaut à $\alpha \leqslant \beta$.*

Les propositions (22) et (23) sont des conséquences faciles de (20) et (21). Je passe au cas où q est quelconque; on trouve que les facteurs irréductibles de S^n_{rsq} sont encore les $S^{(\alpha)}_{11}$ avec $\alpha \in \boldsymbol{N}_n[z]$, mais chacun est répété q fois; ces répétitions sont responsables du fait que le treillis des sous-foncteurs de S^n_{rsq} est infini si $q \geqslant 2$. Heureusement on peut déduire de (19) une providentielle décomposition en somme directe, qui simplifie énergiquement la situation. J'appelle R l'application de $\boldsymbol{Z}$ dans $\{0, 1, 2, \ldots, r+s-1\}$ qui associe à tout entier le reste de la division euclidienne de cet entier par $r+s$.

(24) PROPOSITION. *Choisissons un élément γ dans $\boldsymbol{N}_n[z]$. Pour tout $j \in \{0, 1, 2, \ldots, r+s-1\}$, soit F^n_{rsqj} la somme (en général non directe) de tous les sous-foncteurs $\varepsilon^{R(j-rV(\alpha,\gamma))} S^{(\alpha)}_{rsq}$, où $\alpha \in \boldsymbol{N}_n[z]$; le foncteur S^n_{rsq} est la somme directe des $(r+s)$ sous-foncteurs F^n_{rsqj}. Si $q = r+s$, les foncteurs F^n_{rsqj} sont indécomposables.*

En effet, à cause de (19) et (20), $F^n_{rsqj}U$ admet pour base la famille des $\varepsilon^{R(j-rV(\beta,\gamma))} e'$, où e' est un élément de E' de type β tel que $R(j - rV(\beta, \gamma)) < q$ (condition superflue si $q = r+s$). Dorénavant je supposerai toujours que $q = r+s$ et je montrerai plus loin que F^n_{rsqj} est alors indécomposable en somme directe. Le choix de γ est en fait le choix d'une fonction « niveau »: le niveau de α est $V(\alpha, \gamma)$; un autre choix de γ provoquerait une permutation circulaire sur la suite des $(r+s)$ sous-foncteurs F^n_{rsqj}.

Dans la proposition suivante j'ai besoin d'ajouter l'hypothèse $rs \neq 0$; je précise donc que si $r = 0$ (resp. $s = 0$), tous les foncteurs $F^n_{rs(r+s)j}$ sont isomorphes à S^n (resp. Γ^n), et on peut leur appliquer (23).

(25) PROPOSITION. *Si $q = r+s$, les facteurs irréductibles de F^n_{rsqj} sont les sous-foncteurs irréductibles $S^{(\alpha)}_{11}$ de S^n_{11}, sans répétition aucune; les sous-foncteurs élémentaires sont les sous-foncteurs $F^{(\alpha)}_{rsqj} = \varepsilon^{R(j-V(\alpha,\gamma))} S^{(\alpha)}_{rsq}$.*

La relation d'ordre (relation d'inclusion) sur l'ensemble de ces sous-foncteurs élémentaires peut être construite grâce aux deux propriétés suivantes:

d'une part $F^{(\alpha)}_{rsqj}$ et $F^{(\beta)}_{rsqj}$ sont adjacents si et seulement si α et β sont adjacents dans $\boldsymbol{N}_n[z]$;

d'autre part, si $rs \neq 0$, la fonction qui à $F^{(\alpha)}_{rsqj}$ associe $R(j - rV(\alpha, \gamma))$ est strictement décroissante.

DÉMONSTRATION. La seule difficulté est de trouver les relations d'inclusion entre les sous-foncteurs élémentaires de F^n_{rsqj}; à cause de (20), l'inclusion

$F^{(\alpha)}_{rsqj} \supset F^{(\beta)}_{rsqj}$ est équivalente à l'égalité

$$R(j - rV(\beta, \gamma)) = R(j - rV(\alpha, \gamma)) + \theta(\alpha, \beta) ;$$

à cause de (19), cette égalité est toujours vérifiée modulo $(r + s)$.

Si cette égalité est vraie, alors $\theta(\alpha, \beta) < r + s$, ce qui implique que $\alpha \geqslant \beta$ ou $\alpha \leqslant \beta$. On remarque déjà que si α et β ne sont pas adjacents, $F^{(\alpha)}_{rsqj}$ et $F^{(\beta)}_{rsqj}$ ne peuvent pas être adjacents. Si au contraire α et β sont adjacents, alors $\theta(\alpha, \beta)$ et $\theta(\beta, \alpha)$ sont tous deux compris entre 1 et $r + s - 1$ (parce que $rs \neq 0$), et on en déduit une relation d'inclusion entre $F^{(\alpha)}_{rsqj}$ et $F^{(\beta)}_{rsqj}$; si ceux-ci n'étaient pas adjacents, il existerait une chaine croissante ou décroissante de longueur $\geqslant 2$ qui les joint; à cette chaine de sous-foncteurs élémentaires est associée une chaine de même longueur joignant α et β dans $\boldsymbol{N}_n[z]$; si sa longueur est $\geqslant 2$, elle ne peut pas être monotone; elle contient donc deux éléments α' et β' tels que $V(\alpha', \beta') = 0$; d'où $\theta(\alpha', \beta') \geqslant r + s$, ce qui est impossible.

Commentaires.

Soit G_{rsj} le graphe orienté associé à la relation d'ordre sur $\boldsymbol{N}_n[z]$ définie comme ceci: $\alpha \geqslant \beta$ si (par définition) $F^{(\alpha)}_{rs(r+s)j} \supset F^{(\beta)}_{rs(r+s)j}$; comparons G_{rsj} au graphe G de la relation d'ordre initiale sur $\boldsymbol{N}_n[z]$ (celle du § 7). Les graphes non orientés sous-jacents à G_{rsj} et à G sont les mêmes, ce qui implique que le foncteur $F^n_{rs(r+s)j}$ est indécomposable. Le graphe G_{rsj} ne diffère de G que par l'orientation de ses arêtes; l'orientation d'une arête de G_{rsj} ne dépend que des niveaux des deux éléments qu'elle joint. On peut démontrer que l'égalité $G_{rsj} = G_{r's'j'}$ est équivalente à l'isomorphie des foncteurs $F^n_{rs(r+s)j}$ et $F^n_{r's'(r'+s')j'}$; en effet les entiers $h(X)$ qui interviennent dans l'expression de $P(x_{ij})$ au § 7, ne dépendent pas de (r, s). Si r est petit devant s, presque toutes les arêtes de G_{rsj} ont la même orientation que dans G; il peut même arriver qu'elles aient toutes la même orientation que dans G, et dans ce cas $F^n_{rs(r+s)j}$ est isomorphe à S^n; si γ est le polynôme constant n, cette éventualité apparait lorsque $j + r\tau(n) < r + s$; l'intervention de $\tau(n)$ dans ce contexte provient du fait que c'est la valeur maximale de $V(\alpha, \beta)$ (voir fin du § 7). Si au contraire s est petit devant r, presque toutes les arêtes de G_{rsj} ont l'orientation opposée à celle qu'elles ont dans G; si elles ont toutes l'orientation opposée, le foncteur $F^n_{rs(r+s)j}$ est isomorphe à Γ^n; si γ est le polynôme de $\boldsymbol{N}_n[z]$ dont tous les coefficients sont $< p$, cette éventualité apparait lorsque $j + s\tau(n) < r + s$. Si l est un entier positif tel que $r \leqslant ls \leqslant l^2 r$, aucune chaine monotone extraite de G_{rsj} ne peut avoir une longueur supérieure à l; en particulier si $r = s$, les sous-foncteurs élémentaires de $F^n_{rs(r+s)j}$ forment un ensemble ordonné à deux niveaux. Enfin si j et k sont liés par la relation $j + k = r +$

$+ s - 1$, les graphes G_{rsj} et G_{srk} ont toutes leurs arêtes respectivement orientées dans des sens opposés, et les relations d'ordre qu'ils représentent sont opposées; ceci traduit le fait que les foncteurs $F^n_{rs(r+s)j}$ et $F^n_{sr(r+s)k}$ sont duaux l'un de l'autre; c'est-à-dire si U' est le dual de U, $F^n_{sr(r+s)k}U'$ est le dual de $F^n_{rs(r+s)j}U$.

Remarquez encore que la multiplication par ε détermine un morphisme du foncteur F^n_{rsqj} vers le foncteur $F^n_{rsq(j+1)}$ pour tout $j \in \{0, 1, \ldots, r+s-1\}$, à condition de poser $F^n_{rsq(r+s)} = F^n_{rsq0}$.

Supplément aux §§ 7 et 8.

Vu le rôle joué par l'ensemble $\boldsymbol{N}_n[z]$ dans les §§ 7 et 8, on peut se poser quelques questions sur son cardinal $c(n)$. Pour calculer par récurrence les nombres $c(n)$, on part de $c(0) = 1$, on remarque que $c(n) = c(n-1)$ si n n'est pas divisible par p, et si n est divisible par p, on utilise l'une des deux égalités suivantes:

$$c(n) = c(n-1) + c(n/p)\,, \qquad c(n) = c(0) + c(1) + c(2) + \ldots + c(n/p)\,.$$

On en déduit que la suite $c(n)/n^k$ tend vers l'infini quel que soit k. Mais la suite $\sqrt[n]{c(n)}$ tend vers 1, car la série entière $\sum c(n)t^n$ a pour rayon de convergence 1:

$$\sum_{j\geqslant 0} c(n)\,t^n = \prod_{j\geqslant 0} \frac{1}{1-t^{p^k}}\,.$$

Je ne sais rien de plus précis sur le comportement à l'infini de la suite $c(n)$. L'ensemble ordonné $\boldsymbol{N}_n[z]$ admet une fonction « différence de niveau » qui détermine $1 + \tau(n)$ niveaux; le nombre de niveaux croît beaucoup moins vite que $c(n)$, puisque c'est un infiniment grand équivalent à $n/(p-1)$. Si $\sum n_i p^i$ est l'écriture de n dans le système de numération de base p, on a:

$$c(n) = \prod_{i\geqslant 1} (1 + n_i) \qquad \bmod p\,.$$

Les espaces vectoriels $S^n_{11}U$, S^nU, Γ^nU et $F^n_{rs(r+s)j}U$ ont la même dimension, à savoir $(n+h-1)!/(n!(h-1)!)$, si $h = \dim U \geqslant 1$; quand n tend vers l'infini (h restant fixe), cette dimension croît beaucoup moins vite que $c(n)$; donc quand n est grand (par rapport à h), presque tous les sous-espaces $S^{(\alpha)}_{11}U$ sont nuls. Posons $d(h, n) = \dim S^{(n)}_{11}U$; connaissant les nombres $d(h, n)$, on calcule facilement la dimension de $S^{(\alpha)}_{11}U$:

$$\dim S^{(\alpha)}_{11}U = \prod_{i\geqslant 0} d(h, \alpha_i)\,;$$

en effet le foncteur $S_{11}^{(\alpha)}$ est isomorphe au produit tensoriel des foncteurs irréductibles associés aux types $\alpha_i z^i$. Je peux donner une valeur explicite de $d(h, n)$:

$$d(h, n) = \sum_{\substack{0 \leqslant j \leqslant h \\ jp \leqslant n}} (-1)^j \frac{h!}{j!(h-j)!} \frac{(n-jp+h-1)!}{(n-jp)!(h-1)!};$$

cette formule montre que, lorsque h tend vers l'infini (n restant fixe), les dimensions de $S_{11}^n U$ et de $S_{11}^{(n)} U$ sont des infiniment grands équivalents (ils sont équivalents à $h^n/n!$); mais elle ne laisse pas apparaître les deux propriétés évidentes que voici:

$$d(h, n) = 0 \quad \text{si } n > h(p-1);$$

$$d(h, n) = d\big(h, h(p-1) - n\big);$$

voilà qui incite à poser $d(h, n) = 0$ si n est un entier négatif.

Le calcul par récurrence des nombres $d(h, n)$ peut se faire facilement avec l'une ou l'autre de ces deux formules (où $h \geqslant 1$):

$$d(h, n) = d(h, n-1) + d(h-1, n) - d(h-1, n-p);$$

$$d(h, n) = d(h-1, n) + d(h-1, n-1) + \\ + d(h-1, n-2) + \ldots + d(h-1, n-p+1);$$

la récurrence démarre avec $d(0, n) = 0$ si $n \neq 0$, et $d(0, 0) = 1$.

De la deuxième formule de récurrence on déduit que:

$$(1 + t + t^2 + \ldots + t^{p-1})^h = \sum d(h, n) t^n.$$

Si $p = 2$, les foncteurs $S_{11}^{(n)}$ et Λ^n sont isomorphes.

9. – Quelques disgressions.

Considérons d'abord le foncteur « algèbre extérieure » Λ et sa partie paire Λ^+; parmi ses propriétés, je rappelle les deux suivantes: d'abord ce foncteur est son propre dual (comme le foncteur S_{11}, voir § 5); ensuite, quel que soit le module M sur K (anneau commutatif unifère quelconque), l'algèbre $\Lambda^+ M$ est une algèbre commutative augmentée, munie d'un système de puissances divisées (comme l'algèbre $S_{11}^+ M$, voir § 6). En effet si $u \in \Lambda'^+ M$,

on peut écrire u comme une somme $u_1 + u_2 + \ldots + u_k$ d'éléments décomposables (donc de carré nul); on peut montrer que

$$(1 + u_1)\wedge(1 + u_2)\wedge\ldots\wedge(1 + u_k)$$

ne dépend pas du choix de cette écriture de u, et on l'appelle $\exp u$; de la même façon on calcule $\exp tu$ dans $\Lambda^+M \otimes K[t]$, et on en déduit les puissances divisées de u, car $\exp tu = \sum t^i u^{(i)}$. Supposons que B soit une application bilinéaire de $M \times M'$ dans K; on en déduit un produit intérieur de $\Lambda M \times \Lambda M'$ dans ΛM; soient $u \in \Lambda^2 M$ et $v \in \Lambda^2 M'$, et soient φ_u (resp. φ_v) l'application de M' dans M (resp. de M dans M') telle que

$$\varphi_u(b) = i(b)\cdot u \qquad (\text{resp. } \varphi_v(a) = i(a)\cdot v)\ ;$$

si K est un corps, on a le résultat suivant:

(26) PROPOSITION. *Si $\varphi_u\varphi_v$ ne laisse invariant aucun élément non nul de M, il existe $\lambda \in K$ et $w \in \Lambda^2 M$ tels que $i(\exp v)\cdot\exp u = \lambda \exp w$, et l'on a:*

$$\lambda^2 = \det(I - \varphi_u\varphi_v) = \det(I - \varphi_v\varphi_u)\ ,$$

$$\varphi_w = \varphi_u(I - \varphi_v\varphi_u)^{-1} = (I - \varphi_u\varphi_v)^{-1}\varphi_u\ .$$

Ces égalités ont un sens, parce que φ_u et φ_v sont des applications linéaires de rang fini. La proposition suivante montre ce qui se passe lorsque $I - \varphi_u\varphi_v$ n'est pas inversible.

(27) PROPOSITION. *Soit XM l'ensemble des éléments de ΛM de la forme $x\wedge\exp u$, où $u \in \Lambda^2 M$ et où x est un élément décomposable de ΛM (donc x peut être un élément de K); on définit de même XM'; le produit intérieur d'un élément de XM et d'un élément de XM' est encore dans XM.*

Pour démontrer (26) et (27), on peut, ou bien s'inspirer des méthodes utilisées plus loin au § 10, ou bien se ramener au cas où M et M' sont des espaces vectoriels de dimension finie n sur K, que B met en dualité, et utiliser la transformation $\mathcal{F}$ que voici: soient $\omega \in \Lambda^n M$ et $\omega' \in \Lambda^n M'$ tels que $B(\omega, \omega') = 1$; si $x \in \Lambda M$, on pose $\mathcal{F}(x) = i(x)\cdot\omega'$; réciproquement si $y \in \Lambda^q M'$, $\mathcal{F}^{-1}(y) = (-1)^{q(n-q)} i(y)\cdot\omega$; or si $x \in \Lambda M$ et $y \in \Lambda^q M'$, on a l'identité: $i(y)\cdot x = (-1)^{q(n-q)}\mathcal{F}^{-1}(\mathcal{F}(x)\wedge y)$; on est ainsi ramené à étudier la bijection de XM sur XM' induite par $\mathcal{F}$. Notez que si $x \in XM$, il existe une décomposition de M en somme directe de sous-espaces $M_1, M_2, \ldots, M_k$ de dimension 1 ou 2, tels que l'on puisse écrire $x = x_1\wedge x_2\wedge\ldots\wedge x_k$ avec $x_j \in XM_j$ pour $j = 1, 2, \ldots, k$.

A ma connaissance, c'est C. Chevalley qui le premier a étudié XM; il a obtenu le résultat suivant (voir [3]): si M' est le dual de M comme ci-dessus, et si $M \oplus M'$ est muni de sa forme quadratique évidente $((a, b) \mapsto \mapsto B(a, b))$, alors XM est un cône dont les génératrices sont en correspondance biunivoque avec les sous-espaces totalement singuliers de dimension maximale n dans $M \oplus M'$. Ensuite j'ai signalé (voir [4]) que XM permet de construire le groupe de Clifford associé à toute forme quadratique Q sur M. Je vais expliquer quel rôle peuvent jouer (26) et (27) dans l'étude de l'algèbre de Clifford $C(M, Q)$; soit $\beta(M \times M \to K)$ une forme bilinéaire telle que $\beta(a, a) = = Q(a)$ pour tout $a \in M$; on sait (voir [2]) que β permet de construire un isomorphisme entre les espaces vectoriels sous-jacents aux algèbres $C(M, Q)$ et ΛM; mais je préfère voir les choses ainsi: β permet de déformer le produit extérieur en un nouveau produit associatif $(\Lambda M \times \Lambda M \to \Lambda M)$, que je note $(x, y) \mapsto x * y$, et qui vérifie les propriétés suivantes: il admet toujours 1 comme élément unité, et $a * a = Q(a)$ pour tout $a \in M$. Voici la définition de ce nouveau produit: comme je suppose que B met M et M' en dualité, je peux identifier β avec un élément de $M' \otimes M'$, qui est canoniquement plongé dans $\Lambda^2(M' \oplus M')$, ce qui permet de définir $\exp \beta$ dans l'algèbre $\Lambda(M' \oplus M')$; soit μ l'application de $\Lambda(M \oplus M) = \Lambda M \otimes \Lambda M$ dans ΛM qui résulte de la structure d'algèbre de ΛM; avec ces notations:

$$x * y = \mu(i(\exp \beta) \cdot (x \otimes y)) .$$

Soit β' une autre forme bilinéaire telle que $\beta'(a, a) = Q(a)$ si $a \in M$; le produit $(x, y) \mapsto \mu(i(\exp \beta') \cdot (x \otimes y))$ est isomorphe au précédent; en effet il existe $\theta \in \Lambda^2 M'$ tel que $\beta'(a, b) - \beta(a, b) = B(a \wedge b, \theta)$, quels que soient a et $b \in M$; l'application $x \mapsto i(\exp \theta) \cdot x$ est un isomorphisme du premier produit sur le second. Chacun de ces deux produits fait de ΛM une algèbre isomorphe à $C(M, Q)$, et on retrouve ainsi le fait que la donnée de β permet d'identifier les espaces vectoriels sous-jacents aux algèbres $C(M, Q)$ et ΛM. Après cette identification, on peut énoncer les propositions suivantes, dans lesquelles interviennent l'automorphisme principal $x \mapsto \tilde{x}$ et l'anti-automorphisme principal $x \mapsto \bar{x}$ de l'algèbre $C(M, Q)$ (je rappelle que $\tilde{a} = -a$ et $\bar{a} = a$ si $a \in M$).

(28) PROPOSITION. *Si $x \in XM$, alors $\bar{x} \in XM$ et $x * \bar{x} = \bar{x} * x \in K$; si en outre $a \in M$, alors $x * a * \bar{x} \in M$. Si x et $y \in XM$, alors $x * y \in XM$.*

(29) PROPOSITION. *Soit $X(M, \beta)$ l'ensemble des $x \in XM$ tels que $x * \bar{x} \neq 0$; $X(M, \beta)$ est un groupe (pour le produit noté $*$); l'application $x \mapsto x * \bar{x}$ est un homomorphisme de $X(M, \beta)$ dans le groupe des scalaires non nuls; à tout $x \in X(M, \beta)$ on peut associer une transformation linéaire g_x de*

M: $g_x(a) = \tilde{x} * a * x^{-1}$; et l'application $x \mapsto g_x$ est un homomorphisme surjectif de $X(M, \beta)$ sur le groupe des transformations linéaires qui conservent Q et qui laissent fixes les éléments de M orthogonaux à tous les autres; si ces derniers éléments forment un sous espace de dimension $\leqslant 3$, $X(M, \beta)$ est le groupe des éléments pairs ou impairs, inversibles dans $C(M, Q)$, tels que $x * M * x^{-1} = M$.

On trouvera dans [4] des résultats plus précis, correspondant au choix canonique de β, lorsque K n'est pas de caractéristique 2:

$$\beta(a, b) = \tfrac{1}{2}\big(Q(a + b) - Q(a) - Q(b)\big) .$$

J'ai repris la théorie des algèbres de Clifford à son début dans l'espoir de faire une théorie commune aux algèbres de Clifford et aux algèbres de Weyl (que certains auteurs appellent algèbres de Clifford symplectiques); voici ce que devient (26) dans ce deuxième contexte. Soient M et M' deux espaces vectoriels sur un corps K de *caractéristique nulle*, et soit B une application bilinéaire de $M \times M'$ dans K. Je remplace les algèbres extérieures par les algèbres symétriques SM et SM' et je prends u dans S^2M et v dans S^2M'; pour définir $\exp u$, je dois utiliser l'algèbre complétée $\bar{S}M = \prod S^k M$; de même $\exp v \in \bar{S}M'$. Je veux montrer que le produit intérieur $i(\exp v)\cdot \exp u$ est de la forme $\lambda \exp w$, avec $\lambda \in K$ et $w \in S^2M$; mais je me heurte tout de suite à un problème trés grave: ce produit intérieur est une somme infinie, dont la convergence est problématique. Pour régler ce problème de convergence, je n'utiliserai ici que des méthodes formelles: je fais une extension du corps de base, en prenant comme nouveau corps de base le corps $K((t))$ des fractions de l'anneau $K[\![t]\!]$ des séries formelles en une indéterminée; je choisis u dans $S^2M \otimes K[\![t]\!]$ et v dans $S^2M' \otimes K[\![t]\!]$; si je suppose que $u(0)$ ou $v(0)$ est nul (c'est l'élément de S^2M ou S^2M' obtenu en remplaçant t par 0), alors le produit intérieur $i(\exp v)\cdot \exp u$ est formellement convergent dans l'algèbre $\bar{S}M \otimes K[\![t]\!]$. Je définis φ_u et φ_v comme ci-dessus:

$$\varphi_u(b) = i(b)\cdot u \qquad \text{et} \qquad \varphi_v(a) = i(a)\cdot v ;$$

ce sont des applications linéaires $\big(\text{sur } K((t))\big)$ de $M' \otimes K((t))$ dans $M \otimes K((t))$ et vice-versa; l'hypothèse de nullité de $u(0)$ ou $v(0)$ implique que dét $(I - \varphi_u\varphi_v)$ est une série formelle dont le terme initial (de degré 0 en t) est égal à 1.

(30) PROPOSITION. *Il existe $\lambda \in K[\![t]\!]$ et $w \in S^2M \otimes K[\![t]\!]$ tels que $i(\exp v)\cdot \cdot \exp u = \lambda \exp w$, et l'on a:*

$$\lambda^{-2} = \text{dét}\,(I - \varphi_u\varphi_v) = \text{dét}\,(I - \varphi_v\varphi_u) ,$$

$$\varphi_w = \varphi_u(I - \varphi_v\varphi_u)^{-1} = (I - \varphi_u\varphi_v)^{-1}\varphi_u .$$

A part le problème de convergence, la seule différence entre (26) et (30) est le changement de λ^2 en λ^{-2}. La démonstration de (30), que j'exposerai au § 10, est un peu laborieuse, parce qu'on ne dispose de rien qui puisse jouer un rôle analogue à celui de $\mathcal{F}$ plus haut.

Supposons de nouveau M et M' de dimension finie et mis en dualité par B. Soit Φ une forme bilinéaire alternée sur M, et soit β une forme bilinéaire telle que $\beta(a, b) - \beta(b, a) = \Phi(a, b)$ quels que soient a et $b \in M$ (par exemple $\beta = \Phi/2$). On peut définir sur l'espace vectoriel $\bar{S}M \otimes K[\![t]\!]$ un nouveau produit associatif, avec même élément unité:

$$(x, y) \mapsto x * y = \mu(i(\exp t\beta) \cdot (x \otimes y)) \ ;$$

dans cette formule, β est identifié avec un élément de $M' \otimes M'$, canoniquement plongé dans $S^2(M' \otimes M')$, et la signification de μ est évidente. Cette façon de déformer le produit symétrique, est aussi celle utilisée dans [6], malgré les différences de langage et de notations. Si a et $b \in M$, alors $a * b - b * a = t\Phi(a, b)$. Grâce à cette nouvelle structure d'algèbre sur $\bar{S}M \otimes K[\![t]\!]$, on peut faire une théorie analogue à celle que j'ai esquissée plus haut. L'application $x \mapsto \bar{x}$ est ici un anti-automorphisme gradué, ce qui signifie que $\overline{x * y} = \bar{y} * \bar{x}$ si x ou y est pair, mais $\overline{x * y} = -\bar{y} * \bar{x}$ si x et y sont impairs. Le groupe de Clifford symplectique formel est l'ensemble des $\lambda \exp u$, où $u \in S^2 M \otimes K[\![t]\!]$ et où λ est un élément inversible de $K[\![t]\!]$; si Φ est non dégénérée, c'est le groupe des éléments x inversibles (pour le nouveau produit) tels que $x * M * x^{-1} \subset M \otimes K[\![t]\!]$; ce groupe ne permet pas d'obtenir toutes les transformations symplectiques de M; on obtient seulement le groupe des transformations symplectiques formelles $\sum t^j g_j$, dont le terme initial g_0 est l'application identique de M; cette théorie n'a donc qu'une valeur locale.

Pour obtenir une théorie globale, il faut d'abord résoudre le problème de la convergence des produits intérieurs infinis par des méthodes autres que formelles, sans recourir à $K[\![t]\!]$; c'est ce que j'ai réussi à faire lorsque K est le corps $\boldsymbol{R}$ des nombres réels. J'ai construit une variété (non algébrique) qui joue un rôle analogue à celui de XM plus haut; à l'exception d'un élément ∞ (qui joue un rôle analogue à celui de 0 dans XM), ses éléments sont des distributions, presque toutes identifiables avec des fonctions holomorphes sur $M' \otimes \boldsymbol{C}$ (fonctions du type $\lambda \exp u$, où u est une forme quadratique à coefficients réels, et $\lambda \in \boldsymbol{C}$, $\lambda^2 \in \boldsymbol{R}$, $\lambda \neq 0$); la transformation de Fourier (appliquée à l'espace $M' \otimes \exp(i\pi/4)$, sur lequel ces fonctions holomorphes sont bornées) joue un rôle analogue à celui de $\mathcal{F}$ plus haut. Grâce à cette variété, je peux construire les groupes métaplectiques associés aux formes alternées Φ non nulles sur M. En reprenant les techniques de C. Chevalley,

j'obtiens la variété de Maslov de l'espace $M \oplus M'$, muni de sa forme symplectique évidente.

Je ne dirai rien de plus sur la possibilité de faire une théorie globale, car mon but ici est seulement de montrer que, même si K est un corps de caractéristique non nulle, mais différente de 2, on peut encore faire une théorie locale; autrement dit, on peut encore donner un sens à la proposition (30). C'est pour réaliser ce but que j'ai imaginé le foncteur S_{11}, puis les autres foncteurs S_{rs}.

10. – La proposition (30) en caractéristique $p > 2$.

Soit K un corps de caractéristique p supérieure à 2, soient M et M' deux espaces vectoriels sur K et soit B une application bilinéaire de $M \times M'$ dans K; pour la raison donnée au § 9, je fais tout de suite une extension du corps de base: le nouveau corps de base est $K((t))$, encore que l'anneau $K[[t]]$ suffirait pour la plupart des calculs. Puisque K est un corps, je dois poser $\varepsilon = 0$; mais je ferai à la fin quelques remarques pour les cas où l'on fait des hypothèses plus faibles sur l'anneau de base, et c'est pourquoi je conserverai la lettre ε dans les calculs. Je choisis u dans $S^2M \otimes K[[t]]$ et v dans $S^2M' \otimes K[[t]]$; puisque $p \neq 2$, les foncteurs S^2 et S^2_{11} peuvent être identifiés; je calcule $\exp u$ et $\exp v$ dans les algèbres complétées $\bar{S}_{11}M \otimes K((t))$ et $\bar{S}_{11}M' \otimes K((t))$; pour que le produit intérieur $i(\exp v) \cdot \exp u$ soit (formellement) convergent, je suppose que u ou v s'annule quand on remplace t par 0. Je vais démontrer que la proposition (30) reste valable dans ce cas; la démonstration se fait en 4 étapes; pour fixer les idées, c'est à v que j'impose la condition d'être nul pour $t = 0$.

1ière étape: Soit V l'ensemble des $v \in S^2M' \otimes K[[t]]$ tels que $v(0) = 0$ et tels que (30) soit vrai lorsqu'on accouple v à n'importe quel $u \in S^2M \otimes K[[t]]$; je vais montrer que V est stable par addition. Soient v' et $v'' \in V$; je pose $v = v' + v''$. Pour tout u je peux écrire:

$$i(\exp v') \cdot \exp u = \lambda' \exp w' ,$$

avec $\lambda'^{-2} = \det(I - \varphi_{v'}\varphi_u)$ et $\varphi_{w'} = \varphi_u(I - \varphi_{v'}\varphi_u)^{-1}$.

Ensuite, à cause de (10*b*),

$$i(\exp v) \cdot \exp u = \lambda' \, i(\exp v'') \cdot \exp w' .$$

Cependant $i(\exp v'') \cdot \exp w' = \lambda'' \exp w''$, avec

$$\lambda''^{-2} = \det(I - \varphi_{v''}\varphi_{w'}) \quad \text{et} \quad \varphi_{w''} = \varphi_{w'}(I - \varphi_{v''}\varphi_{w'})^{-1} .$$

Or $I - \varphi_{v'}\varphi_{w'} = (I - \varphi_v\varphi_u)(I - \varphi_{v'}\varphi_u)^{-1}$; on en tire $i(\exp v)\cdot\exp u = \lambda \exp w$, avec

$$\lambda^{-2} = (\lambda'\lambda'')^{-2} = \det(I - \varphi_v\varphi_u) \quad \text{et} \quad \varphi_w = \varphi_{w'} = \varphi_u(I - \varphi_v\varphi_u)^{-1}.$$

J'ai donc démontré que $v \in V$.

2ième étape: Tout élément de $S^2M' \otimes K[\![t]\!]$ peut s'écrire comme somme d'éléments de la forme μb^2, avec $\mu \in K[\![t]\!]$ et $b \in M'$; si v s'annulle pour $t = 0$, on peut imposer aux séries formelles μ d'être nulles pour $t = 0$. Il suffit donc de démontrer que (30) est vrai lorsque v est de la forme μb^2, et $\mu(0) = 0$.

3ième étape: Pour calculer $i(\exp \mu b^2)\cdot\exp u$, j'ai besoin d'une part de la formule (13) du § 6, et d'autre part de la formule suivante, où les deux membres sont des éléments de $\boldsymbol{Q}[\![t]\!]$, et où $k \in \boldsymbol{N}$:

$$(1 - 4t)^{-k-\frac{1}{2}} = \sum_{j\geqslant 0} \frac{(2k+2j)!\,k!}{(k+j)!\,j!\,(2k)!}\, t^j. \tag{31}$$

Remarquez que les séries formelles $(1 - 4t)^{-k}$ et $(1 - 4t)^{-\frac{1}{2}}$ sont à coefficients entiers; par conséquent les coefficients de la série formelle qui figure dans (31), sont aussi des nombres entiers; d'où:

$$\tau(2k + 2j) - \tau(k + j) - \tau(j) - \tau(2k) + \tau(k) \geqslant 0.$$

Grâce à cette inégalité, on peut transformer (13) en faisant intervenir $(b^2)^{(n)}$ et $(a^2)^{(n-j)}$; je rappelle que $a = i(b)\cdot u$ et $\omega = B(u, b^2)$; en outre, d'après (12):

$$(b^2)^{(n)} = \frac{1}{n!^*}\,\varepsilon^{\sigma(n,n)}\, b^{[2n]} \qquad \text{(formule analogue pour } (a^2)^{(n-j)}\text{)};$$

la formule (13) se transforme en celle-ci, où $m \geqslant n$:

$$i\big((b^2)^{(n)}\big)\cdot u^{(m)} = \sum_{0\leqslant j\leqslant n} \left(\frac{\omega}{2}\right)^j \frac{(2n)!^*(n-j)!^*}{n!^*j!^*(2n-2j)!^*}\, \varepsilon^{2k(j)}(a^2)^{(n-j)}\, u^{(m-2n+j)};$$

il est essentiel d'observer que $k(j)$ n'est pas négatif:

$$k(j) = \tau(2n) - \tau(n) - \tau(j) - \tau(2n-2j) + \tau(n-j) \geqslant 0.$$

On reconnaît maintenant que:

$$i\big((b^2)^{(n)}\big)\cdot u^{(m)} = \sum_{0\leqslant j\leqslant n} \left(\frac{\omega}{2}\right)^j \frac{(2n)!(n-j)!}{n!\,j!(2n-2j)!}\, (a^2)^{(n-j)}\, u^{(m-2n+j)}. \tag{32}$$

C'est grâce à (31) que nous savons que les coefficients qui figurent dans le second membre de (32), sont des nombres entiers. A partir de (32), les calculs continuent ainsi:

$$i(\exp \mu b^2)\cdot \exp u = \sum_{n\geqslant 0}\ \sum_{0\leqslant j\leqslant n} \mu^n \left(\frac{\omega}{2}\right)^j \frac{(2n)!(n-j)!}{n!j!(2n-2j)!}\,(a^2)^{(n-j)} \exp u =$$

$$= (\exp u) \sum_{k\geqslant 0} (\mu a^2)^{(k)} \sum_{j\geqslant 0} \frac{(2k+2j)!\,k!}{(k+j)!\,j!\,(2k)!} \left(\frac{\mu\omega}{2}\right)^j .$$

La formule (31) intervient ici de façon décisive; elle est aussi valable pour l'anneau $K[\![t]\!]$:

$$i(\exp \mu b^2)\cdot \exp u = (\exp u) \sum_{k\geqslant 0} (\mu a^2)^{(k)} (1-2\mu\omega)^{-k-\frac{1}{2}} =$$

$$= \frac{1}{\sqrt{1-2\mu\omega}} \exp\left(u + \frac{\mu a^2}{1-2\mu\omega}\right).$$

4ième étape: Pour montrer que le résultat du calcul précédent est conforme à ce qui est écrit dans (30), on se ramène à un simple problème d'algèbre linéaire; les problèmes de convergence ne viennent plus nous tourmenter, et le fait que le corps de base est $K(\!(t)\!)$, n'a plus aucune importance ici; pour simplifier les écritures, je suppose que le corps de base est de nouveau K. Soient $u \in S^2M$, $b \in M'$ et $\mu \in K$; je pose $v = \mu b^2$, $a = i(b)\cdot u$ et $\omega = B(a, b)$. Il s'agit de démontrer que $1 - 2\mu\omega = \det(I - \varphi_v\varphi_u)$, et que, si $2\mu\omega \neq 1$, alors

$$\varphi_w(I - \varphi_v\varphi_u) = \varphi_u \qquad \text{si l'on pose } w = u + \frac{\mu a^2}{1-2\mu\omega}.$$

Je peux me limiter aux cas où $\omega \neq 0$; la conclusion restera valable lorsque $\omega = 0$, parce qu'on peut faire un passage à la limite en utilisant la topologie de Zariski de $(S^2M)\times M'\times K$. J'appelle N l'ensemble des $x \in M$ tels que $B(x, b) = 0$, et N' l'ensemble des $y \in M'$ tels que $B(a, y) = 0$; l'hypothèse $\omega \neq 0$ me permet d'écrire: $M = Ka \oplus N$ et $M' = Kb \oplus N'$.

Or on trouve que:

$$\varphi_u(b) = a\,, \qquad \varphi_u(N') \subset N\,,$$

$$\varphi_v(a) = 2\mu\omega b\,, \qquad \varphi_v(N) = 0\,,$$

$$\varphi_w(b) = (1-2\mu\omega)^{-1} a\,, \qquad \varphi_{w-u}(N') = 0\,.$$

Il est maintenant facile de vérifier les deux égalités qui permettent de terminer la démonstration de (30).

REMARQUES. Plus généralement soit K un anneau commutatif unifère tel que tous les entiers premiers autres que p soient inversibles dans K, et dans lequel existe un élément ε dont le carré est l'image de p dans K; je précise que $p \neq 2$. Donnons aux lettres M, M', B, u et v des significations analogues à celles qu'elles avaient ci-dessus, et considérons $i(\exp v)\cdot\exp u \in \in \bar{S}_{11} M \otimes K[\![t]\!]$; puisque la formule (32) est encore valable dans ce contexte, les calculs précédents montrent au moins que $i(\exp v)\cdot\exp u$ est de la forme $\lambda \exp w$, avec $\lambda \in K[\![t]\!]$ et $w \in S^2 M \otimes K[\![t]\!]$. Mais ensuite il y a quelque difficulté à donner un sens aux formules indiquées dans (30) pour le calcul explicite de λ et w; ce dernier problème est hors du sujet de cet article.

BIBLIOGRAPHIE

[1] BOURBAKI, Livre II (*Algèbre*), Chap. III (*Algèbre multilinéaire*), édition de 1970.
[2] BOURBAKI, Livre II, Chap. IX (*Formes sesquilinéaires et formes quadratiques*), § 9.
[3] C. CHEVALLEY, *The algebraic theory of spinors*, Columbia University Press, 1954.
[4] J. HELMSTETTER, *Groupe de Clifford pour des formes quadratiques de rang quelconque*, Note aux C. R. Acad. Sci. Paris, **285** (1977), série A, pp. 175-177.
[5] N. ROBY, *Les algèbres à puissances divisées*, Bull. Sci. Math., **89** (1965), pp. 75-91.
[6] J. VEY, *Déformation du crochet de Poisson sur une variété symplectique*, Comment. Math. Helv., **50** (1975), pp. 421-454.
[7] TH. VUST, *Foncteurs polynomiaux et théorie des invariants*, Séminaire d'algèbre P. Dubreil et M. P. Malliavin, Proceedings, Paris 1979, Lecture Notes in Math. **795**, Springer-Verlag, 1980.

Université scientifique et médicale de Grenoble
Institut Fourier (Mathématiques pures)
Boîte postale 116
38402 Saint-Martin d'Hères (France)