BULLETIN DE LA S. M. F.

N. ROBY

Construction de certaines algèbres à puissances divisées

Bulletin de la S. M. F., tome 96 (1968), p. 97-113
<http://www.numdam.org/item?id=BSMF_1968__96__97_0>

Bull. Soc. math. France,
96, 1968, p. 97 à 113.

CONSTRUCTION DE CERTAINES ALGÈBRES A PUISSANCES DIVISÉES

PAR

NORBERT ROBY

[Montpellier].

Nous nous proposons de donner des procédés de construction de certaines algèbres à puissances divisées. Pour cette notion, on pourra se reporter à notre article cité [1].

Première partie.

1. Quelques notations.

On désigne

— par $\mathfrak{S}_p$ le groupe des permutations des entiers $(1, \ldots, p)$;

— par $H_{p_1, \ldots, p_n}$ le sous-groupe de $\mathfrak{S}_{p_1+\ldots+p_n}$ formé des permutations qui laissent globalement invariants chacun des blocs constitués respectivement par les p_1 premiers entiers, puis les p_2 suivants, ..., enfin les p_n derniers;

— par $K_{p_1, \ldots, p_n}$ le sous-ensemble de $\mathfrak{S}_{p_1+\ldots+p_n}$ constitué par les permutations qui respectent l'ordre relatif des éléments de chacun des blocs précédents, c'est-à-dire qui sont croissantes sur chacun de ces blocs. Cet ensemble constitue un système de représentants pour l'ensemble des classes à gauche de $\mathfrak{S}_{p_1+\ldots+p_n}$ modulo $H_{p_1, \ldots, p_n}$;

— par $P_{p_1, \ldots, p_n}$ le sous-groupe de $\mathfrak{S}_{p_1+\ldots+p_n}$ formé des permutations dont le seul effet est de permuter entre eux les blocs précédents. Pour $n \geq 1$, on utilisera les notations H_p^n (resp. K_p^n, P_p^n), au lieu de $H_{\underbrace{p, \ldots, p}_{n}}$ $\Big($resp. $K_{\underbrace{p, \ldots, p}_{n}}$, $P_{\underbrace{p, \ldots, p}_{n}}\Big)$.

Nous désignons par K'^n_p le sous-ensemble de K^n_p formé des permutations σ qui vérifient en outre : $\sigma(p) < \sigma(2p) < \ldots < \sigma(np)$. On voit facilement que K'^n_p est un système de représentants pour les classes à gauche de $\mathfrak{S}_{np}$ modulo le sous-groupe L^n_p engendré par H^n_p et P^n_p.

2. L'algèbre $\mathbf{Z}_S(\mathcal{M})$.

Soit $\mathcal{M}$ un monoïde *libre* associatif noté *multiplicativement*. Soit $\mathbf{Z}(\mathcal{M})$ l'algèbre *libre* de ce monoïde sur l'anneau des entiers. On désigne par $\mathbf{Z}_p(\mathcal{M})$ le sous-module engendré par les mots de longueur $p \geqq 0$; ces modules déterminent une graduation de l'algèbre $\mathbf{Z}(\mathcal{M})$. On pose aussi : $\mathbf{Z}_+(\mathcal{M}) = \bigoplus_{p \geqq 1} \mathbf{Z}_p(\mathcal{M})$; la décomposition de $\mathbf{Z}(\mathcal{M})$ en $\mathbf{Z}_0(\mathcal{M}) \oplus \mathbf{Z}_+(\mathcal{M})$ est une prégraduation (*cf.* [1]).

On peut faire opérer le groupe symétrique $\mathfrak{S}_p$ sur $\mathbf{Z}_p(\mathcal{M})$ comme suit : si $\sigma \in \mathfrak{S}_p$, pour définir l'action de σ sur un mot de longueur p, soit $m = a_1, \ldots, a_p$, on pose : $\sigma(m) = a_{\sigma(1)}, \ldots, a_{\sigma(p)}$; par linéarité, on prolonge cette action de σ à $\mathbf{Z}_p(\mathcal{M})$ tout entier. Notons que, $\mathfrak{S}_0$ et $\mathfrak{S}_1$ n'ayant que l'élément neutre, ils opèrent trivialement sur $\mathbf{Z}_0(\mathcal{M})$ et $\mathbf{Z}_1(\mathcal{M})$.

Pour deux mots m_p et m'_q, de longueurs respectives p et q, on pose

$$m_p \star m'_q = \sum_{\sigma \in K_{p,q}} \sigma(m_p m'_q).$$

(Intuitivement, les permutations considérées sont celles qui « imbriquent » l'un dans l'autre les mots m_p et m'_q de toutes les manières possibles, de la même manière qu'on imbrique l'un dans l'autre deux parties d'un jeu de cartes à chaque opération d'un mélange).

On vérifie que $m_p \star m'_q = m'_q \star m_p$; si m_p est le mot vide, la définition donne $m_p \star m'_q = m'_q$.

Par bilinéarité, on en déduit une multiplication bilinéaire et commutative dans $\mathbf{Z}(\mathcal{M})$, que nous notons encore $\star$.

Pour trois mots m_p, m'_q, m''_r, on vérifie aussi que

$$(m_p \star m'_q) \star m''_r = m_p \star (m'_q \star m''_r).$$

Donc, avec la multiplication $\star$, $\mathbf{Z}(\mathcal{M})$ est devenue une algèbre *commutative* et *associative* dont 1 est élément unité; avec cette structure-là, on la notera $\mathbf{Z}_S(\mathcal{M})$. La graduation canonique (resp. la prégraduation) de $\mathbf{Z}(\mathcal{M})$ est aussi une graduation (resp. une prégraduation pour l'algèbre $\mathbf{Z}_S(\mathcal{M})$).

On peut préciser la multiplication $\star$ comme suit : si $z_i \in \mathbf{Z}_{p_i}(\mathfrak{M})$ ($i = 1, \ldots, n$), on a

$$z_1 \star \ldots \star z_n = \sum_{\sigma \in K p_1, \ldots, p_n} \sigma(z_1 \ldots z_n).$$

3. Puissances divisées dans $\mathbf{Z}_S(\mathfrak{M})$.

Proposition 1. — *Pour tout élément z de $\mathbf{Z}_+(\mathfrak{M})$ et tout entier $n \geqq 0$, il existe un élément $\gamma_n(z)$ de $\mathbf{Z}(\mathfrak{M})$, et un seul, tel que*

$$z^{\star n} = n!\, \gamma_n(z).$$

L'unicité est évidente, puisque $\mathbf{Z}(\mathfrak{M})$ est libre sur $\mathbf{Z}$.

Existence :

— pour $n = 0$, on doit prendre $\gamma_0(z) = 1$;

— pour $n \geqq 1$, considérons d'abord le cas d'un élément z_p homogène de degré $p \geqq 1$. On a

$$z_p^{\star n} = \sum_{\sigma \in K_p^n} \sigma(z_p^n).$$

Il est clair que tout élément de P_p^n laisse invariant l'élément z_p^n, puisque son seul effet est de permuter entre eux les n facteurs z_p de cette puissance. D'autre part, si $\sigma \in K_p^n$, il est clair aussi que la classe à gauche σP_p^n est encore dans K_p^n. Donc, K_p^n est une réunion de ces classes disjointes, et tous les éléments d'une classe ont le même effet sur z_p^n. Or, chaque classe a autant d'éléments que P_p^n, c'est-à-dire $n!$. Donc $z_p^{\star n}$ est divisible par $n!$

C. Q. F. D.

Un système de représentants pour les classes à gauche modulo P_p^n qui sont contenues dans K_p^n est l'ensemble $K_p'^n$. On pourra donc poser

$$\gamma_n(z_p) = \sum_{\sigma \in K_p'^n} \sigma(z_p^n). \tag{1}$$

Maintenant, soit $z = \sum_{i=1}^{q} z_i$ un élément quelconque de $\mathbf{Z}_+(\mathfrak{M})$, où les z_i sont homogènes de degré $\geqq 1$. On a

$$\begin{aligned} z^{\star n} &= \sum_{h_1 + \ldots + h_q = n} \frac{n!}{h_1! \ldots h_q!} z_1^{\star h_1} \star \ldots \star z_q^{\star h_q} \\ &= n! \sum_{h_1 + \ldots + h_q = n} \gamma_{h_1}(z_1) \star \ldots \star \gamma_{h_q}(z_q). \end{aligned}$$

C. Q. F. D.

De la relation : $\gamma_n(z) = \frac{z^{\star n}}{n!}$ on déduit immédiatement que les applications $\gamma_n : \mathbf{Z}_+(\mathfrak{M}) \to \mathbf{Z}(\mathfrak{M})$ vérifient tous les axiomes des puissances divisées (*cf.* [1], § 2). D'où la proposition suivante :

Proposition 2. — *L'algèbre prégraduée* $\mathbf{Z}_S(\mathfrak{M})$ *est (et de manière unique) une algèbre à puissances divisées.*

4. **La *PD*-algèbre** $A_S(\mathfrak{M})$.

Soient un monoïde *libre* $\mathfrak{M}$ et un anneau commutatif unitaire A. L'algèbre *libre* du monoïde $\mathfrak{M}$ à coefficients dans A, notée $A(\mathfrak{M})$, peut être définie par

$$A(\mathfrak{M}) = A \bigotimes_{\mathbf{Z}} \mathbf{Z}(\mathfrak{M}).$$

Si l'on considère que $\mathbf{Z}(\mathfrak{M})$ est munie de la multiplication $\star$, on en déduit aussi sur $A(\mathfrak{M})$ une multiplication $\star$. On notera $A_S(\mathfrak{M})$ l'algèbre ainsi définie. De façon précise, on pose

$$A_S(\mathfrak{M}) = A \bigotimes_{\mathbf{Z}} \mathbf{Z}_S(\mathfrak{M}) \tag{2}$$

(produit tensoriel de $\mathbf{Z}$-algèbres, érigé en A-algèbre de manière évidente).

Soit $A(\mathfrak{M}) = \bigoplus_{p \geqq 0} A_p(\mathfrak{M})$ la graduation canonique de l'algèbre $A(\mathfrak{M})$ [ou $A_S(\mathfrak{M})$]. On pose : $A_+(\mathfrak{M}) = \bigoplus_{p \geqq 1} A_p(\mathfrak{M})$.

Il est clair qu'on peut faire opérer le groupe symétrique $\mathfrak{S}_p$ sur $A_p(\mathfrak{M})$ comme ci-dessus sur $\mathbf{Z}_p(\mathfrak{M})$, et qu'on pourrait définir directement la multiplication $\star$ de $A_S(\mathfrak{M})$ comme précédemment pour $\mathbf{Z}_S(\mathfrak{M})$. Mais c'est la formule (2) qui nous permettra d'introduire des puissances divisées dans $A_S(\mathfrak{M})$.

Si l'on considère A comme une $\mathbf{Z}$-*PD*-algèbre triviale, on voit que $A_S(\mathfrak{M})$, prégraduée en $A_0(\mathfrak{M}) \oplus A_+(\mathfrak{M})$, est, en tant que produit tensoriel de deux $\mathbf{Z}$-*PD*-algèbres, une $\mathbf{Z}$-*PD*-algèbre (donc aussi une A-*PD*-algèbre) (*cf.* [1], § 11). Les puissances divisées de $A_S(\mathfrak{M})$ sont entièrement déterminées par la connaissance des $\gamma_n(z_p)$, ou $z_p \in A_p(\mathfrak{M})$ $(p \geqq 1)$. Or, il est clair que $\gamma_n(z_p)$ est encore explicité par la formule (1) du paragraphe 3 ci-dessus. D'où le théorème suivant :

Théorème 1. — *Dans l'algèbre prégraduée* $A_S(\mathfrak{M})$ *il existe un système de puissances divisées* γ_n, *et un seul, tel que, pour* $z_p \in A_p(\mathfrak{M})$ $(p \geqq 1)$, *on ait*

$$\gamma_n(z_p) = \sum_{\sigma \in K'^n_p} \sigma(z_p^n). \tag{1}$$

Remarque. — Si $z_1 \in A_1(\mathfrak{M})$, on a

$$\gamma_n(z_1) = z_1^n.$$

5. La *PD*-algèbre $T_S(M)$.

Soit M un A-module. On désigne par $T_p(M)$ le module $\bigotimes^p M$ et par $T(M) = \bigoplus_{p \geqq 0} T_p(M)$ l'algèbre tensorielle de M. On pose aussi :

$$T_+(M) = \bigoplus_{p \geqq 1} T_p(M).$$

Il est habituel de faire opérer $\mathfrak{S}_p$ sur $T_p(M)$ par

$$(2) \qquad \sigma(x_1 \otimes \ldots \otimes x_p) = x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(p)}.$$

En posant

$$(x_1 \otimes \ldots \otimes x_p) \star (y_1 \otimes \ldots \otimes y_q) = \sum_{\sigma \in K_{p,q}} \sigma(x_1 \otimes \ldots \otimes x_p \otimes y_1 \otimes \ldots \otimes y_q),$$

on définit encore sur $T(M)$ une multiplication notée $\star$, qui est *commutative, associative* et *unitaire*; cela se voit exactement comme au paragraphe 2. Avec cette structure d'algèbre, $T(M)$ se notera $T_S(M)$. La décomposition $T_S(M) = T_0(M) \oplus T_+(M)$ est une prégraduation de $T_S(M)$.

Soit maintenant $\mathfrak{M}$ le monoïde libre construit sur M comme ensemble de base; $\mathfrak{M}$ est l'ensemble des mots construits avec des signes mis en correspondance bijective avec les éléments de M : nous notons u_x le signe associé à $x \in M$.

On sait que l'algèbre $T(M)$ est le quotient de $A(\mathfrak{M})$ par l'idéal bilatère J engendré par les éléments des types suivants :

$$(3) \qquad \begin{cases} u_{x+y} - u_x - u_y & (x, y \in M), \\ u_{\lambda x} - \lambda u_x & (\lambda \in A,\ x \in M). \end{cases}$$

L'application canonique $q : A(\mathfrak{M}) \to T(M)$ est définie par

$$q(u_x) = x.$$

Elle applique $A_p(\mathfrak{M})$ sur $T_p(M)$, et est alors compatible avec les opérations de $\mathfrak{S}_p$. Il en résulte que, pour deux mots m et m' dans $\mathfrak{M}$, on a : $q(m \star m') = q(m) \star q(m')$. Par bilinéarité, on en déduit que q est aussi un homomorphisme d'algèbres de $A_S(\mathfrak{M})$ sur $T_S(\mathfrak{M})$.

En particulier, J est aussi un idéal dans $A_S(\mathfrak{M})$; mais, en tant qu'idéal de $A_S(\mathfrak{M})$, il n'est peut-être pas engendré seulement par les éléments de type (3). Or, nous avons besoin de connaître un système de générateurs pour J en tant qu'idéal de $A_S(\mathfrak{M})$. Pour cela, il suffit de prendre un système de générateurs de J en tant que module, et pour cela il suffit de considérer les éléments homogènes de J (car J est un idéal homogène).

Posons $J_p = J \cap A_p(\mathfrak{M})$, et soit $z_p \in J_p$ $(p \geqq 1)$. On a $z_p^n \in J_{np}$ pour $n \geqq 1$. Or, puisque q commute aux opérations de $\mathfrak{S}_{np}$, on voit que J_{np} est stable pour ces opérations. La formule (1) du théorème 1 montre alors que $\gamma_n(z_p) \in J_{np}$.

Soit $F = \bigcup_{p \geqq 1} J_p$. Nous avons vu :

1° que F engendre J dans $A_S(\mathfrak{M})$;

2° que $\gamma_n(z) \in J$ pour $z \in F$ et $n \geqq 1$.

D'après ([1], § 5, p. 4), on peut dire que J est un idéal divisé de $A_S(\mathfrak{M})$. Par passage au quotient, on déduit donc du théorème 1 le théorème suivant :

THÉORÈME 2. — *Dans l'algèbre prégraduée $T_S(M)$, il existe un système de puissances divisées γ_n, et un seul, tel que, pour $t_p \in T_p(M)$ $(p \geqq 1)$, on ait :*

$$\gamma_n(t_p) = \sum_{\sigma \in K_p'^n} \sigma(t_p^{\otimes n}). \tag{4}$$

Remarque. — Si $x \in M = T_1(M)$, on a

$$\gamma_n(x) = x^{\otimes n}.$$

6. La *PD*-algèbre $TS(M)$.

Pour tout entier $p \geqq 0$, on désigne par $TS_p(M)$ le sous-module des tenseurs symétriques contenus dans $T_p(M)$ (c'est-à-dire des tenseurs invariants par toutes les opérations de $\mathfrak{S}_p$), et par $TS(M)$[resp. $TS_+(M)$] le module $\bigoplus_{p \geqq 0} \left(\text{resp. } \bigoplus_{p \geqq 1}\right) TS_p(M)$. On sait définir dans $TS(M)$ une structure d'algèbre commutative, associative et unitaire, où la multiplication est notée $\bigstar$; par exemple, cette construction a été faite dans ([2], p. 251). Par construction même, cette algèbre $TS(M)$ est une sous-algèbre de $T_S(M)$. La décomposition $TS(M) = TS_0(M) \oplus TS_+(M)$ est une prégraduation.

THÉORÈME 3. — *L'algèbre prégraduée $TS(M)$ est une sous-PD-algèbre de $T_S(M)$.*

Il faut montrer que, pour $t \in TS_+(M)$, on a $\gamma_n(t) \in TS(M)$; il suffit de le faire pour $n \geqq 1$ et $t = t_p \in TS_p(M)$ $(p \geqq 1)$.

On sait que

$$\gamma_n(t_p) = \sum_{\sigma \in K_p'^n} \sigma(t_p^{\otimes n}).$$

Le tenseur $t_p^{\otimes n}$ est invariant par les opérations de H_p^n (les t_p étant symétriques) et de P_p^n (les n facteurs de $t_p^{\otimes n}$ étant égaux); il est donc invariant par les opérations du groupe L_p^n (pour les notations, *cf.* § 1).

Pour $\sigma \in \mathfrak{S}_{np}$, l'élément $\sigma(t_p^{\otimes n})$ ne dépend donc que de la classe à gauche σL_p^n. Si E est un système de représentants pour ces classes à gauche, le tenseur $t' = \sum_{\sigma \in E} \sigma(t_p^{\otimes n})$ ne dépend pas du choix fait pour ces représentants; et c'est un tenseur symétrique, car transformer t' par un élément de $\mathfrak{S}_{np}$ revient à changer le système des représentants. Or, $K_p'^n$ est un système de représentants possibles; donc $\gamma_n(t_p)$ est symétrique.

C. Q. F. D.

Nous faisons maintenant intervenir l'algèbre $\Gamma(M)$ des puissances divisées du module M. Considérons l'injection canonique

$$M \to TS_1(M) = M \subset TS_+(M).$$

En vertu de la propriété universelle de $\Gamma(M)$ (*cf.* [1], th. 2, p. 89), cette injection se prolonge de manière unique, en un *PD*-homomorphisme $\Phi : \Gamma(M) \to TS(M)$. Pour $x \in M$, on a

$$\Phi(x^{[n]}) = \Phi \circ \gamma_n(x) = \gamma_n \circ \Phi(x) = x^{\otimes n}.$$

Cet homomorphisme était déjà connu de nous, mais seulement comme homomorphisme d'algèbres (*cf.* [2], prop. III.1, p. 254). On peut donc énoncer le théorème suivant :

THÉORÈME 4. — *L'application canonique* $\Phi : \Gamma(M) \to TS(M)$ *est un PD-homomorphisme.*

On peut faire à ce sujet une remarque intéressante. On sait que, si M est un module *libre*, l'application Φ est un *isomorphisme* (*cf.* [2], prop. IV.5, p. 272). Pour définir les puissances divisées de $\Gamma(M)$, il suffit donc de transporter par Φ la structure de *PD*-algèbre de $TS(M)$, telle qu'elle est définie par le théorème 3, à $\Gamma(M)$. Si M n'est pas un module libre, on en déduit tout de même aisément la structure de *PD*-algèbre sur $\Gamma(M)$, en considérant M comme le quotient d'un module libre. En un sens, cette construction est peut-être plus simple que celle que nous avons donnée dans [1].

Remarque. — On pourrait espérer que, dans tous les cas, Φ soit un isomorphisme. Mais il n'en est rien; voici un contre-exemple :

On prend pour A l'anneau $\mathbf{Z}$, pour module M le groupe $\mathbf{Z}/a\mathbf{Z}$ ($a \geq 2$). On a $TS_n(M) = T_n(M)$. Si e est la classe de 1 modulo a, $\Gamma_n(M)$ [resp. $TS_n(M)$] est monogène, engendré par $e^{[n]}$ (resp. $e^{\otimes n}$); on a $\Phi(e^{[n]}) = e^{\otimes n}$. L'annulateur de $e^{\otimes n}$ est l'idéal principal (a), tandis que l'annulateur de $e^{[n]}$ est l'idéal principal $(d_n(a))$, où $d_n(a)$ est le p. g. c. d. de na et a^n (*cf.* [3]). Or, il existe beaucoup de n pour lesquels $d_n(a)$ est strictement plus grand que a; alors, $TS_n(M)$ a strictement plus de torsion que $\Gamma_n(M)$ et ne lui est donc pas isomorphe.

Deuxième partie.

Dans cette deuxième partie, A désigne toujours un *anneau commutatif unitaire.* Les *modules* sont des A-modules. Les *algèbres* sont des A-algèbres *commutatives, associatives.* Tous les *monoïdes* considérés sont *commutatifs*; sauf mention contraire, ils sont notés *additivement.*

7. Algèbres graduées sur un monoïde.

Soit $\mathcal{M}$ un monoïde.

On dit qu'une algèbre R est graduée sur $\mathcal{M}$ si l'on s'est donné une décomposition en somme directe du module R de la forme

$$R = \bigoplus_{m \in \mathcal{M}} R_m,$$

telle que $R_m R_{m'} \subset R_{m+m'}$ quels que soient m et m' dans $\mathcal{M}$. Un élément de R contenu dans l'un des R_m est dit homogène.

Exemple. — L'algèbre *libre* $A(\mathcal{M})$ du monoïde $\mathcal{M}$ à coefficients dans A est le module libre ayant une base formée d'éléments e_m $(m \in \mathcal{M})$, avec la multiplication : $e_m e_{m'} = e_{m+m'}$. Alors, $A(\mathcal{M})$ est graduée sur $\mathcal{M}$ si l'on prend pour $A_m(\mathcal{M})$ le sous-module engendré par e_m.

Très souvent, $\mathcal{M}$ possède un élément neutre ω, $\mathcal{M} - \{\omega\}$ est stable pour l'addition, R possède un élément unité 1, et l'on a $1 \in R_\omega$. Dans ce cas, sans explication supplémentaire, on posera : $R_0 = R_\omega$; $R_+ = \bigoplus_{m \neq \omega} R_m$. Alors, la décomposition $R = R_0 \oplus R_+$ est une prégraduation de R.

8. Transport de graduations.

Soient $\mathcal{M}$ et $\mathcal{M}'$ deux monoïdes, $v : \mathcal{M} \to \mathcal{M}'$ un homomorphisme de monoïdes, R une algèbre graduée sur $\mathcal{M}$.

Pour $m' \in \mathcal{M}'$, posons

$$R_{m'} = \bigoplus_{m \in v^{-1}(m')} R_m$$

(on convient de ce qu'une somme directe vide représente un module nul).

Il est clair qu'on a $R = \bigoplus_{m' \in \mathcal{M}'} R_{m'}$ et qu'on définit ainsi dans R une graduation sur $\mathcal{M}'$. On dit que cette graduation sur $\mathcal{M}'$ est la *transportée* par v de la graduation initiale sur $\mathcal{M}$.

Le transport des graduations est une opération transitive; si $v : \mathfrak{M} \to \mathfrak{M}'$ et $v' : \mathfrak{M}' \to \mathfrak{M}''$ sont des homomorphismes de monoïdes et si R est graduée sur $\mathfrak{M}$, on peut transporter cette graduation successivement par v, puis par v', ou directement par $v' \circ v$, on obtient dans les deux cas la même graduation sur $\mathfrak{M}''$.

Une algèbre R étant donnée, on peut donc dire que la correspondance qui, à tout monoïde, associe l'ensemble de toutes les graduations de R sur ce monoïde, est un foncteur covariant qui fait passer de la catégorie des monoïdes à la catégorie des ensembles.

9. **Les algèbres *I*-graduées.**

On note $\mathbf{N}$ le monoïde additif des entiers $\geqq 0$.

Soit I un ensemble d'indices. On note $\mathbf{N}^{(I)}$ le monoïde additif des applications f de I dans $\mathbf{N}$ qui sont à support fini, c'est-à-dire telles que $f(i) = 0$, sauf pour un nombre fini d'indices i. Ce monoïde possède un élément neutre ω, défini par $\forall i \in I,\ \omega(i) = 0$; le complémentaire de $\{\omega\}$ est stable pour l'addition.

Une algèbre graduée sur $\mathbf{N}$ (resp. $\mathbf{N} \times \mathbf{N}$, etc.) est communément appelée une algèbre graduée (resp. bigraduée, etc.).

On dira qu'une algèbre R est *I-graduée* si elle est munie d'une graduation sur $\mathbf{N}^{(I)}$. Si $f \in \mathbf{N}^{(I)}$ et si $r \in R_f$, on dit que f est le I-degré de r.

Si une algèbre I-graduée R est unitaire, on a nécessairement $1 \in R_\omega$, et l'on peut, dès lors, considérer la prégraduation $R = R_0 \oplus R_+$.

Exemple 1. — L'algèbre libre du monoïde $\mathbf{N}^{(I)}$, c'est-à-dire l'algèbre de polynômes $A[X_i]_{i \in I}$, est I-graduée (*cf.* exemple du paragraphe 7).

Rappelons à ce sujet que la notation polynomiale revient à représenter un élément $f \in \mathbf{N}^{(I)}$ par la notation $\prod_{i \in I} X_i^{f(i)}$.

Exemple 2 (Exemple que je dois à une remarque de J.-L. Koszul). — Soit un monoïde $\mathfrak{M}$. On appelle I-valuation de $\mathfrak{M}$ un homomorphisme v du monoïde $\mathfrak{M}$ dans le monoïde $\mathbf{N}^{(I)}$. Une telle I-valuation v est équivalente à la donnée, pour tout $i \in I$, d'un homomorphisme v_i de $\mathfrak{M}$ dans $\mathbf{N}$ en sorte que, pour tout $m \in \mathfrak{M}$, on ait $v_i(m) = 0$, sauf pour un nombre fini d'indices i; cette correspondance $v \Longleftrightarrow (v_i)$ est explicitée par la relation : $[v(m)](i) = v_i(m)$.

Alors, si R est une algèbre graduée sur $\mathfrak{M}$ et si v est une I-valuation de $\mathfrak{M}$, on en déduit par transport une I-graduation de R.

10. **Quelques définitions relatives à $\mathbf{N}^{(I)}$.**

Pour $f \in \mathbf{N}^{(I)}$, on pose

$$f! = \prod_{i \in I} f(i)\,!\,.$$

(Ce produit infini a un sens car presque tous ses facteurs sont égaux à 1.) Pour calculer $f!$, il suffit de faire varier i dans le support de f. Donc, si $f_1, \ldots, f_p$ sont à supports deux à deux disjoints, on a :

$$(f_1 + \ldots + f_p)! = f_1! \ldots f_p!.$$

Pour des éléments $f_1, \ldots, f_p$ dans $\mathbf{N}^{(I)}$, on pose :

$$((f_1, \ldots, f_p)) = \frac{(f_1 + \ldots + f_p)!}{f_1! \ldots f_p!} = \prod_{i \in I} \frac{[f_1(i) + \ldots + f_p(i)]!}{f_1(i)! \ldots f_p(i)!}$$

(c'est un entier $\geqq 1$).

Cette expression est symétrique en $f_1, \ldots, f_p$. Si ces éléments de $\mathbf{N}^{(I)}$ sont à supports deux à deux disjoints dans I, on a $((f_1, \ldots, f_p)) = 1$.

Pour $q > p$, on vérifie immédiatement la formule

$$((f_1, \ldots, f_p))((f_1 + \ldots + f_p, f_{p+1}, \ldots, f_q)) = ((f_1, \ldots, f_q)).$$

Pour $f \in \mathbf{N}^{(I)}$ et un entier $n \geqq 1$, on a

$$((\underbrace{f, \ldots, f}_{n})) = \frac{(nf)!}{(f!)^n} = \prod_{i \in I} \frac{[nf(i)]!}{[f(i)!]^n}.$$

Si $f \neq \omega$, il existe dans I un i, avec $f(i) \geqq 1$, et alors le facteur correspondant du produit est divisible par $n!$. On définit alors l'entier

$$C_{n,f} = \frac{(nf)!}{n!(f!)^n} \quad \text{pour } f \neq \omega \quad (\text{même si } n = 0).$$

11. L'algèbre des éléments divisés d'une algèbre I-graduée et ses puissances divisées.

Soient R une algèbre I-graduée, f et g des éléments de $\mathbf{N}^{(I)}$. Pour des éléments r (resp. s) de R_f (resp. R_g), on pose :

$$r \star s = ((f, g))\, rs.$$

On définit ainsi une application bilinéaire de $R_f \times R_g$ dans R_{f+g}. Si $h \in \mathbf{N}^{(I)}$ et $t \in R_h$, on a aussi :

$$(r \star s) \star t = r \star (s \star t) = ((f, g, h))\, rst.$$

En prolongeant toutes ces opérations par bilinéarité, on en déduit une autre structure multiplicative sur R, avec une multiplication $\star$ qui est commutative et associative.

Avec cette structure-là, R se notera $R_\star$, et $R_\star$ s'appellera (pour une raison qui apparaîtra) *l'algèbre des éléments divisés de l'algèbre I-graduée R.*

On peut préciser la multiplication $\star$ comme suit : si, pour $k = 1, \ldots, p$, on a $r_k \in R_{f_k}$, alors

$$r_1 \star \ldots \star r_p = ((f_1, \ldots, f_p))\, r_1 \ldots r_p.$$

En particulier, si les supports des f_k sont deux à deux disjoints, on a

$$r_1 \star \ldots \star r_p = r_1 \ldots r_p.$$

La I-graduation de R est aussi une I-graduation de $R_\star$. Si R est unitaire, alors $R_\star$ est aussi unitaire avec la même unité. La décomposition $R = R_0 \oplus R_+$ est aussi une prégraduation pour $R_\star$.

Nous allons démontrer le théorème suivant :

THÉORÈME 5. — *Soient I un ensemble d'indices et R une algèbre unitaire I-graduée. Alors, dans l'algèbre prégraduée $R_\star$ il existe un système de puissances divisées, et un seul, tel que, pour $r \in R_f$ $(f \in \mathbf{N}^{(I)} - \{\omega\})$, on ait*

$$\gamma_n(r) = C_{n,f}\, r^n.$$

L'unicité est évidente puisque R_+ est engendrée linéairement par ses éléments homogènes. Reste à démontrer l'existence.

LEMME. — *Le théorème 5 est vrai si $A = \mathbf{Z}$ et si R est libre sur $\mathbf{Z}$.*

Si $r \in R_f$ $(f \neq \omega)$, on a

$$r^{\star n} = ((\underbrace{f, \ldots, f}_{n}))\, r^n = n!\, C_{n,f}\, r^n.$$

Donc, $r^{\star n}$ est divisible par $n!$, et l'on posera : $\gamma_n(r) = C_{n,f}\, r^n$. Maintenant, soit $r \in R_+$, s'écrivant : $r = r_1 + \ldots + r_h$, avec $r_k \in R_{f_k}$ $(f_k \neq \omega)$. On a

$$\begin{aligned} r^{\star n} &= \sum_{\alpha_1 + \ldots + \alpha_p = n} \frac{n!}{\alpha_1! \ldots \alpha_p!}\, r_1^{\star \alpha_1} \star \ldots \star r_p^{\star \alpha_p} \\ &= n! \sum_{\alpha_1 + \ldots + \alpha_p = n} \gamma_{\alpha_1}(r_1) \star \ldots \star \gamma_{\alpha_p}(r_p). \end{aligned}$$

Donc, $r^{\star n}$ est divisible par $n!$. On posera alors : $\gamma_n(r) = \dfrac{r^{\star n}}{n!}$ (élément déterminé de manière unique puisque R est libre sur $\mathbf{Z}$). On définit ainsi un système de puissances divisées satisfaisant au théorème 5.

C. Q. F. D.

Cas général. — R est maintenant une A-algèbre unitaire I-graduée quelconque. Soit $\mathbf{Z}(R^\star)$ la $\mathbf{Z}$-algèbre libre (à coefficients dans $\mathbf{Z}$) du monoïde multiplicatif $R^\star$ de R. C'est le Z-module libre ayant pour base des éléments e_r $(r \in R)$, avec la multiplication : $e_r\, e_{r'} = e_{rr'}$. Soit S

le sous-$\mathbf{Z}$-module de $\mathbf{Z}(R^\star)$ engendré par les e_r, où r est homogène dans R. S est un $\mathbf{Z}$-module libre, facteur direct de $\mathbf{Z}(R^\star)$, sous-algèbre unitaire de $\mathbf{Z}(R^\star)$.

Pour $f \in \mathbf{N}^{(I)}$, soit S_f le sous-module de S engendré par les e_r, où $r \in R_f$. On a : $S = \bigoplus_{f \in \mathbf{N}^{(I)}} S_f$, et cette décomposition est une I-graduation de S.

On peut considérer l'algèbre unitaire $S_\star$. Si $r \in R_f$ et $r' \in R_{f'}$, on a, dans $S_\star$,

$$e_r \star e_{r'} = ((f, f'))\, e_r\, e_{r'} = ((f, f'))\, e_{rr'}.$$

D'après le lemme, $S_\star$ est une $\mathbf{Z}$-PD-algèbre et l'on a, pour $r \in R_f$ $(f \neq \omega)$:

$$\gamma_n(e_r) = C_{n,f}\, e_r^n = C_{n,f}\, e_{r^n}.$$

Maintenant, soit $A(R^\star)$ l'algèbre libre sur A du monoïde multiplicatif $R^\star$ On a

$$A(R^\star) = A \bigotimes_{\mathbf{Z}} \mathbf{Z}(R^\star),$$

en tant que module et en tant qu'algèbre. Puisque S est un facteur direct de $\mathbf{Z}(R^\star)$, $L = A \bigotimes_{\mathbf{Z}} S$ s'identifie à un sous-groupe additif de $A(R^\star)$: c'est le sous-groupe engendré par les $\lambda\, e_r$, où r est homogène $(\lambda \in A)$. L est donc aussi un sous-A-module et une sous-algèbre de $A(R^\star)$, et l'on a ensuite $L = A \bigotimes_{\mathbf{Z}} S$ en tant qu'algèbre.

Pour $f \in \mathbf{N}^{(I)}$, soit L_f le sous-module de L engendré par les e_r avec $r \in R_f$. On voit que L est I-graduée par les L_f et que $L_f = A \bigotimes_{\mathbf{Z}} S_f$. En outre, L est unitaire, $L_0 = A \bigotimes_{\mathbf{Z}} S_0$, $L_+ = A \bigotimes_{\mathbf{Z}} S_+$, et enfin :

$$L_\star = A \bigotimes_{\mathbf{Z}} S_\star$$

en tant qu'algèbre. Si $r \in R_f$ et $r' \in R_{f'}$, on a encore

$$e_r \star e_{r'} = ((f, f'))\, e_r\, e_{r'} = ((f, f'))\, e_{rr'}$$

dans $L_\star$.

En considérant A comme une $\mathbf{Z}$-PD-algèbre triviale, on voit que $L_\star$, produit tensoriel de deux $\mathbf{Z}$-PD-algèbres est, avec sa prégraduation canonique, une PD-algèbre (sur $\mathbf{Z}$, donc aussi sur A). Pour $r \in R_f$ et $f \neq \omega$, on a encore

$$\gamma_n(e_r) = C_{n,f}\, e_r^n = C_{n,f}\, e_{r^n}.$$

Plus généralement, le théorème 5 est vrai pour $L_\star$.

Maintenant, soit $q : L \rightarrow R$ l'homomorphisme de modules défini par $q(e_r) = r$, si r est homogène.

Il est *surjectif*, car R est linéairement engendré par ses éléments homogènes. Plus précisément, il applique L_f sur R_f; il respecte donc les prégraduations. C'est un homomorphisme d'algèbres, car

$$q(e_r e_{r'}) = q(e_{rr'}) = rr' = q(e_r)\, q(e_{r'}).$$

De la même façon, on voit que q est un homomorphisme d'algèbres de L_* sur R_*.

Soit J le sous-module de L engendré par les éléments

$$(1) \qquad \begin{cases} e_{r+r'} - e_r - e_{r'} & (r,\ r' \text{ homogènes de même } I\text{-degré}), \\ e_{\lambda r} - \lambda e_r & (r \text{ homogène, } \lambda \in A). \end{cases}$$

Pour $f \in \mathbf{N}^{(I)}$, soit J_f le sous-module de J engendré par les éléments de type (1) de I-degré f.

Il est clair que J est la somme directe des J_f et, d'autre part, que J_f est le noyau de $q : L_f \to R_f$. Donc, J est le noyau de q.

Montrons que J est un idéal divisé de la PD-algèbre L_*. Compte tenu de ([1], prop. 4, p. 79) et du fait que les éléments de type (1) engendrent linéairement, donc algébriquement, l'idéal J, il suffit de montrer que $\gamma_n(v) \in J$ chaque fois que n est $\geqq 1$ et que v est un élément de type (1) de I-degré $f \neq \omega$.

Si r et $r' \in R_f (f \neq \omega)$ et $n \geqq 1$, on a, dans L_* :

$$\gamma_n(e_{r+r'} - e_r - e_{r'}) = C_{n,f}(e_{r+r'} - e_r - e_{r'})^n \in J,$$

puisque J est un idéal et, si $\lambda \in A$:

$$\gamma_n(e_{\lambda r} - \lambda e_r) = C_{n,f}(e_{\lambda r} - \lambda e_r)^n \in J,$$

pour la même raison.

Puisque, dès lors, l'idéal J est divisé dans L_*, on peut passer au quotient et définir sur R_* des puissances divisées. Si $r \in R_f$ $(f \neq \omega)$, on aura

$$\gamma_n(r) = \gamma_n \circ q(e_r) = q \circ \gamma_n(e_r) = q[C_{n,f}\, e_{r^n}] = C_{n,f}\, r^n.$$

Le théorème est démontré.

12. Premier exemple.

On prend d'abord $A = \mathbf{Z}$.

Soit I un ensemble d'indices. L'algèbre unitaire $R = \mathbf{Z}[X_i]_{i \in I}$ est canoniquement I-graduée. La PD-algèbre R_* qu'on en déduit, par le théorème 5, s'appelle l'*algèbre des polynômes divisés* aux indéterminées (X_i) à coefficients dans $\mathbf{Z}$.

Considérons l'application linéaire injective φ de R_* dans $\mathbf{Q}[X_i]_{i\in I}$ définie par : $\varphi(P) = \frac{P}{f!}$ pour un polynôme P homogène de I-degré f. On a, par exemple :

$$\varphi(X_i^n) = \frac{X_i^n}{n!},$$

car X_i^n a le I-degré f défini par : $f(j) = 0$ si $j \neq i$, $f(i) = n$, de sorte que $f! = n!$. On a $\varphi(1) = 1$.

Si P (resp. Q) est homogène de I-degré f (resp. g), on a

$$\varphi(P \star Q) = ((f, g))\, \varphi(PQ) = ((f, g))\, \frac{PQ}{(f+g)!} = \frac{PQ}{f!\, g!} = \varphi(P)\, \varphi(Q),$$

de sorte que $\varphi : R_* \to \mathbf{Q}[X_i]_{i\in I}$ est un homomorphisme d'algèbres. On peut donc identifier, par φ, l'algèbre R_* à son image dans $\mathbf{Q}[X_i]_{i\in I}$.

Remarquons que R_* est engendrée algébriquement par les éléments X_i^n. En effet, si $i_1, \ldots, i_p$ sont tous distincts, on a

$$X_{i_1}^{n_1} \ldots X_{i_p}^{n_p} = X_{i_1}^{n_1} \star \ldots \star X_{i_p}^{n_p},$$

car les I-degrés f_k des $X_{i_k}^{n_k}$ ont des supports deux à deux disjoints. Donc, par φ, R_* s'identifie au sous-anneau de $\mathbf{Q}[X_i]_{i\in I}$ engendré par les monômes $\frac{X_i^n}{n!}$. On voit ainsi l'origine de l'expression « *algèbre des éléments divisés* » dans le cas général.

Si A est un anneau quelconque, on note $A_*[X_i]_{i\in I}$ l'algèbre des éléments divisés de l'algèbre I-graduée $A[X_i]_{i\in I}$. On l'appelle encore l'*algèbre des polynômes divisés à coefficients dans A aux indéterminées* (X_i).

On voit, comme ci-dessus, que cette algèbre est encore engendrée par les éléments X_i^n. On a $\gamma_n(X_i) = X_i^n$, car, si f est le I-degré de X_i, on voit immédiatement que $C_{n,f} = 1$.

THÉORÈME 6 (*Propriété universelle des algèbres de polynômes divisés*). — *Soient A un anneau, $R = R_0 \oplus R_+$ une algèbre à puissances divisées sur A. Soit I un ensemble d'indices, identifié à un ensemble d'indéterminées $(X_i)_{i\in I}$. Soit φ une application de I dans R_+. Alors φ se prolonge, et de manière unique, en un PD-homomorphisme Φ de $A_*[X_i]_{i\in I}$ dans R.*

Unicité. — Soit un monôme littéral $P = X_{i_1}^{n_1} \ldots X_{i_p}^{n_p}$ de $A_*[X_i]$ (les i_k étant distincts).

On peut écrire aussi :

$$P = X_{i_1}^{n_1} \star \ldots \star X_{i_p}^{n_p} = \gamma_{n_1}(X_{i_1}) \star \ldots \star \gamma_{n_p}(X_{i_p}).$$

On doit avoir

$$\Phi(\gamma_n(X_i)) = \gamma_n \circ \varphi(X_i) = \gamma_n \circ \varphi(i),$$

donc aussi

$$\Phi(P) = [\gamma_{n_1} \circ \varphi(i_1)] \ldots [\gamma_{n_p} \circ \varphi(i_p)].$$

D'où l'unicité.

Existence. — Définissons Φ sur les monômes littéraux par la formule précédente, et prolongeons-la à toute l'algèbre par linéarité. Si p est un monôme littéral de I-degré f, la formule précédente peut s'écrire :

$$\Phi(P) = \prod_{i \in I} \gamma_{f(i)} \circ \varphi(i).$$

Si Q est un monôme littéral de I-degré g, on aura :

$$\begin{aligned}\Phi(P)\,\Phi(Q) &= \prod_{i \in I} [\gamma_{f(i)} \circ \varphi(i)][\gamma_{g(i)} \circ \varphi(i)] \\ &= \prod_{(i \in I)} ((f(i), g(i))) \prod_{i \in I} \gamma_{(f+g)(i)} \circ \varphi(i) \\ &= ((f, g))\, \Phi(PQ) = \Phi(P \star Q).\end{aligned}$$

Donc, Φ est un homomorphisme d'algèbres.

Si P est vide, on a $\Phi(1) = 1$. Si p n'est pas vide, $\Phi(P) \in R_+$. Donc Φ est un homomorphisme d'algèbres prégraduées. Enfin, pour $p \geqq 1$, on a

$$\begin{aligned}\Phi \circ \gamma_n(X_i^p) &= \Phi \circ \gamma_n \circ \gamma_p(X_i) = C_{n,p}\, \Phi \circ \gamma_{np}(X_i) = C_{n,p}\, \Phi(X_i^{np}) \\ &= C_{n,p}\, \gamma_{np} \circ \varphi(i) = \gamma_n \circ \gamma_p \circ \varphi(i) = \gamma_n \circ \Phi(X_i^p).\end{aligned}$$

Comme les $X_i^p\,(p \geqq 1)$ engendrent l'idéal $(A_*)_+[X_i]$, on voit que Φ est un PD-homomorphisme ([1], prop. 3, p. 79).

C. Q. F. D.

Soit M le module engendré par les X_i dans $A[X_i]$. En somme, M est le module libre de base I. On vérifie immédiatement qu'on peut identifier les algèbres $A_*[X_i]$ et $\Gamma(M)$, en identifiant les monômes $X_{i_1}^{n_1} \ldots X_{i_p}^{n_p}$ (les i_k tous distincts) à l'élément de base $X_{i_1}^{[n_1]} \ldots X_{i_p}^{[n_p]}$ de $\Gamma(M)$. Comme, d'autre part, une application de I dans un module équivaut à un homomorphisme de M dans ledit module, on vient de redémontrer la chose suivante : pour un module libre M, $\Gamma(M)$ est une PD-algèbre et l'injection $M \to \Gamma_+(M)$ est universelle pour les homomorphismes $M \to R_+$ où R est une PD-algèbre. Il n'est pas difficile d'étendre ces résultats au cas d'un module quelconque, en le présentant comme quotient d'un module libre.

13. **Second exemple.**

Si I n'a qu'un élément, le théorème 5 prend la forme suivante :

Soit $R = \bigoplus_{n \geqq 0} R_n$ une algèbre graduée. On définit sur R une structure d'algèbre R_* en posant

$$r_n \bigstar r_m = ((m, n))\, r_n r_m \qquad (r_i \in R_i).$$

Alors, R_* est une PD-algèbre et, pour $r \in R_p$ ($p \geqq 1$), on a

$$\gamma_n(r) = C_{n,p} r^n.$$

Par exemple, si M est un module, on déduit de l'algèbre symétrique de M, notée $S(M)$. une algèbre $S_*(M)$.

Proposition 3. — *L'application canonique $q : T(M) \to S(M)$ est un PD-homomorphisme de $T_S(M)$* [1] *sur $S_*(M)$.*

Pour $t_i \in T_i(M)$ ($i = m, n$), on a en effet :

$$q(t_m \bigstar t_n) = q\left[\sum_{\sigma \in K_{m,n}} \sigma(t_m \otimes t_n)\right].$$

Mais $q \circ \sigma(t_m \otimes t_n) = q(t_m \otimes t_n) = q(t_m)\, q(t_n)$. Comme $\mathrm{K}_{m,n}$ a $((m, n))$ éléments, on a

$$q(t_m \bigstar t_n) = ((m, n))\, q(t_m)\, q(t_n) = q(t_m) \bigstar q(t_n).$$

En outre, si $p \geqq 1$:

$$q \circ \gamma_n(t_p) = q \circ \sum_{\sigma \in K'^n_p} \sigma(t_p^{\otimes n}).$$

Comme $q \circ \sigma(t_p^{\otimes n}) = q(t_p^{\otimes n}) = q(t_p)^n$ et que K'^n_p a $C_{n,p}$ éléments, on a

$$q \circ \gamma_n(t_p) = C_{n,p}\, q(t_p)^n = \gamma_n \circ q(t_p).$$

Donc q est un PD-homomorphisme.

Remarque. — La restriction de q à $T\,S(M)$ est aussi un PD-homomorphisme, sans doute non surjectif en général.

---

[1] Rappelons que $T_S(M)$ désigne le module $T(M)$ muni de la structure de PD-algèbre définie au n° 5.

BIBLIOGRAPHIE.

[1] ROBY (Norbert). — Les algèbres à puissances divisées, *Bull. Sc. math.*, Série 2, t. 89, 1965, p. 75-91.
[2] ROBY (Norbert). Lois polynômes et lois formelles en théorie des modules, *Ann. scient. Éc. Norm. Sup.*, Série 3, t. 80, 1963, p. 213-348 (Thèse Sc. math. Strasbourg, 1963).
[3] ROBY (Norbert). — L'anneau des puissances divisées d'un groupe monogène, *Bol. Soc. Matem. São Paulo*, t. 18, 1963-1966, p. 39-47.

(Manuscrit reçu le 21 janvier 1968.)

Norbert ROBY,
Professeur à la Faculté des Sciences de Montpellier,
7, rue de l'Imprimerie,
34-Montpellier.