ANNALES SCIENTIFIQUES DE L'É.N.S.

NORBERT ROBY

Sur l'algèbre des puissances divisées d'un module et le module de ses différentielles

Annales scientifiques de l'É.N.S. 3e série, tome 83, nº 2 (1966), p. 75-89
<http://www.numdam.org/item?id=ASENS_1966_3_83_2_75_0>

Ann. scient. Éc. Norm. Sup.,
3e série, t. 83, 1966, p. 75 à 89.

SUR L'ALGÈBRE DES PUISSANCES DIVISÉES D'UN MODULE
ET LE MODULE DE SES DIFFÉRENTIELLES

PAR M. NORBERT ROBY.

On désigne par A un anneau commutatif unitaire. Par *module* nous entendons un A-*module unitaire*. Par *algèbre*, nous entendons une A-*algèbre associative et commutative*. Une algèbre n'a pas nécessairement d'élément unité; si elle en a un, elle est dite unitaire. Un *homomorphisme d'algèbres* $\varphi : R \to S$ est un homomorphisme de modules qui respecte la multiplication. Si R et S sont unitaires et si $\varphi(1) = 1$, on dit que φ est *unitaire*.

Tous les produits tensoriels considérés sont pris sur l'anneau A.

En algèbre commutative, la distinction entre « module à droite » et « module à gauche » est en principe sans objet. Ici, toutefois, nous considérerons des modules P où, pour noter le produit d'un élément $x \in P$ par un scalaire $\lambda \in A$, nous aurons à utiliser soit la notation λx, soit la notation $x\lambda$. Dans le premier cas (resp. le second), nous dirons que P est un module à gauche (resp. à droite); cette distinction tient donc avant tout à une convention d'écriture. En principe, tous les modules sont considérés comme modules à gauche. Mais il arrivera que, pour un même groupe abélien P, on ait à considérer deux structures de A-modules, l'une notée à gauche et l'autre notée à droite. Si l'on a, en outre, $(\lambda x)\,\mu = \lambda(x\mu)$, on dira que P est un *bimodule*. Le module à gauche (resp. à droite) sous-jacent au bimodule P sera noté P^g (resp. P^d).

I. — Les bimodules M_{p^h}.

1. LE BIMODULE A_{p^h}. — Soit p un nombre premier $\geqq 2$. L'idéal principal engendré par $p.1$ dans A est noté (p). On pose

$$A/(p) = A_p.$$

Nous n'utiliserons pas la structure d'anneau quotient de A_p; par contre, nous utiliserons sa structure de A-module quotient, que nous notons à gauche.

Pour tout entier $h \geqq 1$, nous désignerons par A_{p^h} la donnée du *groupe* additif A_p et des deux applications

$$A \times A_p \to A_p \quad \text{et} \quad A_p \times A \to A_p$$

définies respectivement par

$$(\lambda, \alpha) \to \lambda\alpha \quad \text{et} \quad (\alpha, \mu) \to \mu^{p^h}\alpha \quad (\text{que nous notons } \alpha\mu).$$

La première de ces applications confère à A_p une structure de module à gauche, qui n'est rien d'autre que sa structure de module quotient. La seconde confère à A_p une structure de module à droite; la seule chose non tout à fait triviale à vérifier est

$$x(\mu + \mu') = x\mu + x\mu',$$

et cela résulte de la relation dans A,

$$(\mu + \mu')^{p^h} \equiv \mu^{p^h} + \mu'^{p^h} \quad (p).$$

On vérifie aussi que $\lambda(x\mu) = (\lambda x)\mu$. Ainsi, nous venons de définir un bimodule noté A_{p^h}, avec $A^g_{p^h} = A_p$.

De la relation $\lambda(x\mu) = (\lambda x)\mu$ il résulte que l'homothétie de rapport λ dans $A^g_{p^h}$ est un endomorphisme de $A^d_{p^h}$, que nous notons $\hat{\lambda}$.

2. Les bimodules M_{p^h}. — Soit, à présent, un module M. Nous formons le produit tensoriel

$$M^d_{p^h} = A^d_{p^h} \otimes M$$

que nous considérons comme *module à droite*.

Pour $\alpha \in A_p$ et $x \in M$, nous notons $\alpha \underset{p^h}{\otimes} x$ l'élément $\alpha \otimes x$ de $M^d_{p^h}$, où α est considéré comme appartenant à $A^d_{p^h}$.

On fait maintenant opérer A *à gauche* sur le groupe abélien M_{p^h} sous-jacent à $M^d_{p^h}$, de la manière suivante : la multiplication à gauche par λ est l'endomorphisme de $M^d_{p^h}$ égal à $\hat{\lambda} \otimes \varepsilon_M$, où ε_M est l'application identique de M. On vérifie que cette loi externe fait de M_{p^h} un *module à gauche*, que nous notons $M^g_{p^h}$. Enfin, ces deux structures de modules sur M_{p^h} en font un bimodule. Les deux lois externes du bimodule M_{p^h} sont explicitées par les formules suivantes :

$$\left\{\begin{array}{l} \forall\, \lambda \in A, \quad \alpha \in A_p, \quad x \in M : \\ \lambda\left(\alpha \underset{p^h}{\otimes} x\right) = (\lambda\alpha) \underset{p^h}{\otimes} x, \\ \left(\alpha \underset{p^h}{\otimes} x\right)\lambda = \alpha \underset{p^h}{\otimes} (\lambda x) = (\alpha\lambda) \underset{p^h}{\otimes} x = (\lambda^{p^h}\alpha) \underset{p^h}{\otimes} x = \lambda^{p^h}\left(\alpha \underset{p^h}{\otimes} x\right). \end{array}\right.$$

Remarques. — 1° Si $M = A$, le bimodule M_{p^h} s'identifie au bimodule A_{p^h} défini auparavant (notations cohérentes).

2° Si $A = \mathbf{Z}$, on a $\mathbf{Z}^g_{p^h} = \mathbf{Z}^d_{p^h} = \mathbf{F}_p$ (corps à p éléments), car dans $\mathbf{Z}$ on a la relation $\lambda^{p^h} \equiv \lambda(p)$. On en déduit que, pour tout h :

$$M^g_{p^h} = M^d_{p^h} = M \otimes \mathbf{F}_p = M/pM.$$

3° Si A contient un sous-corps de caractéristique 0, on a $A_p = 0$, car $(p) = A$. Il en résulte que $M_{p^h} = 0$.

4° Si A contient un sous-corps de caractéristique $q \geqq 2$, on a

$$(p) = \begin{cases} A & \text{si } p \neq q \\ 0 & \text{si } p = q \end{cases} \quad \text{donc} \quad A_p = \begin{cases} 0 & \text{si } p \neq q, \\ A & \text{si } p = q. \end{cases}$$

Il en résulte que $M_{p^h} = 0$ si $p \neq q$.

Supposons en outre que $A = \mathbf{F}_q$. Alors, les multiplications externes à droite et à gauche coïncident toujours, en vertu de la relation $\lambda^{q^h} = \lambda$ dans $\mathbf{F}_q$. On a donc

$$M^g_{q^h} = M^d_{q^h} = A \otimes M = M.$$

II. — Le résidu de $\Gamma_+(M)$.

3. Le résidu d'une algèbre. — Soit R une algèbre. La loi multiplicative de R étant bilinéaire, il existe une application linéaire $\mu : R \otimes R \to R$, avec $\mu(r \otimes s) = rs$.

On appelle *résidu* de R le conoyau de μ. Le résidu de R est donc le module quotient de R par le sous-module I engendré par les produits deux à deux d'éléments de R.

On peut noter que I est aussi un idéal de R; mais la multiplication induite sur le résidu par passage au quotient est tout à fait inintéressante, car avec cette structure le produit de deux éléments est toujours nul.

4. Le résidu de $\Gamma_+(M)$. — Soit M un module. Nous introduisons l'algèbre $\Gamma(M)$ des puissances divisées du module M (*cf.* [2], essentiellement chap. III).

Nous désignons par $G(M)$ le résidu de l'idéal $\Gamma_+(M)$ et par $\rho : \Gamma_+(M) \to G(M)$ l'application canonique. Nous allons expliciter la structure du module $G(M)$.

Soit I le noyau de ρ; c'est l'idéal de $\Gamma_+(M)$ engendré par les produits $x^{[n]} y^{[m]}$ ($x, y \in M$; $n, m \geqq 1$). Comme ces éléments sont homogènes, I est un sous-module homogène de l'algèbre graduée $\Gamma_+(M) = \bigoplus_{n \geqq 1} \Gamma_n(M)$. Si l'on pose

$$I_n = I \cap \Gamma_n(M) \qquad \text{et} \qquad G_n(M) = \Gamma_n(M)/I_n,$$

on a donc une graduation du module G(M) sous la forme

$$G(M) = \bigoplus_{n \geqq 1} G_n(M).$$

THÉORÈME 1. — *On a*

$$\begin{cases} G_1(M) \simeq M; \\ \textit{Pour } n \geqq 2 : \\ G_n(M) = 0 \quad \textit{si } n \textit{ n'est pas une puissance de nombre premier}; \\ G_n(M) \simeq M^g_{p^h} \quad \textit{si} \quad n = p^h \quad (p, \textit{ nombre premier}). \end{cases}$$

1° *Pour* $n = 1$:

Le produit de deux éléments de $\Gamma_+(M)$ a toutes ses composantes homogènes de degrés $\geqq 2$, de sorte que $I_1 = 0$. Comme $\Gamma_1(M) \simeq M$, on a bien $G_1(M) \simeq M$.

Si l'on identifie, comme d'habitude, M à $\Gamma_1(M)$, on pourra donc écrire

$$G_1(M) = M$$

à condition de poser $\rho(x) = x$ pour $x \in M$.

2° *Pour* $n \geqq 2$, *non puissance de nombre premier :*

Il suffit de montrer que $\Gamma_n(M) \subset I_n$.

Un élément de $\Gamma_n(M)$ est une combinaison linéaire d'éléments u de la forme $x_1^{[k_1]} \ldots x_p^{[k_p]} (k_1 + \ldots + k_p = n, k_i \geqq 1)$. Si $p \geqq 2$, on a $u \in I_n$. Il suffit donc de montrer encore que, pour tout $x \in M$, on a $x^{[n]} \in I_n$.

Or, I_n contient tous les produits $x^{[r]} x^{[s]} = ((r, s)) x^{[n]}$, avec $r \geqq 1$, $s \geqq 1$ $r + s = n$ et $((r, s)) = (r+s)!/r!\,s!$; il contient donc aussi l'élément $d_n x^{[n]}$, où d_n est le p. g. c. d. des nombres $((r, s))$ précédents. Mais il est connu que, si n n'est pas une puissance de nombre premier, d_n est égal à 1. Donc $x^{[n]} \in I_n$, C. Q. F. D.

3° *Pour* $n = p^h$ *(p premier* $\geqq 2$, $h \geqq 1$) :

Il est connu qu'alors $d_n = p$. Par un raisonnement analogue à celui du 2° on peut donc déjà affirmer que :

— $G_n(M)$ est linéairement engendré par les $\rho(x^{[n]})$;

— $\rho(px^{[n]}) = p\rho(x^{[n]}) = 0$; autrement dit : *tout élément de* $G_n(M)$ *est annulé par* p.

Il en résulte qu'on peut équiper $G_n(M)$ en *module à droite*, la multiplication à droite par λ étant la multiplication à gauche par λ^n. Ce module à droite sera noté $G_n^d(M)$, tandis que pour la structure initiale de module à gauche on gardera la notation $G_n(M)$.

Pour $\lambda \in A$, désignons par $\bar{\lambda}$ sa classe modulo (p).

Considérons l'application

$$\varphi : \quad A^{d}_{p^h} \times M \to G^{d}_{n}(M)$$

définie par

$$\varphi(\bar{\lambda}, x) = \lambda\rho(x^{[n]}).$$

Cette définition a un sens, car $\lambda\rho(x^{[n]})$ ne dépend que de la classe de λ modulo (p).

• φ est linéaire en x, car :

$$\begin{aligned} -: \quad \varphi(\bar{\lambda}, x+y) &= \lambda\rho((x+y)^{[n]}) = \sum_{r+s=n} \lambda\rho(x^{[r]}y^{[s]}) \\ &= \lambda\rho(x^{[n]}) + \lambda\rho(y^{[n]}) \quad (\text{car } \rho \text{ annule } x^{[r]}y^{[s]} \text{ si } r \text{ et } s \geqq 1) \\ &= \varphi(\bar{\lambda}, x) + \varphi(\bar{\lambda}, y); \end{aligned}$$

$$-: \quad \varphi(\bar{\lambda}, \mu x) = \lambda\rho(\mu^n x^{[n]}) = \lambda\mu^n\rho(x^{[n]}) = \lambda\rho(x^{[n]})\,\mu = \varphi(\bar{\lambda}, x)\,\mu.$$

• φ est linéaire en $\bar{\lambda}$, car :

$$-: \quad \varphi(\bar{\lambda} + \bar{\mu}, x) = (\lambda + \mu)(\rho x^{[n]}) = \varphi(\bar{\lambda}, x) + \varphi(\bar{\mu}, x);$$

$$\begin{aligned} -: \quad \varphi(\bar{\lambda}\mu, x) &= \varphi(\mu^n\bar{\lambda}, x) = \varphi(\overline{\mu^n\lambda}, x) = \mu^n\lambda\rho(x^{[n]}), \\ &= \lambda\rho(x^{[n]})\,\mu = \varphi(\bar{\lambda}, x)\,\mu. \end{aligned}$$

Il en résulte une application linéaire

$$u : \quad M^{d}_{p^h} = A^{d}_{p^h} \otimes M \to G^{d}_{n}(M)$$

telle que

$$u\left(\bar{\lambda} \underset{n}{\otimes} x\right) = \lambda\rho(x^{[n]}).$$

Mais on vérifie aussi que u est linéaire à gauche :

$$u\left[\mu\left(\bar{\lambda} \underset{n}{\otimes} x\right)\right] = u\left[(\mu\bar{\lambda}) \underset{n}{\otimes} x\right] = u\left[(\overline{\mu\lambda}) \underset{n}{\otimes} x\right] = \mu\lambda\rho(x^{[n]}) = \mu u\left(\bar{\lambda} \underset{n}{\otimes} x\right).$$

Autrement dit, *u est une application linéaire de $M^{g}_{p^h}$ dans $G_n(M)$.*

Nous allons maintenant fabriquer une application en sens inverse.

Soit R une algèbre unitaire quelconque. Formons le module à gauche :

$$T^g = M^{g}_{p^h} \otimes R.$$

Comme tous les éléments de M_{p^h} sont annulés par p, il en est de même de ceux de T^g. On peut donc définir sur T^g une loi externe à droite, la multiplication à droite par λ étant la multiplication à gauche par λ^n. On obtient ainsi un module à droite T^d.

Considérons l'application

$$\psi : \quad M \times R \to T^d.$$

définie par

$$\psi(x, r) = \left(\bar{1} \underset{n}{\otimes} x\right) \otimes r^n.$$

• ψ est linéaire en x :

— : additivité évidente ;

— : $\psi(\lambda x, r) = \left(\bar{1} \underset{n}{\otimes} \lambda x\right) \otimes r^n = \lambda^n \left(\bar{1} \underset{n}{\otimes} x\right) \otimes r^n = \psi(x, r)\, \lambda.$

• ψ est linéaire en r :

— : $\psi(x, r+r') = \left(\bar{1} \underset{n}{\otimes} x\right) \otimes (r+r')^n = \left(\bar{1} \underset{n}{\otimes} x\right) \otimes r^n + \left(\bar{1} \underset{n}{\otimes} x\right) \otimes r'^n$
$= \psi(x, r) + \psi(x, r')$

on a utilisé le fait que $(r+r')^n = r^n + r'^n +$ multiple de p ;

— : $\psi(x, \lambda r) = \lambda^n \psi(x, r) = \psi(x, r)\, \lambda.$

Il en résulte une application linéaire

$$F_R : \ M \otimes R \to T^d$$

telle que

$$F_R(x \otimes r) = \left(\bar{1} \underset{n}{\otimes} x\right) \otimes r^n.$$

Plus généralement :

$$F_R(x_1 \otimes r_1 + \ldots + x_q \otimes r_q) = \sum_{k=1}^{q} \left(\bar{1} \underset{n}{\otimes} x_k\right) \otimes r_k^n.$$

Si l'on considère F_R comme une application de $M \otimes R$ dans $T^g = M^g_{ph} \otimes R$, F_R n'est plus linéaire. Cependant, si $\Theta : R \to R'$ est un homomorphisme unitaire d'algèbres, il est clair que le diagramme suivant est commutatif :

$$\begin{array}{ccc} M \otimes R & \xrightarrow{F_R} & M^g_{ph} \otimes R \\ \Big\downarrow{\scriptstyle \varepsilon_M \otimes \Theta} & & \Big\downarrow{\scriptstyle \varepsilon_N \otimes \Theta} \\ M \otimes R' & \xrightarrow{F_{R'}} & M^g_{ph} \otimes R' \end{array} \qquad (N = M^g_{ph}).$$

Autrement dit, les F_R constituent une *loi polynome* F sur le couple (M, M^g_{ph}) (*cf.* [2], p. 219). Il est clair que F est homogène de degré n ([2], p. 226). D'après ([2], th. IV-1, p. 266), il existe une application linéaire $\varphi : \Gamma_n(M) \to M^g_{ph}$ telle qu'on ait

$$F_R(x_1 \otimes r_1 + \ldots + x_q \otimes r_q) = \sum_{k_1 + \ldots + k_q = n} \varphi(x_1^{[k_1]} \ldots x_q^{[k_q]}) \otimes r_1^{k_1} \ldots r_q^{k_q}.$$

D'après l'unicité d'une telle écriture ([2], th. I-1, p. 220), on a donc :

— : $\varphi(x_1^{[k_1]} \ldots x_p^{[k_p]}) = 0$ si deux k_i au moins sont ≥ 1, autrement dit : φ s'annule sur I_n ;

— : $\varphi(x^{[n]}) = \bar{1} \underset{n}{\otimes} x.$

La première de ces assertions montre que φ se factorise en $w \circ \rho$, où w est une application linéaire de $G_n(M)$ dans M^g_{ph}, et l'on a

$$w \circ \rho(x^{[n]}) = \bar{1} \underset{n}{\otimes} x,$$

Si l'on rapproche cette formule de celle déjà établie ci-dessus :

$$u\left(\bar{1} \underset{n}{\otimes} x\right) = \rho(x^{[n]}),$$

si l'on remarque enfin que les $\rho(x^{[n]})$ engendrent linéairement $G_n(M)$ et que les $\bar{1} \underset{n}{\otimes} x$ engendrent linéairement $M^g_{p^h}$, on voit que u et w sont des isomorphismes inverses l'un de l'autre, et le théorème est démontré. Désormais, nous identifierons $G_n(M)$ et $M^g_{p^h}$, en posant

$$\rho(x^{[n]}) = \bar{1} \underset{n}{\otimes} x$$

et l'on pourra écrire

$$G(M) = M \oplus \bigoplus_{p,h} M^g_{p^h},$$

où la sommation est étendue aux nombres premiers $p \geqq 2$ et aux entiers $h \geqq 1$.

5. La PD-Algèbre $\overline{G(M)} = A \oplus G(M)$. — L'idéal I précédent est aussi un idéal de $\Gamma(M)$. On peut donc considérer l'algèbre-quotient $\overline{G(M)} = \Gamma(M)/I$.

Il est clair que le module $\overline{G(M)}$ est la somme directe de $\Gamma_0(M) = A$ et de $G(M)$:

$$\overline{G(M)} = A \oplus G(M).$$

L'anneau A est une *sous-algèbre* de $\overline{G(M)}$ et $G(M)$ est un *idéal* de $\overline{G(M)}$. De façon précise :

— le produit de deux éléments de A est le produit usuel dans A;

— le produit d'un $\lambda \in A$ par un $g \in G(M)$ est λg [multiplication scalaire dans le module $G(M)$];

— le produit de deux éléments de $G(M)$ est nul.

L'application canonique

$$\Gamma(M) = A \oplus \Gamma_+(M) \to A \oplus G(M) = \overline{G(M)}$$

est un homomorphisme d'*algèbres prégraduées* ([3], § 1). En outre, on sait que $\Gamma(M)$ est une PD-algèbre ([3], § 2 et 10). Montrons que I est un *idéal divisé* ([3], § 5).

I est l'idéal engendré dans $\Gamma(M)$ par les $x^{[p]}y^{[q]}$ ($x, y \in M$; $p, q \geqq 1$). Or, pour $n \geqq 1$, on a $\gamma_n(x^{[p]}y^{[q]}) = (x^{[p]})^n \gamma_n(y^{[q]}) \in I$, car $(x^{[p]})^n$ et $\gamma_n(y^{[q]})$ sont dans $\Gamma_+(M)$. Donc I est divisé ([3], § 5, prop. 4).

Par passage au quotient, il en résulte une *structure de* PD-*algèbre sur* l'algèbre prégraduée $\overline{G(M)}$ ([3], § 6).

Cette structure est assez intéressante; car si la multiplication dans $G(M)$ est tout à fait triviale, les puissances divisées le sont beaucoup moins.

On a vu que le module $G(M)$ est linéairement engendré par les éléments de la forme x et $\rho(x^{[p^h]})$ ($x \in M$, p premier, $h \geqq 1$). Les puissances divisées γ_n dans $\overline{G(M)}$ seront donc connues si, pour $n \geqq 0$, on connaît tous les $\gamma_n(x)$ et les $\gamma_n \circ \rho(x^{[p^h]})$.

Tous les γ_0 sont égaux à 1. Étudions donc les cas où $n \geqq 1$.

• Détermination de $\gamma_n(x)$:

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

Donc :

$\gamma_n(x) = 0$ si n n'est pas une puissance (éventuellement nulle) de nombre premier;

$\gamma_n(x) = \rho(x^{[p^h]})$ si $n = p^h$ (p premier, $h \geqq 0$).

• Détermination de $\gamma_n \circ \rho(x^{[p^k]})$ (p premier, $k \geqq 1$) :

$$\gamma_n \circ \rho(x^{[p^k]}) = \rho \circ \gamma_n(x^{[p^k]}) = [(n p^k)!/n!\,(p^k!)^n]\,\rho(x^{[np^k]}).$$

Donc, si n n'est pas une puissance (éventuellement nulle) de p, on a

$$\gamma_n \circ \rho(x^{[p^k]}) = 0.$$

Si $n = p^h$ ($h \geqq 0$), on a

$$\gamma_n \circ \rho(x^{[p^k]}) = [(n p^k)!/n!\,(p^k!)^n]\,\rho(x^{[p^{h+k}]}).$$

Dans cette expression, le coefficient numérique $(n\,p^k)!/n!\,(p^k!)^n$ peut être remplacé par tout autre entier qui lui est congru modulo p, car p annule $M_{p^{h+k}}$. Or, il est congru à 1 modulo p (*cf.*, par exemple, [2], lemme p. 343). Donc $\gamma_n \circ \rho(x^{[p^k]}) = \rho(x^{[p^{k+h}]})$.

On constate que tous ces résultats sont rassemblés dans le

THÉORÈME 2. — *Dans la* PD-*algèbre* $\overline{G(M)}$, *on a*

$$\left\{\begin{array}{l} \forall x \in M, \quad h \geqq 0, \quad k \geqq 0, \quad p \text{ premier} \geqq 2 \quad \text{et} \quad n \geqq 1 : \\ \gamma_0 \circ \rho(x^{[p^k]}) = 1 ; \\ \gamma_n \circ \rho(x^{[p^k]}) = 0 \quad \textit{si } n \textit{ n'est pas une puissance (éventuellement nulle) de } p ; \\ \gamma_{p^h} \circ \rho(x^{[p^k]}) = \rho(x^{[p^{k+h}]}). \end{array}\right.$$

En outre, pour $n \geqq 1$, *les applications* γ_n *sont additives.*

La dernière assertion précise encore la structure des puissances divisées dans $\overline{G(M)}$. Elle se vérifie immédiatement; pour $u, v \in G(M)$, on a

$$\gamma_n(u+v) = \gamma_n(u) + \gamma_n(v) + \sum_{k=1}^{n-1} \gamma_k(u)\,\gamma_{n-k}(v) ;$$

or le $\sum$ est nul, car le produit de deux éléments de $G(M)$ est nul.

III. — Les lois formelles additives.

6. PARAGRAPHE UNIQUE. — Soient deux modules M et N :

Une loi formelle F (*cf.* [2], chap. VI) sur le couple (M, N) est dite *additive*, si, m et m' désignant deux exemplaires de la loi identique sur M, on a

$$\mathrm{F}(m+m') = \mathrm{F}(m) + \mathrm{F}(m').$$

Autrement dit, pour toute algèbre R et pour z et $z' \in \mathrm{M}(\mathrm{R})$ ([2], chap. VI, § 1), on a

$$\mathrm{F}_{\mathrm{R}}(z+z') = \mathrm{F}_{\mathrm{R}}(z) + \mathrm{F}_{\mathrm{R}}(z').$$

D'une manière générale, une loi formelle $\mathrm{F} \in \mathscr{F}(\mathrm{M}, \mathrm{N})$ est décrite par une application linéaire $\varphi : \Gamma_+(\mathrm{M}) \to \mathrm{N}$ et, pour $z = x_1 \otimes r_1 + \ldots + x_q \otimes r_q \in \mathrm{M}(\mathrm{R})$ (les r_i étant nilpotents), on a la « formule de Taylor » :

$$\mathrm{F}_{\mathrm{R}}(x_1 \otimes r_1 + \ldots + x_q \otimes r_q) = \sum_{k_1+\ldots+k_q \geqq 1} \varphi(x_1^{[k_1]} \ldots x_q^{[k_q]}) \otimes r_1^{k_1} \ldots r_q^{k_q}.$$

En particulier :

$$\mathrm{F}_{\mathrm{R}}(x \otimes r) = \sum_{k \geqq 1} \varphi(x^{[k]}) \otimes r^k.$$

PROPOSITION 1. — *Pour que* F *soit additive, il faut et il suffit que* φ *s'annule sur* I.

- Nécessité : Si F est additive, on a aussi

$$\mathrm{F}_{\mathrm{R}}(x_1 \otimes r_1 + \ldots + x_q \otimes r_q) = \sum_{i=1}^{q} \mathrm{F}_{\mathrm{R}}(x_i \otimes r_i) = \sum_{i=1}^{q} \sum_{h_i \geqq 1} \varphi(x_i^{[h_i]}) \otimes r_i^{h_i}.$$

D'après l'unicité d'une telle écriture générale, on en déduit que $\varphi(x_1^{[k_1]} \ldots x_q^{[k_q]}) = 0$ si deux des k_i au moins sont $\geqq 1$. Autrement dit, φ s'annule sur I.

- Suffisance : Si φ s'annule sur I, la formule de Taylor montre que

$$\mathrm{F}_{\mathrm{R}}(x_1 \otimes r_1 + \ldots + x_q \otimes r_q) = \sum_{i=1}^{q} \sum_{k_i \geqq 1} \varphi(x_i^{[k_i]}) \otimes r_i^{k_i} = \sum_{i=1}^{q} \mathrm{F}_{\mathrm{R}}(x_i \otimes r_i),$$

C. Q. F. D.

Pour que F soit additive, il faut et suffit donc que φ se factorise en $\psi \circ \rho$, où ψ est une application (nécessairement unique) de G(M) dans N.

En particulier, l'application $\rho : \Gamma_+(\mathrm{M}) \to \mathrm{G}(\mathrm{M})$ définit une loi formelle additive sur le couple (M, G(M)), que nous notons α_{M} : nous disons que

α_M est la *loi additive canonique sur le couple* (M, G(M)). Elle se définit par additivité à partir de la formule

$$(\alpha_M)_R(x \otimes r) = x \otimes r + \sum_{p,h} \left(\overline{1} \underset{p^h}{\otimes} x \right) \otimes r^{p^h}$$

(p premier $\geqq 2$, $h \geqq 1$).

On peut donc énoncer le

Théorème 3. — *Il existe un isomorphisme bijectif entre le module des lois formelles additives sur le couple* (M, N) *et le module des applications linéaires de* G(M) *dans* N. *Si* $F \in \mathcal{F}(M, N)$ (*additive*) *et* $\psi \in \mathcal{L}(G(M), N)$ *se correspondent de cette manière, on a*

$$F = \psi \circ \alpha_M,$$

où α_M *est la loi additive canonique sur le couple* (M, G(M)).

IV. — Le module des différentielles de l'algèbre Γ(M).

7. Des remarques et un lemme. — Soient deux A-modules M et N. On désigne par $\mathcal{C}(M, N)$ le module des *lois complètes* sur le couple (M, N) (*cf.* [4]).

Soit R une algèbre unitaire et supposons, plus précisément, que N soit un module sur R. Nous savons déjà (*cf.* [4]) que $\mathcal{C}(M, R)$ peut être muni d'une structure d'algèbre unitaire sur A; nous allons montrer ici qu'on peut faire de $\mathcal{C}(M, N)$ un module sur $\mathcal{C}(M, R)$.

On peut dire que la structure de N comme R-module est définie par une application A-bilinéaire

$$\beta : \quad R \times N \to N, \qquad \text{avec} \quad \beta(r, y) = ry,$$

ou par une application A-linéaire,

$$\mu : \quad R \otimes N \to N, \qquad \text{avec} \quad \mu(r \otimes y) = ry.$$

On peut considérer β comme une loi bihomogène de bidegré (1, 1) sur le couple (R $\times$ N, N). Pour deux lois complètes

$$u \in \mathcal{C}(M, R) \quad \text{et} \quad F \in \mathcal{C}(M, N),$$

considérons alors la loi $uF \in \mathcal{C}(M, N)$ définie par

$$uF = \beta(u, F).$$

De manière explicite, pour une algèbre unitaire S et pour $z \in M(S)$, on pose

$$(uF)_S(z) = u_S(z)\, F_S(z);$$

ce dernier produit, avec $u_S(z) \in R \otimes S$ et $F_S(z) \in N \otimes S$, se calcule à partir de $u_S(z) \otimes F_S(z) \in R \otimes S \otimes N \otimes S$, en contractant $R \otimes N$ sur N par μ et $S \otimes S$ sur S par le produit dans S.

Il est tout à fait trivial de vérifier ensuite que la loi de composition externe

$$\mathcal{C}(M, R) \times \mathcal{C}(M, N) \to \mathcal{C}(M, N)$$

définie par $(u, F) \to uF$, confère à $\mathcal{C}(M, N)$ une structure de module sur $\mathcal{C}(M, R)$. Si $N = R$, on retrouve la multiplication déjà connue de $\mathcal{C}(M, R)$.

Exemple. — Supposons que $R = \Gamma(M)$ et que N soit un $\Gamma(M)$-module (donc aussi un A-module). Soit $g \in \mathcal{C}(M, N)$. On peut écrire

$$g = \varphi \circ \mathbf{e}^M,$$

où $\mathbf{e}^M$ est la loi complète universelle sur le couple $(M, \Gamma(M))$ (*cf.* [4]), et où φ est une application A-linéaire de $\Gamma(M)$ dans N.

Nous utiliserons plus loin le lemme suivant :

Lemme 1. — *En posant*

$$F = \mathbf{e}^M g$$

on a

$$F = D \circ \mathbf{e}^M,$$

où D, *application* A-*linéaire de* $\Gamma(M)$ *dans* N, *est donné par la formule*

$$D = \mu \circ (\varepsilon_{\Gamma(M)} \otimes \varphi) \circ \Delta.$$

[On rappelle que Δ est l'application diagonale $\Gamma(M) \to \Gamma(M) \otimes \Gamma(M)$ définie en [2], (p. 290), et que $\mu : \Gamma(M) \otimes N \to N$ est l'application qui définit N comme $\Gamma(M)$-module.]

En effet, soit S une algèbre unitaire et soit

$$z = x_1 \otimes s_1 + \ldots + x_p \otimes s_p \in M \otimes S \qquad (\text{les } s_i \text{ nilpotents})\,;$$

on a

$$\begin{aligned}
F_S(z) &= \Big(\sum_{h_1, \ldots, h_p} x_1^{[h_1]} \ldots x_p^{[h_p]} \otimes s_1^{h_1} \ldots s_p^{h_p}\Big)\Big(\sum_{k_1, \ldots, k_p} \varphi(x_1^{[k_1]} \ldots x_p^{[k_p]}) \otimes s_1^{k_1} \ldots s_p^{k_p}\Big) \\
&= \sum_{n_1, \ldots, n_p} \mu \circ (\varepsilon_{\Gamma(M)} \otimes \varphi)\Big(\sum_{h_1+k_1=n_1} \cdots \sum_{h_p+k_p=n_p} x_1^{[h_1]} \ldots x_p^{[h_p]} \otimes x_1^{[k_1]} \ldots x_p^{[k_p]}\Big) \otimes s_1^{n_1} \ldots s_p^{n_p} \\
&= \sum_{n_1, \ldots, n_p} \mu \circ (\varepsilon_{\Gamma(M)} \otimes \varphi) \circ \Delta(x_1^{[n_1]} \ldots x_p^{[n_p]}) \otimes s_1^{n_1} \ldots s_p^{n_p}.
\end{aligned}$$

Donc,

$$F = \mu \circ (\varepsilon_{\Gamma(M)} \otimes \varphi) \circ \Delta \circ \mathbf{e}^M.$$

C. Q. F. D.

8. Les dérivations et le module des différentielles d'une algèbre. — Soient R une algèbre, N un R-module. On appelle *A-dérivation de* R *dans* N une application $D : R \to N$ telle que :

a. D est A-linéaire;

b. $\forall r, s \in R : D(rs) = r\,D(s) + s\,D(r)$.

Si P est un R-module et si $\psi : N \to P$ est R-linéaire, alors $\psi \circ D$ est une A-dérivation de R dans P.

Il est connu (*cf.* par exemple [1]) qu'on peut associer à toute algèbre R un R-module $\mathcal{D}(R)$ et une application $d : R \to \mathcal{D}(R)$, de telle sorte que :

1° d est une A-dérivation;

2° toute A-dérivation de R dans un R-module N se factorise de manière *unique* sous la forme $D = u \circ d$, où u est une application R-linéaire de $\mathcal{D}(R)$ dans N.

Les conditions 1°, 2° déterminent le couple $(\mathcal{D}(R), d)$ à un isomorphisme près.

Le R-module $\mathcal{D}(R)$ s'appelle le *module des* A-*différentielles* de l'algèbre R, et d est *l'application différentielle* de R dans $\mathcal{D}(R)$. On dit que $d(r)$ est la A-différentielle de r.

On trouve dans la littérature, par exemple dans [1], une construction devenue classique de $\mathcal{D}(R)$. Ici, nous en donnerons une autre pour l'algèbre $\Gamma(M)$, qui permettra de l'expliciter entièrement.

9. Les A-dérivations et le module des différentielles de l'algèbre $\Gamma(M)$. — Soit M un module. Nous notons par m et m' les deux projections canoniques du module $M \times M$ sur M; nous notons aussi par γ et γ' les deux projections canoniques de $\Gamma(M) \times \Gamma(M)$ sur $\Gamma(M)$.

Lemme 2. — *Soit* N *un* $\Gamma(M)$-*module. Pour qu'une application* A *linéaire* $D : \Gamma(M) \to N$ *soit une* A-*dérivation, il faut et il suffit que, dans le module* $\mathcal{C}(\Gamma(M) \times \Gamma(M), N)$ *considéré comme module sur* $\mathcal{C}(\Gamma(M) \times \Gamma(M), \Gamma(M))$, *on ait la relation*

$$D(\gamma\gamma') = \gamma\,D(\gamma') + \gamma'\,D(\gamma).$$

En effet, chacun des deux membres représente une loi bilinéaire sur le couple $(\Gamma(M) \times \Gamma(M), N)$. Pour que ces lois soient égales, il faut et il suffit que leurs restrictions au module $\Gamma(M) \times \Gamma(M)$ coïncident, c'est-à-dire que D soit une dérivation.

Lemme 3. — *Pour qu'une application* A-*linéaire* $D : \Gamma(M) \to N$ *soit une* A-*dérivation, il faut et il suffit que, dans le module* $\mathcal{C}(M \times M, N)$ *considéré comme module sur* $\mathcal{C}(M \times M, \Gamma(M))$, *on ait la relation*

$$D(\mathbf{e}^{M}(m)\,\mathbf{e}^{M}(m')) = \mathbf{e}^{M}(m).D(\mathbf{e}^{M}(m')) + \mathbf{e}^{M}(m').D(\mathbf{e}^{M}(m)).$$

• Nécessité : Elle découle du lemme 2, où l'on compose γ avec $\mathbf{e}^{\mathrm{M}}(m)$ et γ' avec $\mathbf{e}^{\mathrm{M}}(m')$.

• Suffisance : En égalant dans les deux membres la composante bihomogène de bidegré (p, q), il vient

$$\mathrm{D}(m^{[p]}m'^{[q]}) = m^{[p]}.\mathrm{D}(m'^{[q]}) + m'^{[q]}.\mathrm{D}(m^{[p]}).$$

Composons m avec $m_1 + \ldots + m_r$ et m' avec $m'_1 + \ldots + m'_s$, où les m_i et m'_j sont les projections canoniques de M^r et M^s sur M, et prenons la composante multihomogène de multidegré $(h_1, \ldots, h_r; k_1, \ldots, k_s)$ (avec $h_1 + \ldots + h_r = p$ et $k_1 + \ldots + k_s = q$). Il vient, en posant

$$u = m_1^{[h_1]} \ldots m_r^{[h_r]} \qquad \text{et} \qquad v = m_1'^{[k_1]} \ldots m_s'^{[k_s]} :$$
$$\mathrm{D}(uv) = u\,\mathrm{D}(v) + v\,\mathrm{D}(u).$$

Si l'on compose enfin, dans cette égalité des lois polynomes, chaque m_i (resp. m'_j) par un élément x_i (resp. y_j) de M, on obtient une relation qui montre que D est une dérivation.

Proposition 2. — *Soient* M *un module et* N *un* $\Gamma(\mathrm{M})$-*module. Pour une application* A-*linéaire* $\mathrm{D} : \Gamma(\mathrm{M}) \to \mathrm{N}$, *posons* $\mathrm{F}(m) = \mathrm{D} \circ \mathbf{e}^{\mathrm{M}}(m)$ *et* $g(m) = \mathbf{e}^{\mathrm{M}}(-m)\,\mathrm{F}(m)$, *de sorte qu'aussi* $\mathrm{F}(m) = \mathbf{e}^{\mathrm{M}}(m)\,g(m)$. *Alors, pour que* D *soit une dérivation, il faut et il suffit que* $g(m)$ *soit une loi formelle additive.*

La formule du lemme 3 s'écrit en effet

$$\mathrm{F}(m + m') = \mathbf{e}^{\mathrm{M}}(m)\,\mathrm{F}(m') + \mathbf{e}^{\mathrm{M}}(m')\,\mathrm{F}(m).$$

Si l'on multiplie chaque membre par $\mathbf{e}^{\mathrm{M}}(-m-m') = \mathbf{e}^{\mathrm{M}}(-m)\,\mathbf{e}^{\mathrm{M}}(-m')$, on obtient la formule équivalente

$$g(m + m') = g(m) + g(m').$$

On voit que g est une loi formelle en composant m et m' avec o, ce qui donne $g(\mathrm{o}) = \mathrm{o}$, et que dès lors g est une loi formelle additive,

C. Q. F. D.

D'après le théorème 3 du présent article, une loi formelle g sur le couple (M, N) est additive si et seulement si elle est de la forme $\varphi \circ q \circ \mathbf{e}^{\mathrm{M}}$, où φ est une application A-linéaire de G(M) dans N et où q est l'application linéaire de $\Gamma(\mathrm{M})$ sur G(M) qui s'annule sur A et qui coïncide avec ρ sur $\Gamma_+(\mathrm{M})$.

D'après le lemme 1 ci-dessus, on voit que l'application $\mathrm{D} : \Gamma(\mathrm{M}) \to \mathrm{N}$ est une A-dérivation si et seulement si elle est de la forme

$$\mathrm{D} = \mu \circ (\varepsilon_{\Gamma(\mathrm{M})} \otimes \varphi) \circ (\varepsilon_{\Gamma(\mathrm{M})} \otimes q) \circ \Delta.$$

Posons

$$d = (\varepsilon_{\Gamma(\mathrm{M})} \otimes q) \circ \Delta.$$

C'est une application A-linéaire de $\Gamma(M)$ dans $\Gamma(M)\otimes G(M)$. Posons aussi $\Phi=\mu\circ(\varepsilon_{\Gamma(M)}\otimes\varphi)$; Φ est l'application A-linéaire de $\Gamma(M)\otimes G(M)$ dans N définie par $\Phi(\gamma\otimes g)=\gamma\varphi(g)$. On voit que Φ est aussi $\Gamma(M)$-linéaire, si l'on fait de $\Gamma(M)\otimes G(M)$ un module sur $\Gamma(M)$ de manière évidente.

Ainsi, pour une dérivation D de $\Gamma(M)$ dans N, on a $D=\Phi\circ d$, où Φ est une application $\Gamma(M)$-linéaire de $\Gamma(M)\otimes G(M)$ dans N.

Réciproquement, soit Φ une application $\Gamma(M)$-linéaire de $\Gamma(M)\otimes G(M)$ dans N. Définissons $\varphi: G(M)\to N$ par $\varphi(g)=\Phi(1\otimes g)$; alors, φ est A-linéaire et l'on a $\Phi=\mu\circ(\varepsilon_{\Gamma(M)}\otimes\varphi)$. Si l'on définit D par $D=\Phi\circ d$, on voit que D est une dérivation. De façon plus précise, on a

$$D\circ \mathbf{e}^{M}(m)=\mathbf{e}^{M}(m)\,g(m),\qquad \text{où}\quad g(m)=\varphi\circ q\circ\mathbf{e}^{M}(m).$$

Supposons qu'on ait aussi $D=\Phi'\circ d$, avec $\Phi':\Gamma(M)\otimes G(M)\to N$ et $\Gamma(M)$-linéaire; définissons $\varphi': G(M)\to N$ par $\varphi'(g)=\Phi'(1\otimes g)$. Alors on aura aussi $D\circ\mathbf{e}^{M}(m)=\mathbf{e}^{M}(m)\,g'(m)$, avec $g'(m)=\varphi'\circ q\circ\mathbf{e}^{M}(m)$. De là il résulte successivement

$$\mathbf{e}^{M}(m)\,g(m)=\mathbf{e}^{M}(m)\,g'(m);\qquad g(m)=g'(m);$$
$$\varphi'\circ q=\varphi\circ q;\qquad \varphi=\varphi';\qquad \Phi=\Phi'.$$

Ainsi, pour que D soit une dérivation, il faut et il suffit que D soit de la forme $\Phi\circ d$, où Φ est une application $\Gamma(M)$-linéaire définie sur $\Gamma(M)\otimes G(M)$; en outre, un tel Φ est unique.

En particulier, d est une dérivation de $\Gamma(M)$ dans $\Gamma(M)\otimes G(M)$.

En vertu des résultats rappelés au paragraphe précédent, on peut donc énoncer le

THÉORÈME 4. — *Le module des* A-*différentielles de l'algèbre* $\Gamma(M)$ *est le module* $\mathcal{D}(\Gamma(M))=\Gamma(M)\otimes G(M)$. *L'application différentielle* $d:\Gamma(M)\to\mathcal{D}(\Gamma(M))$ *est définie par la relation*

$$d=(\varepsilon_{\Gamma(M)}\otimes q)\circ\Delta,$$

où Δ *est l'application diagonale et où* q *est l'application linéaire de* $\Gamma(M)$ *sur* $G(M)$ *qui s'annule sur* A *et coïncide avec* ρ *sur* $\Gamma_{+}(M)$.

Soit N *un* $\Gamma(M)$-*module. Il existe une correspondance bijective entre l'ensemble des* A-*dérivations* D *de* $\Gamma(M)$ *dans* N *et l'ensemble des applications* A-*linéaires* φ *de* $G(M)$ *dans* N. *Si* D *et* φ *se correspondent de cette manière, on a*

$$D=\mu\circ(\varepsilon_{\Gamma(M)}\otimes\varphi)\circ d,$$

où $\mu:\Gamma(M)\otimes N\to N$ *est l'application qui définit* N *comme* $\Gamma(M)$-*module.*

10. EXPRESSION DES DIFFÉRENTIELLES DANS $\Gamma(M)$. — Comme $\Gamma(M)$ est engendrée algébriquement par les $x^{[n]}$ ($x\in M$, $n\geq 0$), l'application

différentielle $d : \Gamma(M) \to \Gamma(M) \otimes G(M)$ sera explicitée dès qu'on aura explicité $d(x^{[n]})$. Nous supposons $n \geqq 1$, car $d(1) = 0$.

On a

$$\Delta(x^{[n]}) = \sum_{k=0}^{n} x^{[n-k]} \otimes x^{[k]},$$

d'où

$$d(x^{[n]}) = \sum_{k=1}^{n} x^{[n-k]} \otimes \rho(x^{[k]}).$$

Finalement

PROPOSITION 3. — *A la décomposition*

$$\mathcal{D}(\Gamma(M)) = (\Gamma(M) \otimes M) \oplus \bigoplus_{p,h} (\Gamma(M) \otimes M^g_{p^h})$$

(p premier, $h \geqq 1$), correspond pour $n \geqq 1$ la formule

$$d(x^{[n]}) = (x^{[n-1]} \otimes x) + \sum_{p^h \leqq n} x^{[n-p^h]} \otimes \binom{\bar{1} \otimes x}{p^h}.$$

Remarque. — Définissons les applications

$$d_1 : \quad M \to \Gamma(M) \otimes M \qquad \text{et} \qquad d_{p^h} : \quad M \to \Gamma(M) \otimes M^g_{p^h}$$

par

$$d_1(x) = 1 \otimes x \qquad \text{et} \qquad d_{p^h}(x) = 1 \otimes \binom{\bar{1} \otimes x}{p^h}.$$

Alors on a

$$d(x^{[n]}) = x^{[n-1]} d_1(x) + \sum_{p^h \leqq n} x^{[n-p^h]} d_{p^h}(x).$$

BIBLIOGRAPHIE.

[1] Y. NAKAI, *On the theory of differentials in commutative rings* (*J. Math. Soc. Japan*, vol. 13, nº 1, 1961).

[2] N. ROBY, *Lois polynomes et lois formelles en théorie des modules* (*Ann. scient. Éc. Norm. Sup.*, fasc. 3, 1963, p. 213).

[3] N. ROBY, *Les algèbres à puissances divisées* (*Bull. Sc. math.*, 2e série, t. 89, 1965, p. 75 à 91).

[4] N. ROBY, *Sur les lois complètes et les algèbres de puissances divisées* (*Boletim da Sociedade de Matematica de São-Paulo*, vol. 18, fasc. 1 e 2, dez. 1966).