REDACTION CHEVALLEY

Rédaction n° 045

Nombre de pages : 29

Nombre de feuilles : 29

A 45 2

RÉDACTION CHEVALLEY

§1. ANNEAUX SUR UN CORPS Etat 4

n° 1. APPLICATIONS MULTILINÉAIRES

Nous avons déjà défini la notion de forme bilinéaire sur le produit de deux espaces vectoriels. Nous allons maintenant généraliser cette notion en définissant les applications multilinéaires d'un produit de plusieurs espaces vectoriels dans un espace vectoriel.

Définition 1. Soit $(V_\iota)_{\iota\in I}$ une famille finie d'espaces vectoriels ayant tous le même corps de base K, que nous supposons commutatif. Si $\iota\in I$, $(y_K)\in\prod_{K\in I,K\neq\iota}V_K$, nous désignons par $H_{\iota,(y_K)}$ l'application de V_ι dans $\prod_{\iota\in I}V_\iota$ qui fait correspondre à tout $x\in V_\iota$ l'élément de $\prod_{\iota\in I}V_\iota$ dont la ι-coordonnée est x et dont la K-coordonnée est y_K si $K\neq\iota$. Soit W un espace vectoriel sur K ; une application γ de $\prod_{\iota\in I}V_\iota$ dans W est dit multilinéaire si, pour tout $\iota\in I$ et tout $(y_K)\in\prod_{K\in I,K\neq\iota}V_K$, l'application $\gamma\circ H_{\iota,(y_K)}$ de V_ι dans W est linéaire.

Dans le cas où I ne contient qu'un seul élément, cette notion se réduit à celle d'application linéaire. Par contre, si I possède plus d'un seul élément, une application multilinéaire de $\prod_{\iota\in I}V_\iota$ n'est en général pas une application linéaire de la structure d'espace vectoriel de $\prod_{\iota\in I}V_\iota$. Si I contient deux éléments (resp.: trois éléments), une application multilinéaire du produit d'une famille d'espaces vectoriels ayant I pour ensemble d'indices est appelée une application bilinéaire (resp.: trilinéaire). Dans le cas où I a deux éléments et où W est le corps de base K lui-même (considéré comme espace vectoriel sur K), on retrouve la notion de forme bilinéaire définie plus haut.

Proposition 1. Soit $(V_\iota)_{\iota\in I}$ une famille finie d'espaces vectoriels ayant ayant tous le même corps de base K, que nous supposons commutatif, et soit γ une application multilinéaire de $\prod_{\iota\in I}V_\iota$ dans un espace

vectoriel W sur K . Donnons-nous, pour chaque $\iota \in I$, une famille finie $(u_{\iota,k})_{1 \leqslant k \leqslant n_\iota}$ d'éléments de V_ι et une famille finie $(a_{\iota,k})_{1 \leqslant k \leqslant n_\iota}$ d'éléments de K ; posons $x_\iota = \sum_{k=1}^{n_\iota} a_{\iota,k} u_{\iota,k}$. On a alors

$$(1) \qquad \gamma((x_\iota)) = \sum_{\alpha \in A} \Big(\prod_{\iota \in I} a_{\iota,\alpha(\iota)}\Big) \gamma((u_{\iota,\alpha(\iota)}))$$

où A est l'ensemble des applications α de I dans l'ensemble $\mathbb{N}$ des entiers positifs telles que $1 \leqslant \alpha(\iota) \leqslant n_\iota$ pour tout $\iota \in I$.

Soit I' une partie quelconque de I , et soit A(I') l'ensemble des applications α' de I' dans $\mathbb{N}$ telles que $1 \leqslant \alpha'(\iota) \leqslant n_\iota$ pour tout $\iota \in I'$. Nous démontrerons par récurrence sur le nombre m d'éléments de I' que l'on a

$$(2) \qquad \gamma((x_\iota)) = \sum_{\alpha' \in A(I')} \Big(\prod_{\iota \in I'} a_{\iota,\alpha'(\iota)}\Big) \gamma(X_{\alpha'})$$

où $X_{\alpha'}$ est l'élément de $\prod_{\iota \in I} V_\iota$ dont la ι-coordonnée est $u_{\iota,\alpha'(\iota)}$ si $\iota \in I'$, mais x_ι si $\iota \notin I'$. La formule est triviale si $m = 0$. Supposons que $m > 0$ et que (2) soit vraie pour toutes les parties ayant moins de m éléments. Soit K un élément de I' et soit I" l'ensemble des éléments de I' distincts de K . On a donc

$$\gamma((x_\iota)) = \sum_{\alpha'' \in A(I'')} \Big(\prod_{\iota \in I''} a_{\iota,\alpha''(\iota)}\Big) \gamma(X_{\alpha''})$$

On a $x_K = \sum_{k=1}^{n_K} a_{K,k} u_{K,k}$, d'où, en vertu de la multilinéarité de γ , $\gamma(X_{\alpha''}) = \sum_{k=1}^{n_K} a_{K,k} \gamma(X_{\alpha'',k})$, où $X_{\alpha'',k}$ est l'élément de $\prod_{\iota \in I} V_\iota$ dont la ι-coordonnée est $u_{\iota,\alpha''(\iota)}$ si $\iota \in I''$, $u_{K,k}$ si $\iota = K$, x_ι si $\iota \notin I'$. On a donc

$$(3) \qquad \gamma((x_\iota)) = \sum_{\alpha'' \in A(I''),\, 1 \leqslant k \leqslant n_K} \Big(\prod_{\iota \in I''} a_{\iota,\alpha''(\iota)}\Big) a_{K,k} \gamma(X_{\alpha'',k})$$

Or, à toute paire $(\alpha'',k) \in A(I'') \times [1,n_K]$ on peut faire correspondre l'élément $\alpha' \in A(I')$ qui prolonge α'' et qui applique K sur k ; on obtient ainsi une application bi-univoque de $A(I'') \times [1,n_K]$ sur A(I'). De plus, si α' correspond à (α'',k) , on a

$$\Big(\prod_{\iota \in I''} a_{\iota,\alpha''(\iota)}\Big) a_{K,k} = \prod_{\iota \in I'} a_{\iota,\alpha'(\iota)} \quad ; \quad X_{\alpha'',k} = X_{\alpha'}$$

et la formule (3) devient la formule (2), qui se trouve ainsi démontrée pour I' . Cette formule est donc vraie pour toute partie I' de I . Prenant I'=I , on obtient la formule (1) .

Proposition 2.- Soit $(V_\iota)_{\iota\in I}$ une famille finie d'espaces vectoriels ayant tous le même corps de base K , que nous supposons commutatif, et soit W un espace vectoriel sur K . Donnons-nous, pour chaque $\iota\in I$, une base B_ι de V_ι . Toute application dans W de l'ensemble $\prod_{\iota\in I} B_\iota$ peut alors d'une manière et d'une seule se prolonger par une application multilinéaire de $\prod_{\iota\in I} V_\iota$ dans W .

Posons $B = \prod_{\iota\in I} B_\iota$, et désignons par γ_0 une application de B dans W . Si (x_ι) est un élément quelconque de $\prod_{\iota\in I} V_\iota$, nous pouvons exprimer chaque x_ι comme combinaison linéaire des éléments de B_ι , soit $x_\iota = \sum_{u_\iota\in B_\iota} a(x_\iota,u_\iota)u_\iota$; si $u=(u_\iota)\in B$, nous poserons $a((x_\iota),u) = \prod_{\iota\in I} a(x_\iota,u_\iota)$. Pour chaque $u_\iota\in B_\iota$, l'application $x_\iota \longrightarrow a(x_\iota,u_\iota)$ est une forme linéaire sur V_ι . Soit ι un élément déterminé de I , et soit (y_K) un élément de $\prod_{K\in I, K\neq\iota} V_K$; utilisant les notations de la définition 1, nous voyons tout de suite que, si $u=(u_\iota)\in B$, l'application

$$x_\iota \longrightarrow a(H_{\iota,(y_K)}(x_\iota),u) = \prod_{K\in I, K\neq\iota} a(y_K,u_K)\cdot a(x_\iota,u_\iota)$$

de V_ι dans K est linéaire ; il en résulte que l'application $(x_\iota)\longrightarrow a((x_\iota),u)$ de $\prod_{\iota\in I} V_\iota$ dans K est multilinéaire. D'autre part, pour un (x_ι) déterminé, l'application $u_\iota \longrightarrow a(x_\iota,u_\iota)$ de B_ι dans K est nulle à l'infini (cf. §2,n°2), d'où il résulte aisément que l'application $u\longrightarrow a((x_\iota),u)$ de B dans K est nulle à l'infini. Nous pouvons donc définir un élément $\gamma((x_\iota))\in W$ par la formule $\gamma((x_\iota)) = \sum_{u\in B} a((x_\iota),u)\gamma_0(u)$; il résulte de ce que nous avons dit plus haut que γ est multilinéaire ; par ailleurs, il est évident que γ prolonge γ_0 . Le fait qu'il n'existe qu'une seule application multilinéaire de $\prod_{\iota\in I} V_\iota$ dans W qui prolonge γ_0 résulte immédiatement de la proposition 1 .

n° 2. ANNEAUX DE MONOIDES.

Définition 2.- Soit K un corps commutatif. On entend par anneau sur le corps K un anneau à opérateurs σ admettant K comme domaine d'opérateurs et qui satisfait à la condition suivante : le groupe additif à opérateurs formé par les éléments de σ (avec K comme domaine d'opérateurs) est un espace vectoriel sur K .

Les notions de sous-anneau, d'anneau quotient, d'idéal (à gauche, à droite, ou bilatère) s'appliquent en particulier aux anneaux sur un corps K . Tout idéal dans un anneau sur K est un espace vectoriel sur K .

Si σ est un anneau sur K , l'application $(x,y) \to xy$ est évidemment une application bilinéaire de la structure d'espace vectoriel de $\sigma \times \sigma$ dans celle de σ .

Nous allons maintenant indiquer un procédé qui permet, étant donnés un monoïde quelconque et un corps commutatif, de construire un anneau sur le corps K .

Définition 3.- Soient M un monoïde et K un corps commutatif. On dit qu'un anneau σ sur le corps K est un anneau du monoïde M sur le corps K s'il existe une base B de la structure d'espace vectoriel de σ qui satisfait aux conditions suivantes : 1) B est stable par rapport à la multiplication dans σ ; 2) la restriction à $B \times B$ de la multiplication dans σ définit sur B une structure de monoïde isomorphe à M .

Nous allons montrer qu'étant donnés un monoïde M et un corps commutatif K , il est toujours possible de construire un anneau de M sur K . Formons l'espace vectoriel V des applications nulles à l'infini de M dans K . Si $\lambda \in M$, désignons par φ_λ l'application de M dans K définie par $\varphi_\lambda(\lambda) = e$ (l'élément unité de K), $\varphi_\lambda(\lambda') = 0$ si $\lambda' \neq \lambda$. Si $\varphi \in V$, on a $\varphi = \sum_{\lambda \in M} \varphi(\lambda)\varphi_\lambda$, d'où il résulte que l'application $\lambda \longrightarrow \varphi_\lambda$ applique M bi-univoquement sur une base B_0 de V . Il existe une application bilinéaire $(\varphi, \psi) \to \varphi\psi$ de $V \times V$ dans V qui prolonge

l'application $(\varphi_\lambda , \varphi_\mu) \to \varphi_{\lambda\mu}$ de $B_0 \times B_0$ dans V ; cette application bilinéaire définit une multiplication dans V .

La restriction à $B_0 \times B_0$ de la multiplication dans V applique $B_0 \times B_0$ dans B_0 et définit sur B_0 une structure de monoïde isomorphe à M . Il ne reste donc plus qu'à faire voir que la multiplication dans V est associative. Les applications $(\varphi , \psi , \theta) \to (\varphi\psi)\theta$ et $(\varphi , \psi , \theta) \to \varphi(\psi\theta)$ de $V \times V \times V$ dans V sont visiblement trilinéaires ; la multiplication dans M étant associative, ces deux applications coïncident l'une avec l'autre sur $B_0 \times B_0 \times B_0$, donc aussi partout en vertu de la proposition 2, n°1, ce qui complète la démonstration de notre assertion. Soit $\mathcal{O}_0$ l'anneau de H sur K que nous venons de construire, et soit $\mathcal{O}$ un anneau quelconque de M sur K ; nous allons démontrer que $\mathcal{O}$ est isomorphe à $\mathcal{O}_0$. Soit B une base de la structure d'espace vectoriel de $\mathcal{O}$ qui satisfasse les conditions de la définition 3 . Il existe alors une application bi-univoque $\varphi \to x_\varphi$ de B_0 sur B telle que $x_{\varphi\psi} = x_\varphi x_\psi$ pour tout $(\varphi , \psi) \in B_0 \times B_0$. Cette application peut se prolonger par un isomorphisme J de la structure d'espace vectoriel de $\mathcal{O}_0$ sur celle de $\mathcal{O}$. Les applications $(\varphi\psi) \to J(\varphi\psi)$ et $(\varphi , \psi) \to J(\varphi)J(\psi)$ de $\mathcal{O}_0 \times \mathcal{O}_0$ dans $\mathcal{O}$ sont visiblement bilinéaires et coïncident l'une avec l'autre sur $B_0 \times B_0$; elles coïncident donc partout, ce qui prouve que J est un isomorphisme de la structure d'anneau de $\mathcal{O}_0$ sur celle de $\mathcal{O}$.

Soit $\mathcal{O}$ un anneau d'un monoïde M sur un corps K , et soit B une base de $\mathcal{O}$ qui satisfasse aux conditions de la définition 3 . Supposons M commutatif ; dans ce cas, les applications bilinéaires $(x,y) \to xy$ et $(x,y) \to yx$ de $\mathcal{O} \times \mathcal{O}$ dans $\mathcal{O}$ coïncident sur $B \times B$, donc partout, ce qui prouve que $\mathcal{O}$ est commutatif. Supposons maintenant que M possède

un élément unité u , et soit x_u l'élément de B qui correspond à u ; les applications linéaires $x \to x$, $x \to x_u x$ et $x \to x x_u$ de $\mathcal{O}$ dans lui-même coïncident les unes avec les autres sur B , donc aussi partout, ce qui montre que x_u est élément unité de $\mathcal{O}$. Nous avons donc démontré la

Proposition 3.- Soient M un monoïde et K un corps commutatif. On peut alors construire un anneau du monoïde M sur le corps K , soit $\mathcal{O}$. Tout anneau de M sur K est isomorphe à $\mathcal{O}$. Si M est commutatif, il en est de même de $\mathcal{O}$. Si M possède un élément unité, il en est de même de $\mathcal{O}$.

§ 2. ANNEAUX DE POLYNOMES.

n° 1. DÉFINITION.

Nous aurons principalement à considérer dans ce qui suit des anneaux qui possèdent un élément unité. C'est pourquoi nous définissons de la manière suivante la notion de système de générateurs d'un sous-anneau d'un anneau à opérateurs :

Définition 1.- Soit $\mathcal{O}$ un anneau à opérateurs qui possède un élément unité ε, et soit S une partie de $\mathcal{O}$. Le plus petit sous-anneau $\mathcal{O}'$ de $\mathcal{O}$ contenant les éléments de S et ε est appelé le sous-anneau engendré par S ; on dit aussi que S est un ensemble de générateurs de $\mathcal{O}'$.

L'existence de l'anneau $\mathcal{O}'$ résulte tout de suite du fait que l'intersection de toute famille de sous-anneaux de $\mathcal{O}$ est un sous-anneau.

Ceci posé, considérons un anneau $\mathcal{O}$ sur un corps (commutatif) K et une suite finie $(x_1,\dots,x_n)$ d'éléments de $\mathcal{O}$; nous supposerons que $\mathcal{O}$ possède un élément unité et que $x_1,\dots,x_n$ commutent les uns avec les autres. Soit $\mathcal{O}'$ le sous-anneau de $\mathcal{O}$ engendré par $x_1,\dots,x_n$; nous nous proposons de montrer comment l'on peut construire les éléments de $\mathcal{O}'$. L'anneau $\mathcal{O}'$ contient tout d'abord tous les éléments de la forme $x_1^{k_1}\dots x_n^{k_n}$, où $(k_1,\dots,k_n)\in N^n$ (rappelons que x_i^0 est l'élément unité de $\mathcal{O}$), puis aussi toutes les combinaisons linéaires

$$\sum_{(k_1,\dots,k_n)\in N^n} a(k_1,\dots,k_n)\, x_1^{k_1}\dots x_n^{k_n}$$

des éléments $x_1^{k_1}\dots x_n^{k_n}$ (a représente donc, dans la formule précédente, une application nulle à l'infini de N^n dans K). Soit $\mathcal{O}'_1$ l'ensemble de ces combinaisons linéaires ; nous allons montrer que $\mathcal{O}'_1 = \mathcal{O}'$. Il est clair que $\mathcal{O}'_1$ est un sous-espace de la structure d'espace vectoriel de $\mathcal{O}'$. D'autre part, puisque $x_1,\dots,x_n$ commutent entre eux, on a $(x_1^{k_1}\dots x_n^{k_n})\,.\,(x_1^{l_1}\dots x_n^{l_n}) = x_1^{k_1+l_1}\dots x_n^{k_n+l_n}$. L'application $(x,y)\to xy$ de $\mathcal{O}\times\mathcal{O}$ dans $\mathcal{O}$ étant bilinéaire, il résulte alors immédiatement de la proposition, §1, n°1 que $\mathcal{O}'_1\mathcal{O}'_1\subset\mathcal{O}'_1$, donc que $\mathcal{O}'_1$ est un sous-anneau de $\mathcal{O}$.

L'élément unité de $\mathcal{O}$ peut s'écrire $x_1^0 \ldots x_n^0$ et appartient par suite à $\mathcal{O}_1'$; par ailleurs, si $(k_1,..,k_n)$ est l'élément de $\mathbb{N}^n$ défini par $k_j=0$ pour $j \neq i$, $k_i=1$, on a $x_i = x_1^{k_1} \ldots x_n^{k_n} \in \mathcal{O}_1'$; on voit donc que $\mathcal{O}_1' = \mathcal{O}'$.

Définition 2.- Soient $\mathcal{O}$ un anneau sur un corps K , et $x_1,..,x_n$ des éléments de $\mathcal{O}$. Supposons que $\mathcal{O}$ possède un élément unité et que $x_1,\ldots,x_n$ commutent entre eux. Le sous-anneau de $\mathcal{O}$ engendré par $x_1,\ldots,x_n$ se désigne alors par $K\left[x_1,..,x_n\right]$.

On observera que la notation $K\left[x_1,\ldots,x_n\right]$ n'indique pas l'anneau dont $K\left[x_1,\ldots,x_n\right]$ est un sous-anneau ; on n'emploiera donc cette notation que s'il n'y a pas d'ambiguité possible sur $\mathcal{O}$.

Il résulte de ce que nous avons dit plus haut que tout élément x de $K\left[x_1,..,x_n\right]$ peut se mettre sous la forme

$$x = \sum_{(k_1,\ldots,k_n)\in \mathbb{N}^n} a(k_1,..,k_n) x_1^{k_1} \ldots x_n^{k_n}$$

où a est une application nulle à l'infini de $\mathbb{N}^n$ dans K . Donner une application a pour laquelle la formule (1) soit vraie, cela s'appelle exprimer algèbriquement x au moyen de $x_1,\ldots,x_n$.

Définition 3.- Soient $\mathcal{O}$ un anneau sur un corps K et $x_1,\ldots,x_n$ des éléments de $\mathcal{O}$. Supposons que $\mathcal{O}$ possède un élément unité et que $x_1,..,x_n$ commutent les uns avec les autres. On entend par relation algèbrique entre $x_1,..,x_n$ toute formule vraie de la forme

$$\sum_{(k_1,\ldots,k_n)\in \mathbb{N}^n} a(k_1,\ldots,k_n) x_1^{k_1} \ldots x_n^{k_n} = 0$$

où a est une application nulle à l'infini de $\mathbb{N}^n$ dans K . Les éléments $a(k_1,..,k_n)$ sont appelés les coefficients de la relation en question. Si tous ces coefficients sont nuls, on dit que la relation est triviale. Si la seule relation algèbrique qui existe entre $x_1,\ldots,x_n$ est la relation triviale, on dit que $x_1,..,x_n$ sont algèbriquement indépendants sur K . Si n=1, on dit que x_1 est transcendant par rapport à K .

Supposons les éléments $x_1,\ldots,x_n$ algèbriquement indépendants sur K .

L'application $(k_1,\ldots,k_n) \longrightarrow x_1^{k_1}\ldots x_n^{k_n}$ applique alors N^n bi-univoquement sur une base de $\mathcal{O}$. Définissons une structure de monoïde sur N^n au moyen de la loi de composition (notée additivement) définie par la formule

$$(k_1,..,k_n) + (l_1,\ldots,l_n) = (k_1+l_1,\ldots,k_n+l_n)$$

On voit alors, que, si $x_1,\ldots,x_n$ sont algèbriquement indépendants sur K, $K\left[x_1,\ldots,x_n\right]$ est un anneau du monoïde N^n sur K.

Soit inversement P un anneau de N^n sur K, et soit B une base de la structure d'espace vectoriel de P telle que la restriction à $B\times B$ de la multiplication dans P définisse sur B une structure de monoïde isomorphe à N^n. Désignons par $\mathfrak{b}_i$ l'élément de N^n dont la i-ième coordonnée est 1, toutes les autres coordonnées étant 0 ; on voit alors tout de suite que $(k_1,\ldots,k_n) = \sum_{i=1}^{n} k_1\,\mathfrak{b}_i$ pour tout $(k_1,..,k_n)\in N^n$. Soit X_i l'élément de B qui correspond à $\mathfrak{b}_i$; l'élément de B qui correspond à $(k_1,..,k_n)$ est alors $X_1^{k_1}\ldots X_n^{k_n}$. L'anneau P est commutatif ; les éléments $X_1,\ldots,X_n$ y sont algèbriquement indépendants et on a $P = K\left[X_1,\ldots,X_n\right]$.

<u>Définition 4</u>.- <u>Soient</u> P <u>un anneau sur un corps</u> K <u>et</u> $X_1,\ldots,X_n$ <u>des éléments de</u> P. <u>Supposons les conditions suivantes satisfaites</u> : 1) P <u>est commutatif et possède un élément unité</u> ; 2) <u>on a</u> $P = K\left[X_1,\ldots,X_n\right]$; 3) $X_1,\ldots,X_n$ <u>sont algèbriquement indépendants sur</u> K. <u>On dit alors que</u> P <u>est l'anneau des polynomes en</u> $X_1,\ldots,X_n$ <u>à coefficients dans</u> K, <u>et que tout élément de</u> P <u>est un polynome en</u> $X_1,\ldots,X_n$ <u>à coefficients dans</u> K.

L'emploi de l'article défini dans l'expression "l'anneau des polynomes en $X_1,\ldots,X_n$" ne se justifie à proprement parler que si l'anneau P est donné à l'avance, de sorte que l'on sache quel est l'ensemble des éléments de P et quelles sont les lois de composition dans P. Néanmoins, nous nous permettrons d'employer cette expression même quand P n'est pas donné à l'avance, et ceci dans les circonstances suivantes.

Supposons le corps commutatif K donné ; soient $X_1,\ldots,X_n$ des symboles qui n'ont encore reçu (dans la question dont on traite) aucune signification ; si nous disons alors : "formons l'anneau des polynomes en les lettres $X_1,\ldots,X_n$ à coefficients dans K" , nous entendrons par là que nous introduisons dans la question un nouvel anneau P qui contient n éléments $X_1,..,X_n$ tels que les conditions 1),2),3) de la définition 4 soient satisfaites. Il résulte de ce que nous avons dit plus haut et de la proposition 3, §1,n°2 qu'il existe toujours de pareils anneaux, et qu'ils sont tous isomorphes les uns aux autres.

De même, si nous disons : " soient $X_1,..,X_n$ n lettres, et soit $\sum_{(k_1,\ldots,k_n)\in N^n} a(k_1,..,k_n)X_1^{k_1}\ldots X_n^{k_n}$ un polynome en ces n lettres à coefficients dans K" , nous supposerons implicitement qu'on a introduit dans la question un anneau qui soit l'anneau des polynomes en $X_1,\ldots,X_n$ à coefficients dans K , et que l'expression écrite représente un élément de cet anneau. Les éléments $a(k_1,..,k_n)$ sont appelés les <u>coefficients</u> du polynome en question ; plus spécifiquement, $a(k_1,..,k_n)$ s'appelle le coefficient de $X_1^{k_1}\ldots X_n^{k_n}$.

Soit E l'élément unité de l'anneau des polynomes en n lettres $X_1,\ldots,X_n$ à coefficients dans un corps K . L'application $a \longrightarrow aE$ est alors, comme on le voit tout de suite, un isomorphisme de K sur un sous-corps de P . On fait souvent la convention de représenter le polynome aE par le même symbole a que l'élément a de K . Il s'agit là d'un abus de notation qui n'est en général pas dangereux du fait que l'application $a \longrightarrow aE$ est un isomorphisme.

On dit qu'un polynome $\sum_{(k_1\ldots k_n)\in N^n} a(k_1,\ldots,k_n)X_1^{k_1}\ldots X_n^{k_n}$ en les lettres $X_1,..,X_n$ <u>ne contient aucune des lettres</u> $X_{i_1},\ldots,X_{i_m}$ (où $i_1,..,i_m$ sont m entiers distincts pris entre 1 et n) si l'on a

$a(k_1,\ldots,k_n) = 0$ toutes les fois que l'un au moins des entiers $k_{i_1},\ldots,k_{i_m}$ est >0. Soient $j_1,\ldots,j_{n-m}$ ceux des entiers de 1 à n qui ne figurent pas parmi $i_1,\ldots,i_m$. Les polynomes qui ne contiennent aucune des lettres $X_{i_1},\ldots,X_{i_m}$ sont alors les éléments de $K[X_{j_1},\ldots,X_{j_{n-m}}]$, qui est l'anneau des polynomes en $X_{j_1},\ldots,X_{j_{n-m}}$ à coefficients dans K.

n° 2. POLYNOMES SUR UN ANNEAU

Soit A un anneau d'intégrité (cf. Alg.I, § 8, n°3, définition 3). Nous pouvons alors former le corps des fractions K de A (définition 2 et proposition 5, Alg.I, § 9, n°4). Introduisons n lettres $X_1,\ldots,X_n$ et formons l'anneau $K[X_1,\ldots,X_n]$ des polynomes en $X_1,\ldots,X_n$ à coefficients dans K. Si $F = \sum_{(k_1,\ldots k_n)\in N^n} a(k_1,\ldots,k_n) X_1^{k_1}\ldots X_n^{k_n}$ et $G = \sum_{(k_1,\ldots k_n)\in N^n} b(k_1,\ldots,k_n)\ X_1^{k_1}\ldots X_n^{k_n}$ sont des polynomes de cet anneau, on a $F+G = \sum_{(k_1,\ldots k_n)\in N^n} c(k_1,\ldots,k_n)\ X_1^{k_1}\ldots X_n^{k_n}$ et $FG = \sum_{(k_1,\ldots k_n)\in N^n} d(k_1,\ldots,k_n) X_1^{k_1}\ldots X_n^{k_n}$, où

$$(1)\quad \begin{cases} c(k_1,\ldots,k_n) = a(k_1,\ldots,k_n) + b(k_1,\ldots,k_n) \\ d(k_1,\ldots,k_n) = \sum_{(l_1,\ldots l_n)+(m_1,\ldots m_n)=(k_1,\ldots,k_n)} a(l_1,\ldots,l_n) b(m_1,\ldots,m_n) \end{cases}$$

Il résulte tout de suite de ces formules que ceux des polynomes de l'anneau $K[X_1,\ldots,X_n]$ dont les coefficients appartiennent à A forment un anneau. Cet anneau s'appelle l'anneau des polynomes en $X_1,\ldots,X_n$ à coefficients dans A.

Théorème 1.- Soit A un anneau d'intégrité qui possède un élément unité, et soit P l'anneau des polynomes en n lettres $X_1,\ldots,X_n$ à coefficients dans A. Supposons d'autre part donnés un anneau $\mathcal{O}$, un homomorphisme φ de A dans $\mathcal{O}$ et n éléments $x_1,\ldots,x_n$ de $\mathcal{O}$ qui satisfassent aux conditions suivantes : 1) $\mathcal{O}$ possède un élément unité ; 2) les éléments $x_1,\ldots,x_n$ commutent entre eux et avec les éléments de $\varphi(A)$.

Il existe alors un homomorphisme h et un seul de P dans $\mathcal{O}$ qui satisfasse aux conditions suivantes : 1) E étant l'élément unité de P, on a $h(aE) = \varphi(a)$ pour tout $a \in A$; 2) on a $h(X_i) = x_i$ $(1 \leqslant i \leqslant n)$.

Ecrivons un élément quelconque F de P sous la forme

$$F = \sum_{(k_1,\ldots,k_n) \in \mathcal{N}^n} a(k_1,\ldots,k_n) X_1^{k_1} \ldots X_n^{k_n}$$

et définissons h(F) par la formule

$$h(F) = \sum_{(k_1,\ldots,k_n) \in \mathcal{N}^n} \varphi(a(k_1,\ldots,k_n) x_1^{k_1} \ldots x_n^{k_n}$$

Puisque $x_1,\ldots,x_n$ commutent entre eux et avec les éléments de $\varphi(A)$, on a, si a et b sont dans A,

$$\varphi(a) x_1^{k_1} \ldots x_n^{k_n} \varphi(b) x_1^{l_1} \ldots x_n^{l_n} = \varphi(ab) x_1^{k_1+l_1} \ldots x_n^{k_n+l_n}$$

Il résulte alors immédiatement de l'expression par les formules (1) ci-dessus des coefficients de la somme et du produit de deux polynomes que l'application h est un homomorphisme. C'est évidemment le seul homomorphisme satisfasisant aux conditions imposées.

Une convention de notations.

Utilisant les notations du théorème 1, supposons de plus que A soit un sous-anneau de $\mathcal{O}$ et que φ soit l'application identique de A dans $\mathcal{O}$. Dans ces conditions, si $F \in P$, on dénote souvent par $F(x_1,..,x_n)$ l'élément $h(F) \in \mathcal{O}$. Supposons que l'anneau $\mathcal{O}$ soit commutatir ; on peut alors considérer l'application $(F,(x_1,..,x_n)) \longrightarrow F(x_1,\ldots,x_n)$ comme une loi de composition externe entre éléments de P et de $\mathcal{O}^n$ à valeurs dans $\mathcal{O}$. Si F est donné, l'application $(x_1,..,x_n) \longrightarrow F(x_1,\ldots,x_n)$ est une application de $\mathcal{O}^n$ dans $\mathcal{O}$; toute application de cette espace s'appelle une fonction polynome. L'opération qui consiste à appliquer l'homomorphisme h du théorème 1 à un polynome $F \in P$ se décrit souvent en disant qu'elle consiste à remplacer $X_1,\ldots,X_n$ par $x_1,\ldots,x_n$ dans F. On notera que nos conventions nous permettent d'écrire $F=F(X_1,\ldots,X_n)$.

Soit maintenant J un automorphisme de l'anneau A , et soit E l'élément unité de l'anneau P . L'application $a \to J(a)E$ est un homomorphisme de A dans P . En vertu du théorème 1, il correspond à J un homomorphisme h de P dans lui-même tel que $h(a)E = J(a)E$ et que $h(X_i) = X_i$ $(1 \leqslant i \leqslant n)$. Si $F = \sum_{(k_1,\dots,k_n) \in \mathcal{N}^n} a(k_1,\dots,k_n) X_1^{k_1} \dots X_n^{k_n}$ est un élément quelconque de P , on a $h(F) = \sum_{(k_1,\dots,k_n) \in \mathcal{N}^n} J(a(k_1,\dots,k_n)) X_1^{k_1} \dots X_n^{k_n}$. On vérifie tout de suite que h est un automorphisme de P .

Considérons maintenant le cas où A est l'anneau Z des entiers. Si $\mathcal{O}$ est un anneau commutatif quelconque ayant un élément unité ε , il existe un homomorphisme φ et un seul de Z dans $\mathcal{O}$ qui applique 1 sur ε . Si $x_1,\dots,x_n$ sont n éléments quelconques de $\mathcal{O}$, toute égalité vraie entre polynomes en $X_1,\dots,X_n$ à coefficients dans Z fournira, en lui appliquant l'homomorphisme décrit par le théorème 1, une égalité vraie entre certaines expressions algèbriques construites avec $x_1,\dots,x_n$. Les égalités vraies entre polynomes à coefficients entiers, ainsi considérées comme matrices d'égalités vraies dans tout anneau commutatif, sont souvent appelés <u>identités algèbriques</u>. Le lecteur vérifiera facilement que les formules suivantes sont des identités algèbriques :

$$X_1^n - X_2^n = (X_1 - X_2) \cdot \sum_{n=0}^{n-1} X_1^r X_2^{n-1-r}$$

$$X_1^{2n+1} + X_2^{2n+1} = (X_1 + X_2) \cdot \sum_{r=0}^{2n} (-1)^r X_1^r X_2^{2n-r}$$

Nous établirons un peu plus loin un certain nombre d'autres importantes identités.

n° 2. LE DEGRÉ .

Définition 5.- Un polynome en n lettres $X_1,\dots,X_n$ à coefficients dans un corps K est dit être homogène de degré d s'il est une combinaison linéaire à coefficients dans K de ceux des éléments de la forme $X_1^{k_1}\dots X_n^{k_n}$ pour lesquels $k_1+\dots+k_n = d$. Un tel polynome s'appelle aussi une forme de degré d(en $X_1,\dots,X_n$, à coefficients dans K).

Il est clair que, d étant donné, il n'y a qu'un nombre fini d'éléments $(k_1,..,k_n)\in \mathbb{N}^n$ tels que $k_1+\dots+k_n = d$. Les formes de degré d forment donc un espace vectoriel de dimension finie. Nous allons calculer la dimension $p(n,d)$ de cet espace .

Si n est un entier $\geqslant 0$, nous désignerons par n ! l'entier

$$n\,! = \prod_{0<i\leqslant n} i$$

On a donc $0\,! = 1,\ 1\,! = 1, 2\,! = 2, 3\,! = 6, 4\,! = 24, \dots$.

Nous nous proposons de démontrer que

$$p(n,d) = \frac{(d+n-1)!}{d\,!\,(n-1)!}$$

La formule est vraie pour $d = 0$, car les deux membres sont alors égaux à 1 . Supposons la vraie pour un certain entier $d-1 \geqslant 0$; nous allons alors démontrer sa validité pour d . Si $n=1$, les deux membres de la formule à démontrer sont égaux à 1 ; supposons donc $n \geqslant 1$. Soit $E_{n,d}$ l'ensemble des éléments $(k_1,..,k_n)\in \mathbb{N}^n$ tels que $k_1+\dots+k_n = d$; divisons cet ensemble en deux parties E' et E", E' se composant de ceux des éléments $(k_1,..,k_n)\in E_{n,d}$ pour lesquels $k_1 > 0$ et E" de ceux pour lesquels $k_1 = 0$. L'application $(k_1,\dots,k_n)\to(k_1-1,\dots,k_n)$ applique E' bi-univoquement sur $E_{n,d-1}$, tandis que E" est évidemment équipotent à $E_{n-1,d}$. On a donc

$$p(n,d) - p(n-1,d) = p(n,d-1)$$

Posons aussi

$$p^*(n,d) = \frac{(d+n-1)!}{d!\ (n-1)!}$$

On a alors

$$p^*(n,d)-p^*(n-1,d) = \frac{(d+n-2)!}{d!(n-2)!}\left[\frac{d+n-1}{n-1}-1\right] = \frac{(d-1+n-1)!}{(d-1)!(n-1)!} = p^*(n,d-1)$$

Nous savons déjà que $p(n,d-1) = p^*(n,d-1)$; on a donc

$$p(n,d)-p^*(n,d) = p(n-1,d) - p^*(n-1,d)$$

pour tout $n \geqslant 1$. Il en résulte immédiatement que $p(n,d)-p^*(n,d)=p(1,d)-p^*(1,d) = 0$, ce qui démontre notre assertion pour d .

Proposition 1.- Soient K un corps commutatif. Formons l'anneau des polynomes en n+1 lettres $T,X_1,..,X_n$ à coefficients dans K . Pour qu'un polynome F qui ne contient que les lettres $X_1,..,X_n$ soit une forme de degré d , il faut et suffit que l'on ait $F(TX_1,...,TX_n)= T^dF(X_1,...,X_n)$.

Ecrivons en effet

$$F = \sum_{(k_1,...,k_n)\in N^n} a(k_1,...,k_n)X_1^{k_1}...X_n^{k_n}$$

On a donc

$$F(TX_1,...,TX_n)= \sum_{(k_1,...k_n)\in N^n} a(k_1,..,k_n)T^{k_1+...+k_n}X_1^{k_1}...X_n^{k_n}$$

et la proposition 1 résulte de cette formule.

Corollaire. Soient F et G des formes de degrés respectifs d et e à coefficients dans un corps K , le produit FG est alors une forme de degré d+e .

Cela résulte immédiatement de la proposition 1 .

Soit maintenant F un polynome quelconque en n lettres $X_1,...,X_n$ à coefficients dans un corps K . Il est clair qu'on peut, d'une manière et d'une seule, mettre F sous la forme

$$F = \sum_0^\infty \Phi_d \qquad (1)$$

ou, pour chaque $d \geqslant 0$, Φ_d est une forme de degré d , et $\Phi_d = 0$ excepté pour un nombre fini de valeurs de d . Représenter F sous la forme (1), cela s'appelle décomposer F en ses parties homogènes.

Définition 6. Soit F un polynome $\neq 0$ à coefficients dans un corps K, et soit $F = \sum_0^\infty \Phi_d$ la décomposition de F en ses parties homogènes. On appelle degré de F le plus grand entier d pour lequel $\Phi_d \neq 0$.

Si F est une forme $\neq 0$ de degré δ, δ est aussi le degré de F au sens de la définition précédente. Par contre, si a est un entier $\geqslant 0$ quelconque, la forme nulle est de degré d, mais n'a pas de degré.

Proposition 2.- L'anneau des polynomes en n lettres $X_1,\dots,X_n$ à coefficients dans un corps K n'a pas de diviseur de zéro. Le degré du produit de deux polynomes $\neq 0$ est la somme des degrés de ces polynomes.

Observons d'abord qu'il suffit pour établir la proposition 2 de démontrer que le produit de deux formes $\neq 0$ est $\neq 0$. Supposant en effet ce point établi, soient F et G des polynomes $\neq 0$, de degrés respectifs d et e ; écrivons $F = \sum_{k=0}^{d} \Phi_k$, $G = \sum_{l=0}^{e} \Psi_l$, ou les Φ_k, Ψ_l sont des formes de degrés égaux à leurs indices et où $\Phi_d \neq 0$, $\Psi_e \neq 0$. On a, en posant $\Phi_h = \Psi_h = 0$ si $h < 0$,

$$FG = \Phi_d \Psi_e + \sum_{m=0}^{d+e-1} \left(\sum_{k=0}^{m} \Phi_k \Psi_{m-k} \right)$$

or $\Phi_k \Psi_{m-k}$ est une forme de degré m ; puisque, par hypothèse, $\Phi_d \Psi_e \neq 0$, on a $FG \neq 0$ et FG est de degré d+e.

Ceci dit, pour établir notre assertion relative aux formes, nous procéderons par récurrence sur n. L'assertion est évidente pour $n = 1$. Supposons la vraie pour les formes en n-1 lettres, où n est un entier > 1. Soient F et G des formes $\neq 0$ en $X_1,\dots,X_n$; nous pouvons écrire

$$F = \sum_{k=0}^{d} X_n^k F_k \qquad G = \sum_{l=0}^{e} X_n^l G_l .$$

ou les F_k, G_l sont des formes de degrés égaux à leurs indices en les lettres $X_1,\dots,X_{n-1}$ et où $F_d \neq 0$, $G_e \neq 0$. On a

$$FG = \sum_{m=0}^{d+e} X_n^m \left(\sum_{k+l=m} F_k G_l \right)$$

Or on a par hypothèse $F_d G_e \neq 0$; il en résulte immédiatement que $FG \neq 0$.

Le résultat contenu dans la proposition 2 justifie la définition suivante :

Définition 7. Soient K un corps commutatif et P l'anneau des polynomes en n lettres $X_1,..,X_n$ à coefficients dans K . Le corps des quotients de P s'appelle alors le corps des fractions rationnelles en $X_1,...,X_n$ à coefficients dans K , tout élément de ce corps s'appelle une fraction rationnelle en $X_1,...,X_n$ à coefficients dans K .

Soient K un corps commutatif, $X_1,...,X_n$ n lettres et L le corps des fractions rationnelles en $X_1,...,X_n$ à coefficients dans K . Introduisons m autres lettres $Y_1,...,Y_m$ et formons l'anneau P des polynomes en $Y_1,...,Y_m$ à coefficients dans L . Les polynomes appartenant à P et dont les coefficients sont dans $K[X_1,..,X_n]$ forment un anneau $K[X_1,...,X_n,Y_1,...,Y_m]$ qui n'est autre que l'anneau des polynomes en $X_1,...,X_n,Y_1,..,Y_m$ à coefficients dans K . Tout polynome F en $X_1,..,X_n,Y_1,..,Y_m$ peut donc se mettre sous la forme

$$F = \sum_{(k_1,...,k_m) \in \mathbb{N}^m} F_{k_1,..,k_n} Y_1^{k_1} ... Y_m^{k_m}$$

où chaque $F_{k_1 ... k_m}$ est un polynome en $X_1,...,X_n$ à coefficients dans K , et $F_{k_1,...,k_m} = 0$ excepté pour un nombre fini d'éléments $(k_1,...,k_m) \in \mathbb{N}^m$. Mettre F sous cette forme, cela s'appelle développer F par rapport à $Y_1,...,Y_m$; le polynome $F_{k_1,...,k_m}$ s'appelle le coefficient de $Y_1^{k_1} ... Y_m^{k_m}$ dans ce développement. Considéré comme polynome en $Y_1,...,Y_m$ à coefficients dans L , le polynome F a (s'il est $\neq 0$) un certain degré ; ce degré s'appelle le degré de F par rapport à $Y_1,...,Y_m$. Ce nombre est naturellement au plus égal au degré de F .

n° 3. DIFFERENTIELLES ET DERIVEES DE POLYNOMES.

Soient K un corps commutatif et $P = K[X_1,..,X_n]$ l'anneau des polynomes en n variables $X_1,..,X_n$ à coefficients dans K . Introduisons 2n nouvelles variables $X'_1,..,X'_n,X''_1,..,X''_n$ et formons l'anneau P' des polynomes en ces 2n variables à coefficients dans K . A tout polynome $F \in P$ nous pouvons faire correspondre le polynome $\Delta F = F(X''_1,...,X''_n)-F(X'_1,...,X'_n)$ $\in P'$. D'autre part, si $\Phi \in P'$, nous pouvons faire correspondre à Φ le polynome $h(\Phi) = \Phi(X_1,..,X_n,X_1,..,X_n) \in P$. Il est clair que h est un homomorphisme de P' sur P et que $h(\Delta F) = 0$ pour tout $F \in P$. Désignons par $\mathfrak{p}'$ l'ensemble des polynomes $\Phi \in P'$ tels que $h(\Phi) = 0$; $\mathfrak{p}'$ est donc un idéal dans P' et l'homomorphisme h définit par passage aux quotients un isomorphisme h de $P'/\mathfrak{p}'$ avec P . L'idéal $\mathfrak{p}'$ contient les n éléments $\Delta X_i = X''_i - X'_i$ $(1 \leqslant i \leqslant n)$. Nous allons montrer que ces éléments forment un système de générateurs de $\mathfrak{p}'$, c'est-à-dire que tout élément de $\mathfrak{p}'$ peut se mettre sous la forme $\sum_{i=1}^{n} \Phi_i \cdot \Delta X_i$, avec $\Phi_i \in P'$ $(1 \leqslant i \leqslant n)$. Introduisons pour cela n nouvelles variables $Y_1,..,Y_n$ et désignons par Q' l'anneau des polynomes en $X'_1,..,X'_n$, $Y_1,..,Y_n$ à coefficients dans K . Les formules

$$\theta(\Phi(X'_1,..,X'_n,X''_1,..,X''_n)) = \Phi(X'_1,..,X'_n,X'_1+Y_1,...,X'_n+Y_n)$$

$$\theta'(\Psi(X'_1,..,X'_n,Y_1,..,Y_n)) = \Psi(X'_1,..,X'_n,X''_1-X'_1,..,X''_n-X'_n)$$

définissent, la première un homomorphisme θ de P' dans Q', la seconde un homomorphisme θ' de Q' dans P' . On aperçoit tout de suite que $\theta \circ \theta'$ est l'application identique de Q' sur lui-même et que $\theta' \circ \theta$ est l'application identique de P' sur lui-même ; on en déduit que θ et θ' sont des isomorphismes. Si $\Psi \in \theta(\mathfrak{p}')$, on a $\Psi(X_1,...,X_n,0,...,0) = 0$. Or on peut écrire

$$\Psi = \sum_{e_1,...,e_n} \Psi_{e_1,...,e_n} Y_1^{e_1} \cdots Y_n^{e_n}$$

où chaque $\Psi_{e_1,\dots,e_n}$ est un polynome en $X'_1,\dots,X'_n$. Donc, $\Psi = \theta(\Phi)$, $\Phi \in \mathfrak{p}'$, implique que $\Psi_{0,\dots,0} = 0$, d'où il résulte immédiatement que Ψ appartient à l'idéal engendré par $Y_1,\dots,Y_n$ dans Q' ; donc que Φ appartient à l'idéal engendré par $\Delta X_1,\dots,\Delta X_n$ dans P', ce qui démontre notre assertion.

Désignons maintenant par $\mathfrak{p}'^2$ l'idéal engendré par les éléments de la forme $\Phi\,\Phi$, où $\Phi \in \mathfrak{p}'$, $\Phi \in \mathfrak{p}'$ (c'est un cas particulier de la notion de produit d'idéaux que nous étudierons plus tard). On peut considérer $\mathfrak{p}'$ comme un module sur l'anneau P', $\mathfrak{p}'^2$ en est alors un sous-module, d'où il résulte que le quotient, $\mathfrak{p}'/\mathfrak{p}'^2$ possède une structure de module par rapport à P'. Si $\omega \in \mathfrak{p}'/\mathfrak{p}'^2$, $\Phi \in P'$, le produit $\Phi\,\omega$ est la classe de $\Phi\,\Omega$ module $\mathfrak{p}'^2$, où Ω est un élément quelconque de la classe ω modulo $\mathfrak{p}'^2$. La valeur de $\Phi\,\Omega$ ne dépend que de la classe de Φ module $\mathfrak{p}'$; en effet, si $\Phi' \equiv \Phi \pmod{\mathfrak{p}'}$, on a $\Phi'\Omega = \Phi\Omega + (\Phi' - \Phi)\Omega \equiv \Phi\,\Omega \pmod{\mathfrak{p}'^2}$. Si $\varphi \in P'/\mathfrak{p}'$, on peut donc définir $\varphi\omega$ comme étant la valeur commune des $\Phi\,\omega$ pour tous les Φ appartenant à la classe φ modulo $\mathfrak{p}'$, et on vérifie sans peine que $\mathfrak{p}'/\mathfrak{p}'^2$ se trouve ainsi muni d'une structure de module sur $P'/\mathfrak{p}'$. Enfin, l'isomorphisme h^* de $P'/\mathfrak{p}'$ avec P nous permet, par transport de structure, de conférer à $\mathfrak{p}'/\mathfrak{p}'^2$ une structure de module sur P. Désignons par $\mathfrak{d}$ le module ainsi obtenu.

Si F est un élément de P, nous désignerons par dF la classe de l'élément $\Delta F \in \mathfrak{p}'$ modulo $\mathfrak{p}'^2$. On obtient donc ainsi une application $F \longrightarrow dF$ de P dans $\mathfrak{d}$ dont nous nous proposons d'étudier les propriétés. Si F et G sont dans P et a dans K, on a

$$\Delta(F+G) = \Delta F + \Delta G, \quad \Delta(aF) = a\,\Delta F, \text{ d'où}$$

$$d(F+G) = dF + dG \qquad d(aF) = a.dF$$

D'autre part, un calcul facile montre que $\Delta(FG)=F(X'_1,..,X'_n)\,\Delta G + G(X''_1,...,X''_n).\,\Delta F$. Du fait que $h(F(X''_1,..,X'_n)) = F$, $h(G(X''_1,..,X''_n)) = G$, il résulte alors que l'on a la formule

$$d(FG) = FdG + G\,dF .$$

Nous avons montré plus haut que tout élément de $\mathfrak{P}'$ peut se mettre sous la forme $\sum_{i=1}^{n} \Phi_i \Delta X_i$ (avec $\Phi \in P'$, $1 \leqslant i \leqslant n$); il en résulte immédiatement que tout élément de ϑ peut se mettre sous la forme $\sum_{i=1}^{n} F_i dX_i$, avec $F_i \in P$, $1 \leqslant i \leqslant n$. Nous allons montrer que cette représentation est unique, c'est-à-dire que l'égalité $\sum_{i=1}^{n} F_i dX_i = 0$ (où $F_i \in P$, $1 \leqslant i \leqslant n$) entraîne $F_1 = \ldots = F_n = 0$. Supposons en effet $\sum_{i=1}^{n} F_i dX_i = 0$; on a alors $\sum_{i=1}^{n} F_i(X'_1,\ldots,X'_n)(X''_i - X'_i) \in \mathfrak{P}'^2$, d'où puisque les éléments $X''_i - X'_i$ engendrent $\mathfrak{P}'$,

$$F_i(X'_1,..,X'_n)(X''_i - X'_i) = \sum_{1 \leqslant i \leqslant j \leqslant n} \Phi_{ij}(X''_i - X'_i)(X''_j - X'_j)$$

où $\Phi_{ij} \in P'$ $(1 \leqslant i \leqslant j \leqslant n)$, et par suite

$$\sum_{i=1}^{n} F_i(X'_1,..,X'_n)Y_i = \sum_{1 \leqslant i \leqslant j \leqslant n} \theta(\Phi_{ij})Y_iY_j$$

Ordonnant le second membre par rapport aux variables $Y_1,\ldots,Y_n$, on voit tout de suite que les coefficients de $Y_1,..,Y_n$ y sont nuls, d'où $F_i = 0$ $(1 \leqslant i \leqslant n)$, ce qui démontre notre assertion.

Nous avons donc démontré qu'il existe un module ϑ sur l'anneau P et une application $F \longrightarrow dF$ de P dans ϑ qui satisfont aux conditions suivantes :

1) Tout élément de ϑ peut se mettre et d'une seule sous la forme $\sum_{i=1}^{n} F_i dX_i$, avec $F_i \in P$ $(1 \leqslant i \leqslant n)$,

2) Si F et G sont dans P et a dans K , on a

$$d(F+G) = dF + dG , \quad d(aF) = a\,dF ; \quad d(FG) = FdG + GdF .$$

Nous allons montrer que la structure déterminée sur $\mathfrak{d}$ par son caractère de module sur P et par l'existence de l'application $F \to dF$ satisfaisant aux conditions 1) et 2) ci-dessus est uniquement déterminée à une isomorphie près. Plus généralement, supposons donnée un module $\mathfrak{m}$ sur P et une application δ de P dans $\mathfrak{m}$ qui satisfassent aux conditions suivantes : 1) tout élément de $\mathfrak{m}$ peut se mettre d'au moins une manière sous la forme $\sum_{i=1}^{n} F_i \delta x_i$ (avec $F_i \in P$, $1 \leqslant i \leqslant n$) ; 2) si F et G sont dans P et a dans K , on a $\delta(F+G) = \delta F + \delta G$, $\delta(aF) = a\delta F$; $\delta(FG) = F.\delta G + G.\delta F$. Dans ces conditions, nous allons montrer qu'il existe une application λ de $\mathfrak{d}$ dans $\mathfrak{m}$ qui est un homomorphisme de la structure de module sur P de $\mathfrak{d}$ sur celle de $\mathfrak{m}$ et qui est telle que $\lambda(dF) = \delta F$ pour tout $F \in P$. Puisqu'un élément de $\mathfrak{d}$ ne peut se mettre que d'une manière sous la forme $\sum_{i=1}^{n} F_i dX_i$, nous pouvons définir une application λ de $\mathfrak{d}$ dans $\mathfrak{m}$ par la formule $\lambda\left(\sum_{i=1}^{n} F_i dX_i\right) = \sum_{i=1}^{n} F_i \delta X_i$. Il est évident que λ est un homomorphisme de la structure de module sur P de $\mathfrak{d}$ sur celle de $\mathfrak{m}$. Il résulte immédiatement des propriétés que possèdent les opérations d et δ que les hypothèses $\lambda(dF) = \delta F$, $\lambda(dG) = \delta G$ entraînent $\lambda(d(F+G)) = \delta(F+G)$, $\lambda(d(aF)) = \delta(aF)$ (où $a \in K$) et $\lambda(d(FG)) = \delta(FG)$. Nous en concluons que la formule $\lambda(dF) = \delta F$ sera vraie pour tout $F \in P$ si elle l'est pour les polynomes particuliers suivants : $1, X_1, \ldots, X_n$. On a $\delta(1) = \delta(1.1) = 1.\delta(1) + 1.\delta(1)$, d'où $1.\delta(1) = 2.\delta(1)$ et par suite $1.\delta(1) = 0$, $\delta(1) = 0$; on voit de même que $d(1) = 0$. Si F est l'une des variables $X_1, \ldots, X_n$, l'égalité $\lambda(dF) = \delta F$ résulte immédiatement de la définition de λ . L'existence de l'homomorphisme λ est donc établie. Si un élément de $\mathfrak{m}$ ne peut se mettre que d'une seule manière sous la forme $\sum_{i=1}^{n} F_i \delta X_i$, λ est évidemment un isomorphisme.

Définition 1.- Soit P l'anneau des polynomes en n variables $X_1,\dots,X_n$ à coefficients dans un corps K . Soit $\mathfrak{M}$ un module sur P tel qu'il existe une application d de P dans $\mathfrak{M}$ qui satisfasse aux conditions 1),2) ci-dessus. On dit alors que la structure déterminée par le module $\mathfrak{M}$ et par l'application d est la structure du module des différentielles de P . Soit F un élément de P ; si on met dF sous la forme $\sum_{i=1}^{n} F_i dX_i$, F_i s'appelle la dérivée partielle de F par rapport à X_i et se note $\partial F / \partial X_i$.

Toutes les fois que l'on parlera de différentielle d'un polynome, on suppcsera implicitement qu'un module de différentielles a été introduit dans la question. Comme tous les modules de différentielles sont isomorphes entre eux au sens précisé plus haut, il ne sera pas nécessaire en général de spécifier la nature des éléments que l'on emploie comme différentielles.

En particulier, on notera que les dérivées partielles ne dépendent pas du module de différentielles qu'on emploie pour les définir.

Il résulte immédiatement de la définition des dérivées partielles que l'on a, pour $F,G \in P$ et $a \in K$,

$$\frac{\partial(F+G)}{\partial X_i} = \frac{\partial F}{\partial X_i} + \frac{\partial G}{\partial X_i} \qquad \frac{\partial(aF)}{\partial X_i} = a\frac{\partial F}{\partial X_i} \qquad \frac{\partial(FG)}{\partial X_i} = F\frac{\partial G}{\partial X_i} + G\frac{\partial F}{\partial X_i}$$

$$\frac{\partial a}{\partial X_i} = 0 \qquad \frac{\partial X_i}{\partial X_i} = 1 \qquad \frac{\partial X_j}{\partial X_i} = 0 \text{ si } j \neq i$$

Si on dénote par P_i l'anneau des polynomes qui ne contiennent pas X_i , les formules $\partial 1 / \partial X_i = 0$, $\partial X_j / \partial X_i = 0$ pour $j \neq i$ entraînent que $\partial F / \partial X_i = 0$ pour tout $F \in P_i$, d'où $\partial(FX_i^e)/\partial X_i = F\,\partial X_i^e / \partial X_i$. On a $\partial X_i^e / \partial X_i = 0$; si $e > 0$, la formule $\partial X_i^e / \partial X_i = (\partial X_i^{e-1}/\partial X_i).X_i + X_i^{e-1}(\partial X_i / \partial X_i)$ permet d'établir facilement par récurrence sur e que $\partial X_i^e / \partial X_i = eX_i^{e-1}$.

Si donc $F = \sum_e F_e X_i^e$ est un polynome quelconque, ordonné par rapport à X_i (d'où $F_e \in P_i$), on a

$$\partial F / \partial X_i = \sum_{e>0} e F_e X_i^{e-1} .$$

Si $n=1$, la dérivée partielle $\partial F / \partial X_1$ se note aussi dF/dX_1 et s'appelle la dérivée de F.

Si L est un sous-corps de K et si F est un polynome en $X_1,\dots,X_n$ à coefficients dans L, les dérivées partielles de F sont les mêmes que l'on considère F comme un élément de $L[X_1,\dots,X_n]$ ou de $K[X_1,\dots,X_n]$. Si A est un sous-anneau de K, les dérivées partielles d'un polynome à coefficients dans A sont elles-mêmes des polynomes à coefficients dans A.

Proposition 1.- Soient P l'anneau des polynomes en les variables $X_1,\dots,X_n$ à coefficients dans un corps K et Q celui des polynomes en les variables $Z_1,\dots,Z_m$ à coefficients dans K. Soient $H_1,\dots,H_m$ m éléments de P et F un élément de Q. On a alors

$$d(F(H_1,\dots,H_m)) = \sum_{i=1}^{m} \partial F / \partial Z_i (H_1,\dots,H_m)\, dH_i$$

Soit ϑ le module des différentielles de P, et soit θ l'homomorphisme $\Phi \to \Phi(H_1,\dots,H_m)$ de Q dans P. Si $\Phi \in Q$, $\omega \in \vartheta$, posons $\Phi\,\omega = \theta(\Phi)\omega$; on voit tout de suite que ϑ acquiert ainsi une structure de module sur Q. Si $\Phi \in Q$, posons $\delta\Phi = d(\theta(\Phi))$; on a alors, si Φ, $\Psi \in Q$ et $a \in K$, $\delta(\Phi+\Psi) = \delta\Phi + \delta\Psi$, $\delta(a\Phi) = a\,\delta\Phi$, $\delta(\Phi\Psi) = \Phi\delta\Psi + \Psi\delta\Phi$. Introduisons le module ϑ_1 des différentielles sur Q ; il résulte de ce qu'on a démontré plus haut qu'il existe une application λ de ϑ_1 dans ϑ telle que $\lambda(\Phi\,\omega_1) = \Phi\,\lambda(\omega_1)$, $\lambda(d\Phi) = d(\theta(\Phi))$ pour tout $\Phi \in Q$ et tout $\omega_1 \in \vartheta_1$. La formule à démontrer résulte alors immédiatement de la formule $dF = \sum_{i=1}^{m} \partial F / \partial Z_i\, dZ_i$.

Définition 2.- *Soient* A *et* B *des anneaux tels que* A *soit un sous-anneau de* B . *On entend par dérivation de* A *dans* B *une application* D *de* A *dans* B *telle que l'on ait, quels que soient* x *et* y *dans* A ,

$$D(x+y) = Dx + Dy \quad ; \quad D(xy) = (Dx)y + x(Dy)$$

Par exemple, les n applications D_i $(1 \leqslant i \leqslant n)$ dans lui-même de l'anneau des polynomes en $X_1,\ldots,X_n$ définies par $D_iF = \partial F/\partial X_i$ sont évidemment des dérivations.

Soient D_1 et D_2 des dérivations d'un anneau A dans un anneau B dont A est un sous-anneau. On voit alors tout de suite que l'opération D_1+D_2 définie par $(D_1+D_2)(x) = D_1x + D_2x$ est une dérivation de A dans B . Si $B \neq A$, l'opération $D_1 \circ D_2$ n'est en général pas définie ; même si $B = A$, $D_1 \circ D_2$ n'est en général pas une dérivation. Par contre, si $B = A$, l'opération $D = [D_1, D_2]$ définie par

$$[D_1, D_2] = D_2 \circ D_1 - D_1 \circ D_2$$

est une dérivation. En effet, il est tout d'abord évident que $D(x+y) = Dx + Dy$. D'autre part, on a

$$\begin{aligned} D(xy) &= D_2((D_1x)y + x(D_1y)) - D_1((D_2x)y+x(D_2y)) = \\ &= (D_2D_1x)y + (D_1x)(D_2y) + (D_2x)(D_1y) + x(D_2D_1y) - \\ &- (D_1D_2x)y-(D_2x)(D_1y)-(D_1x)(D_2y)-x(D_1D_2y) = (Dx)y + x(Dy) \end{aligned}$$

Proposition 2.- *Soit* P *l'anneau des polynomes en* n *variables* $X_1,\ldots,X_n$ *à coefficients dans un corps* K . *Désignons par* D_i *l'opération de dérivation partielle dans* P *par rapport à* X_i . *On a alors* $D_i \circ D_j = D_j \circ D_i$ $(1 \leqslant i, j \leqslant n)$.

Posons $\Delta_{ij} = [D_i, D_j]$; on sait que Δ_{ij} est une dérivation de P . Si $a \in K$, on a $\Delta_{ij}(a) = 0$; de plus, $\Delta_{ij}(X_k) = 0$ $(1 \leqslant k \leqslant n)$ puisque $D_iX_k \in K$, $D_jX_k \in K$. Du fait que Δ_{ij} est une dérivation, on déduit que les conditions $\Delta_{ij}F = 0$, $\Delta_{ij}G = 0$ entraînent $\Delta_{ij}(F+G) = 0$, $\Delta_{ij}(FG) = 0$. Il résulte immédiatement de là que $\Delta_{ij} = 0$.

Désignant toujours par $D_1,\dots,D_n$ les dérivations partielles dans P par rapport à $X_1,..,X_n$, on voit que $D_1,\dots,D_n$ engendrent un sous-anneau commutatif de l'anneau des applications linéaires de P (considéré comme espace vectoriel sur K) dans lui-même. Si $e_1,\dots,e_n$ sont des entiers $\geqslant 0$, on pose

$$\frac{\partial^{e_1+\dots+e_n} F}{\partial X_1^{e_1} \dots \partial X_n^{e_n}} = D_1^{e_1} \dots D_n^{e_n} F$$

(ou il faut entendre que D_i^0 est l'application identique de P dans lui-même).

Si e,f sont des entiers $\geqslant 0$, posons

$$p(e,f) = 0 \text{ si } f > e \; ; \quad p(e,f) = \prod_{m=e-f+1}^{e} m \text{ si } f \leqslant e$$

Nous allons montrer que

$$\frac{\partial^{f_1+\dots+f_n} X_1^{e_1} \dots X_n^{e_n}}{\partial X_1^{f_1} \dots \partial X_n^{f_n}} = p(e_1,f_1)\dots p(e_n,f_n)\, X_1^{e_1-f_1} \dots X_n^{e_n-f_n}$$

Nous procéderons par récurrence sur le nombre $f_1+\dots+f_n$. La formule est évidente si $f_1+\dots+f_n = 0$. Supposons la formule vraie pour tous les systèmes $(f_1,..,f_n)$ tels que $f_1+\dots+f_n < h$, où h est un certain entier >0, et soient $f_1,\dots,f_n$ des entiers $\geqslant 0$ tels que $f_1+\dots+f_n = h$.

Choisissons un indice i tel que $f_i > 0$ et posons $f_i' = f_i - 1$, $f_j' = f_j$ si $j \neq i$. On a

$$\frac{\partial^{f_1+\dots+f_n} X_1^{e_1} \dots X_n^{e_n}}{\partial X_1^{f_1} \dots \partial X_n^{f_n}} = \frac{\partial}{\partial X_i} \left(\frac{\partial^{f_1'+\dots+f_n'} X_1^{e_1} \dots X_n^{e_n}}{\partial X_1^{f_1'} \dots \partial X_n^{f_n'}} \right)$$

$$= \frac{\partial}{\partial X_i} \left[\prod_{j=1}^{n} p(e_j,f_j') X_j^{e_j-f_j'} \right] = \prod_{j=1}^{n} p(e_j,f_j)\, X_j^{e_j-f_j}$$

ce qui démontre la formule en question pour le système $(f_1,\dots,f_n)$.

On voit en particulier que

$$\frac{\partial^{f_1+\dots+f_n} X_1^{e_1} \dots X_n^{e_n}}{\partial X_1^{f_1} \dots \partial X_n^{f_n}} (0,\dots,0) = \begin{cases} 0 & \text{si } (e_1,\dots,e_n) \neq (f_1,\dots,f_n) \\ e_1'\dots e_n! & \text{si } (e_1,\dots,e_n) = (f_1,\dots,f_n) \end{cases}$$

n° 4. FORMULES DE TAYLOR ET DE LEIBNITZ.

Soient P l'anneau des polynomes en n variables $X_1,\dots,X_n$ à coefficients dans un corps K , et soit F un élément de P . Introduisons n nouvelles variables $Y_1,\dots,Y_n$ et posons

$$F(X_1+Y_1,\dots,X_n+Y_n) = \sum_{e_1,\dots,e_n} F_{e_1,\dots,e_n} Y_1^{e_1}\dots Y_n^{e_n}$$

où chaque $F_{e_1,\dots,e_n}$ est un élément de P . Appliquant aux deux membres de cette formule l'opération $\partial^{e_1+\dots+e_n} / \partial Y_1^{e_1}\dots \partial Y_n^{e_n}$, puis remplaçant $Y_1,\dots,Y_n$ par 0 et faisant usage de la formule ( ), n°3, nous obtenons

$$e_1!\dots e_n!\, F_{e_1\dots e_n} = \frac{\partial^{e_1+\dots+e_n} F}{\partial X_1^{e_1}\dots \partial X_n^{e_n}}$$

Soit d le degré de F , supposé $\neq 0$. Donc, introduisant une nouvelle variable T, $F(TX_1,\dots,TX_n)$ est un polynome de degré d à coefficients dans P , d'où il résulte aisément que $F(TX_1+TY_1,\dots,TX_n+TY_n)$ est un polynome en T de degré d à coefficients dans $K\left[X_1,\dots,X_n,Y_1,\dots,Y_n\right]$ et par suite que $F(X_1+Y_1,\dots,X_n+Y_n)$ est de degré d . On a donc $F_{e_1\dots e_n} = 0$ si $e_1+\dots+e_n > d$. Supposons que d! , considéré comme élément de K , soit $\neq 0$ (i.e. que $d!\,\varepsilon \neq 0$, où ε est l'élément unité de K). On voit alors tout de suite que $e! \neq 0$ si $e \leqslant d$, d'où $e_1!\dots e_n! \neq 0$ si $e_1+\dots+e_n \leqslant d$, et on peut alors écrire

$$(1)\qquad F(X_1+Y_1,\dots,X_n+Y_n) = \sum_{e_1+\dots+e_n\leqslant d} \frac{1}{e_1!\dots e_n!} \frac{\partial^{e_1+\dots+e_n} F}{\partial X_1^{e_1}\dots \partial X_n^{e_n}}$$

Cette formule est appelée la <u>formule de Taylor</u>. On notera qu'elle est en particulier valable toutes les fois que K contient un corps isomorphe au corps des rationnels.

Appliquons en particulier la formule de Taylor au cas particulier suivant : K est le corps Q des rationnels, $n = 1$, $F = X_1^m$, où m est un entier $\geqslant 0$. Il résulte des formules démontrées au n°3 que l'on a $d^e F/dX_1^e = p(m,e) X_1^{m-e}$, d'où

$$(X_1+Y_1)^m = \sum_{e=0}^{m} \frac{p(m,e)}{e\,!}\, X_1^{m-e} Y_1^{e}$$

Les polynomes à coefficients entiers formant un anneau, il est clair que les coefficients du polynome $(X_1+Y_1)^m$ sont entiers. On voit donc que, si $0 \leqslant e \leqslant m$, le nombre $p(m,e)/e\,!$ est un entier. Cet entier se désigne par le symbole $\binom{m}{e}$; les nombres de la forme $\binom{m}{e}$ sont appelés les <u>coefficients binomiaux</u>. On notera qu'il résulte immédiatement de la définition de $p(m,e)$ que l'on a

$$\binom{m}{e} = \frac{m\,!}{e!\,(m-e)!}$$

Du fait que la formule

$$(2) \qquad (X_1+Y_1)^m = \sum_{e=0}^{m} \binom{m}{e} X_1^{m-e} Y_1^{e}$$

est vraie dans $\mathbb{Q}\left[X_1,Y_1\right]$ et de ce que les coefficients $\binom{m}{e}$ sont des entiers, on déduit immédiatement que la formule en question est vraie dans $K\left[X_1,Y_1\right]$ quel que soit le corps K . Cette formule est appelée la <u>formule du binome</u>.

Soit maintenant p un entier $\geqslant 2$. Nous nous proposons de montrer que, si $e_1,..,e_p$ sont des entiers $\geqslant 0$ de somme m , le

$$\binom{m}{e_1,\ldots,e_p} = \frac{m!}{e_1!\ldots e_p!}$$

est entier et que l'on a l'identité

$$(3) \qquad (X_1+\ldots+X_p)^m = \sum_{e_1+\cdots+e_p=m} \binom{m}{e_1,\ldots,e_p} X_1^{e_1}\ldots X_p^{e_p}$$

La formule est vraie pour $p = 2$. Supposons la vraie pour un certain p , et remplaçons yX_p par $X_p + X_{p+1}$: il vient

$$(X_1+\ldots+X_p+X_{p+1})^m = \sum_{e_1+\cdots+e_p=m} \binom{m}{e_1,..,e_p} X_1^{e_1}\ldots X_{p-1}^{e_{p-1}}(X_p+X_{p+1})^{e_p}$$

Appliquant la formule du binome, il vient

$$(X_1+\ldots+X_{p+1})^m = \sum_{e_1+\cdots+e_p=m} \left(\left(\frac{m}{e_1\ldots e_p}\right)\right) \sum_{f_p+f_{p+1}=e_p} \binom{m}{e_1,..,e_p} \binom{e_p}{f_p} X_1^{e_1}\ldots X_{p-1}^{e_{p-1}}$$

Or, on vérifie tout de suite que

$$\binom{m}{e_1,..,e_{p-1},f_p,f_{p+1}} = \binom{m}{e_1,..,e_{p-1},f_p+f_{p+1}} \binom{f_p+f_{p+1}}{f_p}$$

La formule est donc démontrée pour $p+1$.

Observons maintenant que l'on peut écrire

$$(X_1+..+X_p)^{m+1} = (X_1+...+X_p)^m(X_1+...+X_p) =$$

$$= \sum_{i=1}^{p} \sum_{e_1+\cdots+e_p=m} \binom{m}{e_1,..,e_p} X_1^{e_1}...X_p^{e_p} X_i$$

d'où l'on déduit l'égalité (où $f_1,..,f_p$ sont des entiers $\geqslant 0$ de somme $m+1$)

$$(4) \qquad \binom{m+1}{f_1,..,f_p} = \sum_{i=1}^{p} \binom{}{e_1^{(i)},\ldots,e_p^{(i)}}$$

où on a posé $e_j^{(i)} = f_j$ si $j \neq i$, $e_i^{(i)} = f_i - 1$, et ou on fait la convention que le symbole $\binom{m}{e_1,..,e_p}$ représente 0 si l'un des entiers $e_1,\ldots,e_p$ est < 0 .

La formule de Leibnitz.

Soit A un anneau commutatif, $u_1,..,u_p$ des éléments de A et D une dérivation de A . On se propose de montrer que

$$D^m(u_1...u_p) = \sum_{e_1+\cdots+e_p=m} \binom{m}{e_1,\ldots,e_p} D^{e_1}u_1....D^{e_p}u_p$$

(ou on fait la convention habituelle que D^0 représente l'application identique de A sur lui-même). Considérons d'abord le cas où $m = 1$. Dans ce cas, on procède par récurrence sur p . Si $p=2$, la formule est évidente. Supposons la vraie pour un certain p . On a alors $D(u_1...u_p u_{p+1}) = D(u_1...u_p)\, u_{p+1} + u_1...u_p . Du_{p+1}$, et on en déduit aisément que la formule est vraie pour $m=1$ et pour un produit de $p+1$ facteurs. La formule est donc vraie pour $m = 1$. Elle est évidente pour $m = 0$. Supposons la vraie pour un certain $m \geqslant 1$. On a alors

$$(5) \quad D^{m+1}(u_1...u_p) = \sum_{e_1+\cdots+e_p=m} \binom{m}{e_1,..,e_p} \left[D^{e_1+1}u_1,..,D^{e_p}u_p + \ldots + D^{e_1}u_1,\ldots,D^{e_{p+1}}u_p \right]$$

et la validité de la formule pour $m+1$ résulte immédiatement de la formule (4) ci-dessus.

La formule (5) est appelée la formule de Leibnitz.
