RÉDACTION N° 097

COTE : NBR 008

TITRE : LIVRE II. ALGÈBRE
CHAPITRE IV. (ÉTAT 6)
POLYNÔMES ET FRACTIONS RATIONNELLES

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 61

NOMBRE DE FEUILLES : 61

LIVRE II

ALGEBRE - CHAPITRE IV (Etat 6)

POLYNOMES ET FRACTIONS RATIONNELLES

Sommaire

§ 1. Polynomes : 1. Définition des polynomes. 2. La notion de degré. 3. Polynomes sur un anneau d'intégrité. 4. Division euclidienne des polynomes à une indéterminée. 5. Polynomes à une indéterminée sur un corps commutatif.

§ 2. Fonctions polynomes : 1. Opérateurs polynomes. 2. Fonctions polynomes sur une algèbre. 3. Racines d'un polynome à une indéterminée. 4. Fonctions polynomes sur un anneau d'intégrité ayant une infinité d'éléments.

§ 3. Fractions rationnelles et fonctions rationnelles : 1. Fractions rationnelles sur un corps commutatif. 2. Fonctions rationnelles.

§ 4. Différentielles et dérivations : 1. Différentielles et dérivées des polynomes. 2. Application : caractérisation des racines simples d'un polynome. 3. Dérivations dans une algèbre. 4. Prolongement d'une dérivation : dérivées des fractions rationnelles. 5. Formes différentielles.

Commentaires.

Le rédacteur s'est inspiré sur plusieurs points de la dernière rédaction Chevalley, notamment pour la suppression des séries formelles la définition du degré et la théorie des dérivations sur une algèbre. Il a pris soin en outre d'introduire les propriétés de l'anneau des polynomes à une indéterminée sur un corps qui sont indispensables pour le chap. des corps commutatifs, maintenant que la théorie de la divisibilité a été rejetée au chap. VI. Les notions d'algèbre stratifiée et de forme différentielle ont été introduites à la demande de Weil.

LIVRE II

ALGEBRE

CHAPITRE IV (Etat 6)

POLYNOMES ET FRACTIONS RATIONNELLES

§ 1. Polynomes.

1. Définition des polynomes.

DEFINITION 1.- Soit A un anneau commutatif ayant un élément unité. On appelle algèbre des polynomes à une indéterminée sur l'anneau A l'algèbre du monoïde (additif) $\mathbb{N}$ des entiers $\geqslant 0$, relative à l'anneau A (chap.II, § 7, n° 9). Les éléments de cette algèbre sont appelés polynomes à une indéterminée sur A.

La base canonique (chap.II, § 7, n° 9) de cette algèbre de monoïde a donc pour ensemble d'indices $\mathbb{N}$; si on la note $(e_n)_{n\in\mathbb{N}}$, on voit que la table de multiplication correspondante est $e_m e_n = e_{m+n}$. On en conclut en premier lieu que l'algèbre est commutative et admet e_0 comme élément unité ; cet élément étant libre, on peut identifier A à la sous-algèbre Ae_0 par l'application $\lambda \to \lambda e_0$, ce qui identifie e_0 à l'élément unité de A (que nous noterons 1 si aucune confusion n'est à craindre). D'autre part, pour tout $n\in\mathbb{N}$, on a $e_n=(e_1)^n$, comme on le voit par récurrence sur n ; les éléments 1 et e_1 forment donc un système de générateurs de l'algèbre des polynomes à une indéterminée sur A. Il est d'usage, dans l'écriture d'un raisonnement où intervient l'algèbre des polynomes à une indéterminée sur A, de remplacer e_1 par une lettre telle que X, Y, Z ; dans ce qui suit, nous remplacerons e_1 par X, et nous noterons $A[X]$ l'algèbre des polynomes à une indéterminée sur A. Avec cette notation, tout élément $u\in A[X]$ s'écrit d'une seule manière sous la forme $u=\sum_{n\in\mathbb{N}} a_n X^n$ où les a_n appartiennent à A ; on dit que u

est <u>un polynome par rapport à l'indéterminée</u> X (ou simplement un <u>polynome par rapport à X</u> ; ou encore un <u>polynome en</u> X) ; les éléments a_n (nuls sauf pour un nombre fini d'indices) sont dits les <u>coefficients</u> du polynome u , les éléments $a_n X^n$ sont dits les <u>termes</u> du polynome u .

De façon plus précise, le terme $a_n X^n$ est souvent appelé "le terme en X^n " de u ; le terme $a_0 = a_0 X^0$ est encore dit <u>terme constant</u> de u . Un polynome dont tous les coefficients sauf un au plus sont nuls, est appelé <u>monôme</u>. La somme et le produit de deux polynomes en X , $u = \sum_n a_n X^n$, $v = \sum_n \beta_n X^n$ sont donnés par les formules

$$(1) \qquad u+v = \sum_n (a_n+\beta_n) X^n$$

$$(2) \qquad uv = \sum_n \gamma_n X^n , \text{ avec } \gamma_n = \sum_{p=0}^{n} a_p \beta_{n-p} .$$

Soit maintenant I un ensemble d'indices non vide quelconque ; dans le monoïde $\mathcal{N}^I$, <u>produit</u> (chap.I, § 4, n°5) d'une famille de monoïdes ayant I comme ensemble d'indices, et tous identiques à $\mathcal{N}$, soit $\mathcal{N}^{(I)}$ la partie stable formée des familles (n_ι) pour lesquelles $n_\iota = 0$ sauf pour un nombre <u>fini</u> d'indices ι ; elle est identique au produit $\mathcal{N}^I$ si I est fini. Considérons <u>l'algèbre du monoïde</u> $\mathcal{N}^{(I)}$, relative à l'anneau A ; elle admet une base canonique $(e_{(n_\iota)})_{(n_\iota)\in\mathcal{N}^{(I)}}$ (chap.II, § 7, n°9) dont la table de multiplication est $e_{(m_\iota)} \cdot e_{(n_\iota)} = e_{(m_\iota+n_\iota)}$. On en déduit comme ci-dessus que l'algèbre considérée est commutative, et admet comme élément unité l'élément e_ω de la base canonique, où ω désigne l'élément de $\mathcal{N}^{(I)}$ dont toutes les coordonnées sont 0 ; on identifie encore e_ω à l'élément unité 1 de A . Pour chaque indice $\kappa \in I$, désignons par X_κ l'élément $e_{(n_\iota)}$ de la base canonique correspondant à l'élément (n_ι) de $\mathcal{N}^{(I)}$ tel que $n_\kappa = 1$ et $n_\iota = 0$ pour tout $\iota \neq \kappa$; d'après la table de multiplication précédente, tout élément $e_{(n_\iota)}$

de la base canonique peut s'écrire d'une seule manière $e_{(n_\iota)} = \prod_{\iota \in I} X_\iota^{n_\iota}$ (expression qui a un sens puisque les n_ι sont nuls à l'exception d'un nombre fini d'entre eux) ; l'algèbre du monoïde $M^{(I)}$ est donc engendrée par les éléments 1 et X_ι (où ι parcourt I).

DEFINITION 2.- Les éléments de l'algèbre du monoïde $M^{(I)}$ relative à l'anneau A sont appelés polynomes par rapport aux indéterminées X_ι ($\iota \in I$), à coefficients dans A.

L'algèbre du monoïde $M^{(I)}$ relative à A se notera $A\left[X_\iota\right]_{\iota \in I}$; on dit encore qu'elle s'obtient par adjonction à A des indéterminées X_ι ($\iota \in I$). Lorsque I est une partie finie de M, on écrit $A\left[X_{i_1}, X_{i_2}, \ldots, X_{i_p}\right]$ au lieu de $A\left[X_\iota\right]_{\iota \in I}$; $(i_k)_{1 \leqslant k \leqslant p}$ étant la suite d'éléments de I rangés dans l'ordre croissant. Tout polynome $u \in A\left[X_\iota\right]_{\iota \in I}$ s'écrit d'une seule manière sous la forme $u = \sum_{(n_\iota)} a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$, où (n_ι) parcourt $M^{(I)}$; les éléments $a_{(n_\iota)}$ de A nuls sauf un nombre fini d'entre eux) sont appelés les coefficients du polynome u, les éléments $a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ ses termes (l'élément $a_{(n_\iota)} \prod_{\iota \in I} X^{n_\iota}$ sera souvent dit "le terme en $\prod_{\iota \in I} X_\iota^{n_\iota}$" ; lorsque tous les n_ι sont nuls, on l'appelle aussi "terme constant" de u). Un polynome dont tous les coefficients sauf un au plus sont nuls, est appelé un monôme.

Remarques.- 1) Lorsque le coefficient $a_{(n_\iota)}$ d'un polynome u est nul, on dit (par abus de langage) que u ne contient pas de terme en $\prod_{\iota \in I} X_\iota^{n_\iota}$. En particulier, quand le "terme constant" de u est nul, on dit que u est un polynome "sans terme constant".

2) Soient u_i ($1 \leqslant i \leqslant q$) un nombre fini de polynomes par rapport aux X_ι ($\iota \in I$) tels que $u_1 + u_2 + \ldots + u_q = 0$, et que, pour chaque $(n_\iota) \in M^{(I)}$, il n'y ait qu'un indice i au plus tel que u_i

contienne un terme en $\prod_{\iota \in I} X_\iota^{n_\iota}$; dans ces conditions, on a $u_i = 0$ pour tout indice i.

Si I et I' sont deux ensembles équipotents, les algèbres de polynomes $A[X_\iota]_{\iota \in I}$ et $A[X_\varkappa]_{\varkappa \in I'}$ sont isomorphes.

En particulier, les algèbres de polynomes correspondant à tous les ensembles d'indices finis ayant un même nombre d'éléments n sont toutes isomorphes ; on les identifie d'ordinaire à l'algèbre des polynomes correspondant à $I = [1,n]$, et on l'appelle l'algèbre des polynomes à n indéterminées ; au lieu des lettres X_i $(1 \leqslant i \leqslant n)$, on peut naturellement désigner les indéterminées par des lettres quelconques ; par exemple, on pourra noter Y_1, Y_2, Y_3 ou X, Y, Z les indéterminées dans les polynomes à trois indéterminées ; quelles que soient les notations adoptées, on ne perdra pas de vue qu'il s'agit toujours d'une même algèbre, ayant pour module sous-jacent le module $A^{(M)}$, et que les trois "indéterminées" sont toujours les trois mêmes éléments e_{100}, e_{010}, e_{001} de la base canonique de ce module.

Soit J une partie non vide quelconque de I ; le monoïde $M^{(J)}$ peut être identifié à la partie stable de $M^{(I)}$ formée des éléments (n_ι) tels que $n_\iota = 0$ pour tout $\iota \in \complement J$. Par suite (chap. II, § 7, n° 9), l'algèbre $A[X_\iota]_{\iota \in J}$ peut être identifiée à la sous-algèbre de $A[X_\iota]_{\iota \in I}$ ayant pour base les produits $\prod_{\iota \in I} X_\iota^{n_\iota}$, où $n_\iota = 0$ pour tout $\iota \in \complement J$; cette sous-algèbre est la sous-algèbre de $A[X_\iota]_{\iota \in I}$ engendrée par 1 et les X_ι d'indice $\iota \in J$; on dit encore qu'elle est formée des polynomes qui ne contiennent pas les X_i d'indice $i \in \complement J$.

Cette identification faite, on peut dire que l'algèbre $A[X_\iota]_{\iota \in I}$ est la réunion des sous-algèbres $A[X_\iota]_{\iota \in J}$, où J parcourt l'ensemble

des parties finies de I ; en effet, tout polynome u est somme d'un nombre fini de termes $\neq 0$ de la forme $a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$, et dans chacun de ces termes, il n'y a qu'un nombre fini d'indices ι tels que $n_\iota \neq 0$; si J est la partie finie de I formée de tous ces indices (pour tous les termes $\neq 0$ de u), il est clair que u appartient à l'algèbre $A[X_\iota]_{\iota \in J}$.

Si J et J' sont deux parties équipotentes de I, les sous-algèbres $A[X_\iota]_{\iota \in J}$ et $A[X_\iota]_{\iota \in J'}$ de $A[X_\iota]_{\iota \in I}$ sont isomorphes. Par exemple, dans l'algèbre $A[X,Y,Z]$ des polynomes à trois indéterminées sur A, $A[X]$, $A[Y]$ et $A[Z]$ sont des sous-algèbres isomorphes, qui bien entendu ne sont pas identiques. On observera à ce propos que tant que, dans un raisonnement, n'interviennent que des polynomes par rapport à une indéterminée, il n'y a pas lieu de distinguer les anneaux $A[X]$, $A[Y]$, $A[Z]$, etc. comme nous l'avons dit plus haut ; par contre, ces notations désignent des anneaux distincts dans tout raisonnement où interviennent des polynomes par rapport à plusieurs des indéterminées X, Y, Z, etc.

Soit J une partie quelconque de I, $K = \complement J$ le complémentaire de J dans I ; le monoïde $M^{(I)}$ est isomorphe au monoïde produit $M^{(J)} \times M^{(K)}$ (chap. I, § 4, n° 5). Il en résulte (chap. III, § 3, n°) que l'algèbre $A[X_\iota]_{\iota \in I}$ est isomorphe au produit tensoriel des algèbres $A[X_\iota]_{\iota \in J}$ et $A[X_\iota]_{\iota \in K}$; en outre, si on pose $B = A[X_\iota]_{\iota \in J}$, et qu'on considère B comme sous-anneau de $A[X_\iota]_{\iota \in I}$, l'anneau $A[X_\iota]_{\iota \in I}$, considéré comme algèbre par rapport à son sous-anneau B, n'est autre que l'algèbre obtenue par extension à B de l'anneau d'opérateurs A de l'algèbre $A[X_\iota]_{\iota \in K}$ (chap. III, § 3) ; en d'autres termes, tout polynome par rapport aux X_ι d'indice $\iota \in I$, à coefficients dans A, peut s'écrire d'une seule manière comme un polynome par rapport aux X_ι d'indice $\iota \in K$,

à coefficients dans l'anneau B des polynomes par rapport aux X_ι d'indice $\iota \in J$ (à coefficients dans A) ; $A[X_\iota]_{\iota\in I}$ (considéré comme algèbre sur B) est ainsi identifié à l'algèbre de polynomes $B[X_\iota]_{\iota\in K}$.

Soit A' un sous-anneau de A, ayant même élément unité que A ; par restriction à A' de l'anneau d'opérateurs, $A[X_\iota]_{\iota\in I}$ peut être considéré comme algèbre sur A' ; l'algèbre $A'[X_\iota]_{\iota\in I}$ des polynomes par rapport aux X_ι d'indice $\iota \in I$, à coefficients dans A', peut alors être considérée comme sous-algèbre de $A[X_\iota]_{\iota\in I}$ (chap.II, § 7, n°).

Enfin, en raison de ses applications, nous énoncerons sous forme de proposition le cas particulier suivant d'une propriété générale des algèbres de monoïdes (chap.II, § 7, n°) :

PROPOSITION 1.- *Soit φ une représentation de A sur un anneau B ; il existe une représentation $\overline{\varphi}$ et une seule de l'anneau $A[X_\iota]_{\iota\in I}$ sur l'anneau $B[X_\iota]_{\iota\in I}$, qui prolonge φ et laisse invariantes chacune des indéterminées X_ι. Si φ est un isomorphisme de A sur B, $\overline{\varphi}$ est un isomorphisme de $A[X_\iota]$ sur $B[X_\iota]$.*

De façon précise, l'image par $\overline{\varphi}$ d'un polynome $\sum_{(n_\iota)} a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$ est le polynome $\sum_{(n_\iota)} \varphi(a_{(n_\iota)}) \prod_\iota X_\iota^{n_\iota}$.

2. La notion de degré.

DEFINITION 3.- *Etant donné un polynome $u \in A[X_\iota]_{\iota\in I}$, on appelle termes de degré total p dans u les termes $a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$ tels que $\sum_{\iota\in I} n_\iota = p$. On dit qu'un polynome u est homogène et de degré total p si tous les termes $\neq 0$ de u sont de degré total p.*

Il est clair que l'ensemble des polynomes homogènes de degré total p est un sous-module H_p de $A[X_\iota]_{\iota\in I}$ (considéré comme A-module), ayant pour base l'ensemble des $\prod_\iota X_\iota^{n_\iota}$, tels que $\sum_\iota n_\iota = p$ (p entier quelconque ≥ 0) ; il en résulte que le A-module $A[X_\iota]_{\iota\in I}$ est somme directe

des sous-modules H_p ($p \in \mathbb{N}$) ; un polynome quelconque u peut donc se mettre d'une seule manière ~~manière~~ sous la forme $u = \sum_{p=0}^{\infty} u_p$, où $u_p \in H_p$ ($u_p = 0$ sauf pour un nombre fini d'indices) le polynome homogène u_p est appelé la partie homogène de degré p de u : c'est la somme de tous les termes de degré total p de u .

L'intersection de deux H_p distincts se réduit à 0 ; un polynome homogène $u \neq 0$ ne peut donc appartenir qu'à un seul des H_p ; l'entier p tel que $u \in H_p$ est appelé le degré (total) de u . Plus généralement, on pose la définition suivante :

DEFINITION 4.- Pour tout polynome $u \neq 0$, on appelle degré (total) de u et on désigne par deg u le plus grand des entiers $p \geqslant 0$ tels que la partie homogène de degré p de u soit $\neq 0$.

Remarques.- 1) On notera que, conformément aux déf. 3 et 4, 0 est un "polynome homogène de degré p " pour tout entier $p \geqslant 0$ mais que le degré de 0 n'est pas défini.

2) Les polynomes homogènes de degré p sont encore appelés formes de degré p par rapport aux indéterminées X_ι ; les formes par rapport à n indéterminées sont aussi appelées formes n-aires (binaires, ternaires, quaternaires, pour n=2,3,4 respectivement).

3) Les polynomes homogènes de degré 0 ne sont autres que les éléments de l'anneau A ; on dit encore que ce sont les constantes dans l'anneau $A\left[X_\iota\right]_{\iota \in I}$.

PROPOSITION 2.- Si u et v sont deux polynomes $\neq 0$ tels que $u+v \neq 0$, on a

$$\deg(u+v) \leqslant \operatorname{Max}(\deg u, \deg v) \tag{3}$$

En outre, si $\deg u \neq \deg v$, on a $u+v \neq 0$ et les deux membres de (3) sont égaux.

PROPOSITION 3.- Si u et v sont deux polynomes homogènes, de degrés respectifs p et q , uv est un polynome homogène de degré p+q .

Les deux propositions sont évidentes à partir des définitions.

COROLLAIRE.- Si u et v sont deux polynomes $\neq 0$ et si $uv \neq 0$, on a

(4) $$\deg(uv) \leqslant \deg u + \deg v .$$

Il résulte des formules (3) et (4) (la seconde appliquée au cas où $\deg u = 0$) que les polynomes $\neq 0$ de degré total $\leqslant p$ et 0 forment un sous-module de $A[X_\iota]_{\iota \in I}$, ayant pour base les $\prod_\iota X_\iota^{n_\iota}$ tels que $\sum_\iota n_\iota \leqslant p$.

Si maintenant J est une partie non vide quelconque de I, nous avons vu qu'on peut considérer tout polynome u de $A[X_\iota]_{\iota \in I}$ comme un polynome par rapport aux X_ι d'indice $\iota \in J$, à coefficients dans l'anneau des polynomes $B = A[X_\iota]_{\iota \in (I-J)}$. Les définitions 3 et 4 s'appliquent naturellement dans l'anneau $B[X_\iota]_{\iota \in J}$, et il leur correspond de nouvelles définitions pour les polynomes $u \in A[X_\iota]_{\iota \in I}$: on dira qu'un terme $a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$ est de degré p par rapport aux X_ι d'indice $\iota \in J$ si on a $\sum_{\iota \in J} n_\iota = p$; u sera dit homogène et de degré p par rapport aux X_ι d'indice $\iota \in J$ si tous ses termes $\neq 0$ sont de degré p par rapport à ces indéterminées ; l'ensemble $H_{p,J}$ de ces polynomes est un sous-module de $A[X_\iota]_{\iota \in I}$, et $A[X_\iota]_{\iota \in I}$ est somme directe de ces sous-modules ($p \in \mathcal{N}$). Pour tout polynome $u \neq 0$, on appelle degré de u par rapport aux X_ι d'indice $\iota \in J$ le plus grand des entiers p tels qu'il existe un terme $a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ de u non nul et tel que $\sum_{\iota \in J} n_\iota = p$. Dans le cas particulier où J est réduit à un seul élément $\varkappa$, le degré de u par rapport à $X_\varkappa$ se notera $\deg_\varkappa u$. Nous laissons au lecteur le soin d'énoncer, avec ces définitions, les propositions 2 et 3 et leur corollaire dans l'anneau $B[X_\iota]_{\iota \in J}$.

Dans l'anneau $A[X]$ des polynomes par rapport à une seule indéterminée, il n'y a naturellement qu'une seule notion de degré, et les

les polynômes homogènes sont les monômes ; un polynome $u \neq 0$ de $A[X]$, de degré n, s'écrit $u = \sum_{k=0}^{n} a_k X^k$; le coefficient a_n, qui est $\neq 0$ par hypothèse, est appelé le coefficient dominant de u ; un polynome $u \neq 0$ dont le coefficient dominant est égal à 1 est appelé polynome unitaire.

Algèbres stratifiées.- La notion de degré dans une algèbre de polynomes est un cas particulier d'une notion plus générale dont nous rencontrerons plus tard d'importants exemples.

Soit A un anneau commutatif ayant un élément unité, E une algèbre sur A ; soit d'autre part L un monoïde commutatif, noté additivement. Par définition, une stratification de l'algèbre E suivant le monoïde L est une famille $(H_\lambda)_{\lambda \in L}$ de sous-modules de E (considéré comme A-module) ayant les propriétés suivantes :

(ST_I) E est somme directe des H_λ ;

(ST_{II}) pour tout $x \in H_\lambda$ et tout $y \in H_\mu$ (λ et μ quelconques dans L), xy appartient à $H_{\lambda+\mu}$.

L'ensemble E, muni de sa structure d'algèbre et de la stratification (H_λ) sera dit une algèbre stratifiée. On dira d'ordinaire que les éléments de H_λ sont les éléments homogènes (ou parfois les formes) de degré (ou de poids) λ ; d'après (ST_I), tout élément $x \in E$ s'écrit d'une seule manière sous la forme $x = \sum_{\lambda \in L} x_\lambda$, où $x_\lambda \in H_\lambda$; x_λ est appelé la partie homogène de degré λ (ou le composant homogène de degré λ) de x. Un élément homogène $x \neq 0$ ne peut appartenir qu'à un seul des H_λ ; l'élément $\lambda \in L$ tel que $x \in H_\lambda$ est appelé le degré (ou le poids) de x ; le degré de 0 n'est naturellement pas défini. Dans la plupart des cas, E admettra un élément unité e tel que A puisse être identifié à la sous-algèbre Ae de E, L admettra un élément neutre (noté 0), et H_0 sera identique à A.

Exemples.- 1) Dans une algèbre de polynomes $A[X_\iota]_{\iota\in I}$, les sous-modules H_p (resp. $H_{p,J}$) de polynomes homogènes définissent une stratification de cette algèbre suivant le monoïde additif $\mathbb{N}$, le "degré" dans cette stratification étant le degré total (resp. degré par rapport aux X_ι d'indice $\iota \in J$) défini ci-dessus.

2) Soient maintenant J, J' deux parties de I sans élément commun ; pour tout couple (p,q) d'entiers naturels, soit $H_{p,q}$ l'ensemble des polynomes qui sont homogènes et de degré p par rapport aux X_ι d'indice $\iota \in J$, et aussi homogènes et de degré q par rapport aux X_ι d'indice $\iota \in J'$; on vérifie aussitôt que les $H_{p,q}$ définissent une stratification de l'algèbre $A[X_\iota]_{\iota\in I}$ suivant le monoïde $\mathbb{N}\times\mathbb{N}$. On définit de même des stratifications de $A[X_\iota]_{\iota\in I}$ suivant un produit d'un nombre quelconque (au plus égal à la puissance de I) de monoïdes identiques à $\mathbb{N}$.

3) Soit M un monoïde commutatif quelconque, admettant un élément neutre (noté 0) ; soit $(\omega_\iota)_{\iota\in I}$ une famille quelconque d'éléments de M. Pour tout élément $\omega \in M$, et tout polynome $u \in A[X_\iota]_{\iota\in I}$, appelons termes de poids ω dans u les termes $a_{(n_\iota)} \prod_\iota X_\iota^{n_\iota}$ tels que $\sum_\iota n_\iota \omega_\iota = \omega$; soit H_ω l'ensemble des polynomes dont tous les termes $\neq 0$ sont de poids ω ; on vérifie aussitôt que les H_ω définissent une stratification de l'algèbre $A[X_\iota]_{\iota\in I}$ suivant le monoïde M. La stratification de l'exemple 2 peut s'obtenir comme cas particulier de cette stratification générale, en prenant $M = \mathbb{N}\times\mathbb{N}$, $\omega_\iota = (1,0)$ pour $\iota \in J$, $\omega_\iota = (0,1)$ pour $\iota \in J'$, et $\omega_\iota = (0,0)$ lorsque ι n'appartient ni à J ni à J'.

4) Dans l'algèbre tensorielle $T(E)$ (resp. l'algèbre extérieure $\bigwedge E$) sur un A-module quelconque E, si on désigne par H_p le sous-module des tenseurs contravariants d'ordre p (resp. des p-vecteurs) pour

tout entier $p \geqslant 0$, les H_p définissent une stratification suivant le monoïde $\mathbb{N}$.

5) Si L est un monoïde commutatif (noté additivement), E l'algèbre du monoïde L par rapport à A (chap.II, § 7, n°9), $(e_\lambda)_{\lambda \in L}$ la base canonique de E , les sous-modules $A.e_\lambda$ de E (où λ parcourt L) forment une stratification de E suivant L).

3. Polynomes sur un anneau d'intégrité.

THEOREME 1.- Si A est un anneau d'intégrité (ayant un élément unité) tout anneau de polynomes $A[X_\iota]_{\iota \in I}$ sur A est un anneau d'intégrité.

Soient u,v deux polynomes de $A[X_\iota]_{\iota \in I}$; les trois polynomes u,v et uv appartiennent à un même anneau $A[X_\iota]_{\iota \in J}$, où J est une partie finie de I . Il faut montrer que si $u \neq 0$ et $v \neq 0$, on a $uv \neq 0$; on peut donc se borner au cas où I est fini. D'autre part, l'anneau $A[X_1, X_2, \ldots, X_p]$ est identique à l'anneau des polynomes par rapport à l'indéterminée X_p , à coefficients dans l'anneau $A[X_1, X_2, \ldots, X_{p-1}]$. Par récurrence sur p, on est donc ramené à démontrer le théorème pour $p=1$, c'est-à-dire pour l'anneau $A[X]$ des polynomes à une indéterminée sur A .

Or, si $u = a_0 + a_1 X + \ldots + a_m X^m$ est un polynome de degré m , $v = \beta_0 + \beta_1 X + \ldots + \beta_n X^n$ un polynome de degré n sur A , le coefficient de X^{m+n} dans le produit uv est $a_m \beta_n$; comme $a_m \neq 0$ et $\beta_n \neq 0$ par hypothèse, on a $a_m \beta_n \neq 0$, puisque A est un anneau d'intégrité ; a fortiori, $uv \neq 0$.

Dans le cas général où A contient des diviseurs de 0 , le raisonnement précédent prouve que si le coefficient dominant a_m de u n'est pas diviseur de 0 dans A , u n'est pas un diviseur de 0 dans $A[X]$; en particulier, il en est toujours ainsi lorsque u est un polynome unitaire (cf. exerc. 12).

COROLLAIRE 1.- Si A est un anneau d'intégrité, u et v deux polynomes $\neq 0$ de l'anneau $A[X_\iota]_{\iota\in I}$, on a

(5) $$\deg(uv) = \deg u + \deg v .$$

En effet, si $\deg u=m$, $\deg v=n$, on peut écrire $u=u_0+u_1+\ldots+u_m$, $v=v_0+v_1+\ldots+v_n$, où u_h (resp. v_k) est la partie homogène de degré h (resp. k) de u (resp. v) pour $0\leqslant h\leqslant m$ (resp. $0\leqslant k\leqslant n$) ; comme $u_m\neq 0$ et $v_n\neq 0$ par hypothèse, on a $u_m v_n\neq 0$ d'après le th.1 ; comme $u_m v_n$ est la partie homogène de degré $m+n$ dans uv, le corollaire est démontré.

COROLLAIRE 2.- Si A est un anneau d'intégrité, u et v deux polynomes $\neq 0$ de l'anneau $A[X_\iota]_{\iota\in I}$, on a, pour tout $\varkappa\in I$,

(6) $$\deg_\varkappa(uv) = \deg_\varkappa u+\deg_\varkappa v .$$

4. Division euclidienne despolynomes à une indéterminée.

On peut définir, dans l'anneau $A[X]$ des polynomes à une indéterminée sur A, un processus analogue à celui de la division euclidienne dans l'ensemble $\mathbb{N}$ des entiers naturels (Ens., chap.III).

PROPOSITION 4.- Soient u et v deux polynomes $\neq 0$ de $A[X]$, m et n les degrés de u et v respectivement, β_0 le coefficient dominant de v ($\beta_0\neq 0$) ; si $n\leqslant m$, il existe dans $A[X]$ un polynome q nul ou de degré $\leqslant m-n$ et un polynome r nul ou de degré $<n$, tels que

(7) $$\beta_0^{m-n+1}u = qv+r .$$

Raisonnons par récurrence sur la différence $m-n$; si $m=n$, et si α_0 est le coefficient dominant de u, il est immédiat que $q=\alpha_0$ répond à la question. Dans le cas général, soit encore α_0 le coefficient dominant de u ; le polynome $u_1=\beta_0 u-\alpha_0 X^{m-n}v$ est nul ou de degré $<m$; l'hypothèse de récurrence montre qu'il existe un polynome q_1 nul ou de degré $<m-n$ et un polynome r_1 nul ou de degré $<n$, tels que $\beta_0^{m-n}u_1=q_1v+r_1$; d'où on tire $\beta_0^{m-n+1}u=(\alpha_0\beta_0^{m-n}X^{m-n}+q_1)v+r_1$ et les polynomes $q=\alpha_0\beta_0^{m-n}X^{m-n}+q_1$ et $r=r_1$ répondent à la question.

COROLLAIRE.- Si A est un anneau d'intégrité (ayant un élément unité), les polynomes q et r satisfaisant aux conditions de la proposition 4 sont déterminés de façon unique.

En effet, si $qv+r=q_1v+r_1$, on a $(q-q_1)v=r_1-r$; comme $\deg r < n$ et $\deg r_1 < n$, on a $\deg(r_1-r)<n$ si r_1-r n'est pas nul ; mais dans ce cas $q-q_1\neq 0$, donc $\deg((q-q_1)v)=\deg(q-q_1)+\deg v \geqslant n$, ce qui est absurde ; on a donc nécessairement $r=r_1$ et $q=q_1$.

Plus particulièrement, on a la proposition suivante :

PROPOSITION 5.- Soit K un corps commutatif, u et v deux polynomes de $K[X]$; si $v\neq 0$, il existe deux polynomes q et r de $K[X]$, tels que

(8) $$u=qv+r$$

et que $r=0$ ou $\deg r < \deg v$; en outre, ces polynomes sont déterminés de façon unique par les conditions précédentes.

En effet, si $u=0$ ou $\deg u < \deg v$ il suffit de prendre $q=0$, $r=u$; dans le cas contraire, si β_0 est le coefficient dominant de v , $\beta_0^{-1}v$ est un polynome unitaire, et d'après le corollaire de la prop4, il existe deux polynomes q_1, r_1 uniquement déterminés par les conditions $u=q_1(\beta_0^{-1}v)+r_1$ et $\deg r_1 < \deg v$ (ou $r_1=0$) ; les polynomes $q=\beta_0^{-1}q_1$ et $r=r_1$ répondent à la question et sont évidemment uniques.

La formation des polynomes q et r à partir de u et v s'appelle division euclidienne de u par v ; q est dit le quotient euclidien de u par v , r le reste de la division euclidienne de u par v.

COROLLAIRE.- Pour qu'un polynome $u\in K[X]$ soit divisible par un polynome $v\neq 0$ de $K[X]$, il faut et il suffit que le reste de la division euclidienne de u par v soit nul.

Le quotient euclidien de u par v est alors égal à u/v .

5. Polynomes à une indéterminée sur un corps commutatif.

PROPOSITION 6.- Soit K un corps commutatif quelconque. Tout idéal de l'anneau $K[X]$ des polynomes à une indéterminée sur K est principal.

En effet, soit $\mathfrak{a}$ un idéal quelconque dans $K[X]$; si $\mathfrak{a} \neq (0)$, soit f un élément $\neq 0$ de $\mathfrak{a}$ dont le degré soit le plus petit possible ; si g est un autre élément quelconque de $\mathfrak{a}$, il existe deux polynomes q et r tels que $g=qf+r$ avec $r=0$ ou $\deg r < \deg f$ (prop.5) ; comme $r=g-qf$, r appartient à $\mathfrak{a}$, donc si on avait $r \neq 0$, on aurait $\deg r \geqslant \deg f$, ce qui est absurde ; on a par suite $r=0$, donc $\mathfrak{a}=(f)$.

Si f et f_1 sont deux polynomes $\neq 0$ tels que $(f)=(f_1)$, il existe deux polynomes u,v tels que $f_1=uf$ et $f=vf_1$; de ces relations, on tire $f=uvf$, donc (formule (5)), $\deg(uv)=0$, u et v sont des constantes ; pour tout idéal $\mathfrak{a} \neq (0)$ de $K[X]$, les polynomes f tels que $\mathfrak{a}=(f)$ sont donc déterminés à un facteur constant près ; en particulier, il existe un polynome unitaire f_0 et un seul tel que $\mathfrak{a}=(f_0)$.

DEFINITION 5.- Etant donné un corps commutatif K , on dit qu'un polynome f de degré >0 de $K[X]$ est irréductible s'il n'est divisible par aucun polynome g tel que $0<\deg g<\deg f$.

Il revient au même (formule (5)) de dire que les seuls diviseurs de f dans $K[X]$ sont les constantes et les produits de f par les constantes. La relation $(f) \subset (g)$ signifiant que g divise f , on voit que les polynomes irréductibles peuvent encore être définis comme les polynomes f tels que l'idéal (f) soit maximal.

On sait (chap.I, § 8, th.2) que tout idéal de $K[X]$ distinct de (1) est contenu dans un idéal maximal ; il revient au même de dire que :

PROPOSITION 7.- Tout polynome non constant de $K[X]$ est divisible par un polynome irréductible.

La démonstration de cette proposition peut d'ailleurs ici se faire sans avoir recours à l'axiome de choix : si f est un polynome quelconque $\neq 0$ et non constant, soit g un diviseur de f non constant et dont le degré est le plus petit possible ; il est immédiat que g est irréductible.

COROLLAIRE.- Tout polynome $f \in K[X]$, de degré >0, est égal à un produit de polynomes irréductibles (distincts ou non).

Il suffit de raisonner par récurrence sur le degré de f ; le corollaire est évident si f est irréductible ; sinon, il existe un diviseur irréductible g de f tel que $0 < \deg g < \deg f$; on a $f=gh$, où $0 < \deg h < \deg f$; h est donc égal à un produit de polynomes irréductibles, et il en est de même de f (cf. chap.VI, § 3).

Exercices.- 1) Montrer que le A-module des formes de degré n par rapport à p indéterminées a une base de $\binom{p+n-1}{n}$ éléments.

2) Soit A un anneau commutatif ayant un élément unité, E un A-module quelconque. Soit $S_n(E)$ (ou simplement S_n) le sous-module de la puissance tensorielle n-ème $\overset{n}{\otimes} E$, engendré par les tenseurs $z-\sigma z$, où z parcourt $\overset{n}{\otimes} E$, et σ le groupe symétrique $\mathfrak{S}_n$. On appelle puissance symétrique n-ème de E, et on note $\overset{n}{\vee} E$, le module quotient $(\overset{n}{\otimes} E)/S_n(E)$; pour qu'une application multilinéaire de E^n dans un A-module F soit symétrique, il faut et il suffit qu'elle soit de la forme $(x_1,..x_n) \to f(\varphi(x_1 \otimes x_2 \otimes \dots \otimes x_n))$, où φ est l'application canonique de $\overset{n}{\otimes} E$ sur $\overset{n}{\vee} E$, et f une application linéaire de $\overset{n}{\vee} E$ dans F.

Si E admet une base $(e_\iota)_{\iota \in I}$, montrer que les éléments $\varphi(e_{\iota_1} \otimes e_{\iota_2} \otimes \dots \otimes e_{\iota_n})$ distincts forment une base de $\overset{n}{\vee} E$, et que l'application linéaire de $\overset{n}{\vee} E$ dans le A-module $A[X_\iota]_{\iota \in I}$ qui, à tout élément $\varphi(e_{\iota_1} \otimes e_{\iota_2} \otimes \dots \otimes e_{\iota_n})$ fait correspondre

le monome $X_{\iota_1} X_{\iota_2} \dots X_{\iota_n}$ est un isomorphisme de $\bigvee^n E$ sur le sous-module H_n des polynomes homogènes de degré n par rapport aux X_ι.

Montrer que, dans ce cas, $\bigvee^n E$ est aussi isomorphe au module des tenseurs contravariants symétriques d'ordre n sur E (établir une correspondance biunivoque entre les bases de ces deux modules).

3) Montrer que l'application $(z,z') \to z.z'$ de $(\bigotimes^m E) \times (\bigotimes^n E)$ dans $\bigotimes^{m+n} E$ est compatible avec les relations d'équivalence modulo S_m, modulo S_n et modulo S_{m+n} dans les modules $\bigotimes^m E$, $\bigotimes^n E$ et $\bigotimes^{m+n} E$ respectivement ; par passage aux quotients, on en déduit une application bilinéaire, dite produit symétrique, de $(\bigvee^m E) \times (\bigvee^n E)$ dans $\bigvee^{m+n} E$. Lorsque E admet une base $(e_\iota)_{\iota \in I}$, et qu'on identifie $\bigvee^m E$, $\bigvee^n E$ et $\bigvee^{m+n} E$ avec les sous-modules H_m, H_n et H_{m+n} de $A[X_\iota]_{\iota \in I}$ (au moyen des isomorphismes définis dans l'exerc.2 à partir de la base (e_ι)), montrer que le produit symétrique n'est autre que le produit dans l'anneau $A[X_\iota]_{\iota \in I}$.

4) Soit $\underline{S}$ l'opérateur de symétrie $\sum_{\sigma \in \mathfrak{S}_n} \sigma$ dans le produit tensoriel $\bigotimes^n E$ (chap.III, § 4, n° ; on a donc $\underline{S} z = \sum_{\sigma \in \mathfrak{S}_n} \sigma z$) ; pour tout tenseur $z \in \bigotimes^n E$, $\underline{S} z$ est un tenseur symétrique, dit symétrisé de z. montrer que si, dans E, l'équation $n!x=a$ admet une solution et une seule pour tout $a \in E$, tout tenseur symétrique d'ordre n sur E est symétrisé d'un tenseur d'ordre n sur E ; en outre, la représentation biunivoque associée à l'application linéaire $z \to \underline{S} z$ de $\bigotimes^n E$ dans lui-même, est un isomorphisme de $\bigvee^n E$ sur le sous-module des tenseurs symétriques.

Donner un exemple de module E tel que le sous-module des tenseurs symétriques et le sous-module des tenseurs symétrisés d'ordre n ne soient pas isomorphes (cf. chap.III, § 4, exerc.)

5) Montrer que, si un module E est somme directe de deux sous-modules E_1, E_2, la puissance symétrique $\overset{n}{\vee} E$ est isomorphe à la somme directe des n+1 modules $(\overset{p}{\vee} E_1) \otimes (\overset{n-p}{\vee} E_2)$, où $0 \leqslant p \leqslant n$ (méthode de l'exerc. du chap. III, § 4). Généraliser au cas où E est somme directe d'un nombre fini quelconque de sous-modules.

6) Soit u une application linéaire d'un module E dans un module F, u_n la puissance tensorielle n-ème de u ; on a $u_n(S_n(E)) \subset S_n(F)$, et par passage aux quotients, on déduit de u_n une application linéaire $\overset{n}{\vee} u$ de $\overset{n}{\vee} E$ dans $\overset{n}{\vee} F$, dite puissance symétrique n-ème de u. Montrer que, si E et F sont deux espaces vectoriels sur un même corps commutatif A, et si u est de rang fini r, $\overset{n}{\vee} u$ est une application de rang $\binom{r+n-1}{n}$ (méthode de l'exerc. du chap. III, § 4).

7) Soit E une algèbre sur un anneau A, $(H_\lambda)_{\lambda \in L}$ une stratification de E suivant un monoïde L. Soit φ une représentation de L sur un monoïde M ; pour tout $\mu \in M$, soit H'_μ la somme (directe) des H_λ tels que $\varphi(\lambda) = \mu$; montrer que les H'_μ forment une stratification de E suivant le monoïde M.

8) Soient E, F deux algèbres sur un anneau A, $(H_\lambda)_{\lambda \in L}$ une stratification de E suivant le monoïde L, $(H'_\mu)_{\mu \in M}$ une stratification de F suivant le monoïde M. Montrer que, dans le produit tensoriel $E \otimes F$, les sous-modules $H_\lambda \otimes H'_\mu$ forment une stratification de $E \otimes F$ suivant le monoïde $L \times M$.

9) Soit E une algèbre sur un anneau A, $(H_\lambda)_{\lambda \in L}$ une stratification de E suivant un monoïde L. Soit $\mathfrak{a}$ un idéal à gauche (resp. à droite bilatère) de E, engendré par une famille (u_ι) d'éléments homogènes ; si C_λ est le composant homogène de $\mathfrak{a}$ dans H_λ, montrer que $\mathfrak{a}$ est somme directe des C_λ. Lorsque $\mathfrak{a}$ est un idéal bilatère, en déduire que les images canoniques des H_λ dans l'algèbre quotient

E/α forment une stratification de cette algèbre suivant L .

10) a) Soit M un monoïde muni d'une relation d'ordre $x \leqslant y$ telle que M soit totalement ordonné par cette relation, et que les relations $x < y$, $x' \leqslant y'$ entraînent $x \top x' < y \top y'$ (où $\top$ désigne la loi de composition dans M). Montrer que si A est un anneau d'intégrité (ayant un élément unité), l'algèbre du monoïde M relative à A est un anneau d'intégrité.

b) On suppose en outre que M est un groupe abélien, noté additivement, tel que pour tout couple d'éléments $\alpha > 0$, $\beta > 0$ de M , il existe un entier $n > 0$ tel que $\beta < n\alpha$. Généraliser à l'algèbre du groupe M la division euclidienne des polynomes à une indéterminée.

11) Si A est un anneau d'intégrité, f et g deux polynomes de $A[X_\iota]_{\iota \in I}$ tels que fg soit homogène et $\neq 0$, montrer que f et g sont homogènes. En particulier, montrer que les éléments inversibles de l'anneau $A[X_\iota]_{\iota \in I}$ sont les éléments inversibles de A .

12) Soit A un anneau commutatif quelconque ayant un élément unité, $u = \sum_{k=0}^{m} a_k X^k$ un diviseur de 0 dans l'anneau $A[X]$. Montrer que, si $v = \sum_{k=0}^{n} \beta_k X^k$ est un élément $\neq 0$ de $A[X]$, de degré $n > 0$, tel que $uv = 0$, il existe un polynome $w \neq 0$ de degré $\leqslant n-1$, tel que $uw = 0$ (se ramener au cas où $\beta_0 \neq 0$; si $a_k v = 0$ pour $0 \leqslant k \leqslant m-1$, montrer qu'on peut prendre $w = \beta_0$; si $a_k v = 0$ pour $0 \leqslant k < p \leqslant m-1$, et $a_p v \neq 0$, montrer qu'on peut prendre $w = \sum_{k=0}^{n-1} a_p \beta_{k+1} X^k$). En déduire qu'il existe un élément $v \neq 0$ de A tel que $vu = 0$.

§2. Fonctions polynomes.

1. Opérateurs polynomes.

Soit A un anneau commutatif ayant un élément unité, E une algèbre sur A , commutative ou non, ayant un élément unité e . Pour tout polynome

$f = a_0 + a_1 X + \ldots + a_n X^n$ de l'anneau $A[X]$ des polynomes à une indéterminée sur A, et tout élément $x \in E$, on pose $f(x) = a_0 e + a_1 x + \ldots + a_n x^n$.

Plus généralement, soit $\mathcal{x} = (x_\iota)_{\iota \in I}$ une famille d'éléments de E, deux à deux permutables. Pour tout polynome $f = \sum_{(n_\iota)} a_{(n_\iota)} \prod_{\iota \in I} X_\iota^{n_\iota}$ de l'anneau $A[X_\iota]_{\iota \in I}$, on pose $f(\mathcal{x}) = f((x_\iota)) = \sum_{(n_\iota)} a_{(n_\iota)} \prod_{\iota \in I} x_\iota^{n_\iota}$. On dit que l'élément $f(\mathcal{x})$ est obtenu en substituant l'élément x_ι à l'indéterminée X_ι dans le polynome f, pour tout $\iota \in I$.

PROPOSITION 1.- Si $\mathcal{x} = (x_\iota)_{\iota \in I}$ est une famille d'éléments deux à deux permutables de l'algèbre E, l'application $f \longrightarrow f(\mathcal{x})$ de l'algèbre des polynomes $A[X_\iota]_{\iota \in I}$ dans l'algèbre E est une représentation. L'image de $A[X_\iota]_{\iota \in I}$ par cette représentation est la sous-algèbre (commutative) de E engendrée par l'ensemble formé de l'élément unité e et des éléments x_ι $(\iota \in I)$.

Soient f, g deux éléments de $A[X_\iota]_{\iota \in I}$, a un élément de A, et posons $h_1 = f + g$, $h_2 = af$, $h_3 = fg$. Il faut prouver que $h_1(\mathcal{x}) = f(\mathcal{x}) + g(\mathcal{x})$, $h_2(\mathcal{x}) = af(\mathcal{x})$ et $h_3(\mathcal{x}) = f(\mathcal{x})g(\mathcal{x})$. Les deux premières relations sont évidentes ; en tenant compte de la formule de distributivité dans E, on se ramène à démontrer la troisième formule lorsque f et g sont des monômes ; elle résulte alors de la définition du produit de deux monômes, et de l'hypothèse que les x sont deux à deux permutables. Il est clair que l'image de $A[X_\iota]_{\iota \in I}$ par la représentation $f \longrightarrow f(\mathcal{x})$ est une sous-algèbre de E, contenant e et les x_ι ; d'autre part, toute sous-algèbre de E contenant ces éléments contient aussi tous les $f(\mathcal{x})$; donc l'ensemble des $f(\mathcal{x})$, où f parcourt $A[X_\iota]_{\iota \in I}$, est bien la sous-algèbre de E engendrée par l'ensemble formé de e et des éléments x_ι ; on notera cette sous-algèbre $A[\mathcal{x}]$, ou $A[x_\iota]_{\iota \in I}$.

Lorsque I est une partie finie de $\mathbb{N}$ (cas le plus fréquent) et $(i_k)_{1 \leqslant k \leqslant p}$ les éléments de I rangés en une suite strictement croissante, on écrit le plus souvent $f(x_{i_1}, x_{i_2}, \ldots, x_{i_p})$ et $A[x_{i_1}, x_{i_2}, \ldots, x_{i_p}]$ au lieu de $f((x_\iota))$ et $A[X_\iota]_{\iota \in I}$.

COROLLAIRE.- *La sous-algèbre* $A[x]$ *de* E *engendrée par* e *et les éléments de la famille* $x=(x_\iota)$ (deux à deux permutables), *est isomorphe à l'algèbre quotient* $A[X_\iota]_{\iota \in I}/\mathfrak{a}$, *où* $\mathfrak{a}$ *est l'idéal de* $A[X_\iota]_{\iota \in I}$ *formé des polynomes* f *tels que* $f(x)=0$.

L'idéal $\mathfrak{a}$ est appelé (par abus de langage) *l'idéal des relations algébriques entre les* x_ι (ou des *relations algébriques satisfaites par* x, lorsque la famille (x_ι) se réduit à un seul terme x) ; en général, il n'est pas réduit à 0, donc la représentation $f \longrightarrow f(x)$ n'est pas un isomorphisme de $A[X_\iota]_{\iota \in I}$ sur $A[x]$.

Par exemple, dans l'anneau $\mathbb{Z}[X]$ des polynomes à une indéterminée sur l'anneau $\mathbb{Z}$ des entiers rationnels, le polynome $f=X^2-4$ n'est pas nul, mais on a $f(2)=0$.

PROPOSITION 2.- *Soient* A, A' *deux anneaux commutatifs isomorphes ayant un élément unité,* φ *un isomorphisme de* A *sur* A'. *Soit* E (resp. E') *une algèbre sur* A (resp. A') *ayant un élément unité* e (resp. e'), $x=(x_\iota)_{\iota \in I}$ (resp. $x'=(x'_\iota)_{\iota \in I}$) *une famille d'éléments de* E (resp. E') *deux à deux permutables. Soit* $\bar{\varphi}$ *l'isomorphisme de* $A[X_\iota]_{\iota \in I}$ *sur* $A'[X]_{\iota \in I}$ *qui prolonge* φ *et laisse invariants les* X_ι (§ 1, prop. 1). *Si l'image par* $\bar{\varphi}$ *de l'idéal* $\mathfrak{a}$ *des relations algébriques entre les* x_ι *est l'idéal* $\mathfrak{a}'$ *des relations algébriques entre les* x'_ι, *il existe un isomorphisme* ψ *et un seul de l'anneau* $A[x]$ *sur l'anneau* $A'[x']$ *tel que* $\psi(x_\iota)=x'_\iota$ *pour tout* $\iota \in I$, *et* $\psi(ae)=\varphi(a)e'$ *pour tout* $a \in A$.

En effet, comme $\bar{\varphi}(\mathfrak{a}) = \mathfrak{a}'$, il existe un isomorphisme de l'anneau $A[X_\iota]_{\iota\in I}/\mathfrak{a}$ sur $A'[X_\iota]_{\iota\in I}/\mathfrak{a}'$ qui, à la classe modulo $\mathfrak{a}$ d'un élément z de $A[X_\iota]_{\iota\in I}$ fait correspondre la classe modulo $\mathfrak{a}'$ de $\bar{\varphi}(z)$; en particulier à la classe de $a \in A$ (modulo $\mathfrak{a}$) correspond la classe (modulo $\mathfrak{a}'$) de $\varphi(a)$, et à la classe (modulo $\mathfrak{a}$) de X_ι correspond la classe (modulo $\mathfrak{a}'$) de X_ι ; l'existence de l'isomorphisme γ résulte donc du corollaire de la prop.1 ; son unicité est immédiate, d'après la forme des éléments de $A'[\times']$.

Remarques.- 1) On sait que tout anneau E peut être considéré comme une algèbre sur l'anneau $\mathbb{Z}$ des entiers rationnels (avec la loi de composition $(n,x) \to n.x$; cf.chap.II, § 7, n°). La prop.1 détermine donc la structure du sous-anneau d'un anneau E (sans opérateur, ou, ce qui revient au même, considéré comme algèbre sur $\mathbb{Z}$) engendré par l'élément unité de E et une famille d'éléments de E deux à deux permutables.

2) On notera que pour appliquer la prop.1, il n'est pas nécessaire que l'application $a \to ae$ de A dans E soit un isomorphisme. Par exemple, si E est une algèbre sur $\mathbb{Z}$, on peut avoir $n.x=0$ pour tout $x \in E$ et un entier $n \neq 0$ (lorsque la caractéristique de E est $=0$ et divise n).

3) L'application $(f,x) \to f(x)$ de $A[X] \times E$ dans E est une loi de composition externe sur E, ayant $A[X]$ comme anneau d'opérateurs. La prop.1 montre que cette loi est distributive, d'une part par rapport à l'ensemble des deux lois additives dans $A[X]$ et E, d'autre part par rapport à l'ensemble des deux lois multiplicatives de ces anneaux (cf.chap.I, § 5, n°). Le polynome X est opérateur neutre pour cette loi externe. Enfin, si on restreint l'ensemble des opérateurs au sous-anneau A de $A[X]$,

on retrouve la loi externe de l'algèbre E .

4) Lorsque l'algèbre E n'a pas d'élément unité, on peut encore définir $f(x)$ pour toute famille $x=(x_\iota)$ d'éléments de E deux à deux permutables, et tout polynome $f \in A[X_\iota]_{\iota\in I}$, sans terme constant. Si B est la sous-algèbre de $A[X_\iota]_{\iota\in I}$ formée par ces polynomes, l'application $f \longrightarrow f(x)$ de B dans E est une représentation, et l'image de B par cette représentation est la sous-algèbre de E engendrée par l'ensemble des x_ι .

Lorsque l'algèbre E est commutative, on peut évidemment substituer à chaque X_ι , dans un polynome $f \in A[X_\iota]_{\iota\in I}$, un élément quelconque x_ι de E . Considérons en particulier le cas où E est une algèbre de polynomes $A[Y_\lambda]_{\lambda\in L}$; pour toute famille $(g_\iota)_{\iota\in I}$ de polynomes de cette algèbre, on peut alors définir le polynome $h=f((g_\iota))$ (appartenant à $A[Y_\lambda]_{\lambda\in L}$) obtenu par substitution des g_ι aux X_ι ; on vérifie aussitôt que si $(y_\lambda)_{\lambda\in L} = y$ est une famille d'éléments deux à deux permutables dans une algèbre F sur A , ayant un élément unité, on a $h(y)=f((g_\iota(y)))$. On peut plus particulièrement prendre pour E l'algèbre $A[X_\iota]_{\iota\in I}$ elle-même ; cela permet entre autres d'écrire $f=f((X_\iota))$ ($f=f(X_1,X_2,\ldots,X_n)$ pour les polynomes à n indéterminées), en substituant X_ι à lui-même. De même, substituons à X_ι le polynome $X_\iota+a_\iota$, où a_ι est un élément quelconque de A ; si $h=f((X_\iota + a_\iota))$, le terme constant de h s'obtient en substituant 0 à chacun des X_ι , donc est égal à $f((a_\iota))$ d'après ce qui précède.

Prenons maintenant pour E l'algèbre des polynomes (sur A) par rapport aux indéterminées X et à une autre indéterminée Z ; on a $E=B[Z]$, où $B=A[X_\iota]_{\iota\in I}$. Alors :

PROPOSITION 3.- Pour tout polynome $f \in A[X_\iota]_{\iota \in I}$, la partie homogène f_k de degré k de f est égale au coefficient du terme en Z^k dans le polynome $f((X Z))$ (considéré comme polynome en Z, à coefficients dans $A[X_\iota]_{\iota \in I}$).

Il suffit de le démontrer pour un monôme, et dans ce cas la proposition est immédiate.

COROLLAIRE.- Pour qu'un polynome $f \in A[X_\iota]_{\iota \in I}$ soit homogène et de degré k, il faut et il suffit que

$$f((X_\iota Z)) = f((X_\iota))Z^k \quad . \tag{1}$$

2. Fonctions polynomes sur une algèbre.

Soit A un anneau commutatif ayant un élément unité, E une algèbre sur A ayant un élément unité e (on ne suppose pas que la représentation $a \longrightarrow ae$ de A dans E soit un isomorphisme). Pour tout polynome $f \in A[X]$, $f(x)$ est défini pour tout $x \in E$; l'application $x \longrightarrow f(x)$ est donc une application de E dans E, qu'on appelle fonction polynome associée au polynome f.

Supposons maintenant que l'algèbre E soit en outre commutative. Si I est un ensemble d'indices quelconque, f un polynome de l'algèbre $A[X_\iota]_{\iota \in I}$, $f(x)$ est défini pour toute famille $x = (x_\iota)_{\iota \in I}$ d'éléments de E, ayant I pour ensemble d'indices ; l'application $x \longrightarrow f(x)$ est donc une application de E^I dans E, qu'on appelle fonction polynome associée au polynome f. Une fonction polynome définie dans E^I est donc une application de la forme

$$(x_\iota) \longrightarrow \sum_{(n_\iota)} a_{(n_\iota)} \prod_{\iota \in I} x_\iota^{n_\iota}$$

, où (n_ι) parcourt $\mathcal{N}^{(I)}$, et où les $a_{(n_\iota)}$ sont nuls sauf pour un nombre fini d'éléments de $\mathcal{N}^{(I)}$.

Par exemple, si à toute "suite double" (x_{ij}) $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ d'éléments d'un anneau quelconque (sans opérateur) E, on fait correspondre le déterminant $\det(x_{ij})$ de la matrice carrée (x_{ij}),

on définit une fonction polynome associée au polynome $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon_\sigma X_{1,\sigma(1)} X_{2,\sigma(2)} \cdots X_{n,\sigma(n)}$, c'est-à-dire au polynome $\det(X_{ij})$ dans l'anneau $\mathbb{Z}[X_{11}, \ldots, X_{nn}]$ des polynomes sur l'anneau $\mathbb{Z}$, par rapport aux n^2 indéterminées X_{ij} .

Pour tout polynome f de l'algèbre $A[X_\iota]_{\iota \in I}$, nous désignerons par $\tilde{f}$ la fonction polynome $x \longrightarrow f(x)$ qui lui est associée (application de E^I dans E). D'après la prop.1, l'application $f \longrightarrow \tilde{f}$ est une représentation de l'algèbre $A[X_\iota]_{\iota \in I}$ dans l'algèbre E^{E^I} des applications de l'ensemble E^I dans l'algèbre E . Nous allons voir que cette représentation n'est pas toujours un isomorphisme (autrement dit qu'une même fonction polynome peut être associée à plusieurs polynomes distincts ou encore qu'il peut exister des polynomes $f \neq 0$ tels que $f(x)=0$ pour tout $x \in E^I$) ; nous obtiendrons en même temps des conditions suffisantes pour qu'elle le soit.

Même lorsque la représentation $f \longrightarrow \tilde{f}$ n'est pas un isomorphisme, l'application $x \longrightarrow f(x)$ se note souvent f , par abus de langage; aucune confusion n'est possible dans ce cas, si on a soin de préciser, lorsqu'on introduit l'élément f , s'il s'agit du polynome f ou de la fonction polynome f .

3. Racines d'un polynome à une indéterminée.

Etant donnés un polynome $f \in A[X_\iota]_{\iota \in I}$, et une algèbre commutative E sur A (ayant un élément unité), on dit qu'un élément $x=(x_\iota)$ de E^I est un zéro du polynome f dans E^I si $f(x)=0$. Si f est un polynome par rapport à une seule indéterminée X , un zéro x du polynome f dans E s'appelle encore racine du polynome f dans E .

Nous allons d'abord considérer les racines d'un polynome $f \in A[X]$ dans l'anneau A (considéré comme algèbre par rapport à lui-même).

PROPOSITION 4.- Pour que a soit racine de f dans A, il faut et il suffit que $X-a$ soit un diviseur de f dans $A[X]$.

En effet, comme $X-a$ est un polynome unitaire, il existe un polynome $g \in A[X]$ et un élément β de A tels que $f=(X-a)g+\beta$ (§ 1, prop.4). On tire de cette identité que $f(a)=\beta$, donc si $f(a)=0$, $X-a$ divise f ; la réciproque est évidente.

Si a est racine dans A d'un polynome $f \neq 0$ de $A[X]$, f peut être divisible par une puissance $(X-a)^h$ de $X-a$, d'exposant $h > 1$; comme $(X-a)^h$ est unitaire, il n'est pas diviseur de 0 dans $A[X]$; si $f=(X-a)^h g$, le polynome g est donc déterminé de façon unique, et on a $\deg f = h + \deg g$. On peut donc poser la définition suivante :

DEFINITION 1.- On appelle ordre de multiplicité d'une racine a de A d'un polynome $f \neq 0$ de $A[X]$ le plus grand des entiers h tels que $(X-a)^h$ divise f. Une racine dont l'ordre de multiplicité est k est dite racine multiple d'ordre k.

Une racine multiple d'ordre 1 est dite racine simple ; une racine multiple d'ordre 2 (resp. 3,4,...) est dite racine double (resp. triple, quadruple,...)

Pour que $a \in A$ soit racine multiple d'ordre k de f dans A, il faut et il suffit que $f=(X-a)^k g$, où le polynome g n'est pas divisible par $X-a$; d'après la prop.4, il revient au même de dire que $g(a) \neq 0$. Comme $\deg f = k + \deg g$, on a la relation $k \leqslant \deg f$.

Remarques.- 1) Pour un polynome $f \neq 0$ de $A[X]$, on étend la déf.1 aux éléments quelconques $a \in A$, en convenant que lorsque a n'est pas racine de f, son ordre de multiplicité par rapport à f est égal à 0.

2) Dire que l'ordre de multiplicité d'un élément $a \in A$ par rapport à un polynome $f \neq 0$, est $\geqslant h$ signifie que $(X-a)^h$ divise f ; par extension, on convient de dire que pour tout $h \geqslant 0$, l'ordre de multiplicité de a par rapport au polynome 0 est $\geqslant h$; dire que l'ordre de multiplicité de a par rapport à un polynome quelconque f est $\geqslant h$ équivaut alors à dire que $(X-a)^h$ divise f.

3) Si B est un sous-anneau de A, f un polynome de $B[X] \subset A[X]$, a un élément de B qui est racine de f, l'ordre de multiplicité de a par rapport à f est le même, que l'on considère f comme élément de $B[X]$ ou de $A[X]$; en effet, les relations $(X-a)^h g(X)=(X-a)^k g_1(X)$, où $g \in A[X]$, $g_1 \in B[X]$ et $g(a) \neq 0$, $g_1(a) \neq 0$, ne sont possibles que si $h=k$ (puisque $X-a$ n'est pas diviseur de 0 dans $A[X]$).

PROPOSITION 5.- Soient f,g deux polynomes non nuls de $A[X]$, a un élément de A, p et q les ordres de multiplicité de a par rapport à f et g respectivement.

1° L'ordre de multiplicité de a par rapport à $f+g$ est $\geqslant \mathrm{Min}(p,q)$ il est égal à $\mathrm{Min}(p,q)$ si $p \neq q$.

2° L'ordre de multiplicité de a par rapport à fg est $\geqslant p+q$; si A est un anneau d'intégrité, cet ordre de multiplicité est égal à $p+q$.

En effet, on a $f(X)=(X-a)^p f_1(X)$, $g(X)=(X-a)^q g_1(X)$, avec $f_1(a) \neq 0$ et $g_1(a) \neq 0$; supposons par exemple que $p \leqslant q$; alors $f(X)+g(X)=(X-a)^p(f_1(X)+(X-a)^{q-p}g_1(X))$, et si $p < q$, a n'est pas racine de $f_1(X)+(X-a)^{q-p}g_1(X)$, ce qui démontre la première partie de la proposition. La seconde résulte de même de la formule $f(X)g(X)=(X-a)^{p+q}f_1(X)g_1(X)$, et du fait que $f_1(a)g_1(a) \neq 0$ si A est un anneau d'intégrité.

THEOREME 1.- Soit A un anneau d'intégrité (ayant un élément unité) f un polynome de $A[X]$, de degré $n \geqslant 0$; si a_i $(1 \leqslant i \leqslant p)$ sont p racines distinctes de f dans A, k_i $(1 \leqslant i \leqslant p)$ l'ordre de multiplicité de la racine a_i de f, le polynome f est divisible par $(X-a_1)^{k_1}(X-a_2)^{k_2}\dots(X-a_p)^{k_p}$; en particulier, la somme des ordres de multiplicité de toutes les racines de f dans A est $\leqslant n$.

La dernière partie du théorème est une conséquence immédiate de la première et du cor.1 du th.1 du §1 . Pour démontrer la première partie, nous procéderons par récurrence sur p , le théorème étant évident pour p=1 en vertu de la déf.1 . Supposons donc que l'on ait

$$f(X)=(X-a_1)^{k_1}(X-a_2)^{k_2}\dots(X-a_{p-1})^{k_{p-1}}g(X) \tag{2}$$

où $g \in A[X]$; comme a_p est racine d'ordre k_p de f, et n'est pas racine du polynome $\prod_{i=1}^{p-1}(X-a_i)^{k_i}$ puisque $a_i-a_p \neq 0$ par hypothèse pour $1 \leqslant i \leqslant p-1$, et que A est un anneau d'intégrité, il résulte de la prop.5 que a_p est racine d'ordre k_p de g ; g est donc divisible par $(X-a_p)^{k_p}$, d'où le théorème.

COROLLAIRE 1.- Soit A un anneau d'intégrité, f un polynome de $A[X]$, nul ou de degré $\leqslant n$. Si la fonction polynome $\tilde{f}$ sur A s'annule pour n+1 valeurs distinctes de la variable, on a f=0 .

En effet, tout polynome $\neq 0$ et de degré $p \leqslant n$ au plus p racines distinctes dans A .

COROLLAIRE 2.- Soit A un anneau d'intégrité ; si f et g sont deux polynomes de $A[X]$, nuls ou de degré $\leqslant n$, et tels que les fonctions polynomes $\tilde{f}$ et $\tilde{g}$ sur A aient des valeurs égales pour n+1 valeurs distinctes de la variable, on a f=g .

Il suffit d'appliquer le cor.1 à f-g .

2 Le th.1 et ses corollaires sont inexacts lorsque l'anneau A possède des diviseurs de 0 . Par exemple, dans l'anneau $A=\mathbb{Z}/(16)$, le polynome X^2 a quatre racines distinctes, savoir les classes (modulo 16) de 0,4,8 et 12. Même lorsque A est un corps ayant une infinité d'éléments, et E une algèbre ayant un élément unité qu'on peut identifier à l'élément unité de A (le corps A étant ainsi identifié à un sous-corps du centre de E) , un polynome $\neq 0$ de $A[X]$ peut avoir une infinité de zéros dans E . Par exemple, si a et b sont deux éléments de E , linéairement indépendants, et tels que $a^2=ab=ba=b^2=0$, tous les éléments $a+\lambda b$ où λ parcourt A , sont des zéros du polynome X^2 (cf. exerc.7).

Application : Formule d'interpolation de Lagrange.- Soit K un corps commutatif, α_i $(1\leqslant i\leqslant n)$ n éléments distincts de K , β_i $(1\leqslant i\leqslant n)$ n éléments quelconques (distincts ou non) de K . Proposons-nous de déterminer les polynomes $f\in K[X]$ tels que $f(\alpha_i)=\beta_i$ pour $1\leqslant i\leqslant n$. Si f et g sont deux polynomes ayant cette propriété, et si $h=f-g$, on a $h(\alpha_i)=0$ pour $1\leqslant i\leqslant n$, et il résulte du th.1 que $h(X)=(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)q(X)$, où q est un polynome arbitraire de $K[X]$; il suffit donc d'avoir une solution du problème pour les avoir toutes. Supposons d'abord que $\beta_k=1$ et $\beta_i=0$ pour tout $i\neq k$; tout polynome répondant à la question est alors divisible par $(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_{k-1})(X-\alpha_{k+1})\dots(X-\alpha_n)$ d'après le th.1 ; montrons qu'on peut trouver un scalaire $\lambda\in K$ tel que le polynome $u_k(X)=\lambda(X-\alpha_1)\dots(X-\alpha_{k-1})(X-\alpha_{k+1})\dots(X-\alpha_n)$ soit une solution ; la condition $u_k(\alpha_k)=1$ donne en effet

$$\lambda(\alpha_k-\alpha_1)\dots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\dots(\alpha_k-\alpha_n)=1$$

d'où on tire λ puisque les $\alpha_k-\alpha_i$ sont $\neq 0$ par hypothèse pour $i\neq k$

Le polynome u_k étant ainsi déterminé pour $1 \leqslant k \leqslant n$, revenons au cas général où les β_i sont quelconques ; il est immédiat que le polynome $f = \sum_{i=1}^{n} \beta_i u_i$ répond à la question ; son degré est $\leqslant n-1$, et c'est évidemment le seul polynome solution ayant cette propriété (cor. 2 du th.1) ; l'expression trouvée

$$f(X) = \sum_{i=1}^{n} \beta_i \frac{(X-a_1)\ldots(X-a_{i-1})(X-a_{i+1})\ldots(X-a_n)}{(a_i-a_1)\ldots(a_i-a_{i-1})(a_i-a_{i+1})\ldots(a_i-a_n)}$$

est dite formule d'interpolation de Lagrange.

4. Fonctions polynomes sur un anneau d'intégrité ayant une infinité d'éléments.

PROPOSITION 6.- Soit A un anneau d'intégrité (admettant un élément unité) qui a une infinité d'éléments. Pour tout polynome $f \neq 0$ de $A[X_1, X_2, \ldots, X_n]$, il existe une infinité d'éléments $x = (x_1, \ldots, x_n)$ de A^n, tels que $f(x) \neq 0$.

La proposition est vraie pour $n=1$, d'après le cor.1 du th.1 ; nous la démontrerons par récurrence sur n. Le polynome f peut être considéré comme un polynome à une indéterminée X_n sur l'anneau $A[X_1, \ldots, X_{n-1}]$, soit $f = \sum_{k=0}^{p} g_k X_n^k$; comme $f \neq 0$, il y a au moins un coefficient $g_i \in A[X_1, \ldots, X_{n-1}]$ qui n'est pas nul. D'après l'hypothèse de récurrence, il existe $(x_1, x_2, \ldots, x_{n-1})$ dans A^{n-1}, tel que $g_i(x_1, x_2, \ldots, x_{n-1}) \neq 0$. Il en résulte que le polynome $h = \sum_{k=0}^{p} g_k(x_1, \ldots, x_{n-1}) X_n^k$ de $A[X_n]$ n'est pas nul ; d'après le cor.1 du th.1, il existe une infinité d'éléments $x_n \in A$ tels que $h(x_n) \neq 0$; comme $h(x_n) = f(x_1, x_2, \ldots, x_{n-1}, x_n)$, la proposition est démontrée.

COROLLAIRE.- Si A est un anneau d'intégrité ayant une infinité d'éléments, l'application $f \to \tilde{f}$ de l'algèbre de polynomes $A[X_\iota]_{\iota \in I}$ dans l'algèbre A^{A^I} des applications de A^I dans A, est un isomorphisme.

En effet, soit f un polynome $\neq 0$ de $A[X_\iota]_{\iota\in I}$; il existe une partie finie J de I telle que f appartienne à $A[X_\iota]_{\iota\in J}$; d'après la prop.6 , il existe un élément $y=(y_\iota)_{\iota\in J}$ de A^J tel que, pour tout élément $x=(x_\iota)_{\iota\in I}$ de A^I dont la projection sur A^J est y , on ait $f(x)\neq 0$, ce qui démontre le corollaire.

En d'autres termes, ni pour tout élément $x=(x_\iota)\in A^I$, on a $\sum_{(n_\iota)\ \text{tout}\ (n_\iota)\in \mathfrak{N}(I)} a_{(n_\iota)} \prod_\iota x_\iota^{n_\iota} = 0$, on a nécessairement $a_{(n_\iota)}=0$ pour

Lorsque A est un anneau d'intégrité ayant une infinité d'éléments (ce qui est le cas le plus fréquent dans les applications) on identifie le plus souvent l'anneau $A[X_\iota]_{\iota\in I}$, à l'aide de l'isomorphisme $f\to\tilde{f}$, avec l'anneau des fonctions polynomes correspondantes ; lorsqu'on parle d'un "polynome défini dans A^I , à coefficients dans A " , c'est d'une fonction polynome qu'il est question.

Avec l'abus de langage habituel qui consiste à confonde une fonction et sa valeur pour un élément générique (Ens.R , § 2) on parlera donc du "polynome $f(x)$" , ou du "polynome $a_0+a_1x+\ldots+a_nx^n$ " . Tant que les conditions précédentes sont remplies, ce langage ne peut causer aucun inconvénient.

Remarques.- 1) Soit E une algèbre commutative sur A , ayant un élément unité e , tel que A puisse être identifié à la sous-algèbre Ae de E . Si A est un anneau d'intégrité ayant une infinité d'éléments, l'application $f\to\tilde{f}$ de $A[X_\iota]_{\iota\in I}$ dans l'algèbre E^{E^I} des applications de E^I dans E est encore un isomorphisme, car pour tout polynome $f\neq 0$ de $A[X_\iota]_{\iota\in I}$, il existe un élément $x\in A^I\subset E^I$ tel que $f(x)\neq 0$. Lorsqu'il s'agit de polynomes à une seule indéterminée, il n'est pas nécessaire de supposer E commutative (cf. exerc. 11).

2) Soient H_i $(1 \leqslant i \leqslant n)$ n parties infinies de l'anneau d'intégrité A . Si un polynome $f \in A[X_1, X_2, .., X_n]$ est tel que, pour tout élément $x = (x_i) \in \prod_{i=1}^{n} H_i$, on a $f(x)=0$, alors $f=0$; la proposition est une conséquence évidente du cor.1 du th.1 lorsque n=1 , et se démontre par récurrence sur n comme la prop.6, en remplaçant l'ensemble A^n par l'ensemble $\prod_{i=1}^{n} H_i$ dans la démonstration de cette proposition.

3) Dans l'énoncé du cor.de la prop.6, l'anneau A est assujetti à deux conditions : 1° être un anneau d'intégrité ; 2° avoir une infinité d'éléments. Le résultat devient inexact si on suppose seulement que A vérifie l'une de ces deux conditions, mais non l'autre.

Par exemple, si A est un corps ayant un nombre fini q d'éléments, le groupe multiplicatif A^* des éléments $\neq 0$ de A est alors d'ordre q-1 ; on a donc $x^{q-1}=1$ pour tout élément $x \neq 0$ de A (chap.I, § 6, formule ( )), et par suite $x^q = x$ pour tout $x \in A$; cela montre que la fonction polynome correspondant au polynome $X^q - X \neq 0$ de $A[X]$ est identiquement nulle dans A .

Avec les mêmes hypothèses sur A , soit maintenant B l'anneau produit A^I , où I est un ensemble infini,. L'anneau B a une infinité d'éléments, mais la fonction polynome correspondant au polynome $X^q - X \neq 0$ de $B[X]$ est encore identiquement nulle dans B .

On notera toutefois que les deux conditions précédentes ne sont pas nécessaires pour que l'application $f \longrightarrow \tilde{f}$ de $A[X_\iota]_{\iota \in I}$ dans l'algèbre des applications de E^I dans E (où E est une algèbre donnée sur A , ayant un élément unité), soit un isomorphisme (cf.exerc.6). Un exemple intéressant est le suivant : A étant un anneau commutatif quelconque (ayant un élément unité),

$E=A[X_\iota]_{\iota\in I}$ une algèbre de polynomes sur A , pour tout polynome $f\neq 0$ dans $A[Y]$, la fonction polynome correspondante $\tilde{f}$ dans E n'est pas nulle, puisque $f(X_\iota)\neq 0$ pour tout indice ι par définition.

THEOREME 2 (principe de prolongement des identités algèbriques).- Soit A un anneau d'intégrité (admettant un élément unité) qui a une infinité d'éléments, $(g_i)_{1\leqslant i\leqslant m}$ une suite finie de polynomes non nuls de $A[X_1,X_2,\ldots,X_n]$. Si f est un polynome de $A[X_1,X_2,\ldots,X_n]$ tel que $f(x_1,x_2,\ldots,x_n)=0$ pour tout élément $(x_j)\in A^n$ tel que $g_i(x_1,x_2,\ldots,x_n)\neq 0$ pour $1\leqslant i\leqslant m$, on a $f=0$.

En effet, si on avait $f\neq 0$, le polynome $h=fg_1g_2\ldots g_m$ ne serait pas nul (§ 1, th.1), donc (prop.6) il existerait un élément $(x_1,x_2,\ldots,x_n)\in A^n$ tel que $h(x_1,x_2,\ldots,x_n)\neq 0$, ce qui contredit l'hypothèse.

Scholie.- Le th.2 fournit un moyen très commode pour démontrer qu'un polynome f par rapport à n indéterminées sur un anneau d'intégrité A (ayant un élément unité) est nul. Il suffit de considérer un anneau d'intégrité E , ayant une infinité d'éléments, contenant un sous-anneau isomorphe à A et ayant même élément unité que E ; si on démontre que $f(x_1,x_2,\ldots,x_n)=0$ pour tout élément $(x_j)\in E^n$ (ou seulement pour les éléments de E^n qui s'annulent pas un certain nombre fini de fonctions polynomes données, non identiquement nulles), on en conclut que $f=0$. Si A lui-même possède une infinité d'éléments, on peut prendre $E=A$, ou E identifie au corps des fractions de A ; sinon, on peut par exemple prendre pour E l'anneau $A[X]$ des polynomes à une indéterminée sur A (ou son corps des fractions).

Une fois démontrée la relation $f=0$, on en déduit évidemment $f(y_1,y_2,\ldots,y_n)=0$, pour tout élément $(y_i)\in F^n$, où F est une algèbre commutative quelconque sur A (ayant un élément unité e) ; F peut en particulier n'avoir qu'un nombre fini d'éléments, ou avoir des diviseurs de 0, et l'application $a \longrightarrow ae$ de A dans F peut ne pas être biunivoque.

En d'autres termes, la démonstration de l'identité $f(x_1,x_2,\ldots,x_n)=0$ lorsque les x_i parcourent un anneau d'intégrité ayant une infinité d'éléments, contenant A et ayant même élément unité que A, (avec éventuellement la restriction que $g_i(x_1,x_2,\ldots,x_n)\neq 0$ pour $1\leqslant i\leqslant m$, les g_i étant des polynomes non nuls) entraîne la même identité lorsque les x_i parcourent une algèbre commutative quelconque (ayant un élément unité) sur A.

En particulier, si un polynome f à n indéterminées, à coefficients entiers rationnels, est tel que $f(x_1,x_2,\ldots,x_n)=0$ lorsque les x_i parcourent le corps des nombres rationnels Q (avec éventuellement la restriction que $g_i(x_1,\ldots,x_n)\neq 0$, où les g_i sont des polynomes non nuls à coefficients entiers), on a la même identité lorsque les x_i parcourent un anneau commutatif quelconque ayant un élément unité (même lorsque cet anneau a une caractéristique >0), car le principe de prolongement des identités algèbriques montre que $f=0$ dans $Z[X_1,X_2,\ldots,X_n]$.

Exercices.- 1) a) Dans l'algèbre $A[X]$ des polynomes à une indéterminée sur un anneau A, l'application $(u,v) \longrightarrow u(v)$ est une loi de composition interne ; montrer que cette loi est associative et distributive à gauche par rapport à l'addition et à la multiplication dans $A[X]$.

b) Si A est un anneau d'intégrité, montrer que la relation $u(v)=0$ entraîne $u=0$ ou v constant, et que si $u\neq 0$ et v non constant, le degré de $u(v)$ est égal au produit des degrés de u et de v.

c) On suppose désormais que A est un <u>corps commutatif</u>. Soient u et v deux polynomes de degré >0 dans $A[X]$, f un polynome de degré >0 ; montrer que si q est le quotient et r le reste de la division euclidienne de u par v, $q(f)$ et $r(f)$ sont le quotient et le reste de la division euclidienne de $u(f)$ par $v(f)$.

d) Pour tout polynome f de $A[X]$, on désigne par $I(f)$ l'ensemble des polynomes de la forme $u(f)$, où u parcourt $A[X]$; c'est un sous-anneau de $A[X]$. Pour que $I(f)=I(g)$, il faut et il suffit que $g=af+\beta$, où $a\neq 0$ et β sont dans A.

e) Soit f et g deux polynomes de degré >0 dans $A[X]$; montrer que $I(f)\cap I(g)$ est identique à A ou est de la forme $I(h)$, où h est un polynome de degré >0 (écartant la première éventualité, considérer un polynome h de plus petit degré >0 dans $I(f)\cap I(g)$; remarquer ensuite que tout polynome u de $A[X]$ s'écrit d'une seule manière $\sum_k v_k h^k$, où $v_k=0$ ou $\deg v_k < \deg h$, et que si $u\in I(f)$, les v_k appartiennent aussi à $I(f)$ (utiliser c))).

2) Soit K un corps commutatif, $K[X]$ l'anneau des polynomes à une indéterminée sur K. Montrer que tout automorphisme s de l'anneau (sans opérateur) $K[X]$ laisse invariant K (cf. § 1 exerc. 11) et induit sur K un automorphisme σ_s de ce corps ; en outre, montrer qu'on a $s(X)=\lambda X+\mu$, où $\lambda\neq 0$ et μ sont dans K (utiliser l'exerc. 1b)) ; réciproquement, montrer que la donnée d'un automorphisme σ arbitraire de K et de deux éléments λ, μ de K ($\lambda\neq 0$) détermine un automorphisme s de $K[X]$ et un seul tel que $\sigma_s=\sigma$ et $s(X)=\lambda X+\mu$. Si G est le groupe de tous les automorphisme de

de l'anneau $K[X]$ sans opérateur, H le sous-groupe de G formé des automorphismes de l'algèbre $K[X]$ sur K , montrer que H est un sous-groupe distingué de G et que G/H est isomorphe au groupe des automorphismes du corps K ; le groupe H est isomorphe au groupe défini sur l'ensemble $K^* \times K$ par la loi de composition $(\lambda , \mu)(\lambda', \mu') = (\lambda\lambda', \lambda'\mu + \mu')$.

3) Soit A un anneau d'intégrité, f un polynome de l'anneau $A[X_1, X_2, \ldots, X_n]$, de degré $\leqslant k_i$ par rapport à X_i $(1 \leqslant i \leqslant n)$. Pour chaque valeur de i , soit H_i un ensemble de k_i+1 éléments de A . Montrer que, si on a $f(x_1, x_2, \ldots, x_n)=0$ pour tout élément $(x_i) \in \prod_{i=1}^{n} H_i$, on a $f=0$.

4) Soit A un anneau d'intégrité ayant une infinité d'éléments, et soit Φ un ensemble de polynomes $\neq 0$ de l'anneau $A[X_1, X_2, \ldots, X_n]$. Montrer que, si la puissance de Φ est strictement inférieure à celle de A , il existe une partie H de A^n , équipotente à A , telle que, pour tout $x = (x_i) \in H$ et pour tout $f \in \Phi$, on ait $f(x) \neq 0$.

5) Soit A un anneau d'intégrité ayant une infinité d'éléments, et soit B une partie infinie de A . Montrer que si f est un polynome de $A[X]$ de degré > 0 , l'image de B par la fonction polynome $x \longrightarrow f(x)$ est équipotente à B .

6) Soit A un anneau commutatif ayant un élément unité, et tel qu'il existe un sous-groupe infini G du groupe additif A , dont les éléments $\neq 0$ ne sont pas diviseurs de 0 dans A . Montrer que l'application $f \longrightarrow \tilde{f}$ de $A[X_1, X_2, \ldots, X_p]$ dans l'algèbre des applications de A^p dans A , est un isomorphisme (remarquer qu'un polynome de degré n à une indéterminée ne peut avoir plus de n racines distinctes appartenant à G). Il en est ainsi en particulier

quand il existe dans A un élément x_0 non diviseur de 0 et d'ordre infini dans le groupe additif A .

7) Soit K un corps de caractéristique $\neq 2$ contenant une infinité d'éléments, et soit Q une algèbre de quaternions sur K (chap.II, §7,n°) correspondant au couple (-1,-1). Montrer que le polynome X^2+1 a une infinité de zéros dans Q .

8) Soit K un corps fini à q éléments.

a) Dans l'anneau $K[X_1,X_2,\ldots,X_n]$ soit $\mathfrak{a}$ l'idéal engendré par les n polynomes $X_i^q-X_i$ $(1\leqslant i\leqslant n)$. Montrer que si $f\in\mathfrak{a}$, on a $f(x_1,x_2,\ldots,x_n)=0$ pour tout $(x_i)\in K^n$.

b) Si f est un polynome quelconque de $K[X_1,X_2,\ldots,X_n]$, montrer qu'il existe un polynome $\overline{f}$ et un seul, qui est nul ou tel que $\deg_i f\leqslant q-1$ pour $1\leqslant i\leqslant n$, et tel que $f\equiv\overline{f}$ (mod. $\mathfrak{a}$) ; on a $\deg\overline{f}\leqslant\deg f$; si f est tel que $f(x_1,x_2,\ldots,x_n)=0$, f appartient à l'idéal $\mathfrak{a}$, qui est donc l'image réciproque de 0 par la représentation $f\longrightarrow\tilde{f}$ (utiliser l'exerc. 3).

c) Soient $f_1,f_2,\ldots,f_m$ des polynomes $\neq 0$ de $K[X_1,X_2,\ldots,X_n]$, tels que $f_i(0,0,\ldots,0)=0$ $(1\leqslant i\leqslant m)$, et que la somme des degrés (totaux) des f_i soit $<n$. Montrer qu'il existe un élément $(x_1,\ldots x_n)\in K^n$ distinct de $(0,0,\ldots,0)$, et tel que $f_i(x_1,x_2,\ldots,x_n)=0$ pour tout i tel que $1\leqslant i\leqslant m$ (Remarquer que s'il n'en était pas ainsi, le polynome $\prod_{i=1}^{m}(1-f_i^{q-1})$ serait congru modulo $\mathfrak{a}$ au polynome $\prod_{j=1}^{n}(1-X_j^{q-1})$, et utiliser b)).

9) Dans l'anneau des polynomes à 8 indéterminées X_i, Y_i $(1\leqslant i\leqslant 4)$ sur l'anneau $\mathbb{Z}$ des entiers rationnels, établir l'identité

$$(X_1^2+X_2^2+X_3^2+X_4^2)(Y_1^2+Y_2^2+Y_3^2+Y_4^2)=(X_1Y_1-X_2Y_2-X_3Y_3-X_4Y_4)^2$$
$$+(X_1Y_2+X_2Y_1+X_3Y_4-X_4Y_3)^2+(X_1Y_3+X_3Y_1+X_4Y_2-X_2Y_4)^2$$
$$+(X_1Y_4+X_4Y_1+X_2Y_3-X_3Y_2)^2$$

(utiliser le fait que dans l'algèbre des quaternions ordinaires sur le corps Q des nombres rationnels, la norme d'un produit est égale au produit des normes des facteurs).

10) Montrer que, dans l'anneau des polynomes à 6 indéterminées X_i, Y_i $(1 \leqslant i \leqslant 3)$ sur Z, il n'existe pas d'identité de la forme $(X_1^2+X_2^2+X_3^2)(Y_1^2+Y_2^2+Y_3^2) = u^2+v^2+w^2$, où u,v,w sont trois polynomes par rapport aux X_i et Y_i, à coefficients entiers rationnels (Observer que $15=3.5$ ne peut se mettre sous la forme $m^2+n^2+p^2$, où m,n,p sont entiers).

11) Soit E un anneau d'intégrité ayant une infinité d'éléments, possédant un élément unité e, et muni d'une structure d'algèbre par rapport à un anneau d'intégrité A (ayant un élément unité) ; soit $\mathfrak{a}$ l'idéal de A, annulateur de e (pour la structure de A-module de E). Montrer que si A_1 est l'anneau quotient $A/\mathfrak{a}$, l'image de l'anneau $A[X_1,X_2,\ldots,X_n]$ par l'application $f \to \tilde{f}$ dans l'anneau des applications de E^n dans E, est un anneau isomorphe à $A_1[X_1,X_2,\ldots,X_n]$.

§ 3. Fractions rationnelles et fonctions rationnelles.

1. Fractions rationnelles sur un corps commutatif.

DEFINITION 1.- Etant donné un corps commutatif K, on appelle fractions rationnelles à coefficients dans K, par rapport aux indéterminées X_ι $(\iota \in I)$, les éléments du corps des fractions (chap.I, §9,n°) de l'anneau d'intégrité $K[X_\iota]_{\iota \in I}$ des polynomes à coefficients dans K, par rapport aux X_ι ; le corps des fractions rationnelles à coefficients dans K, par rapport aux indéterminées X_ι, se note $K(X_\iota)_{\iota \in I}$.

Lorsque I est un intervalle $[1,n]$ de $\mathbb{N}$, le corps des fractions rationnelles à coefficients dans K, par rapport aux X_i $(1 \leqslant i \leqslant n)$ se note $K(X_1, X_2, \ldots, X_n)$ et est appelé corps des fractions rationnelles à n indéterminées, à coefficients dans K.

D'après la définition du corps des fractions d'un anneau d'intégrité, toute fraction rationnelle du corps $K(X_\iota)_{\iota \in I}$ peut se mettre d'une infinité de manières sous la forme $\frac{u}{v}$, où u et v sont deux polynomes de l'anneau $K[X_\iota]_{\iota \in I}$ tels que $v \neq 0$; si $\frac{u}{v} = \frac{u_1}{v_1}$ $(v \neq 0, v_1 \neq 0)$, on a $uv_1 = vu_1$, donc si $u \neq 0$, $u_1 \neq 0$ et dans ce cas, on a (§ 1, formule (5)) $\deg u + \deg v_1 = \deg v + \deg u_1$, ou encore $\deg u - \deg v = \deg u_1 - \deg v_1$. Le nombre entier (positif ou négatif) $\deg u - \deg v$ ne dépend donc pas de l'expression $\frac{u}{v}$ d'une fraction rationnelle $\neq 0$ comme quotient de deux polynomes ; on dit que c'est le degré (total) de cette fraction ; on définit de même le degré par rapport à une indéterminée X_κ d'une fraction rationnelle $\neq 0$; on vérifie aussitôt que pour les polynomes à coefficients dans K ces notions coïncident avec les notions de même nom définies au § 1, et que les formules (3), (5) et (6) du § 1 sont encore vraies pour les degrés des fractions rationnelles.

Remarque.- Si A est un anneau d'intégrité ayant un élément unité, on sait (§ 1, th. 1) que l'anneau $A[X_\iota]_{\iota \in I}$ est un anneau d'intégrité. Soit K le corps des fractions de l'anneau A ; on peut identifier K avec le sous-corps du corps des fractions de $A[X_\iota]_{\iota \in I}$ formé des fractions $\frac{u}{v}$, où u et v sont des polynomes de degré 0 $(v \neq 0)$ identifiés à des éléments de A. Avec cette convention, le corps des fractions de l'anneau $A[X_\iota]_{\iota \in I}$ est identique au corps de fractions rationnelles $K(X_\iota)_{\iota \in I}$; en effet, tout polynome de $K[X_\iota]_{\iota \in I}$ peut s'écrire $\frac{u}{a}$, où u est un polynome à coefficients dans A, et a un élément de A

(il suffit de réduire au même dénominateur tous les coefficients du polynome considéré) ; toute fraction rationnelle de $K(X_\iota)_{\iota\in I}$ s'écrit donc $(u/\alpha)/(v/\beta)=(\beta u)/(\alpha v)$, où α et β sont dans A , et u et v sont des polynomes de $A[X_\iota]_{\iota\in I}$; c'est donc un élément du corps des fractions de l'anneau $A[X_\iota]_{\iota\in I}$.

Si maintenant K est un corps commutatif quelconque, J une partie non vide de I , on a vu (§ 1,n°1) que l'on peut identifier l'anneau de polynomes $K[X_\iota]_{\iota\in I}$, à l'anneau des polynomes par rapport aux indéterminées X_ι d'indice $\iota \in \complement J$, à coefficients dans l'anneau d'intégrité $B = K[X_\iota]_{\iota\in J}$. La remarque précédente montre qu'on peut identifier le corps de fractions rationnelles $K(X_\iota)_{\iota\in I}$ au corps des fractions rationnelles par rapport aux X_ι d'indice $\iota \in \complement J$, à coefficients dans le corps de fractions rationnelles $K(X_\iota)_{\iota\in J}$.

La prop.1 du § 1, jointe à la prop. du chap.I, § 9, montre que :

PROPOSITION 1.- Soient K,K' deux corps commutatifs isomorphes, φ un isomorphisme de K sur K' ; il existe un isomorphisme $\overline{\varphi}$ et un seul de $K(X_\iota)_{\iota\in I}$ sur $K'(X_\iota)_{\iota\in I}$ qui prolonge φ et laisse invariantes chacune des indéterminées X_ι .

2. Fonctions rationnelles.

Soit K_0 un corps commutatif, K un sous-corps de K_0 , f un élément du corps des fractions rationnelles $K(X_\iota)_{\iota\in I}$ à coefficients dans K . Si u et v sont deux polynomes de $K[X_\iota]_{\iota\in I}$ tels que $f = \frac{u}{v}$, $x=(x_\iota)_{\iota\in I}$ un élément de K_0^I , l'élément $\frac{u(x)}{v(x)}$ de K_0 est défini si $v(x)\neq 0$; en outre, si u_1 et v_1 sont deux autres polynomes tels que $f = \frac{u_1}{v_1}$, et si on a encore $v_1(x)\neq 0$, on a $\frac{u(x)}{v(x)} = \frac{u_1(x)}{v_1(x)}$, car on a $uv_1=u_1v$, et par suite $u(x)v_1(x)=u_1(x)v(x)$ (§ 2, prop.1).

s'il existe au moins une expression $f=\frac{u}{v}$ de f telle que $v(x)\neq 0$, nous dirons que $x=(x_\iota)$ est substituable dans la fraction rationnelle f ; nous venons de voir que pour toutes les expressions de f comme quotient $\frac{u}{v}$ de deux polynomes tels que $v(x)\neq 0$, l'élément $\frac{u(x)}{v(x)}$ de K_0 est le même ; nous le désignerons par $f(x)$, ou $f((x_\iota))$.

PROPOSITION 2.- *Soit $x=(x_\iota)_{\iota\in I}$ une famille quelconque d'éléments du corps K_0. L'ensemble des fractions rationnelles $f\in K(X_\iota)_{\iota\in I}$ telles que x soit substituable dans f est un sous-anneau U de $K(X_\iota)_{\iota\in I}$; l'application $f\to f(x)$ est une représentation de U dans K_0, et l'image de U par cette représentation est le sous-corps de K_0 engendré par la réunion de K et de l'ensemble des éléments x_ι ($\iota\in I$).*

Soient en effet $f_1=\frac{u_1}{v_1}$, $f_2=\frac{u_2}{v_2}$ deux fractions rationnelles telles que $v_1(x)\neq 0$ et $v_2(x)\neq 0$; on a $f_1+f_2=\frac{u_1v_2+u_2v_1}{v_1v_2}$ et $f_1f_2=\frac{u_1u_2}{v_1v_2}$ et si $v=v_1v_2$, on a $v(x)=v_1(x)v_2(x)\neq 0$; donc U est un anneau. Tenant compte de la prop.1 du § 2, on voit aussitôt que $f\to f(x)$ est une représentation de U dans K_0, et que l'image de U par cette représentation est le corps des quotients du sous-anneau $K[x]$ engendré par la réunion de K et de l'ensemble des x_ι ; c'est donc le sous-corps de K_0 engendré par cette réunion. On notera ce sous-corps $K(x)$ ou $K(x_\iota)_{\iota\in I}$ ($K(x_1,x_2,\ldots,x_n)$ lorsque $I=\{1,n\}$).

Considérons en particulier le cas où K_0 est un corps de fractions rationnelles $K(Y_\lambda)_{\lambda\in L}$; si $(g_\iota)_{\iota\in I}$ est une famille d'éléments de ce corps substituable dans f, $f((g_\iota))=h$ est une fraction rationnelle ; il est immédiat que, si $y=(y_\lambda)_{\lambda\in L}$ est une famille d'éléments de K_0 substituable dans chacun des g_ι et telle que la famille $(g_\iota(y))_{\iota\in I}$ soit substituable dans f, alors y est substituable dans h et on a $h(y)=f((g_\iota(y)))$ (cf. § 2, n°1).

En particulier, si $K_0=K(X_\iota)_{\iota\in I}$, la famille $(X_\iota)_{\iota\in I}$ est subtituable dans toute fraction rationnelle f, et on peut écrire $f=f((X_\iota))$ ($f=f(X_1,\dots,X_n)$ pour les fractions rationnelles à n indéterminées).

Etant donnée une fraction rationnelle $f\in K(X_\iota)_{\iota\in I}$, désignons par S_f la partie de K_0^I formée des $x=(x_\iota)_{\iota\in I}$ qui sont substituables dans f ; lorsque K_0 est un corps infini (ayant une infinité d'éléments), la prop.6 du § 2 montre que S_f est un ensemble infini ; l'application $x\longrightarrow f(x)$ de S_f dans K_0 est alors appelée la fonction rationnelle associée à la fraction rationnelle f (et au surcorps K_0 de K) ; nous la désignerons par $\tilde{f}$ (ou simplement par f lorsqu'aucune confusion n'est à craindre). Supposons toujours que K_0 soit infini ; alors si f et g sont deux fractions rationnelles l'ensemble $S_f\cap S_g$ n'est pas vide (§ 2, th.2) ; si on a $f(x)=g(x)$ pour tout élément x de cet ensemble, on a $f=g$. En effet, si $f=\frac{u}{v}$, $g=\frac{u_1}{v_1}$, on a $u(x)v_1(x)=u_1(x)v(x)$ pour tout $x=(x_\iota)$ tel que $v(x)\neq 0$ et $v_1(x)\neq 0$; d'après le principe de prolongement des identités algébriques (§ 2, th.2), on a $uv_1=u_1v$. Autrement dit, l'application $f\to\tilde{f}$ est biunivoque.

Notons maintenant que si f et g sont deux fractions rationnelles quelconques, tout élément de l'ensemble $S_f\cap S_g$ est substituable dans $f+g$ (resp. fg) ; la fonction rationnelle associée à $f+g$ (resp. fg) est donc définie dans $S_f\cap S_g$, et a même valeur que la fonction $\tilde{f}+\tilde{g}$ (resp. $\tilde{f}\tilde{g}$) dans cet ensemble. De même, si $f\neq 0$, la partie S'_f de K_0^I formé des éléments x substituables dans f et tels que $f(x)\neq 0$ est un ensemble non vide (§ 2, th.2) en tout élément x de cet ensemble, la fonction rationnelle associée à la fraction rationnelle $1/f$ est définie et a même valeur que la fonction $1/\tilde{f}$.

Remarques.- 1) Au chap.VI, § 3, nous verrons que, pour toute fraction rationnelle $f \neq 0$, il existe deux polynomes u_0, v_0 tels que $f = u_0/v_0$, et que l'ensemble S_f des x substituables dans f soit identique à l'ensemble des x tels que $v_0(x) \neq 0$.

2) Le principe de prolongement des identités algèbriques (§ 2, th.2) s'étend aux fractions rationnelles : si f et g_i sont des fractions rationnelles de $K(X_\iota)_{\iota \in I}$ les g_i étant $\neq 0$ $(1 \leqslant i \leqslant m)$, et si pour tout $x \in K_0^I$ substituable à la fois dans f et dans tous les g_i, et tel que $g_i(x) \neq 0$ pour $1 \leqslant i \leqslant m$, on a $f(x) = 0$, alors $f = 0$ (K_0 étant toujours supposé infini) ; on ramène en effet immédiatement cet énoncé au th.2 du § 2.

Exercices.- 1) a) Si v est une fraction rationnelle non constante dans $K(X)$, montrer que v est substituable dans toute fraction rationnelle $u \in K(X)$ (remarquer que si un polynome w est tel que $w(v) = 0$, on a $w = 0$, en décomposant w en facteurs linéaires dans une extension algèbriquement fermée de K).

b) Si $u \in K(X)$ est $\neq 0$ et si $v \in K(X)$ est de degré > 0, montrer que le degré de $u(v)$ est égal au produit des degrés de u et v ; si le degré de v est < 0, le degré de $u(v)$ est un multiple du degré de v (non nécessairement égal au produit des degrés de u et de v).

c) Si v est non constante dans $K(X)$, et de degré 0, montrer qu'il existe une constante α telle que $\frac{1}{v-\alpha}$ soit de degré > 0.

2) Soient u et v deux fractions rationnelles non constantes dans $K(X)$. Pour que $u(v)$ soit un polynome, il faut et il suffit que : a) ou bien u et v soient des polynomes ; b) ou bien $u = f/X^n$ et $v = 1/g$, où f et g sont des polynomes et où le degré de f est $\leqslant n$ (passer à un surcorps algèbriquement fermé de K).

3) On dit qu'une fraction rationnelle $f \in K(X_1,\dots,X_n)$ est homogène si elle est égale au quotient de deux polynomes homogènes (le dénominateur étant $\neq 0$). Montrer que, pour que f soit homogène, il faut et il suffit que

$$f(ZX_1,ZX_2,\dots,ZX_n) = Z^d f(X_1,\dots,X_n)$$

où d est le degré de f.

§ 4. Différentielles et dérivations.

1. Différentielles et dérivées des polynomes.

Nous nous bornerons dans ce paragraphe aux polynomes par rapport à un nombre fini d'indéterminées, par rapport à un anneau commutatif quelconque A (ayant un élément unité).

Soit f un polynome de l'anneau $A[X_1,X_2,\dots,X_p] = B$. Dans l'anneau $A[X_1,\dots,X_p,Y_1,\dots,Y_p]$ des polynomes par rapport aux 2p indéterminées X_i,Y_i ($1 \leq i \leq p$), considérons le polynome $f(X_1+Y_1,X_2+Y_2,\dots,X_p+Y_p)$; ce polynome peut être considéré comme polynome par rapport aux Y_i, à coefficients dans B ; considéré comme tel, son terme constant est $f(X_1,X_2,\dots,X_p)$, puisqu'il s'obtient en substituant 0 à chacun des Y_i. Si on pose

$$\Delta f = f(X_1+Y_1,X_2+Y_2,\dots,X_p+Y_p)-f(X_1,X_2,\dots,X_p)$$

le polynome Δf (qu'on écrit aussi $\Delta f(X_1,\dots,X_p;Y_1,\dots,Y_p)$) est donc un polynome de $B[Y_1,Y_2,\dots,Y_p]$ sans terme constant.

DEFINITION 1.- On appelle différentielle du polynome f, et on note df, ou $df(X_1,\dots,X_p ; Y_1,\dots,Y_p)$ la partie homogène du premier degré du polynome Δf (considéré comme polynome par rapport aux Y_i à coefficients dans $B = A[X_1,X_2,\dots,X_p]$).

On peut donc écrire, d'après cette définition

(1) $$df = \sum_{i=1}^{p} g_i Y_i$$

où $g_1, g_2, \ldots, g_p$ sont des éléments de B , c'est-à-dire des polynomes de l'anneau $A\left[X_1, X_2, \ldots, X_p\right]$.

DEFINITION 2.- On appelle dérivée partielle du polynome f par rapport à X_i $(1 \leqslant i \leqslant p)$ et on note $D_i f$ (ou $\frac{\partial f}{\partial X_i}$, ou f'_{X_i} lorsqu'aucune confusion n'est possible) le polynome de l'anneau $B=A\left[X_1, X_2, \ldots, X_p\right]$ coefficient de Y_i dans la différentielle df de f .

La formule (1) s'écrit donc

(2) $$df = \sum_{i=1}^{p} D_i f . Y_i = \sum_{i=1}^{p} \frac{\partial f}{\partial X_i} Y_i$$

Pour le polynome particulier $f=X_i$, on a $df = Y_i$; cela conduit à écrire dX_i les indéterminées Y_i $(1 \leqslant i \leqslant p)$, et à écrire

(3) $$df = \sum_{i=1}^{p} D_i f . dX_i = \sum_{i=1}^{p} \frac{\partial f}{\partial X_i} dX_i \quad .$$

Lorsque f est un polynome à une seule indéterminée X , on a $df = Df . dX$; Df (qu'on note aussi $\frac{df}{dX}$ ou f') s'appelle alors simplement la dérivée de f .

Si f est une constante, on a évidemment $\Delta f = 0$, donc $df = 0$.

PROPOSITION 1.- Si f et g sont deux polynomes de l'anneau $A\left[X_1, X_2, \ldots, X_p\right]$, on a

(4) $$d(f+g) = df + dg$$

(5) $$d(fg) = df . g + f . dg$$

La formule (4) est une conséquence immédiate de la déf.1 . Pour démontrer (4), remarquons qu'on a

$$\Delta(fg) = \Delta f . g + f . \Delta g + \Delta f . \Delta g$$

Or, la partie homogène du premier degré de $\Delta f . g$ est $df . g$, celle de $f . \Delta g$ est $f . dg$, et celle de $\Delta f . \Delta g$ est nulle ; on a donc bien la formule (5) .

COROLLAIRE 1.- L'application $f \to df$ est une application linéaire du A-module $A[X_1,X_2,\ldots,X_p]$ dans le A-module des polynomes homogènes du premier degré dans l'anneau $B[Y_1,Y_2,\ldots,Y_p]$.

COROLLAIRE 2.- Chacune des applications $f \to D_i f$ est un endomorphisme du A-module $A[X_1,X_2,\ldots,X_p]$, tel qu'on ait identiquement

(6) $$D_i(fg) = D_i f.g + f.D_i g \ .$$

De (6) on déduit immédiatement, par récurrence sur n , qu'on a $D_i(X_i^n)=nX_i^{n-1}$; d'autre part, pour tout entier $m \geqslant 0$ et tout indice $j \neq i$, on a $D_i(X_j^m)=0$, puisque $\Delta(Y_j^m)$ ne contient pas Y_i . Le cor.2 prouve donc que si $f = \sum_{(n_i)} a_{n_1 n_2 \ldots n_p} X_1^{n_1} X_2^{n_2} \ldots X_p^{n_p}$, on a $D_i f = \sum_{(n_i)} n_i a_{n_1 n_2 \ldots n_p} X_1^{n_1} \ldots X_{i-1}^{n_{i-1}} X_i^{n_i-1} X_{i+1}^{n_{i+1}} \ldots X_p^{n_p}$.

PROPOSITION 2.- Soient f un polynome de l'anneau $A[X_1,X_2,\ldots,X_p]$, u_i $(1 \leqslant i \leqslant p)$ p polynomes de l'anneau $A[Z_1,Z_2,\ldots,Z_q]$; si on pose $h=f(u_1,u_2,\ldots,u_p)$, on a

(7) $$dh(Z_1,\ldots,Z_q;dZ_1,\ldots,dZ_q)=df(u_1,\ldots,u_p;du_1,\ldots,du_p) \ .$$

Par définition, on a

$$\Delta h = f(u_1+\Delta u_1, u_2+\Delta u_2, \ldots, u_p+\Delta u_p) - f(u_1,u_2,\ldots,u_p)$$

Comme les Δu_i sont des polynomes sans terme constant (par rapport aux dZ_j), la partie homogène du premier degré de Δh est la même que celle du polynome $df(u_1,\ldots,u_p;\Delta u_1,\ldots,\Delta u_p)= \sum_{i=1}^{p} D_i(u_1,\ldots,u_p)\,\Delta u_i$ d'où aussitôt la formule (7) .

COROLLAIRE .- Avec les mêmes notations, on a

(8) $$D_j h = \sum_{i=1}^{p} D_i f(u_1,u_2,\ldots,u_p) D_j u_i \qquad (1 \leqslant j \leqslant q).$$

2. Application : caractérisation des racines simples d'un polynome.

PROPOSITION 3.- Pour qu'une racine $a \in A$ d'un polynome $f \in A[X]$ soit simple, il faut et il suffit que a ne soit pas racine de Df.

En effet, on a par hypothèse $f=(X-a)g$, où g est un polynome ; pour que a soit racine simple de f , il faut et il suffit que $g(a) \neq 0$. Or, on a $Df=g+(X-a)Dg$ d'après la formule (6) ; on en tire $g(a)=Df(a)$, ce qui établit la proposition.

Plus généralement :

PROPOSITION 4.- Si $a \in A$ est racine d'ordre k du polynome $f \in A[X]$, a est racine d'ordre $\geqslant k-1$ de Df ; si dans A la relation $k\xi=0$ entraîne $\xi=0$, a est racine d'ordre $k-1$ de Df .

En effet, on a par hypothèse $f=(X-a)^k g$ et g n'est pas divisible par $X-a$; on en tire $Df=k(X-a)^{k-1}g+(X-a)^k Dg$, ce qui établit la première partie de la proposition. D'autre part, on tire de la relation précédente que, si $(X-a)^k$ divise Df , $(X-a)$ divise le polynome kg (puisque $X-a$ n'est pas diviseur de 0 dans $A[X]$), c'est-à-dire (§ 2, prop.4) que $kg(a)=0$; si dans A la relation $k\xi=0$ entraîne $\xi=0$, on aurait donc $g(a)=0$ contrairement à l'hypothèse.

Si au contraire il existe des éléments $\xi \in A$ tels que $\xi \neq 0$ et $k\xi=0$, a peut être racine d'ordre quelconque $\geqslant k-1$ de Df ; par exemple, si $k\xi=0$ pour tout $\xi \in A$, et si on prend $g=(X-a)^h+\beta$, avec $\beta \neq 0$, a est racine d'ordre k de f , mais racine d'ordre $\geqslant k+h-1$ de Df .

COROLLAIRE.- Si $a \in A$ est racine de f , et racine d'ordre p de Df , et si la relation $p!\xi=0$ entraîne $\xi=0$ dans A , a est racine d'ordre $p+1$ de f .

En effet, d'après la prop.4, a est racine de f avec un ordre de multiplicité k tel que $1 \leqslant k \leqslant p+1$; si on avait $k < p+1$, comme la relation $k\xi=0$ entraîne $p!\xi=0$, donc $\xi=0$ par hypothèse , a serait racine d'ordre $k-1 < p$ de Df , contrairement à l'hypothèse.

3. Dérivations dans une algèbre.

Le cor.2 de la prop.1 conduit à généraliser la notion de dérivée à une algèbre quelconque :

DEFINITION 3.- Soit E une algèbre sur un anneau commutatif A (ayant un élément unité). On appelle dérivation de E tout endomorphisme D du A-module E , tel que $D(xy)=D(x).y+x.D(y)$.

Dans l'algèbre de polynomes $A[X_1,\dots,X_n]$, les n applications D_i sont donc des dérivations, qu'on appelle les n dérivations partielles de cette algèbre.

Remarques.- 1) La valeur pour $x \in E$ d'une dérivation D dans E se notera souvent Dx au lieu de $D(x)$.

2) Un ensemble E peut être muni de diverses structures d'algèbre ayant toutes la même structure d'anneau sous-jacente ; lorsqu'on parle de dérivation dans un anneau E , il faut avoir soin de préciser quelle structure d'algèbre (ayant comme structure d'anneau sous-jacente la structure donnée) on considère sur E . En particulier tout anneau E peut être considéré comme algèbre sur Z ; lorsqu'on parle d'une dérivation dans un anneau E sans préciser la structure d'algèbre de E , il est sous-entendu qu'il s'agit de la structure d'algèbre sur Z ; toute dérivation de E , muni d'une structure d'algèbre ayant comme structure d'anneau sous-jacente la structure d'anneau donnée, est aussi une dérivation de E considéré comme algèbre sur Z .

Si E possède un élément unité e , on a pour toute dérivation D $D(e)=D(e^2)=D(e)e+eD(e)=2D(e)$, d'où $D(e)=0$; on en déduit $D(ne)=nD(e)=0$ pour tout entier n , et $D(ae)=aD(e)=0$ pour tout $a \in A$.

En particulier, dans l'anneau Z et les anneaux quotients $Z/(n)$ (considérés comme algèbres sur Z), toute dérivation est identiquement nulle.

Si z est un élément du centre C de E, Dz appartient à C pour toute dérivation D de E ; en effet, pour tout $x \in E$, on a $zx=xz$, d'où $D(zx)=D(xz)$, ou $Dz.x+z.Dx = Dx.z+x.Dz$; comme $z.Dx = Dx.z$, il vient $Dz.x = x.Dz$, d'où la proposition.

On vérifie aussitôt que si D_1, D_2 sont des dérivations de E , il en est de même de D_1-D_2 et de aD_1 (a quelconque dans A) ; autrement dit, l'ensemble des dérivations de E est un sous-module, que nous noterons $\mathcal{D}(E)$, du A-module $\mathcal{L}(E)$ de tous les endomorphismes du A-module E . Par contre, en général, le produit D_1D_2 $(=D_1 \circ D_2)$ de D_1 et D_2 dans l'anneau $\mathcal{L}(E)$, n'est pas une dérivation.

Par exemple, dans l'algèbre $E=A[X]$, on a $D^2(X^2)=2$, mais $D^2(X)=0$, et par suite $D^2(X)X+XD^2(X)=0$, ce qui montre que D^2 n'est pas une dérivation dans E si A n'est pas de caractéristique

On a toutefois la proposition suivante :

PROPOSITION 5.- Si D_1, D_2 sont deux dérivations quelconques dans E l'endomorphisme $D=D_2D_1-D_1D_2$ du A-module E est une dérivation de l'algèbre E .

En effet, on a, pour tout couple d'éléments x,y de E , $D(xy) = D_2(D_1(x)y+xD_1(y))-D_1(D_2(x)y+xD_2(y))=D_2(D_1(x))y+D_1(x)D_2(y)+D_2(x)D_1(y) + + xD_2(D_1(y))-D_1(D_2(x))y-D_2(x)D_1(y)-D_1(x)D_2(y)-xD_1(D_2(y)) =D(x)y+xD(y)$.

La dérivation $D_2D_1-D_1D_2$ se note d'ordinaire $[D_1,D_2]$.

PROPOSITION 6.- Dans une algèbre E , pour toute dérivation D de E et tout élément a du centre de E , l'endomorphisme $x \longrightarrow aD(x)$ (noté aD) du A-module E , est une dérivation de l'algèbre E .

En effet, si x,y sont des éléments quelconques de E , on a $aD(xy)=aD(x)y+axD(y)=aD(x)y+x(aD(y))$, puisque a est permutable avec tout élément de E .

On notera par contre que l'application $x \longrightarrow D(ax)$ n'est pas une dérivation.

COROLLAIRE.- L'ensemble $\mathscr{D}(E)$ des dérivations d'une algèbre E , muni de l'addition et de la loi externe $(a,D) \longrightarrow aD$, où a appartient au centre C de E , est un C-module.

Il résulte aussitôt de la déf.3 que, si D est une dérivation quelconque dans une algèbre E , l'ensemble des $x \in E$ tels que $D(x)=0$ est une sous-algèbre de E qu'on appelle parfois la sous-algèbre des constantes par rapport à D) . On déduit de cette remarque la proposition suivante :

PROPOSITION 7.- Soit S un système de générateurs d'une algèbre E . Si deux dérivations D_1, D_2 de E ont même valeur en tout élément de S , elles sont identiques.

En effet, $D=D_1-D_2$ est une dérivation de E , et la sous-algèbre de E formée des x tels que $D(x)=0$ contient S , donc est identique à E .

COROLLAIRE 1.- Soit E l'algèbre $A[X_1, X_2, \ldots, X_n]$ des polynomes à n indéterminées sur A . Les n dérivations partielles D_i $(1 \leqslant i \leqslant n)$ forment une base du E-module $\mathscr{D}(E)$ des dérivations dans E .

En effet, soit D une dérivation quelconque dans E , et posons $D(X_i)=u_i$ pour $1 \leqslant i \leqslant n$ (u_i élément de $E=A[X_1, \ldots, X_n]$) ; d'après la prop.6, $D' = \sum_{i=1}^{n} u_i D_i$ est une dérivation dans E , et on a $D'(X_i)=u_i$ pour $1 \leqslant i \leqslant n$; les dérivations D et D' ont même valeur pour l'élément unité de E et chacun des X_i , et ces éléments engendrent E , donc $D=D'$. D'autre part, si v_i $(1 \leqslant i \leqslant n)$ sont n éléments de E tels que $\sum_{i=1}^{n} v_i D_i = 0$ dans $\mathscr{D}(E)$, on a en particulier pour tout indice j , $\sum_{i=1}^{n} v_i D_i(X_j) = 0$, ce qui équivaut à $v_j=0$, donc les D_i forment bien une base de $\mathscr{D}(E)$ par rapport à E .

COROLLAIRE 2.- Avec les notations du corollaire 1 , on a $D_iD_j=D_jD_i$ quels que soient i et j .

En effet (prop.5), $D_{ij}=[D_i,D_j]$ est une dérivation dans E , et on a $D_{ij}(X_k)=0$ pour $1\leqslant k\leqslant n$, d'où le corollaire.

On notera que, d'après le cor.1, deux dérivations quelconques de $A[X_1,\dots,X_n]$ ne sont pas permutables en général.

PROPOSITION 8.- Soit E une algèbre sur A , commutative et ayant un élément unité ; soit D une dérivation dans E . Pour toute famille $(x_i)_{1\leqslant i\leqslant n}$ de n éléments de E et tout polynome $f\in A[X_1,\dots,X_n]$ on a

$$D(f(x_1,\dots,x_n)) = \sum_{i=1}^{n} D_if(x_1,\dots,x_n).Dx_i \quad . \tag{9}$$

En effet, pour tout $f\in A[X_1,X_2,\dots,X_n]$, posons

$$\varphi(f)=D(f(x_1,\dots,x_n))-\sum_{i=1}^{n} D_if(x_1,\dots,x_n).Dx_i$$

On vérifie aussitôt que φ est une application linéaire du A-module $A[X_1,\dots,X_n]$ dans le A-module E , et que l'on a $\varphi(fg)=\varphi(f)g(x_1,\dots,x_n)+f(x_1,\dots,x_n)\varphi(g)$. L'ensemble des éléments $f\in A[X_1,\dots,X_n]$ tels que $\varphi(f)=0$ est donc une sous-algèbre de $A[X_1,\dots,X_n]$, et elle contient évidemment l'élément unité et les X_i $(1\leqslant i\leqslant n)$; elle est donc identique à $A[X_1,\dots,X_n]$, ce qui établit la proposition (que l'on pourrait aussi établir directement à partir de la déf.3).

On notera que le corollaire de la prop.2 est un cas particulier de la prop.8 .

4. Prolongement d'une dérivation ; dérivées des fractions rationnelles.

PROPOSITION 9.- Soit S un monoïde, A un anneau commutatif ayant un élément unité, E l'algèbre du monoïde S relative à l'anneau A . Si D est une dérivation dans A , il existe une dérivation $\overline{D}$ et une seule de l'anneau (sans opérateur) E telle que pour tout $a\in A$ et tout $s\in S$, on ait $\overline{D}(as)=D(a)s$.

En effet, la condition de l'énoncé montre que si $\overline{D}$ existe, pour tout élément $z = \sum_{s \in S} a_s s$ de E, on doit avoir $\overline{D}(z) = \sum_{s \in S} D(a_s)s$; inversement, on vérifie aussitôt que l'application $\overline{D}$ définie par cette formule est une dérivation dans E.

En particulier, si E est une algèbre de polynomes $A[X_1,\ldots,X_p]$ sur A, pour tout polynome $f = \sum_{(n_i)} a_{n_1\ldots n_p} X_1^{n_1}\ldots X_p^{n_p}$, on désignera généralement par f^D le polynome $\sum_{(n_i)} D(a_{n_1\ldots n_p}) X_1^{n_1}\ldots X_p^{n_p}$; la prop.9 montre que $f \to f^D$ est une dérivation dans E, qui prolonge à E la dérivation donnée D dans A.

PROPOSITION 10.- Soit A un anneau d'intégrité, K son corps des quotients. Toute dérivation D dans A peut se prolonger d'une manière et d'une seule en une dérivation $\overline{D}$ dans K ; si u et v sont deux éléments quelconques de A tels que $v \neq 0$, on a

$$D\left(\frac{u}{v}\right) = \frac{D(u)v - uD(v)}{v^2} \tag{10}$$

Si une dérivation $\overline{D}$ dans K prolonge D, son unicité et la formule (10) sont immédiates, car si $w = \frac{u}{v}$ ($u \in A$, $v \in A$, $v \neq 0$), on a $u = vw$ d'où $D(u) = D(v)w + v\overline{D}(w)$, d'où on tire aussitôt pour $\overline{D}(w)$ l'expression (10). Reste à prouver l'existence de $\overline{D}$. Pour cela, montrons que si $\frac{u}{v} = \frac{u_1}{v_1}$ (u, v, u_1, v_1 dans A, $vv_1 \neq 0$), on a $\frac{D(u)v - uD(v)}{v^2} = \frac{D(u_1)v_1 - u_1D(v_1)}{v_1^2}$. Cette dernière relation s'écrit $v(u_1vD(v_1) + v_1^2D(u)) = v_1(uv_1D(v) + v^2D(u_1))$, et, en tenant compte de $uv_1 = u_1v$, $vv_1(uD(v_1) + v_1D(u)) = vv_1(u_1D(v) + vD(u_1))$. Or, cette dernière relation est une conséquence de $uD(v_1) + v_1D(u) = u_1D(v) + vD(u_1)$, qui s'obtient en dérivant $uv_1 = u_1v$. On peut donc pour tout élément $w = \frac{u}{v}$ de K, définir $\overline{D}(w)$ par la formule (10), indépendamment de l'expression de w comme fraction ; on vérifie alors aussitôt que $\overline{D}$ est bien une dérivation (en particulier, si A est une algèbre par rapport à un anneau C, on a encore $\overline{D}(\gamma w) = \gamma\overline{D}(w)$ pour tout $w \in K$ et tout $\gamma \in C$).

Soit K un corps commutatif ; chacune des dérivations D_i $(1 \leqslant i \leqslant n)$ de l'algèbre $K[X_1,\dots,X_n]$ des polynomes à n indéterminées sur K peut, d'après la prop.10, être prolongée en une dérivation et une seule de l'algèbre $E=K(X_1,\dots,X_n)$ des fractions rationnelles à n indéterminées sur K ; cette dérivation sera encore appelée <u>dérivation partielle par rapport à</u> X_i , et notée D_i ; pour une fraction rationnelle quelconque f, $D_i f$ sera encore notée aussi $\frac{\partial f}{\partial X_i}$ ou f'_{X_i} , et appelée la <u>dérivée partielle</u> de f par rapport à X_i . Si deux dérivations de l'algèbre E coïncident pour tout polynome, elles sont identiques, en vertu de la formule (10) ; on conclut de là, en raisonnant comme dans le cor.1 de la prop.7, que les n dérivations partielles D_i forment une <u>base</u> de l'espace vectoriel $\mathfrak{D}(E)$ (sur le corps E) des dérivations de l'algèbre E .

Soit F une algèbre commutative sur le corps K , f une fraction rationnelle du corps $K(X_1,\dots,X_n)$. Si la famille $(x_i)_{1 \leqslant i \leqslant n}$ d'éléments de F est substituable dans f , elle l'est aussi dans chacune des dérivées partielles $D_i f$, en vertu de la formule (10), et on vérifie aussitôt que pour toute dérivation D dans F , la fomule (9) est encore valable.

5. Formes différentielles.

Soit E une algèbre <u>commutative</u>, ayant un élément unité, sur un anneau A . On a vu (prop.6) que l'ensemble $\mathfrak{D}(E)$ des dérivations de E est muni d'une structure de <u>E-module unitaire</u>.

DEFINITION 4.- <u>On appelle forme différentielle sur l'algèbre</u> E <u>toute forme linéaire sur le</u> E-<u>module</u> $\mathfrak{D}(E)$ <u>des dérivations dans</u> E .

Les formes différentielles sur E forment donc un E-module, le <u>dual</u> $\mathfrak{D}^*(E)$ de $\mathfrak{D}(E)$; pour toute forme différentielle ω et toute dérivation D dans E , nous désignerons, suivant les notations générales, par $\langle D,\omega \rangle$ la valeur de ω pour l'élément D (forme bilinéaire fondamentale, cf.chap.II, §4). Si $\mathfrak{D}(E)$ admet une <u>base</u> (D_i) de n éléments,

on sait (loc.cit.) que $\mathscr{D}^*(E)$ admet une base (ω_i) de n éléments, dite base duale de (D_i), telle que $\langle D_i, \omega_j \rangle = \delta_{ij}$ (indice de Kronecker) ; toute dérivation est alors de la forme $D = \sum_{i=1}^{n} \lambda_i D_i$, toute forme linéaire de la forme $\omega = \sum_{i=1}^{n} \mu_i \omega_i$, et on a $\langle D, \omega \rangle = \sum_{i=1}^{n} \lambda_i \mu_i$.

Soit x un élément quelconque de E ; il est clair que l'application $D \to Dx$ de $\mathscr{D}(E)$ dans E est une forme linéaire ; cette forme différentielle est appelée différentielle totale de x et notée dx ; autrement dit, on a, pour tout $x \in E$ et tout $D \in \mathscr{D}(E)$

(11) $$\langle D, dx \rangle = Dx \quad .$$

On notera qu'il y a en général des formes différentielles qui ne sont pas des différentielles totales d'éléments de E (cf. exerc. 14).

PROPOSITION 11.- Pour tout couple d'éléments x,y de E et tout $a \in A$ on a

(12) $$d(x+y)=dx+dy \quad , \quad d(ax)=a\,dx \quad , \quad d(xy)=x.dy+y.dx \quad .$$

Démontrons par exemple la troisième de ces relations ; pour toute dérivation D ; on a, d'après (11) et la déf.3

$$\langle D, d(xy) \rangle = D(xy)=Dx.y+x.Dy = \langle D, y.dx \rangle + \langle D, x.dy \rangle = \langle D, y.dx+x.dy \rangle$$

ce qui démontre notre assertion, d'après la définition d'une forme différentielle. Les deux autres relations (12) se démontrent de même.

Pour l'élément unité e de E , on a $\langle D, de \rangle = De=0$ pour toute dérivation D , donc $de=0$, et par suite $d(ae)=a\,de=0$ pour tout $a \in A$.

Si $\mathscr{D}(E)$ admet une base (D_i), et si (ω_i) est la base duale dans le module $\mathscr{D}^*(E)$ des formes différentielles, on a, pour tout $x \in E$

(13) $$dx = \sum_{i=1}^{n} D_i x . \omega_i \quad .$$

Considérons en particulier le cas où E est une algèbre de polynomes $A[X_1, \ldots, X_n]$; la formule (11) donne en particulier, pour $x=X_j$ et $D=D_i$, $\langle D_i, dX_j \rangle = D_i X_j = \delta_{ij}$, donc les différentielles totales dX_i

$(1 \leqslant i \leqslant n)$ forment dans $\mathscr{D}^*(E)$ la <u>base duale</u> de la base (D_i) formée par les n dérivations partielles ; pour tout polynome $f \in E$, la formule (13) donne donc pour différentielle totale

$$df = \sum_{i=1}^{n} D_i f . dX_i \tag{14}$$

Ceci montre que, si on identifie le E-module des polynomes homogènes du premier degré dans $E[Y_1,\ldots,Y_n]$ au E-module $\mathscr{D}^*(E)$, par l'application qui à chaque élément Y_i fait correspondre dX_i, la différentielle totale df est <u>identique</u> à la différentielle définie au n° 1.

Si maintenant E est le corps $K(X_1,\ldots,X_n)$ des fractions rationnelles à n indéterminées sur un corps K, les dX_i forment encore une base de $\mathscr{D}^*(E)$, duale de la base (D_i), et la formule (14) s'applique à une fraction rationnelle quelconque f ; on notera que si $f=u/v$, où u et v sont deux polynomes (ou fractions rationnelles), on a $df = \frac{v.du-u.dv}{v^2}$.

Notons enfin que si E est une algèbre commutative quelconque sur un anneau A, ayant un élément unité, $(x_i)_{1 \leqslant i \leqslant n}$ une famille d'éléments de E, f un polynome quelconque de $A[X_1,X_2,\ldots,X_n]$, les formules (9) et (11) montrent que

$$d(f(x_1,\ldots,x_n)) = \sum_{i=1}^{n} D_i f(x_1,\ldots,x_n).dx_i \tag{15}$$

formule que l'on pourrait aussi réduire aisément des formules (12).

La formule (15) est encore valable lorsque E est une algèbre sur un corps K, f une fraction rationnelle de $K(X_1,\ldots,X_n)$, et (x_i) une famille d'éléments de E substituable dans f.

<u>Exercices</u>.- 1) Montrer que, pour tout polynome homogène f de degré m, dans l'anneau $A[X_1,\ldots,X_n]$, on a ("identité d'Euler")

$$\sum_{i=1}^{n} X_i \frac{\partial f}{\partial X_i} = mf(X_1,\ldots,X_n)$$

Réciproquement, montrer que si, dans l'anneau A, la relation $m!\xi=0$ entraîne $\xi=0$, tout polynome f satisfaisant à l'identité précédente est homogène de degré m.

2) Soient α_i $(1\leqslant i\leqslant n)$ n éléments distincts d'un corps commutatif K, β_i $(1\leqslant i\leqslant n)$ n éléments quelconques de K ; montrer que le polynome (unique) f de $K[X]$, nul ou dedegré $\leqslant n-1$, tel que $f(\alpha_i)=\beta_i$ pour $1\leqslant i\leqslant n$, est donné par la formule

$$f(X)=\omega(X)\sum_{i=1}^{n}\frac{\beta_i}{\omega'(\alpha_i)(X-\alpha_i)}$$

où $\omega(X)=(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$. En déduire que, si g est un polynome de $K[X]$, nul ou de degré $\leqslant n-2$, on a

$$\sum_{i=1}^{n}\frac{g(\alpha_i)}{\omega'(\alpha_i)}=0$$

(remarquer que si $f(X)=Xg(X)$, f est nul ou de degré $n-1$, et que $f(\alpha_i)=\alpha_i g(\alpha_i)$).

3) Soient α_i $(1\leqslant i\leqslant n)$ n éléments distincts d'un corps commutatif K, $\beta_i(1\leqslant i\leqslant n)$ ~~n éléments~~ et γ_i $(1\leqslant i\leqslant n)$ 2n éléments quelconques de K. Montrer qu'il existe un polynome et un seul $f\in K[X]$, nul ou de degré $\leqslant 2n-1$, tel que $f(\alpha_i)=\beta_i$ et $f'(\alpha_i)=\gamma_i$ pour $1\leqslant i\leqslant n$ (formule d'interpolation d'Hermite) (commencer par considérer deux cas particuliers : 1° tous les β_i sont nuls sauf un, tous les γ_i sont nuls ; 2° tous les β_i sont nuls, tous les γ_i sont nuls sauf un).

4) Soit K un corps commutatif de caractéristique 0. Montrer que si une fraction rationnelle $u\in K(X)$ est telle que $Du=0$, u est une constante.

5) Généraliser l'exerc.1 aux fractions rationnelles homogènes (§ 3, exerc.3) sur un corps de caractéristique 0 (considérer la fraction rationnelle $\frac{1}{Z^m}f(ZX_1,\ldots,ZX_n)$).

6) a) Soit A un anneau commutatif ayant un élément unité, tel que, pour tout $n \in Z$ non nul, la relation $n\xi = 0$ entraîne $\xi = 0$ dans A . Montrer que l'application $f \longrightarrow f(D_1, D_2, \ldots, D_n)$ est un isomorphisme de l'algèbre de polynomes $A[X_1, X_2, \ldots, X_n] = E$ dans l'algèbre (sur A) des endomorphismes du A-module E (raisonner par récurrence sur l'entier n) .

b) Soit A un anneau commutatif ayant un élément unité et de caractéristique $m > 0$. Montrer que l'on a $D_i^m = 0$ pour toute dérivation partielle D_i $(1 \leq i \leq n)$ dans $A[X_1, \ldots, X_n]$.

7) Soit K un corps de caractéristique 0 . Montrer que, pour tout polynome $f \in K[X_1, X_2, \ldots, X_n]$, on a

$$f(X_1+Y_1, X_2+Y_2, \ldots, X_n+Y_n) = \sum_{p=0}^{\infty} \frac{1}{p!}(Y_1D_1+Y_2D_2+\ldots+Y_nD_n)^p(f)$$

("formule de Taylor pour les polynomes") (démontrer d'abord la formule lorsque n=1, puis considérer le polynome $f(X_1+ZY_1, X_2+ZY_2, \ldots, X_n+ZY_n)$ par rapport à Z , à coefficients dans le corps des fractions rationnelles par rapport aux X_i et Y_i , à coefficients dans K).

8) Soient D_1, D_2, D_3 des dérivations quelconques dans une algèbre A ; montrer qu'on a $[D_1, D_1] = 0$, $[D_2, D_1] + [D_1, D_2] = 0$, et $[[D_1, D_2], D_3] + [[D_2, D_3], D_1] + [[D_3, D_1], D_2] = 0$ ("identité de Jacobi" , cf. chap. I, § , exerc.).

9) Soit D une dérivation quelconque dans une algèbre A . Démontrer la formule

$$D^m(xy) = \sum_{p=0}^{m} \binom{m}{p} D^p(x) D^{m-p}(y)$$

("formule de Leibniz").

10) Soit A une algèbre sur un corps K de caractéristique 0 , D une dérivation dans A telle qu'il existe un entier $n > 0$ tel que $D^n = 0$.

Pour tout $t \in K$, on pose $u_t = \sum_{p=0}^{n-1} \frac{t^p}{p!} D^p$ dans l'algèbre des endomorphismes de l'espace vectoriel A (sur K) ; montrer que si t et t' sont deux éléments quelconques de K, on a $u_{t+t'} = u_t u_{t'}$, et en déduire que les u_t sont des automorphismes de l'algèbre A et qu'ils forment un groupe abélien isomorphe à un groupe quotient du groupe additif K

11) a) Soit E une algèbre sur un anneau commutatif A ayant un élément unité. Montrer que pour tout $a \in E$, $x \to xa-ax$ est une dérivation dans E (dite dérivation intérieure).

b) On suppose que E est l'algèbre $\mathcal{M}_n(A)$ des matrices carrées d'ordre n sur A ; soit D une dérivation dans E, (E_{ij}) la base canonique (chap.II, § 6) de E sur A. Montrer qu'on a $D(E_{ij}) = (\beta_j - \beta_i)E_{ij} + \sum_{k \neq i} a_{jk} - \sum_{k \neq j} a_{ki} E_{kj}$, où $(\beta_i)_{1 \leqslant i \leqslant n}$ est une famille d'éléments de A, (a_{ij}) une famille d'éléments de A, définie pour $i \neq j$ (dériver la table de multiplication des E_{ij}). En déduire que toute dérivation D dans E est une dérivation intérieure.

12) Soit E une algèbre, $\mathfrak{a}$ un idéal bilatère dans E, D une dérivation dans E telle que $D(\mathfrak{a}) \subset \mathfrak{a}$. Montrer que l'application de $E/\mathfrak{a}$ dans lui-même obtenue par passage aux quotients sur D, est une dérivation dans l'algèbre $E/\mathfrak{a}$.

13) Soit E une algèbre produit d'un nombre fini d'algèbres E_i sur un anneau A $(1 \leqslant i \leqslant n)$, telles que $E_i . E_i = E_i$ (ce qui a lieu en particulier si E admet un élément unité). Montrer que si D est une dérivation quelconque dans E, la restriction D_i de D à E_i est une dérivation de cette algèbre ; l'ensemble $\mathcal{D}(E)$ des dérivations de E, considéré comme A-module, est somme directe des A-modules $\mathcal{D}(E_i)$; il en est de même lorsque $\mathcal{D}(E)$ est considéré comme E-module ; en outre, chacun des $\mathcal{D}(E_i)$ est annulé par tous les E_j d'indice $\neq i$.

14) Soit E une algèbre commutative sur un anneau A , ayant un élément unité. On désigne par $\mathcal{D}_p(E)$ la puissance extérieure p-ème (chap.III, § 4) du E-module $\mathcal{D}(E)$ des dérivations dans E ; toute forme linéaire Ω sur $\mathcal{D}_p(E)$, qui peut être identifiée à une forme p-linéaire alternée sur $(\mathcal{D}(E))^p$ est dite <u>forme différentielle extérieure de degré</u> p sur E ; on désigne par $\mathcal{D}^*_p(E)$ le module de ces formes.

a) Pour toute forme différentielle extérieure $\Omega \in \mathcal{D}^*_p(E)$, montrer que l'application

$$(D_1,..,D_{p+1}) \to \sum_{i=1}^{p+1} (-1)^{i+1} D_i(\langle \Omega , D_1 \wedge .. \wedge D_{i-1} \wedge D_{i+1} \wedge .. \wedge D_{p+1} \rangle) +$$
$$+ \sum_{i<j} (-1)^{i+j+1} \langle \Omega , [D_i, D_j] \wedge D_1 \wedge .. \wedge D_{i-1} \wedge D_{i+1} \wedge .. \wedge D_{j-1} \wedge D_{j+1} \wedge .. \wedge D_{p+1} \rangle$$

est une forme (p+1)-linéaire alternée sur $(\mathcal{D}(E))^{p+1}$, ou, ce qui revient au même, une forme linéaire sur $\mathcal{D}_{p+1}(E)$ qu'on désigne par $d\Omega$ (<u>différentielle extérieure</u> de Ω).

b) Démontrer qu'on a $d(d\Omega)=0$ pour toute forme différentielle extérieure $\Omega \in \mathcal{D}^*_p(E)$ (utiliser l'exerc.8) .

c) On suppose que $\mathcal{D}(E)$ admet une base $(D_i)_{1 \leqslant i \leqslant n}$, dont $(\omega_i)_{1 \leqslant i \leqslant n}$ est la base duale dans $\mathcal{D}^*(E)$; pour toute partie H de p éléments de $[1,n]$, les formes différentielles extérieures de degré p $\omega_H = \omega_{i_1} \wedge \omega_{i_2} \wedge \ldots \wedge \omega_{i_p}$ ($(i_k)_{1 \leqslant k \leqslant p}$ suite strictement croissante formée des éléments de H) forment une base de $\mathcal{D}^*_p(E)$. Montrer que si Ω , Ω' sont deux formes différentielles de degrés p et q , on a

$$d(\Omega \wedge \Omega') = d\Omega \wedge \Omega' + (-1)^p \Omega \wedge d\Omega' .$$

d) On suppose que E est une algèbre de polynomes $A[X_1,\ldots,X_n]$. Montrer que, pour qu'une forme différentielle extérieure Ω de degré p soit de la forme $d\omega$, il faut et il suffit que $d\Omega = 0$ (raisonner par récurrence sur le nombre d'indéterminées).

15) Soient E_1, E_2 deux algèbres sur A , D_1 une dérivation dans E_1 , D_2 une dérivation dans D_2 . Montrer qu'il existe une dérivation D dans le produit tensoriel $E = E_1 \otimes E_2$ telle que pour tout $x \in E_1$ et tout $y \in E_2$, on ait $D(x \otimes y) = (D_1 x) \otimes y + x \otimes (D_2 y)$.
