LIVRE II
ALGEBRE
CHAPITRE IV (ETAT 2)
POLYNOMES ET FONCTIONS POLYNOMES

Rédaction n° 043

Nombre de pages : 53

Nombre de feuilles : 53

A 43 2

LIVRE II

A L G È B R E

CHAPITRE IV (état 2)

POLYNOMES ET FONCTIONS POLYNOMES

§ 1. Polynomes.

1. Définition des polynomes. Définition 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) $\mathcal{N}$ des entiers $\geqslant 0$ relative à l'anneau A (chap.II, § 4, n°9). Les éléments de cette algèbre sont appelés polynomes à une indéterminée sur A .

La base canonique $(e_n)_{n\in\mathcal{N}}$ de cette algèbre a donc pour table de multiplication $e_m e_n = e_{m+n}$. On en conclut d'abord que l'algèbre est commutative, puis que e_0 est élément unité ; comme c'est un élément régulier, on peut identifier à A la sous-algèbre Ae_0 , et par suite identifier e_0 à l'élément unité de A (que nous noterons 1 si aucune confusion n'est à craindre). D'autre part, on a pour tout $n \in \mathcal{N}$ $e_n = (e_1)^n$; tout polynome u s'écrit donc d'une seule manière sous la forme $\sum_{n\in\mathcal{N}} a_n e_1^n$, où il n'y a qu'un nombre fini de coefficients $a_n \neq 0$; si $u \neq 0$, la plus grande des valeurs r de n telle que $a_n \neq 0$ s'appelle le degré du polynome u , et se note parfois deg.u ; a_r est appelé le coefficient dominant du ~~xxxxx~~ polynome u . La somme et le produit de deux polynomes $u = \sum_n a_n e_1^n$, $v = \sum_n \beta_n e_1^n$ sont donc donnés par les formules

$$u+v = \sum_n (a_n+\beta_n) e_1^n$$

$$uv = \sum_n \gamma_n e_1^n$$

avec $\gamma_n = \sum_{p=0}^{n} a_p \beta_{n-p}$.

Les éléments 1 et e_1 forment un <u>système de générateurs</u> de l'algèbre des polynomes d'une indéterminée sur A ; on dit encore que cette algèbre s'obtient par <u>adjonction à</u> A <u>de l'indéterminée</u> e_1 , et on la note $A[e_1]$.

<u>Définition 2</u>. <u>On appelle algèbre des polynomes à</u> p <u>indéterminées sur l'anneau</u> A , <u>l'algèbre du monoïde produit</u> $\mathcal{N}^p$ <u>relative à l'anneau</u> A ; <u>les éléments de cette algèbre sont appelés polynomes à</u> p <u>indéterminées sur</u> A .

On sait (chap. III, § 2) que cette algèbre est isomorphe au produit tensoriel $A[e_1] \otimes A[e_2] \otimes \dots \otimes A[e_p]$ de p algèbres isomorphes à l'algèbre des polynomes à une indéterminée sur A ; sa base canonique est donc formée des produits $e_1^{\nu_1} e_2^{\nu_2} \dots e_p^{\nu_p}$, où $(\nu_1, \nu_2, \dots, \nu_p)$ parcourt $\mathcal{N}^p$; les éléments 1 (élément unité de A), $e_1, e_2, \dots, e_p$ forment donc un système de générateurs de l'algèbre des polynomes à p indéterminées sur A ; on dit que cette algèbre s'obtient par <u>adjonction à</u> A <u>des</u> p <u>indéterminées</u> $e_1, e_2, \dots, e_p$, et on la note $A[e_1, e_2, \dots, e_p]$.

Tout polynome u à p indéterminées s'écrit d'une seule manière sous la forme $\sum a_{\nu_1 \nu_2 \dots \nu_p} e_1^{\nu_1} e_2^{\nu_2} \dots e_p^{\nu_p}$, un nombre fini seulement des coefficients $a_{\nu_1 \nu_2 \dots \nu_p}$ étant $\neq 0$; on dit que $\sum_{k=1}^{p} \nu_k$ est le <u>degré total</u> (ou simplement <u>degré</u>) du terme $a_{\nu_1 \nu_2 \dots \nu_p} e_1^{\nu_1} e_2^{\nu_2} \dots e_p^{\nu_p}$; si $u \neq 0$ le plus grand des degrés des termes de u dont le coefficient n'est pas nul est appelé le <u>degré total</u> de u et se note encore deg.u ; un polynome est dit <u>homogène</u> si tous ses termes ont même degré ; tout polynome u de degré r peut s'écrire d'une seule manière sous la forme $u = \sum_{k=0}^{r} u_k$, où u_k est le polynome homogène, somme des termes de u de degré total k .

Pour toute suite $(i_k)_{1 \leq k \leq q}$ strictement croissante de $q < p$ indices appartenant à $[1, p]$, l'algèbre $A[e_{i_1}, e_{i_2}, \dots, e_{i_q}]$ est une sous-algèbre

de $A[e_1,e_2,\dots,e_p]$. En particulier, on peut considérer $A[e_1,e_2,\dots,e_p]$ comme une algèbre par rapport à l'anneau $A[e_1,e_2,\dots,e_q]$; c'est alors l'algèbre obtenue à partir de $A[e_{q+1},e_{q+2},\dots,e_p]$ par extension à $A[e_1,\dots,e_q]$ de l'anneau d'opérateurs A (chap.III, 2) ; en d'autres termes, $A[e_1,e_2,\dots,e_p]$ peut être identifié à l'anneau $A[e_1,\dots,e_q]$ $e_{q+1},\dots,e_p$ des polynomes à p-q indéterminées sur $A[e_1,\dots,e_q]$.

Un polynome u à p indéterminées $e_1,\dots,e_p$, peut donc, pour chaque valeur de l'indice k, être considéré comme un polynome à une indéterminée e_k, dont les coefficients sont des polynomes à p-1 indéterminées $e_1,\dots,e_{k-1},e_{k+1},\dots,e_p$; le degré de ce polynome est dit <u>degré de u par rapport à</u> e_k ; c'est la plus grande valeur que prend l'indice ν_k dans les coefficients $a_{\nu_1\nu_2\dots\nu_k}$ non nuls du polynome u.

Si B est un sous-anneau de A (ayant même élément unité), l'algèbre $B[e_1,\dots,e_p]$ sur B peut être considérée comme une sous-algèbre de $A[e_1,\dots,e_p]$ (ce dernier anneau étant muni de sa structure d'algèbre par rapport à B) (cf. chap.II, § 4).

2. <u>Polynomes sur un anneau d'intégrité</u>. <u>Théorème 1</u>. <u>Si A est un anneau d'intégrité</u> (ayant un élément unité), <u>l'algèbre des polynomes à p indéterminées</u> $A[e_1,e_2,\dots,e_p]$ <u>est un anneau d'intégrité</u>.

Il suffit de le démontrer pour p=1 ; on raisonnera ensuite par récurrence, puisque $A[e_1,e_2,\dots,e_p]$ peut être considéré comme l'algèbre des polynomes à une indéterminée sur l'anneau $A[e_1,e_2,\dots,e_{p-1}]$.

Or, si $u=a_0+a_1e+\dots+a_me^m$ est un polynome de degré m sur A, $v=\beta_0+\beta_1e+\dots+\beta_ne^n$ un polynome de degré n, le seule terme de degré m+n dans le produit uv est $a_m\beta_ne^{m+n}$; 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 $uv\neq 0$.

Plus généralement, ce raisonnement prouve que, si le coefficient dominant a_m du polynome u n'est pas un diviseur de 0 dans A, u n'est pas un diviseur de 0 dans $A[e]$; il en est ainsi en particulier lorsque $a_m=1$.

Corollaire 1. Si u et v sont deux polynomes à p indéterminées sur un anneau d'intégrité A , le degré de uv par rapport à e_k est égal à la somme des degrés de u et v par rapport à e_k $(1 \leqslant k \leqslant p)$.

Corollaire 2. Si u et v sont deux polynomes à p indéterminées sur un anneau d'intégrité A , le degré total de uv est égal à la somme des degrés totaux de u et de 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_k (resp. v_k) est un polynome homogène de degré k , $u_m \neq 0$, $v_n \neq 0$; dans le produit uv , tous les termes sont de degré total $< m+n$, sauf ceux du produit $u_m v_n$; tout revient à prouver que $u_m v_n \neq 0$, ce qui résulte du th.1 .

Définition 3. Si A est un anneau d'intégrité (ayant un élément unité), on appelle corps des fractions rationnelles à p indéterminées sur A , et on note $A(e_1,e_2,\ldots,e_p)$ (le corps des fractions (ch. I, § 9) de l'anneau d'intégrité $A[e_1,e_2,\ldots,e_p]$) ; les éléments de ce corps sont appelés fractions rationnelles à p indéterminées sur A .

Toute fraction rationnelle sur A peut donc se mettre (d'une infinité de manières) sous la forme $\frac{u}{v}$, où u et v sont deux polynomes à p indéterminées et $v \neq 0$; l'ensemble des éléments de $A(e_1,\ldots,e_p)$ égaux à une fraction où u et v sont de degré 0 (autrement dit, des éléments de A) est un sous-corps de $A(e_1,e_2,\ldots,e_p)$ isomorphe au corps des fractions K de A , et qu'on identifie avec ce dernier. Avec cette convention, on a $A(e_1,e_2,\ldots,e_p)=K(e_1,e_2,\ldots,e_p)$; en effet, tout polynome sur K peut s'écrire $\frac{u}{a}$, où u est un polynome sur A et $a \in A$

(il suffit de réduire au même dénominateur tous les coefficients) ; toute fraction rationnelle sur K s'écrit donc $\frac{\frac{u}{\alpha}}{\frac{v}{\beta}} = \frac{\beta u}{\alpha v}$ où $\alpha \in A$, $\beta \in A$, et u et v sont des polynomes sur A ; c'est donc une fraction rationnelle sur A .

3. Division euclidienne des polynomes à une indéterminée. Soit K un corps commutatif. On peut définir, dans l'anneau $K[e]$ des polynomes à une indéterminée sur K , un processus analogue à celui de la division euclidienne dans l'ensemble $\mathcal{N}$ des entiers naturels (Ens. chap.III), de la manière suivante :

Soit $u = \sum_{k=0}^{m} \alpha_k e^k$ un polynome de degré m , $v = \sum_{k=0}^{n} \beta_k e^k$ un polynome de degré $n \leqslant m$; on peut trouver un polynome w tel que u-vw soit de degré $< m$; il suffit de prendre $w = \alpha_m \beta_n^{-1} e^{m-n}$. Par récurrence, on peut donc former pour $0 \leqslant k \leqslant m-n$, une suite (g_k) de polynomes telle que $\deg(g_k) < m-k$, g_k étant de la forme $g_{k-1} - w_k v$; le dernier terme $r = g_{m-n}$ de cette suite est de degré $< n$; autrement dit, il existe un polynome q tel que $u-qv=r$ soit de degré $<n$.

Ce polynome est d'ailleurs unique ; en effet, si q_1 est un second polynome tel que le degré de $u-q_1 v$ soit $<n$, $(q-q_1)v$ serait aussi de degré $<n$ s'il n'était pas nul ; mais comme v est de degré n , ceci est impossible, en vertu du cor. 1 du th.1, donc $q=q_1$.

L'opération que nous venons de définir s'appelle division euclidienne de u par v ; q est appelé le quotient , r le reste de la division.

Plus généralement, si A est un anneau commutatif ayant un élément unité, on peut définir de même la division d'un polynome f de $A[e]$ par un polynome g du même anneau si le coefficient dominant de g est inversible ; l'unicité de la division, dans ce cas, est encore assurée si A est un anneau d'intégrité.

4. Polynomes homogènes et tenseurs symétriques. On peut définir aussi les polynomes homogènes à p indéterminées et de degré donné n sur un anneau A , à partir de l'espace T_0^n des tenseurs contravariants d'ordre n sur le A-module $E = A^p$.

D'une façon générale, soit E un A-module quelconque ; on peut à partir de l'espace tensoriel T_0^n , définir la puissance symétrique n-ème de E de la même manière que sa puissance antisymétrique n-ème (chap.III, §4). On sait en effet que toute application n-linéaire de E^n dans un A-module F peut se mettre d'une seule manière sous la forme $(x_1,..,x_n) \to f(x_1 \otimes x_2 \otimes ... \otimes x_n)$, où f est une application linéaire de T_0^n dans F . Pour que cette application n-linéaire soit symétrique, il faut et il suffit qu'on ait, pour toute permutation $\sigma \in \mathfrak{S}_n$, $f(\sigma z)=f(z)$ identiquement ; autrement dit, f doit s'annuler dans le sous-module S de T_0^n engendré par les tenseurs $z-\sigma z$, où z parcourt T_0^n et σ le groupe $\mathfrak{S}_n$; f peut alors s'écrire d'une seule manière sous la forme $g \circ \varphi$, où φ est l'application canonique de T_0^n sur le module quotient T_0^n/S , et g une application linéaire de T_0^n/S dans F .

On dit que le module T_0^n/S est la puissance symétrique n-ème du module E .

Supposons maintenant que E soit isomorphe à A^p , c'est-à-dire admette une base régulière (e_i) de p éléments $(1 \leqslant i \leqslant p)$; pour toute suite $s=(i_k)_{1 \leqslant k \leqslant n}$ de n indices appartenant à $[1,p]$, nous désignerons par e_s le tenseur $e_{i_1} e_{i_2} ... e_{i_n}$; les n^p tenseurs e_s forment une base régulière de l'espace tensoriel T_0^n . Considérons ceux des tenseurs e_s qui correspondent aux suites s croissantes ; toute autre suite de n indices est de la forme σs , où s est croissante et $\sigma \in \mathfrak{S}_n$;

comme $e_{\sigma s}=\sigma^{-1}e_s$ par définition, on a $e_{\sigma s} \equiv e_s \pmod{S}$, et il en résulte que les éléments $\varphi(e_s)=\dot{e}_s$ correspondant aux suites s croissantes forment un système de générateurs de la puissance symétrique n-ème E_0^n/S ; montrons qu'ils forment une <u>base régulière</u> de ce module. En effet, soit Γ l'ensemble des suites s croissantes ; pour chaque $s \in \Gamma$, soit B_s l'ensemble des $e_{\sigma s}$ <u>distincts</u> et <u>différents de</u> e_s ; il est immédiat, d'après la définition de S, que ce sous-module est engendré par les $e_s - e_{\sigma s}$, où s parcourt Γ, et, pour chaque s, $e_{\sigma s}$ parcourt B_s. Cela étant, une relation de la forme $\sum_{s\in\Gamma} \lambda_s \dot{e}_s = 0$ signifierait que $\sum_{s\in\Gamma} \lambda_s e_s = \sum_{\sigma,s} \mu_{\sigma,s}(e_s - e_{\sigma s})$ la somme du second membre étant étendue à tous les $s \in \Gamma$, et pour chaque s, à tous les $e_{\sigma s}$ appartenant à B_s. Or, comme la base (e_s) de E_0^n est régulière, une telle relation ne peut avoir lieu que si tous les $\mu_{\sigma,s}$ sont nuls ; il reste alors $\sum_{s\in\Gamma} \lambda_s e_s = 0$, qui donne $\lambda_s = 0$ pour tout $s \in \Gamma$. Comme l'ensemble Γ est équipotent à l'ensemble des suites $(\nu_k)_{1\leqslant k\leqslant p}$ de p entiers $\geqslant 0$ tels que $\sum_{k=1}^{p} \nu_k = n$, on voit que la puissance symétrique n-ème de $E=A^p$ est bien isomorphe au module des polynomes homogènes de degré n à p indéterminées sur l'anneau A. On <u>identifiera</u> d'ordinaire ces deux modules en choisissant une base (e_i) dans E, et en identifiant l'élément $\varphi(e_{i_1}\otimes e_{i_2}\otimes\ldots\otimes e_{i_n})$ de E_0^n/S au polynome $e_{i_1}e_{i_2}\ldots e_{i_n}$ de l'anneau $A\left[e_1,e_2,\ldots,e_p\right]_n$.

Si u est un automorphisme de $E = A^p$, u_n l'automorphisme de E_0^n, puissance tensorielle n-ème de u, il est clair que $u_n(S) \subset S$; par passage au quotient, on déduit donc de u_n un automorphhisme de la puissance symétrique n-ème de E, et par suite un automorphisme $\bar{u}_n$ du module des polynomes homogènes de degré n dans $A\left[e_1,e_2,\ldots,e_p\right]$,

qui fait correspondre au polynome $e_{i_1} e_{i_2} \dots e_{i_n}$ le polynome $u(e_{i_1})u(e_{i_2})\dots u(e_{i_n})$.

On peut aussi retrouver la multiplication des polynomes à partir de la multiplication des tenseurs ; en effet, considérons deux espaces tensoriels E_0^m , E_0^n , et l'application $(z,z') \to z.z'$ de $E_0^m \times E_0^n$ dans E_0^{m+n} ; si S_m (resp. S_n, S_{m+n}) est le sous-module de E_0^m (resp. E_0^n, E_0^{m+n}) où s'annulent les applications m-linéaires (resp. n-linéaires, (m+n)-linéaires) symétriques, les relations $z_1 \equiv z_2$ (mod. S_m) , $z'_1 \equiv z'_2$ (mod. S_n) entraînent $z_1.z'_1 \equiv z_2.z'_2$ (mod. S_{m+n}) . On déduit donc de l'application $(z,z') \to z.z'$ une application de $(E_0^m/S_m) \times (E_0^n/S_n)$ dans (E_0^{m+n}/S_{m+n}) par passage aux quotients, et on voit sans peine que cette application n'est autre que la multiplication des polynomes définie au n° 1 .

Si u est un automorphisme de la structure de module de E , il se prolonge d'une seule manière en un automorphisme $\bar{u}$ de la structure d'anneau de $A[e_1, e_2, .., e_p]$, la restriction de $\bar{u}$ au module des polynomes homogènes de degré n étant l'automorphisme $\bar{u}_n$ défini ci-dessus.

Supposons maintenant que, dans E , l'équation $n!y=x$ ait une solution et une seule pour tout x (ce qui est par exemple le cas si E est un espace vectoriel sur un corps de caractéristique 0 ou $> n$) ; on sait alors (chap.III, § 5) que tout tenseur symétrique d'ordre n est symétrisé d'un tenseur d'ordre n ; montrons que dans ce cas, il existe un isomorphisme canonique de la puissance symétrique n-ème sur le module S' des tenseurs symétriques d'ordre n . En effet, pour tout tenseur z d'ordre n , on peut écrire $n!z = Sz + \sum_\sigma (z - \sigma z)$, σ parcourant $\mathfrak{S}_n$, ce qui montre que E_0^n est somme des sous-modules S et S' ; comme en outre le symétrisé de tout tenseur de la forme $z - \sigma z$ est nul, on a $S \cap S' = \{0\}$, donc E_0^n est somme directe de

de S et S', et par passage au quotient, l'application $z \to Sz$ donne un isomorphisme de E_0^n/S sur S' .

On notera que ce raisonnement est valable, que E possède une ou non base régulière. Si E a une base régulière (e_i), on peut encore définir un isomorphisme de E_0^n/S sur S' , même si l'équation $n!y=x$ n'a pas toujours de solution dans E , mais cet isomorphisme dépendra de la base (e_i) considérée. En effet, avec les notations ci-dessus, on voit que le module S' admet une base régulière formée des éléments $a_s=e_s+\sum_b e_{cs}$, où s parcourt Γ , et, pour chaque s e_{cs} parcourt l'ensemble B_s ; S' admet donc une base régulière ayant même nombre d'éléments que E_0^n/S , donc est isomorphe à ce dernier.

Exercices. 1) Montrer que le module des polynomes homogènes de degré n à p indéterminées sur un anneau A est isomorphe au module des polynomes de degré $\leqslant n$ à $p-1$ indéterminées sur A .

2) Si f et g sont deux polynomes à p indéterminées tels que le produit fg soit homogène, montrer que f et g sont homogènes.

3) Soit M un groupe abélien, noté additivement, et totalement ordonné par une relation d'ordre $\alpha \leqslant \beta$ telle que $\alpha \leqslant \beta$ entraîne $\alpha+\gamma \leqslant \beta+\gamma$; on suppose en outre que, pour tout couple d'éléments λ , μ de M tels que $\lambda>0$, $\mu>0$, il existe un entier $n>0$ tel que $\lambda<n\mu$. Soit E l'algèbre du groupe M par rapport à un anneau commutatif A ; si A est un anneau d'intégrité, il en estde même de E ; si A est un corps, montrer que la division euclidienne se généralise aux éléments de E .

4) Soit $N^{(I)}$ le monoïde formé des éléments du monoïde produit N^I dont les coordonnées sont nulles à l'exception d'un nombre fini d'entre elles. Pour chaque $\iota \in I$, soit e_ι l'élément de $N^{(I)}$ dont toutes les coordonnées sont nulles, sauf celle d'indice ι,

qui est égale à 1 . On dit que l'algèbre du monoïde $\mathbb{N}^{(I)}$ par rapport à un anneau commutatif A ayant un élément unité, est l'anneau des polynomes par rapport aux e_ι . E le module $A^{(I)}$; montrer que la puissance symétrique n-ème de E est isomorphe au module formé des polynomes homogènes de degré n , dans l'anneau des polynomes par rapport aux e_ι ; montrer en outre que ces deux modules sont isomorphes au module des tenseurs symétriques contravariants d'ordre n sur E .

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

En déduire que, si E admet une base (a_i) de m éléments, et si $\mathfrak{a}_i$ est l'annulateur de a_i , $\bigvee^n E$ admet une base en correspondance biunivoque avec l'ensemble des suites <u>croissantes</u> $(i_k)_{1 \leqslant k \leqslant n}$ de n indices appartenant à $[1,m]$, et telles que l'idéal $\sum_{k=1}^{n} \mathfrak{a}_{i_k}$ soit $\neq A$. Montrer que $\bigvee^n E$ est encore isomorphe dans ce cas au sous-module des tenseurs symétriques d'ordre n sur E .

6) Si u est une application linéaire d'un module E dans un module F , l'application u_n puissance tensorielle n-ème de u est telle que $u_n(S) \subset S'$, où S (resp. S') est le sous-module de E_0^n (resp. F_0^n) où s'annulent toutes les applications multilinéaires symétriques ; par passage au quotient, on en déduit une application linéaire $\bigvee^n u$ de $\bigvee^n E$ dans $\bigvee^n F$, dite puissance symétrique n-ème de u . Si E et F sont deux espaces vectoriels sur un même corps commutatif, et si u est de rang fini r , montrer que $\bigvee^n u$

montrer que $\overset{n}{\bigvee} u$ est de rang $\binom{r+n-1}{n}$ (méthode de l'exerc.6 du chap.III, § 4).

§ 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. Nous allons définir dans E une loi de composition externe, dont l'ensemble des opérateurs est l'anneau $A[e]$ des polynomes à une indéterminée sur A ; pour cela, à tout polynome $f = a_0+a_1e+\dots+a_ne^n$ et à tout élément $x \in E$, on fait correspondre l'élément $a_0+a_1x+\dots+a_nx^n$, que nous noterons $f \circ x$, ou $f(x)$ lorsqu'aucune confusion n'est possible. En particulier, on a $e \circ x = x$ pour tout $x \in E$, e est donc opérateur neutre de la loi externe.

La loi de composition externe ainsi définie possède les propriétés suivantes :

(1) $$(f+g) \circ x = f \circ x + g \circ x$$

(2) $$(fg) \circ x = (f \circ x)(g \circ x)$$

En d'autres termes (chap.I, § 5) cette loi est distributive, d'une part par rapport à l'ensemble des deux lois additives dans $A[e]$ et dans E , d'autre part par rapport à l'ensemble des deux lois multiplicatives dans ces anneaux.

La relation (1) est immédiate ; la relation (2) est une conséquence de la formule de distributivité dans E (toutes les puissances de x étant permutables deux à deux, et permutables avec les opérateurs de A), et de la formule donnant le produit fg de deux polynomes.

On a en outre, pour tout $a \in A$

(3) $$(af) \circ x = a(f \circ x)$$

Les formules (1),(2) et (3) signifient que, pour tout x fixe dans E, l'application $f \to f \circ x$ est une <u>représentation</u> de l'algèbre $A[e]$ sur une sous-algèbre de E contenant x. D'ailleurs, d'après la définition de $f \circ x$, cette sous-algèbre est contenue dans la sous-algèbre <u>engendrée</u> par x. Donc :

<u>Proposition 1</u>. <u>La sous-algèbre E_x de E engendrée par un élément x est identique à l'ensemble des éléments $f \circ x$, où f parcourt l'algèbre $A[e]$</u>.

En général, l'application $f \to f \circ x$ n'est pas un isomorphisme ; l'algèbre E_x est isomorphe à l'algèbre quotient $A[e]/\mathfrak{a}$, où $\mathfrak{a}$ est l'idéal formé des polynomes f tels que $f \circ x = 0$, et cet idéal n'est pas nul en général.

Par exemple, si A est l'anneau $\mathbb{Z}$ des entiers rationnels, E=A et x=2, le polynome $f=e^2-4$ n'est pas nul dans $A[e]$, mais on a $f(2)=0$.

On peut en particulier définir la loi externe précédente sur l'algèbre $A[e]$ elle-même ; cela revient à dire que, dans $A[e]$, l'application $(f,g) \to f \circ g$ est une loi de composition <u>interne</u> ; les formules (1) et (2) prouvent que cette loi est distributive <u>à gauche</u> par rapport à l'addition et à la multiplication dans $A[e]$; par contre elle n'est pas distributive <u>à droite</u> par rapport à aucune de ces deux lois. On a identiquement $f \circ e = e \circ f = f$, autrement dit, e est <u>élément unité</u> pour la loi $f \circ g$. Enfin, on a dans $A[e]$

$$(4) \qquad (f \circ g) \circ h = f \circ (g \circ h)$$

autrement dit, la loi $(f,g) \to f \circ g$ est <u>associative</u> ; en effet, d'après (1) et (3), on peut se ramener au cas où $f=e^m$, autrement dit tout revient à voir que $g^m \circ h = (g \circ h)^m$, ce qui résulte, par récurrence, de la formule (2).

Supposons maintenant que E soit une algèbre commutative sur A, ayant un élément unité. On peut généraliser la loi de composition précédente de la manière suivante : à tout polynome $f = \sum a_{\nu_1 \nu_2 \dots \nu_n} e_1^{\nu_1} e_2^{\nu_2} \dots e_n^{\nu_n}$ de l'anneau $A[e_1, e_2, \dots, e_n]$ à n indéterminées sur A, et à tout élément $(x_1, x_2, \dots, x_n)$ de E^n, on fait correspondre l'élément de E égal à $\sum a_{\nu_1 \nu_2 \dots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$, qu'on notera encore $f \circ (x_1, \dots, x_n)$, ou simplement $f(x_1, \dots, x_n)$. On a $e_i \circ (x_1, x_2, \dots, x_n) = x_i$ pour $1 \leqslant i \leqslant n$, ainsi que les propriétés analogues à (1), (2) et (3) :

(5) $\qquad (f+g) \circ (x_1, \dots, x_n) = f \circ (x_1, \dots, x_n) + g \circ (x_1, \dots, x_n)$

(6) $\qquad (fg) \circ (x_1, \dots, x_n) = (f \circ (x_1, \dots, x_n))(g \circ (x_1, \dots, x_n))$

(7) $\qquad (\alpha f) \circ (x_1, \dots, x_n) = \alpha (f \circ (x_1, \dots, x_n))$

Pour un élément fixe $(x_1, \dots, x_n)$ de E^n, l'application $f \to f \circ (x_1, \dots, x_n)$ est encore une représentation de l'algèbre $A[e_1, \dots, e_n]$ sur une sous-algèbre de E contenant $x_1, \dots, x_n$, et on a la proposition suivante :

Proposition 2. La sous-algèbre de E engendrée par n éléments $x_1, x_2, \dots, x_n$, est identique à l'ensemble des éléments $f \circ (x_1, x_2, \dots, x_n)$, où f parcourt l'algèbre $A[e_1, e_2, \dots, e_n]$.

En particulier, on peut prendre pour E une algèbre de polynomes $A[e_1, e_2, \dots, e_p]$ sur A, où p est un entier quelconque ; si $g_1, \dots, g_n$ sont n polynomes de cette algèbre, f un polynome de $A[e_1, \dots, e_n]$, $f \circ (g_1, g_2, \dots, g_n)$ est un polynome de $A[e_1, e_2, \dots, e_p]$. On a identiquement $f \circ (e_1, e_2, \dots, e_n) = f$. Enfin, si $h_1, h_2, \dots, h_p$ sont p polynomes de l'algèbre $A[e_1, e_2, \dots, e_q]$, on a la formule qui généralise (4)

(8) $\qquad (f \circ (g_1, \dots, g_n)) \circ (h_1, \dots, h_p) = f \circ (g_1 \circ (h_1, \dots, h_p), \dots, g_n \circ (h_1, \dots, h_p))$

qu'il suffit, d'après (5) (6) et (7), de démontrer quand $f = e_i$ $(1 \leqslant i \leqslant n)$ et la relation est alors évidente.

Remarques. 1) Lorsque l'algèbre E n'a pas d'élément unité, on ne peut plus définir $f \circ x$ pour tout polynome $f \in A[e]$, mais seulement pour les polynomes f sans terme de degré 0 (c'est-à-dire de la forme eg , où g est quelconque) ; de même, si E est commutatif, on ne peut définir $f \circ (x_1,\dots,x_n)$ que pour les polynomes $f \in A[e_1,\dots,e_n]$ sans terme de degré (total) 0 . Avec cette restriction, toutes les propriétés démontrées ci-dessus sont encore valables.

2) Si E est une algèbre non commutative, mais si les éléments $x_1,\dots,x_n$ de E sont deux à deux permutables, on peut encore définir comme ci-dessus l'élément $f \circ (x_1,\dots,x_n)$ pour tout polynome $f \in A[e_1,\dots,e_n]$, et les propriétés précédentes restent valables ; il suffit en effet de considérer, au lieu de E , la sous-algèbre de E engendrée par $x_1,\dots,x_n$, qui est commutative.

2. Fonctions polynomes sur une algèbre. Soit E une algèbre sur A , ayant un élément unité ; rappelons que l'ensemble E^E des applications de E dans lui-même est muni d'une structure d'algèbre par rapport à A lorsque, pour deux applications u,v de E dans lui-même, et un $\alpha \in A$, on désigne par u+v (resp. uv , αu) l'application $x \to u(x)+v(x)$ (resp. $x \to u(x)v(x)$, $x \to \alpha u(x)$) de E dans lui-même. Désignons par u_0 l'application identique $x \to x$ de E sur lui-même, et soit $P_1(E)$ la sous-algèbre de E^E engendrée par u_0 ; d'après la prop.1, $P_1(E)$ n'est autre que l'ensemble des fonctions $\tilde{f} = f \circ u_0$, où f parcourt l'anneau des polynomes $A[e]$ et $f \to \tilde{f}$ est une représentation de $A[e]$ sur $P_1(E)$; nous dirons que $\tilde{f}$ est la fonction polynome d'une variable sur E , à coefficients dans A , correspondant à f . Si $f = a_0 + a_1 e + \dots + a_n e^n$, $\tilde{f}$ est l'application

$$x \to a_0 + a_1 x + \ldots + a_n x^n = f \circ x$$

et réciproquement, toute application de cette forme est évidemment une fonction polynome ; en particulier, l'application identique u_0 n'est autre que la fonction polynome $\tilde{e}$.

Si f et g sont deux polynomes de $A[e]$, et $h=f\circ g$, on a $\tilde{h} = \tilde{f} \circ \tilde{g}$; comme $f \to \tilde{f}$ est une représentation, il suffit de le démontrer pour $f=e$, et la proposition est alors évidente.

Supposons maintenant que E soit commutative ; considérons l'algèbre commutative E^{E^n} des applications de l'algèbre E^n dans E , et soit u_i l'application $(x_1,..,x_n) \to x_i$ de E^n sur E (projection d'indice i). La sous-algèbre $P_n(E)$ de E^{E^n} engendrée par les n éléments u_i est formée des fonctions $\tilde{f} = f\circ(u_1,u_2,..,u_n)$, où f parcourt l'anneau $A[e_1,e_2,..,e_n]$, et $f \to \tilde{f}$ est une <u>représentation</u> de $A[e_1,..,e_n]$ sur $P_n(E)$; on dira encore que $\tilde{f}$ est la <u>fonction polynome de n variables</u> sur E^n (ou, par abus de langage, <u>sur</u> E) , <u>à coefficients dans</u> A , correspondant à f ; si $f = \sum a_{\nu_1\nu_2\ldots\nu_n} e_1^{\nu_1} e_2^{\nu_2} \ldots e_n^{\nu_n}$, $\tilde{f}$ est l'application

$$(x_1,\ldots,x_n) \to f\circ(x_1,\ldots,x_n) = \sum a_{\nu_1\nu_2\ldots\nu_n} x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}$$

et réciproquement, toute application de cette forme est une application polynome.

Par exemple, si à toute "suite double" (x_{ij}) $(1\leqslant i\leqslant n, 1\leqslant j\leqslant n)$ de n^2 éléments de E , on fait correspondre le déterminant $\boxed{x_{ij}}$, on définit une fonction polynome de n^2 variables, qui correspond au polynome $\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_\sigma e_{1,\sigma(1)} e_{2,\sigma(2)} \cdots e_{n,\sigma(n)}$ c'est-à-dire au déterminant $\boxed{e_{ij}}$ dans l'anneau de polynomes $A[e_{11},\ldots,e_{nn}]$ à n^2 indéterminées.

Nous allons chercher, dans ce qui suit, des conditions moyennant lesquelles l'application $f \to \tilde{f}$ est un <u>isomorphisme</u> de $A[e_1,\ldots,e_n]$ sur l'anneau $P_n(E)$.

3. Racines d'un polynome à une indéterminée. Nous allons d'abord considérer le cas particulier où $n=1$ et $E=A$. Pour tout polynome $f \in A[e]$, un élément $\alpha \in A$ est dit racine (ou zéro) du polynome f dans A, si on a $\tilde{f}(\alpha) = f \circ \alpha = 0$.

Proposition 3. Pour que α soit racine de f, il faut et il suffit que $e-\alpha$ soit un diviseur de f.

En effet, comme le coefficient du terme dominant dans $e-\alpha$ est l'unité, on peut faire la division euclidienne de f par $e-\alpha$; on peut donc écrire $f=(e-\alpha)g+\beta$, et comme le reste est de degré < 1 s'il n'est pas nul, c'est nécessairement un élément $\beta \in A$; on a donc identiquement pour tout $\xi \in K$,

$$\tilde{f}(\xi) = (\xi-\alpha)\tilde{g}(\xi)+\beta$$

d'où en particulier $\tilde{f}(\alpha)=\beta$; si $\tilde{f}(\alpha)=0$, $e-\alpha$ divise donc f : la réciproque est évidente.

On dit qu'une racine α de f dans A est racine multiple d'ordre k (et que k est son ordre de multiplicité) si f est divisible par $(e-\alpha)^k$, mais non par $(e-\alpha)^{k+1}$; autrement dit, on doit avoir $f=(e-\alpha)^k g$, et le quotient g de f par $(e-\alpha)^k$ est déterminé de façon unique, car $e-\alpha$ n'est pas un diviseur de 0 dans $A[e]$; il faut et il suffit en outre, d'après la prop.3, qu'on ait $\tilde{g}(\alpha) \neq 0$. On a évidemment $k \leqslant \deg.f$, car $\deg.f=k+\deg.g$. Si $k=1$, on dit que α est racine simple de f dans A.

Théorème 1. Si A est un anneau d'intégrité, la somme des ordres de multiplicité des racines dans A d'un polynome de degré n de $A[e]$ est $\leqslant n$.

Supposons en effet que $\alpha_1, \alpha_2, \ldots, \alpha_p$ soient des racines distinctes d'un polynome $f \in A[e]$ de degré n dans A ; si k_i désigne l'ordre de multiplicité de α_i, nous allons voir que f est égal au produit du polynome

au polynome $(e-a_1)^{k_1}(e-a_2)^{k_2}\dots(e-a_p)^{k_p}$ par un polynome (nécessairement de degré $n-\sum_{i=1}^{p} k_i$) ; le théorème en est une conséquence.

La proposition étant vraie pour $p=1$, démontrons-la par récurrence sur p ; supposons donc que l'on ait

$$f = (e-a_1)^{k_1}(e-a_2)^{k_2}\dots(e-a_{p-1})^{k_{p-1}}g \qquad (6)$$

où g est un polynome ; on a donc, pour tout A

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

Par hypothèse, a_p est racine de f, donc

$$\tilde{f}(a_p)=(a_p-a_1)^{k_1}(a_p-a_2)^{k_2}\dots(a_p-a_{p-1})^{k_{p-1}}\tilde{g}(a_p)=0$$

Comme $a_p-a_i\neq 0$ pour $1\leqslant i\leqslant p-1$, et que A est un anneau d'intégrité, on a nécessairement $\tilde{g}(a_p)=0$, autrement dit, a_p est racine de g. Si $(e-a_p)^k$ est la plus grande puissance de $(e-a_p)$ qui divise g, on a $k\leqslant k_p$ d'après la définition de k_p ; si on avait $k<k_p$, en divisant les deux membres de (6) par $(e-a_p)^k$, et posant $g=(e-a_p)^k q$, on déduirait de (6) que

$$(a_p-a_1)^{k_1}(a_p-a_2)^{k_2}\dots(a_p-a_{p-1})^{k_{p-1}}\tilde{q}(a_p)=0$$

d'où $\tilde{q}(a_p)=0$, et par suite q serait divisible par $e-a_p$, contrairement à la définition de k. On a donc $k=k_p$, ce qui achève la démonstration.

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

En effet, tout polynome non nul de degré $p\leqslant n$, a au plus p racines distinctes dans A.

Corollaire 2. Soit A un anneau d'intégrité ; si f et g sont deux polynomes de $A[e]$, de degré $\leqslant n$, tels que les fonctions $\tilde{f}$ et $\tilde{g}$ soient égales pour $n+1$ valeurs distinctes de la variable dans A, on a $f=g$.

Il suffit d'appliquer le cor.1 au polynome $f-g$.

Le th.1 et ses corollaires sont inexacts lorsque l'anneau A possède des diviseurs de 0 . Par exemple, dans l'anneau quotient $\mathbb{Z}/(16)$, la fonction polynome x^2 a quatre racines distinctes, savoir les classes (mod.16) de 0,4,8 et 12.

Application. Formule d'interpolation de Lagrange. Soit K un corps commutatif, a_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 $f \in K[s]$ tels que $\tilde{f}(a_i)=\beta_i$ pour $1 \leqslant i \leqslant n$. Si f et g sont deux polynomes ayant cette propriété, et $h=f-g$, on a $h(a_i)=0$ pour $1 \leqslant i \leqslant n$, donc $h=(s-a_1)\ldots(s-a_n)q$, où q est un polynome arbitraire ; il suffit donc d'avoir une solution du problème pour les avoir toutes. Supposons d'abord que $\beta_i=1$, et $\beta_k=0$ pour $k \neq i$; tout polynome f répondant à la question est alors divisible par $(s-a_1)..(s-a_{i-1})(s-a_{i+1})..(s-a_n)$; montrons qu'on peut trouver une constante λ telle que $u_i=\lambda(s-a_1)..(s-a_{i-1})(s-a_{i+1})\ldots(s-a_n)$ soit une solution ; la condition $u_i(a_i)=1$ donne en effet $\lambda(a_i-a_1)..(a_i-a_{i-1})(a_i-a_{i+1})..(a_i-a_n)=1$, et comme tous les facteurs a_i-a_k $(k \neq i)$ sont $\neq 0$ par hypothèse, λ est bien déterminé.

Le polynome u_i étant ainsi déterminé, revenons au cas général où les β_i sont quelconques ; il est immédiat que $f=\sum_{i=1}^{n} \beta_i u_i$ est un polynome répondant à la question ; son degré est $\leqslant n-1$, et c'est évidemment le seul polynome ayant cette propriété ; l'expression trouvée

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

est dite formule d'interpolation de Lagrange.

4. Fonctions polynomes sur un anneau d'intégrité infini. Le corollaire 1 du th. 1 entraîne en particulier le th. suivant :

Théorème 2. Si A est un anneau d'intégrité infini, l'application $f \to \tilde{f}$ de l'algèbre des polynomes $A[e]$ sur l'algèbre $P_1(A)$ des fonctions polynomes d'une variable sur A est un isomorphisme.

En effet, la relation $\tilde{f}=0$ entraîne $f=0$; car, si f est de degré n, A contient par hypothèse n+1 éléments distincts, en chacun desquels $\tilde{f}$ s'annule ; donc $f=0$.

Le th.2 est inexact si A est un anneau d'intégrité n'ayant qu'un nombre fini d'éléments ; car si a_i $(1 \leqslant i \leqslant q)$ sont ces éléments distincts, le polynome $f=\prod_{i=1}^{q}(e-a_i)$ n'est pas nul, et on a $\tilde{f}(a_i)=0$ pour tout indice i.

Nous allons montrer que le th. 2 s'étend aux polynomes à un nombre quelconque d'indéterminées ; cela va résulter de la proposition suivante :

Proposition 4. Soit A un anneau d'intégrité infini, f un polynome non nul de $A[e_1,e_2,\ldots,e_n]$. Il existe un élément $(a_1,a_2,\ldots,a_n)\in A^n$ tel que $\tilde{f}(a_1,a_2,\ldots,a_n)\neq 0$.

La proposition étant vraie pour n=1, nous la démontrerons par récurrence sur n. Le polynome f peut être considéré comme polynome à une indéterminée e_n sur l'anneau $A[e_1,e_2,\ldots,e_{n-1}]$; comme $f\neq 0$, il y a au moins un coefficient $g_i \in A[e_1,e_2,\ldots,e_{n-1}]$ qui n'est pas nul.
La proposition étant supposée vraie pour les polynomes à n-1 indéterminées, il existe $(a_1,a_2,\ldots,a_{n-1})\in A^{n-1}$, tel que $g_i(a_1,a_2,\ldots,a_{n-1})\neq 0$. Si alors on remplace chaque coefficient g_k de f par $g_k(a_1,a_2,\ldots,a_{n-1})$, on obtient un polynome $h\in A[e_n]$, qui n'est pas nul ; d'après le th.2, il existe $a_n\in A$ tel que $\tilde{h}(a_n)\neq 0$; comme $\tilde{h}(a_n)=\tilde{f}(a_1,a_2,\ldots,a_n)$, la proposition est démontrée.

corollaire. Soit A un anneau d'intégrité infini, $(f_i)_{1 \leqslant i \leqslant m}$ une suite finie de polynomes non nuls de $A[e_1, e_2, \ldots, e_n]$. Il existe une infinité d'éléments $(a_1, a_2, \ldots, a_n) \in A^n$ tels que $\tilde{f}_i(a_1, \ldots, a_n) \neq 0$ pour $1 \leqslant i \leqslant m$. Pour montrer l'existence d'un élément $(a_1, \ldots, a_n) \in A^n$ ayant la propriété voulue, il suffit d'appliquer la prop.4 au polynome $f = f_1 f_2 \ldots f_m$. D'autre part, la démonstration de la prop.4 prouve (par récurrence sur n), en tenant compte du th.1 et du fait que A est infini, l'existence d'une infinité d'éléments $(a_1, \ldots, a_n)$ pour lesquels $\tilde{f}$ n'est pas nulle.

De la prop.4 et de son corollaire, on déduit d'abord l'importante proposition suivante :

Proposition 5 (principe d'inconséquence des inégalités algébriques). Soit A un anneau d'intégrité infini, $(g_i)_{1 \leqslant i \leqslant m}$ une suite finie de polynomes non nuls de $A[e_1, e_2, \ldots, e_n]$. Si f est un polynome de $A[e_1, e_2, \ldots, e_n]$ tels que $\tilde{f}(x_1, x_2, \ldots, x_n) = 0$ pour tout élément $(x_i) \in A^n$ tel que $\tilde{g}_i(x_1, \ldots, x_n) \neq 0$ pour $1 \leqslant i \leqslant m$, f est nul.

En effet, dans le cas contraire, il existerait, d'après le cor. de la prop.4, un élément $(a_1, \ldots, a_n) \in A^n$ tel que $\tilde{f}(a_1, \ldots, a_n) \neq 0$ et $\tilde{g}_i(a_1, \ldots, a_n) \neq 0$ pour $1 \leqslant i \leqslant m$, contrairement à l'hypothèse.

La prop.4 entraîne évidemment la généralisation du th.2 aux polynomes à n indéterminées, puisqu'elle signifie que $f \neq 0$ entraîne $\tilde{f} \neq 0$.

Plus généralement :

Théorème 3. Soit E un anneau d'intégrité infini, A un sous-anneau de E (fini ou non). Si on considère E comme une algèbre sur A, l'application $f \to \tilde{f}$ de l'algèbre des polynomes $A[e_1, e_2, \ldots, e_n]$ sur l'algèbre $F_n(E)$ est un isomorphisme.

En d'autres termes, si pour tout élément $(x_i) \in E^n$, on a $\sum a_{\nu_1 \nu_2 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n} = 0$, on a nécessairement $a_{\nu_1 \nu_2 \ldots \nu_n} = 0$ pour toute suite d'exposants (ν_i).

En effet, $A[e_1,e_2,\ldots,e_n]$ est un sous-anneau de $E[e_1,e_2,\ldots,e_n]$, donc la prop.4 appliquée en y remplaçant A par E, prouve que la relation $\tilde{f}=0$ entraîne $f=0$ pour tout $f\in A[e_1,e_2,\ldots,e_n]$.

Scholie. Le th.3 et le principe d'inconséquence des inégalités fournissent des moyens très commodes pour démontrer qu'un polynome f à n indéterminées sur un anneau d'intégrité A est nul. Il suffit de considérer un anneau d'intégrité infini E, contenant un sous-anneau isomorphe à A (qu'on identifie à A), et de démontrer que la fonction polynome $\tilde{f}$, correspondante à f, est nulle dans E^n, ou seulement pour tous les éléments de E^n qui n'annulent pas un certain nombre (fini) de fonctions polynomes données. Lorsque A est infini, il suffit de prendre E=A ; sinon, on peut par exemple prendre pour E l'algèbre des polynomes $A[e]$. La relation f=0 étant supposée démontrée de la sorte, on en déduit $f\circ(y_1,y_2,\ldots,y_n)=0$ pour tout élément $(y_i)\in F^n$, où F est une autre algèbre commutative quelconque sur A (pouvant en particulier être finie et avoir des diviseurs de 0).

Par exemple, tout déterminant sur un anneau commutatif quelconque A est une valeur de la fonction polynome correspondant au polynome $\det(e_{ij})$ de $\mathbb{Z}[e_{11},\ldots,e_{mn}]$, A étant considéré comme une algèbre sur l'anneau $\mathbb{Z}$. Si on prend $A=\mathbb{Z}$, on voit que toutes les identités entre déterminants démontrées au chap.III, §5, sous la condition que certains déterminants ne s'annulent pas, sont valables dans tous les cas.

De même, si un polynome $f\in\mathbb{Z}[e_1,e_2,\ldots,e_n]$ est tel que $\tilde{f}(x_1,x_2,\ldots,x_n)=0$ pour tout élément d'un corps commutatif quelconque K (considéré comme algèbre sur $\mathbb{Z}$), on a la même identité pour tout élément d'un anneau commutatif quelconque A, car en appliquant l'identité au corps infini Q, on en déduit que f=0.

Lorsque l'anneau A est un anneau d'intégrité infini, ce qui est le cas le plus fréquent dans les applications, on identifie souvent les deux anneaux $A[e_1,\dots,e_n]$ et $P_n(A)$ au moyen de l'isomorphisme $f \to \tilde{f}$, et lorsqu'on parle d'un "polynome défini dans A^n, à coefficients dans A", c'est d'une fonction polynome qu'il est question.

Avec l'abus de langage habituel qui consiste à confondre une fonction et sa valeur pour un élément générique (Bourb. R, § 2), on parle donc du "polynome f(x)", ou du "polynome $a_0+a_1x+\dots+a_nx^n$". Tant que les conditions précédentes sont remplies, ces confusions ne peuvent causer aucun inconvénient sérieux.

Remarque. Les conditions de l'énoncé du th. 3 ne sont pas nécessaires pour que l'application $f \to \tilde{f}$ de $A[e_1,\dots,e_n]$ sur $P_n(E)$ soit un isomorphisme (cf. exerc. 5). Un exemple intéressant est le suivant : A étant un anneau commutatif quelconque ayant un élément unité, prenons pour E l'algèbre des polynomes $A[e_1,\dots,e_m]$ sur A, avec $m \geqslant n$; par définition, $\tilde{f}$ est l'application $(u_1,\dots,u_n) \to f\circ(u_1,\dots,u_n)$ définie au n°1. La relation $\tilde{f}=0$ entraîne donc en particulier $f\circ(e_1,\dots,e_n)=0$, c'est-à-dire $f=0$; donc $f \to \tilde{f}$ est un isomorphisme, même si A admet des diviseurs de 0.

Il ne faudrait pas croire toutefois que $f \to \tilde{f}$ soit un isomorphisme sous la seule condition que A soit un anneau infini. Prenons par exemple pour A un anneau produit de la forme F^I, où F est un anneau fini, et soit $\xi \to \overline{\xi}$ l'isomorphisme de F sur le sous-anneau de A formé des éléments dont toutes les coordonnées sont égales, $\overline{\xi}$ étant l'élément ayant toutes ses coordonnées égales à ξ. On a vu qu'il existe un polynome $f=\sum_k a_k e^k$ sur F, non nul et tel que $\tilde{f}(\xi)=0$ pour tout $\xi \in F$; le polynome $g=\sum_k \overline{a}_k e^k$ sur A est tel que $\tilde{g}(\xi)=0$ pour tout $\xi \in A$, car la coordonnée d'indice ν de $\tilde{g}(\xi)$ n'est autre que $\tilde{f}(\xi_\nu)$.

5. Fonctions polynomes à valeurs dans un module. On peut généraliser la notion de fonction polynome au cas où la fonction prend ses valeurs dans un A-module :

Définition 1. Etant donnés un anneau commutatif A (ayant un élément unité) et un A-module unitaire E, on dit qu'une application f de A^n dans E est une fonction polynome de n variables s'il existe un nombre fini d'éléments $a_{\nu_1 \nu_2 \dots \nu_n}$ de E tels qu'on ait identiquement

$$(9) \qquad f(\xi_1, \xi_2, \dots, \xi_n) = \sum_{\nu_1, \nu_2, \dots \nu_n} a_{\nu_1 \nu_2 \dots \nu_n} \xi_1^{\nu_1} \xi_2^{\nu_2} \dots \xi_n^{\nu_n}$$

Proposition 6. Si A est un anneau d'intégrité infini, et E un A-module régulier, l'identité $\sum_{\nu_1, \nu_2, \dots, \nu_n} a_{\nu_1 \nu_2 \dots \nu_n} \xi_1^{\nu_1} \xi_2^{\nu_2} \dots \xi_n^{\nu_n} = 0$ dans A^n entraîne que les $a_{\nu_1 \nu_2 \dots \nu_n}$ sont tous nuls.

En effet, on sait (chap.II, §) que, si K est le corps des fractions de l'anneau A, E est isomorphe à un sous-module d'un espace vectoriel F sur K (F étant considéré comme A-module). Soit (e_ι) une base de F, et posons $a_{\nu_1 \nu_2 \dots \nu_n} = \sum_\iota e_\iota a_{\iota; \nu_1 \nu_2 \dots \nu_n}$; la relation $\sum_{\nu_1 \nu_2 \dots \nu_n} a_{\nu_1 \nu_2 \dots \nu_n} \xi_1^{\nu_1} \xi_2^{\nu_2} \dots \xi_n^{\nu_n} = 0$ entraîne, pour chaque ι, $\sum_{\nu_1, \nu_2, \dots, \nu_n} a_{\iota; \nu_1 \nu_2 \dots \nu_n} \xi_1^{\nu_1} \xi_2^{\nu_2} \dots \xi_n^{\nu_n} = 0$, quels que soient les ξ_i dans A donc aussi quels que soient les ξ_i dans K ; d'après le th.3, on a donc $a_{\iota; \nu_1 \nu_2 \dots \nu_n} = 0$ pour tout ι et pour tout système d'indices $(\nu_1, \nu_2, \dots, \nu_n)$, d'où la proposition.

De façon plus précise, si l'application $\xi \longrightarrow \sum_{k=0}^{n} a_k \xi^k$ s'annule pour n+1 valeurs distinctes de ξ dans A, on a nécessairement $a_k = 0$ pour $0 \leqslant k \leqslant n$.

On déduit de cette proposition que, lorsque A et E satisfont aux conditions de son énoncé, une application polynome f de A^n dans E ne peut se mettre sous la forme (9) que d'une seule manière ; les éléments bien déterminés $a_{\nu_1 \nu_2 \dots \nu_n}$ de E sont alors appelés les coefficients de f ;

le nombre $\sum_{k=1}^{n} \nu_k$ est appelé le <u>degré total</u> (ou simplement <u>degré</u>) du terme $a_{\nu_1 \nu_2 \dots \nu_n} \xi_1^{\nu_1} \xi_2^{\nu_2} \dots \xi_n^{\nu_n}$; le plus grand des degrés des termes (à coefficients non nuls) de f est le <u>degré total</u> (ou <u>degré</u>) de f . On définit de même le degré de f (et celui de chacun de ses termes) par rapport à l'une quelconque des variables ξ_i .

<u>Définition 2</u>. <u>Etant donnée deux A-modules unitaires E et F , on dit qu'une application f de E dans F est une application polynome si, quels que soient l'entier $m > 0$ et les éléments $x_1, x_2, \dots, x_m$ de E , l'application</u>

$$(\lambda_1, \lambda_2, \dots, \lambda_m) \longrightarrow f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_m x_m)$$

<u>de A^m dans F est une fonction polynome</u>.

<u>Exemples</u>. Une fonction polynome de n variables, à valeurs dans F , est une application polynome du module A^n dans F . Réciproquement, soit f une application polynome de A^n dans F ; si (e_i) est la base canonique de A^n , ξ_i $(1 \leqslant i \leqslant n)$ les coordonnées d'un élément $x \in A^n$ on a $f(x) = f(\sum_{i=1}^{n} \xi_i e_i)$, donc $(\xi_1, \xi_2, \dots, \xi_n) \longrightarrow f(\sum_{i=1}^{n} \xi_i e_i)$ est une fonction polynome. Une application linéaire de E dans F est une application polynome ; si E_k $(1 \leqslant k \leqslant n)$ sont n A-modules unitaires, une application n-linéaire de $\prod_{k=1}^{n} E_k$ dans F est une application polynome

<u>Remarque</u>. La notion d'application polynome de E dans F est essentiellement relative à l'anneau d'opérateurs A de ces deux modules ; si B est un sous-anneau de A , toute application polynome de E dans F , lorsqu'on considère E et F comme des A-<u>modules</u>, est encore une application polynome de E dans F , lorsqu'on les considère comme des B-<u>modules</u>, mais la réciproque est inexacte. * Par exemple, si le corps $\mathbb{C}$ des nombres complexes est considéré comme espace vectoriel sur le corps $\mathbb{R}$, l'application $z \to \bar{z}$ de $\mathbb{C}$ sur lui-même est une application polynome ; mais ce n'est pas une application polynom

lorsqu'on considère le corps $\mathbb{C}$ comme espace vectoriel par rapport à lui-même. *

Si f est une application polynome de E dans F , g une application polynome de F dans G , il est immédiat que la fonction composée $g\,f$ est une application polynome de E dans G . Plus généralement, soient (E_i), (F_j) deux familles finies de A-modules unitaires $(1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q)$; soit f_j une application polynome de $\prod_{i=1}^{p} E_i$ dans F_j pour $1 \leqslant j \leqslant q$, g une application polynome de $\prod_{j=1}^{q} F_j$ dans G ; alors l'application

$$(x_1,\dots,x_p) \to g(f_1(x_1,\dots,x_p), f_2(x_1,\dots,x_p),\dots,f_q(x_1,\dots,x_p))$$

est une application polynome de $\prod_{i=1}^{p} E_i$ dans G .

En particulier, si $(x_1,\dots,x_n) \to f(x_1,x_2,\dots,x_n)$ est une application polynome d'un module E^n , produit de n modules identiques à E , dans un module F , l'application $x \to f(x,x,\dots,x)$ est une application polynome de E dans F qu'on dit obtenue à partir de l'application polynome donnée par identification des variables.

Il est immédiat que, si f est une application polynome de E dans F , et H un sous-module de E , la restriction de f à H est une application polynome de H dans F .

Supposons maintenant que A soit un anneau d'intégrité infini ; si f est une application polynome de E dans F , on peut alors écrire

$$(10)\quad f(\lambda_1 x_1+\lambda_2 x_2+\dots+\lambda_m x_m) = \sum_{\nu_1,\nu_2,\dots,\nu_m} \lambda_1^{\nu_1}\lambda_2^{\nu_2}\dots\lambda_m^{\nu_m} f_{\nu_1\nu_2\dots\nu_m}(x_1,x_2,\dots,x_m)$$

la somme étant étendue à toutes les suites finies ($_k$) de m entiers $\geqslant 0$, les coefficients $f_{\nu_1\nu_2\dots\nu_m}(x_1,\dots,x_m)$ étant bien déterminés pour chaque valeur de $(x_1,\dots,x_n)$, et nuls sauf un nombre fini d'entre eux (ce nombre pouvant dépendre de l'élément (x_i) considéré .

Si dans (10) on remplace chaque x_i par $\sum_{j=1}^{n} \mu_{ij} y_{ij}$ (n quelconque), on a identiquement

$$f\Big(\sum_{i,j} \lambda_i \mu_{ij} y_{ij}\Big) = \sum_{\nu_{11}, \nu_{12}, \dots, \nu_{1n}, \nu_{21}, \dots, \nu_{2n}, \dots, \nu_{mn}} \lambda_1^{\nu_{11}+\dots+\nu_{1n}} \lambda_2^{\nu_{21}+\dots+\nu_{2n}} \lambda_m^{\nu_{m1}+\dots+\nu_{mn}}$$

$$\mu_{11}^{\nu_{11}} \dots \mu_{1n}^{\nu_{1n}} \mu_{21}^{\nu_{21}} \dots \mu_{2n}^{\nu_{2n}} \dots \mu_{mn}^{\nu_{mn}} f_{\nu_{11}, \dots, \nu_{mn}}(y_{11}, \dots, y_{mn}) = \sum_{\nu_1 \dots \nu_m} \lambda_1^{\nu_1} \dots \lambda_m^{\nu_m} f_{\nu_1 \dots \nu_m}\Big(\sum_j \mu_{ij} y_{ij}\Big)$$

d'où, en considérant les deux derniers membres comme des fonctions polynomes de $\lambda_1, \dots, \lambda_m$, on a, d'après la prop.6

$$f_{\nu_1 \dots \nu_m}\Big(\sum_{j=1}^{n} \mu_{1j} y_{1j}, \dots, \sum_{j=1}^{n} \mu_{mj} y_{mj}\Big) = \sum_{\nu_k = \sum_j \nu_{kj}} \mu_{11}^{\nu_{11}} \dots \mu_{mn}^{\nu_{mn}} f_{\nu_{11} \dots \nu_{mn}}(y_{11}, \dots, y_{mn})$$

Autrement dit, les coefficients $f_{\nu_1 \nu_2 \dots \nu_m}$ dans (10) sont des applications polynomes du module F^m dans F. En particulier, on a identiquement

$$(11) \qquad f_{\nu_1 \nu_2 \dots \nu_m}(\mu_1 x_1, \mu_2 x_2, \dots, \mu_m x_m) = \mu_1^{\nu_1} \mu_2^{\nu_2} \dots \mu_m^{\nu_m} f_{\nu_1 \nu_2 \dots \nu_m}(x_1, x_2, \dots, x_m)$$

On exprime cette identité en disant que $f_{\nu_1 \nu_2 \dots \nu_m}$ est homogène de degré ν_k par rapport à x_k $(1 \leqslant k \leqslant m)$; quand, dans $f_{\nu_1 \nu_2 \dots \nu_m}$, on remplace x_k par $\sum_{j=1}^{n} \mu_j y_{kj}$ (n quelconque), l'application

$(\mu_1, \dots, \mu_n) \longrightarrow f_{\nu_1 \nu_2 \dots \nu_m}(x_1, \dots, x_{k-1}, \sum_{j=1}^{n} \mu_j y_{kj}, x_{k+1}, \dots, x_m)$ est une fonction polynome dont tous les termes ont même degré ν_k.

Plus particulièrement, pour $m=1$, on a

$$(12) \qquad f(x) = \sum_{k=0}^{\infty} \lambda^k f_k(x)$$

et d'après ce qui précède, f_k est une application polynome homogène de degré k ; on dit que f_k est la partie homogène de degré k de l'application polynome f. On notera que f_0 est nécessairement constante, car $f_0(x) = f(0)$ pour tout $x \in E$. La plus petite valeur de k pour laquelle f_k n'est pas identiquement nulle est appelée le degré minimum de f. S'il existe un entier p tel que f_n soit identiquement nulle pour $n > p$, mais $f_p \neq 0$, on dit que p est le degré maximum, ou simplement degré de l'application polynome f.

Il peut se faire qu'aucun des f_k ne soit identiquement nul. Par exemple, prenons pour E le module $A^{(\mathcal{N})}$, et soit (e_n) la base canonique de E ; si, pour tout $x = \sum_n \xi_n e_n$, on pose $f(x) = \sum_n \xi_n^n$, f est une application polynome de E dans A, dont aucune partie homogène n'est identiquement nulle.

D'une manière générale, si, pour chaque entier $k \geqslant 0$, on se donne une application polynome homogène f_k de degré k de E dans F, la formule (12), où on fait $\lambda = 1$, définit une application polynome f de E dans F, dont f_k est la partie homogène de degré k, pourvu que, pour tout $x \in E$, il n'y ait qu'un nombre fini d'indices k tels que $f_k(x) \neq 0$.

Les notions de degré minimum et de degré maximum se généralisent de la façon suivante : soit E un module somme directe de p sous-modules E_i $(1 \leqslant i \leqslant p)$, et f une application polynome de E dans F ; pour $x_i \in E_i$, on a

$$(13)\quad f(\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_p x_p) = \sum_{\partial_1 \partial_2 \ldots \partial_p} f_{\partial_1 \partial_2 \ldots \partial_p}(x_1, x_2, \ldots, x_p)$$

et l'application $x_i \to f_{\partial_1 \partial_2 \ldots \partial_p}(x_1, x_2, \ldots, x_p)$ est une application polynome homogène de degré ∂_i de E_i dans F. On en conclut que la partie homogène de degré k de f est égale à la somme des $f_{\partial_1 \partial_2 \ldots \partial_p}$ pour lesquelles $\sum_{i=1}^{p} \partial_i = k$. La plus petite valeur de ∂_i dans les $f_{\partial_1 \partial_2 \ldots \partial_p}$ non nulle est par définition le <u>degré minimum de f par rapport à x_i</u> ; le degré minimum de f (qu'on appelle aussi son degré minimum <u>total</u>) <u>est donc au moins égal</u> à la somme des degrés minima de f par rapport à chacun des x_i. Lorsque, dans les $f_{\partial_1 \partial_2 \ldots \partial_p}$ non nuls, le degré ∂_i admet un maximum fini n_i, on dit que n_i est le <u>degré maximum</u> (ou simplement <u>degré</u>) <u>de f par rapport à x_i</u> ; si f est de degré (dit encore degré <u>total</u>) fini n, on a $n \leqslant \sum_{i=1}^{p} n_i$.

Remarque. Une application polynome homogène f de degré 1 n'est autre qu'une application linéaire de E dans F ; en effet, $f(\lambda x+\mu y)$ doit être une fonction polynome en (λ, μ), dont tous les termes sont de degré 1, donc on a $f(\lambda x+\mu y)=\lambda g(x,y)+\mu h(x,y)$; en faisant $\lambda=1, \mu=0$, on a $g(x,y)=f(x)$ et en faisant $\lambda=0, \mu=1$, $h(x,y)=f(y)$.

De la même manière, une application polynome de $\prod_{k=1}^{m} E_k$ dans F, homogène et de degré 1 par rapport à chacune des variables $x_k \in E_k$, n'est autre qu'une application m-linéaire de $\prod_{k=1}^{m} E_k$ dans F .

Une application polynome homogène de degré k de E dans l'anneau A est dite forme homogène de degré k sur E ; les formes linéaires sur E sont les formes homogènes de degré 1 .

Soit K le corps des fractions de l'anneau A ; on sait (chap.II, §) que E (resp. F) peut être plongé dans un espace vectoriel $\overline{E}$ (resp. $\overline{F}$) sur K, tout élément de $\overline{E}$ (resp. $\overline{F}$) étant de la forme $\frac{1}{\mu} x$, où $\mu \in A$ et $x \in E$ (resp. $x \in F$). Si f est une application polynome de E dans F, f peut se prolonger d'une seule manière en une application polynome $\overline{f}$ de $\overline{E}$ dans $\overline{F}$. D'après (12), il suffit de le démontrer lorsque f est homogène de degré k ; alors, si $y = \frac{1}{\mu} x$ est un élément de $\overline{E}$, avec $\mu \in A$ et $x \in E$, on a $x = \mu y$, donc on doit avoir $f(x)=\overline{f}(\mu y)=\mu^k \overline{f}(y)$, d'où $\overline{f}(\frac{1}{\mu} x)=\frac{1}{\mu^k} f(x)$. Inversement, cette condition définit bien $\overline{f}$; en effet, si on a $\frac{1}{\mu} x = \frac{1}{\nu} y$, avec $\mu \in A$, $\nu \in A$, $x \in E$, $y \in E$, on en tire $\nu x = \mu y$, donc $\nu^k f(x)=\mu^k f(y)$ et par suite $\frac{1}{\mu^k} f(x) = \frac{1}{\nu^k} f(y)$. Il reste à voir que l'application $\overline{f}$ est bien une application polynome ; or, si $x_1, x_2, \ldots, x_m$ sont m éléments fixes de $\overline{E}$, $\lambda_1, \lambda_2, \ldots, \lambda_m$ m éléments variables de K, on peut écrire $x_i = \frac{1}{\rho} y_i$ $(1 \leqslant i \leqslant m)$, $\lambda_i = \frac{1}{\sigma} \mu_i$ avec

avec $\rho \in A$, $\sigma \in A$, $\mu_i \in A$, donc $\overline{F}\left(\sum_{i=1}^{m} \lambda_i x_i\right) = \overline{F}\left(\frac{1}{\rho\sigma} \sum_{i=1}^{m} \mu_i y_i\right) =$

$= \frac{1}{(\rho\sigma)^k} f\left(\sum_{i=1}^{m} \mu_i y_i\right)$, d'où la proposition, en vertu de la relation (10), où tous les termes du second membre ont même degré k .

6. Fonctions rationnelles. Soit K un corps commutatif, f un élément du corps des fractions rationnelles $K(e_1, e_2, \ldots, e_n)$. Si p et q sont deux polynomes tels que $p/q = f$, l'application $(x_1, \ldots, x_n) \to \frac{\tilde{p}(x_1, x_2, \ldots, x_n)}{\tilde{q}(x_1, x_2, \ldots, x_n)}$ est définie en tout point $(x_i) \in K^n$ pour lequel $\tilde{q}(x_1, \ldots, x_n) \neq 0$; en outre, si p_1 et q_1 sont deux autres polynomes tels que $f = p_1/q_1$, on a $\frac{\tilde{p}(x_1, x_2, \ldots, x_n)}{\tilde{q}(x_1, x_2, \ldots, x_n)} = \frac{\tilde{p}_1(x_1, x_2, \ldots, x_n)}{\tilde{q}_1(x_1, x_2, \ldots, x_n)}$ en tout point (x_i) où les fonctions polynomes $\tilde{q}$ et $\tilde{q}_1$ sont toutes deux $\neq 0$; en effet, on a $qp_1 = p_1 q$, d'où identiquement $\tilde{p}(x_1, \ldots, x_n)\tilde{q}_1(x_1, \ldots, x_n) = \tilde{p}_1(x_1, \ldots, x_n)\tilde{q}(x_1, \ldots, x_n)$, ce qui établit la proposition. Désignons par H_f la partie de K^n formée des éléments (x_i) pour lesquels, pour au moins un des polynomes q , dénominateur d'une fraction égale à f , on a $\tilde{q}(x_1, \ldots, x_n) \neq 0$; si K est un corps infini , la prop.4 prouve que l'ensemble H_f n'est pas vide ; on désigne alors par f l'application de H_f dans K , dont la valeur, en tout élément (x_i) de H_f , est la valeur commune des fonctions $\frac{\tilde{p}(x_1, x_2, \ldots, x_n)}{\tilde{q}(x_1, x_2, \ldots, x_n)}$ telles que $\tilde{q}(x_1, \ldots, x_n) \neq 0$ et $f = p/q$, et on dit que $\tilde{f}$ est la fonction rationnelle correspondant à la fraction rationnelle f .

Nous verrons au chap.V que l'ensemble H_f peut être défini d'une manière plus simple : il existe en effet deux polynomes p_0, q_0 tels que $f = p_0/q_0$, et que H_f soit l'ensemble des points (x_i) tels que $\tilde{q}_0(x_1, x_2, \ldots, x_n) \neq 0$.

Si f et g sont deux fractions rationnelles telles que $\tilde{f}(x_1,\ldots,x_n) = \tilde{g}(x_1,\ldots,x_n)$ pour tout élément de l'ensemble $H_f \cap H_g$, on a $f=g$, en vertu du principe d'inconséquence des inégalités algébriques, puisque, si $f=p/q$, $g=p_1/q_1$, on a

$\tilde{p}(x_1,\ldots,x_n)\tilde{q}_1(x_1,\ldots,x_n)=\tilde{p}_1(x_1,\ldots,x_n)\tilde{q}(x_1,\ldots,x_n)$ pour tout élément (x_i) tel que $\tilde{q}(x_1,\ldots,x_n)\neq 0$ et $\tilde{q}_1(x_1,\ldots,x_n)\neq 0$.

Si f et g sont deux fractions rationnelles quelconques, le cor. de la prop.4 montre que l'ensemble $H_f \cap H_g$ est un ensemble infini ; en tout élément de cet ensemble, la fonction rationnelle correspondant à la fraction $f+g$ (resp. fg) est définie et a même valeur que $\tilde{f}+\tilde{g}$ (resp. $\tilde{f}\tilde{g}$). Il résulte du même corollaire que si $f\neq 0$ la partie H'_f où $f(x_1,\ldots,x_n)\neq 0$ est un ensemble infini, et en tout élément de cet ensemble, la fonction rationnelle correspondant à la fraction $1/f$ est définie et a même valeur que $1/\tilde{f}$.

Exercices. 1) Soit A un anneau d'intégrité ; si f et g sont deux polynomes de $A[e]$, montrer que la relation $f\circ g=0$ entraîne $f=0$ ou $g=0$, et que le degré de $f\circ g$ est égal au produit des degrés de f et de g. Généraliser aux polynomes à plusieurs indéterminées.

2) Soit A un anneau d'intégrité, f un polynome à n indéterminées, de degré k_i par rapport à e_i $(1\leqslant i\leqslant n)$. Pour chaque valeur de i, soit B_i un ensemble de k_i+1 éléments de A. Montrer que si $\tilde{f}(x_1,x_2,\ldots,x_n)=0$ pour tout $(x_i)\in \prod_{i=1}^{n} B_i$, on a $f=0$.

3) Soit A un anneau d'intégrité infini, Φ un ensemble de polynomes à n indéterminées sur l'anneau A, tel que la puissance de l'ensemble Φ soit strictement inférieure à celle de A. Montrer qu'il existe un élément $(a_i)\in A^n$ tel que, pour tout polynome $f\in\Phi$, on ait $\tilde{f}(a_1,a_2,\ldots,a_n)\neq 0$.

4) Soit E un anneau d'intégrité infini, muni d'une structure d'algèbre par rapport à un anneau d'intégrité A ; soit $\mathfrak{a}$ l'annulateur de E . Montrer que, si on pose $A_1 = A/\mathfrak{a}$, la structure d'anneau de $P_n(E)$ est isomorphe à celle de $A_1[e_1, e_2, \ldots, e_n]$.

5) Soit A un anneau commutatif, ayant un élément unité, et tel qu'il existe un sous-groupe infini G du groupe additif A , dont tous les éléments sont réguliers dans A (sauf l'élément 0). Montrer que l'application $f \to \tilde{f}$ de $A[e_1, e_2, \ldots, e_n]$ sur $P_n(A)$ est un isomorphisme (remarquer qu'un polynome à une indéterminée, de degré n , ne peut avoir $n+1$ racines distinctes appartenant à G). Cas particulier où tout élément est d'ordre infini dans le groupe additif A .

6) Soit K un corps infini, E un espace vectoriel sur K . Soit f une application de K^2 dans E telle que, pour tout $\xi \in K$, $\eta \to f(\xi, \eta)$ soit une fonction polynome de degré $\leqslant n$, et que pour tout $\eta \in K$, $\xi \to f(\xi, \eta)$ soit une fonction polynome de degré $\leqslant n$. Montrer que f est une fonction polynome de deux variables, de degré $\leqslant 2n$ (écrire $f(\xi, \eta) = \sum_{p=0}^{n} \xi^p f_p(\eta)$ et montrer que les f_p sont des fonctions polynomes de degré n , en donnant à ξ $n+1$ valeurs particulières distinctes). Généraliser aux applications de K^p dans E

7) Soit K un corps infini, E et F deux espaces vectoriels sur K . Soit f une application de E dans F telle que, pour tout couple de points x,y de E , l'application $(\lambda, \mu) \to f(\lambda x + \mu y)$ soit une fonction polynome de degré $\leqslant n$. Montrer que f est une application polynome de degré $\leqslant n$ de E dans F (utiliser l'exerc.6). Si A est un anneau d'intégrité dont K est le corps des quotients, montrer que la conclusion subsiste si on suppose seulement que $(\lambda, \mu) \to f(\lambda x + \mu y)$ est une fonction polynome de degré $\leqslant n$ dans A^2 .

§ 3. Différences et Différentielles.

1. Différences d'une fonction. Soient E et F deux groupes abéliens notés additivement, $G=F^E$ le groupe abélien formé des applications de E dans F. Soit h un élément quelconque de E ; pour toute fonction $f \in F^E$, désignons par $T_h f$ l'application $x \to f(x+h)$ de E dans F. Il est immédiat que T_h est un automorphisme du groupe abélien G ; en outre, dans le groupe $\mathcal{J}$ des automorphismes de G (ou l'anneau $\mathcal{E}$ des endomorphismes de G), on a

$$(1) \qquad T_h T_k = T_k T_h = T_{h+k}$$

pour deux éléments quelconques h,k de E.

En d'autres termes, h T_h est une représentation du groupe E dans le groupe $\mathcal{J}$, et comme la relation $T_h f=0$ entraîne f=0, c'est même un isomorphisme de E dans $\mathcal{J}$.

Désignons par I l'automorphisme identique (égal à T_0) de G ; dans l'anneau $\mathcal{E}$ des endomorphismes du groupe G, on pose $\Delta_h = T_h - I$; autrement dit

$$(2) \qquad \Delta_h f(x) = f(x+h)-f(x)$$

pour toute $f \in G$ et tout $x \in E$; la fonction $\Delta_h f$ est appelée première différence de f (relative à l'élément $h \in E$). D'après (1), deux endomorphismes Δ_h, Δ_k sont des éléments permutables dans l'anneau $\mathcal{E}$, quels que soient les éléments h,k de E : si $h_1, h_2, \ldots, h_n$ sont n éléments quelconques de E, on désigne par $\Delta^n_{h_1 h_2 \ldots h_n}$ le produit (dans un ordre quelconque) des n endomorphismes Δ_{h_i} $(1 \leqslant i \leqslant n)$ de G, et la fonction $\Delta^n_{h_1 h_2 \ldots h_n} f$ est appelée différence $n^{ème}$ de f (relative aux h_i). D'après cette définition, on a, dans l'anneau $\mathcal{E}$

$$(3) \qquad \Delta^n_{h_1 h_2 \ldots h_n} = \prod_{i=1}^{n} (T_{h_i} - I)$$

d'où, en développant par la formule de distributivité, et tenant compte de (1)

(4) $$\Delta^n_{h_1 h_2 \ldots h_n} = \sum_H (-1)^{n-\varphi(H)} T_{s(H)}$$

où H parcourt l'ensemble des 2^n parties distinctes de l'ensemble $[1,n]$, et où, pour tout H, $\varphi(H)$ désigne le nombre d'éléments de H, et on a posé $s(H) = \sum_{i \in H} h_i$.

On pose $\Delta^n_{h_1 h_2 \ldots h_n} f(x) = \Delta^n f(x;h_1,h_2,\ldots,h_n)$. La formule (4) s'écrit donc aussi

(5) $$\Delta^n f(x;h_1,h_2,\ldots,h_n) = \sum_H (-1)^{n-\varphi(H)} f(x + \sum_{i \in H} h_i)$$

D'autre part, de la relation $T_h = I + \Delta_h$, on tire, d'après (1)

(6) $$T_{h_1+h_2+\ldots+h_n} = \prod_{i=1}^{n} (I + \Delta_{h_i}) = \sum_{p=0}^{n} \Big(\sum_{i_1 < i_2 < \cdots < i_p} \Delta^p_{i_1 i_2 \ldots i_p} \Big)$$

ce qui s'écrit aussi

(7) $$f(x+h_1+h_2+\ldots+h_n) = \sum_{p=0}^{n} \Big(\sum_{i_1 < i_2 < \cdots < i_p} \Delta^p f(x;h_{i_1},h_{i_2},\ldots,h_{i_p}) \Big)$$

Les formules (5) et (7) sont souvent utiles lorsqu'on donne à tous les h_i une même valeur h ; on pose alors $\Delta^n f(x;h;h,\ldots,h) = \Delta^n f(x;h)$ pour simplifier. Comme le nombre de parties distinctes de p éléments de l'ensemble $[1,n]$ est égal à $\binom{n}{p}$, il vient

(8) $$\Delta^n f(x;h) = \sum_{p=0}^{n} (-1)^{n-p} \binom{n}{p} f(x+ph)$$

(9) $$f(x+nh) = \sum_{p=0}^{n} \binom{n}{p} \Delta^p f(x;h) \quad .$$

2. <u>Différences d'une fonction polynome</u>. Soient E et F deux espaces vectoriels par rapport à un corps commutatif <u>infini</u> K. Si f est une application polynome de E dans F, l'application $(x,h) \to f(x+h)$ est une application polynome de $E \times E$ dans F, comme composée de deux applications polynomes ; en outre, si f est de degré p, $(x,h) \to f(x+h)$ est aussi de degré p. Il en résulte que l'application $h \to f(x+h)$ est une applicatio polynome, de degré $\leq p$ si f est de degré p ; en outre, la partie homogène de degré 0 de cette application n'est autre que f(x).

Par suite, $h \longrightarrow \Delta f(x;h) = f(x+h)-f(x)$ est une application polynome de degré minimum au moins égal à 1 , et de degré $\leqslant p$ si f est de degré p.

On en déduit la proposition suivante :

Proposition 1. Si f est une application polynome de E dans F , l'application $(h_1,h_2,\ldots,h_r) \longrightarrow \Delta^r f(x;h_1,h_2,\ldots,h_r)$ est une application polynome de E^r dans F , de degré minimum $\geqslant 1$ par rapport à chacun des h_i (si elle n'est pas identiquement nulle) ; son degré est $\leqslant p$ si f est de degré p .

La proposition étant vraie pour r=1 , démontrons-la par récurrence sur r ; par hypothèse, on peut écrire $\Delta^{r-1} f(x;h_1,\ldots,h_{r-1}) = \sum \varphi_{\nu_1\nu_2\ldots\nu_{r-1}}(x,h_1,h_2,\ldots,h_{r-1})$, où $\varphi_{\nu_1\nu_2\ldots\nu_{r-1}}$ est une application polynome de E^r dans F , homogène et de degré ν_i en h_i ($1 \leqslant i \leqslant r-1$) ; par hypothèse, on a $\nu_i \geqslant 1$ pour tout i . Cela étant, on a

$$\Delta^r f(x;h_1,h_2,\ldots,h_{r-1},h_r) = \sum (\varphi_{\nu_1\nu_2\ldots\nu_{r-1}}(x+h_r,h_1,\ldots,h_{r-1}) - \varphi_{\nu_1\nu_2\ldots\nu_{r-1}}(x,h_1,\ldots,h_{r-1})) .$$

Chacun des termes de cette somme est homogène de degré $\nu_i \geqslant 1$ par rapport à h_i pour $1 \leqslant i \leqslant r-1$, et en outre est de degré minimum $\geqslant 1$ en h_r (s'il n'est pas nul), d'où la proposition.

Corollaire. Si f est une application polynome de degré p de E dans F , $\Delta^{p+1} f(x;h_1,h_2,\ldots,h_{p+1})$ est identiquement nulle, et l'application $(h_1,\ldots,h_p) \longrightarrow \Delta^p f(x;h_1,\ldots,h_p)$ est une application p-linéaire symétrique de E^p dans F , indépendante de x .

En effet, si l'application $(x;h_1,\ldots,h_p) \longrightarrow \Delta^p f(x;h_1,\ldots,h_p)$ n'est pas identiquement nulle, c'est une application polynome de degré $\leqslant p$, et de degré minimum $\geqslant 1$ par rapport à chacun des h_i ($1 \leqslant i \leqslant p$) ; elle est donc nécessairement homogène et de degré 1 par rapport à chacun des h_i , et indépendante de x .

Remarque. Il se peut que f soit de degré p et que $\Delta^p f$ soit identiquement nulle. Par exemple, soit K un corps de caractéristique 2, f l'application polynome $\xi \to \xi^2$ de K dans lui-même on a $(\xi+\eta)^2 = \xi^2 + \eta^2$, donc $\Delta^2 f = 0$ (voir n°8).

3. Différentielle première d'une fonction polynome. Soit f une application polynome de E dans F ; on a vu que l'application polynome $h \to \Delta f(x;h)$ est de degré minimum $\geqslant 1$.

Définition 1. On appelle différentielle première de f au point x et on note $d_x f$ la partie homogène du premier degré de l'application $h \to \Delta f(x;h)$.

L'application $h \to d_x f(h)$ est donc une application linéaire de E dans F ; on pose aussi $d_x f(h) = df(x;h)$.

Exemples. Si f est une application linéaire de E dans F, on a, pour pour tout $x \in E$, $df(x;h) = \Delta f(x;h) = f(h)$.

En particulier, l'application identique de E dans lui-même est sa propre différentielle, ce qui conduit souvent à noter dx la variable h dans la différentielle $df(x;h)$ d'un polynome.

Si f est une application p-linéaire de $E = \prod_{i=1}^{p} E_i$ dans F, on a, pour tout $x=(x_1,\dots,x_p) \in E$, et $h=(h_1,\dots,h_p)$

$$df(x;h) = \sum_{i=1}^{p} f(x_1,\dots,x_{i-1},h_i,x_{i+1},\dots,x_p)$$

Proposition 2. Soient f et g deux applications polynomes de E dans F, λ un scalaire quelconque ; on a $d_x(f+g) = d_x f + d_x g$ et $d_x(\lambda f) = \lambda d_x f$.

La proposition est immédiate à partir des définitions.

Théorème 1. (théorème des fonctions composées). Soient f une application polynome de E dans F, g une application polynome de F dans G ; si on pose $\varphi = g \circ f$, on a

$$d\varphi(x;h) = dg(f(x);df(x;h)) \tag{10}$$

en effet, on a $g(f(x+h))-g(f(x))=g(f(x)+\Delta f(x;h))-g(f(x)) =$

$= dg(f(x)\,;\,df(x;h))+dg(f(x);u_1(x,h))+u_2(f(x),\Delta f(x;h))$

où $u_1(x,h)=\Delta f(x;h)-df(x;h)$ est une fonction polynome de degré minimum $\geqslant 2$ par rapport à h, et $u_2(y,k)=\Delta g(y;k)-dg(y;k)$ une fonction polynome de degré $\geqslant 2$ par rapport à k ; comme $dg(f(x);k)$ est linéaire en k, $dg(f(x);u_1(x,h))$ a un degré minimum $\geqslant 2$ par rapport à h, et il en est de même de $u_2(f(x),\Delta f(x;h))$ puisque $\Delta f(x;h)$ a un degré minimum $\geqslant 1$. Le théorème est donc démontré.

Corollaire 1. Soient E,F,G trois espaces vectoriels sur K, u une application linéaire de E dans F, f une application polynome de F dans G ; si on pose $g=f\circ u$, on a $dg(x;h)=df(u(x);u(h))$.

Corollaire 2. Soit (E_i) une famille de p espaces vectoriels, f_i une application polynome d'un espace vectoriel E dans E_i $(1\leqslant i\leqslant p)$ u une application p-linéaire de $\prod_{i=1}^{p} E_i$ dans F ; si on pose $g(x)=u(f_1(x),\ldots,f_p(x))$, on a

(10 bis) $dg(x;h)=\sum_{i=1}^{p} u(f_1(x),..,f_{i-1}(x),df_i(x;h),f_{i+1}(x),\ldots,f_p(x)$

Plus particulièrement :

Corollaire 3. Soit E une algèbre sur K, (f_i) une suite de p application polynomes de E dans K ; si on pose $g(x)=f_1(x)f_2(x)\ldots f_p(x)$, on a

$$dg(x;h)=\sum_{i=1}^{p} f_1(x)..f_{i-1}(x).df_i(x;h).f_{i+1}(x)\ldots f_p(x)$$

4. Différentielles d'ordre supérieur. Pour tout h fixe, l'application $x\longrightarrow df(x;h)$ est une application polynome ; si on la désigne par φ_h, l'application $(h,k)\longrightarrow d\varphi_h(x;k)$ est appelée différentielle seconde de f, et on pose $d^2f(x;h,k)=d\varphi_h(x;k)$. Pour tout couple (h,k) fixe, l'application $x\longrightarrow d^2f(x;h,k)$ est de nouveau une application polynome; par récurrence, on peut donc poser la définition suivante :

Définition 2. On appelle différentielle $n^{ème}$ de f au point x, l'application $(h_1,h_2,\dots,h_n) \to d\varphi_{h_1h_2\dots h_{n-1}}(x;h_n)$, qu'on note $(h_1,h_2,\dots,h_n) \to d^nf(x;h_1,h_2,\dots,h_n)$; dans cette définition, $\varphi_{h_1h_2\dots h_{n-1}}$ est l'application polynome $x \to d^{n-1}f(x;h_1,h_2,\dots,h_{n-1})$.

Théorème 2. La différentielle $n^{ème}$ est une application multilinéaire symétrique de E^n dans F, identique à la partie homogène de degré n de l'application $(h_1,h_2,\dots,h_n) \to \Delta^n f(x;h_1,h_2,\dots,h_n)$.

Il suffit de démontrer la seconde partie de l'énoncé, puisque $\Delta^n f(x;h_1,..,h_n)$ est symétrique par rapport aux h_i, et a un degré minimum $\geqslant 1$ par rapport à chacun d'eux. Raisonnons par récurrence ; par hypothèse, on a $\Delta^{n-1}f(x;h_1,..,h_{n-1}) = d^{n-1}f(x;h_1,\dots,h_{n-1}) + \sum \varphi_{\partial_1\partial_2\dots\partial_{n-1}}(x,h_1,..,h_{n-1})$, où $\varphi_{\partial_1\partial_2\dots\partial_{n-1}}$ est une application polynome de E^n dans F, homogène et de degré ∂_i en h_i pour $1 \leqslant i \leqslant n-1$, et telle que $\partial_i \geqslant 1$ pour tout i et $\sum_{i=1}^{n-1} \partial_i \geqslant n$. Cela étant on a

$$\Delta^n f(x;h_1,..,h_{n-1},h_n) = \sum (\varphi_{\partial_1\partial_2\dots\partial_{n-1}}(x+h_n,h_1,\dots,h_{n-1}) - \varphi_{\partial_1\partial_2\dots\partial_{n-1}}(x,h_1,\dots,h_{n-1})) + (d^{n-1}f(x+h_n;h_1,..,h_{n-1}) - d^{n-1}f(x;h_1,\dots,h_{n-1}))$$

D'après l'hypothèse et les déf.1 et 2, $d^nf(x;h_1,h_2,..,h_n)$ est la partie homogène de degré n de l'application

$$(h_1,\dots,h_n) \to d^{n-1}f(x+h_n;h_1,..,h_{n-1}) - d^{n-1}f(x;h_1,\dots,h_{n-1})$$

d'autre part (prop.1) chacune des différences

$$\varphi_{\partial_1\partial_2\dots\partial_{n-1}}(x+h_n,h_1,..,h_{n-1}) - \varphi_{\partial_1\partial_2\dots\partial_{n-1}}(x,h_1,..,h_{n-1})$$

est de degré minimum $\geqslant 1$ par rapport à h_n, homogène et de degré ∂_i par rapport à h_i pour $1 \leqslant i \leqslant n-1$, donc son degré minimum par rapport à $(h_1,..,h_n)$ est $\geqslant 1 + \sum_{i=1}^{n-1} \partial_i \geqslant n+1$, ce qui démontre le théorème.

Corollaire. Si f est une application polynome de degré p de E dans F, $d^{p+1}f(x;h_1,\dots,h_{p+1})$ est identiquement nulle, et on a $d^pf(x;h_1,\dots,h_p) = \Delta^p f(x;h_1,\dots,h_p)$.

L'application p-linéaire $(h_1,\dots,h_p) \to d^p f(x;h_1,\dots,h_p)$ est encore appelée l'application polaire (ou polarisée) de f ; on dit "forme polaire" lorsque f est une forme homogène de degré p .

La différentielle $n^{ème}$ de f au point x se note encore $d^n_x f$.

Proposition 3. Soient f et g deux applications polynomes de E dans F , λ un scalaire quelconque ; on a $d^n_x(f+g)=d^n_x g$ et $d^n_x(\lambda f)=\lambda d^n_x f$.

La proposition est une conséquence immédiate du th.2 .

La différentielle $n^{ème}$ $d^n_x f$ est un élément de l'espace vectoriel $\mathscr{L}_n(E,F)$ des applications n-linéaires de E^n dans F , et $x \to d^n_x f$ est une application polynome de E dans $\mathscr{L}_n(E,F)$; si $h \to \psi_{x;h}$ est la différentielle première de cette application polynome, on a, pour tout $(h_i)\in E^n$, $\psi_{x;h}(h_1,..,h_n)=d^{n+1}f(x;h,h_1,\dots,h_n)$; cela résulte immédiatement de la déf.2 et du fait que, si $x \to g_x$ est une application polynome de E dans $\mathscr{L}_n(E,F)$, et $x \to g^{(k)}_x$ la partie homogène de degré k de cette application, $g^{(k)}_x(h_1,\dots,h_n)$ est la partie homogène de degré k de l'application polynome $x \to g_x(h_1,..,h_n)$ de E dans F .

5. Différentielles partielles. Supposons que E soit somme directe de p sous-espaces E_i $(1 \leqslant i \leqslant p)$. Soit f une application polynome de E dans F, et considérons sa différentielle $n^{ème}$ $(h_1,\dots,h_n) \to d^n f(x;h_1,..,h_n)$ en un point x . Pour tout indice i tel que 1 i n , on peut écrire $h_i = \sum_{j=1}^{p} h_{ij}$, où $h_{ij}\in E_j$ est le composant (uniquement déterminé) de h_i dans E_j ; comme la différentielle $n^{ème}$ est multilinéaire, on a donc

$$(11)\qquad d^n f(x;h_1,..,h_n)= \sum_{(j_k)} d^n f(x;h_{1,j_1},h_{2,j_2},\dots,h_{n,j_n})$$

la somme étant étendue à toutes les suites (j_k) de n indices appartenant à $\left[1,p\right]$. L'application de $E_{j_1}\times E_{j_2}\times\dots\times E_{j_n}$ dans F^n

$$(h_{1,j_1},h_{2,j_2},\dots,h_{n,j_n}) \to d^n f(x;h_{1,j_1},h_{2,j_2},\dots,h_{n,j_n})$$

est appelée la <u>différentielle partielle</u> de f, d'indices $(j_1,\dots,j_n)$ au point x ; on la note encore

$$(h_1,j_1,h_2,j_2,\dots,h_n,j_n) \to d^n_{j_1j_2\cdots j_n} f(x;h_1,j_1,\dots,h_n,j_n)$$

ou encore $d^n_{x;j_1j_2\cdots j_n} f$. Avec cette notation, (11) s'écrit

$$(12)\quad d^n f(x;h_1,h_2,\dots,h_n) = \sum_{(j_k)} d^n_{j_1j_2\cdots j_n} f(x;h_1,j_1,\dots,h_n,j_n)$$

Les différentielles partielles de f peuvent se définir par récurrence ; si on fixe $h_1,j_1,\dots,h_{n-1},j_{n-1}$ et qu'on pose, pour $y_{j_n}\in E_{j_n}$,

$$\varphi(y_{j_n}) = d^{n-1}_{j_1j_2\cdots j_{n-1}} f(x+y_{j_n};h_1,j_1,\dots,h_{n-1},j_{n-1})$$

φ est une application polynome de E_{j_n} dans F, et on a

$$d\varphi(0;h_n,j_n) = d^n_{j_1j_2\cdots j_n} f(x;h_1,j_1,\dots h_n,j_n)$$

En effet, si pour $y\in E$, on pose $\Psi(y)=d^{n-1}f(x+y;h_1,j_1,\dots,h_{n-1},j_{n-1})$ φ est la restriction de Ψ à E_{j_n}, donc sa différentielle au point 0 est la restriction à E_{j_n} de la différentielle de Ψ en ce point, d'où la proposition, d'après la définition de d^nf et des différentielles partielles.

<u>Proposition 4</u>. <u>Pour toute permutation σ du groupe $\mathfrak{S}_n$, on a</u>

$$(13)\quad d^n_{j_{\sigma(1)}\cdots j_{\sigma(n)}} f(x;h_{\sigma(1)},j_{\sigma(1)},\dots,h_{\sigma(n)},j_{\sigma(n)}) = d^n_{j_1j_2\cdots j_n} f(x;h_1,j_1,\dots,h_n,j_n)$$

En effet, comme d^nf est une fonction multilinéaire symétrique, on a, pour $h_k,j_k\in E_{j_k}$ $(1\leqslant k\leqslant n)$

$$d^n f(x;h_{\sigma(1)},j_{\sigma(1)},\dots,h_{\sigma(n)},j_{\sigma(n)}) = d^n f(x;h_1,j_1,\dots,h_n,j_n)$$

ce qui n'est autre que (13).

6. Différentielles condensées. La différentielle $n^{ème}$ en un point x d'une d'une application polynome f de E dans F est une application de E^n dans F , et non de E dans F . Mais on obtient une application de E dans F en considérant l'application $h \to d^n f(x;h,h,\dots,h)$ où les h_i sont tous remplacés par un même argument $h \in E$. Cette application de E dans F est appelée la différentielle $n^{ème}$ condensée de f au point x ; c'est évidemment une application polynome homogène de degré n de E dans F ; quand aucune confusion n'est à craindre, on la note encore $d_x^n f$, ou simplement $d^n f$, et on note sa valeur pour $h \in E$ par $d^n f(x;h)$. D'après la définition de la différentielle $n^{ème}$, si pour un h fixe dans E , on pose $\varphi(x)=d^{n-1}f(x;h)$, on a $d^n f(x;h) = d\varphi(x;h)$. Par récurrence sur m , on en déduit que, si on pose $\psi(x)=d^n f(x;h)$, on a $d^m \psi(x;h)=d^{m+n}f(x;h)$.

Supposons maintenant que E soit somme directe de p sous-espaces vectoriels E_i $(1 \leqslant i \leqslant p)$; si $h = \sum_{j=1}^{p} h_j$, où $h_j \in E_j$, on appelle différentielle partielle condensée d'indices $(j_1,\dots,j_n)$ de f, l'application $h \to d^n_{j_1 j_2 \dots j_n} f(x;h_{j_1},h_{j_2},\dots,h_{j_n})$ de E dans F . Il résulte de la prop.4 que, pour toute permutation $\sigma \in \mathfrak{S}_n$, la différentielle partielle condensée d'indices $(j_{\sigma(1)},j_{\sigma(2)},\dots,j_{\sigma(n)})$ est identique à celle d'indices $(j_1,\dots,j_n)$; on peut donc se borner à considérer celles dont les suites d'indices sont croissantes ;si r_k est le nombre des termes d'une telle suite égaux à k (pour $1 \leqslant k \leqslant p$), cette différentielle se note encore $h \to d_1^{r_1} d_2^{r_2} \dots d_p^{r_p} f(x;h)$ (en supprimant éventuellement ceux des $d_k^{r_k}$ pour lesquels $r_k=0$), ou (si $x=x_1+x_2+\dots+x_p$), avec $x_k \in E_k$), $d_{x_1}^{r_1} \dots d_{x_p}^{r_p} f$. Si on pose $\varphi(x)= d_1^{r_1} \dots d_p^{r_p} f(x;h)$, on a $d_k \varphi(x;h) = d_1^{r_1} \dots d_k^{r_k+1} \dots d_p^{r_p} f(x;h)$, d'où, par récurrence

$d_1^{s_1} d_2^{s_2} \cdots d_p^{s_p} \varphi(x;h) = d_1^{r_1+s_1} d_2^{r_2+s_2} \cdots d_p^{r_p+s_p} f(x;h)$

En raison de ces propriétés, si $\Phi = \sum_{(r_k)} a_{r_1 r_2 \cdots r_p} e_1^{r_1} \cdots e_p^{r_p}$ est un polynome quelconque à p indéterminées, on désigne par $(d_{x_1}, d_{x_2}, \ldots, d_{x_p})f$ l'application $h \to \sum_{(r_k)} a_{r_1 r_2 \cdots r_p} d_1^{r_1} \cdots d_p^{r_p} f(x;h)$, et on note sa valeur $\Phi(d_1, d_2, \ldots, d_p)f(x;h)$. Si Φ et Ψ sont deux polynomes à p indéterminées et $\Theta = \Phi\Psi$, on a, en posant

$g(x) = \Psi(d_1, d_2, \ldots d_p)f(x;h)$, $\Phi(d_1, \ldots, d_p)g(x;h) = \Theta(d_1, \ldots, d_p)f(x;h)$

Avec cette notation, il est immédiat, par récurrence sur n , que la différentielle $n^{\text{ème}}$ condensée de f s'exprime à l'aide des différentielles partielles condensées par la formule

(14) $$d_x^n f = (d_{x_1} + d_{x_2} + \ldots + d_{x_p})^n f \ .$$

7. Dérivées et dérivées partielles des fonctions polynomes. Soit f une application polynome de degré n de K dans un espace vectoriel F sur K ; sa différentielle $d_\xi f$ est une application linéaire de K dans F , donc de la forme $\lambda \to \varphi(\xi)\lambda$, où φ est une fonction scalaire de ξ ; d'ailleurs comme $\xi \to df(\xi;h)$ est une application polynome de degré $\leqslant n-1$ de K dans F , φ est une fonction polynome d'une variable de degré $\leqslant n-1$. Cette fonction est appelée dérivée première de f , et notée f' ou Df ; en raison de la relation $df(\xi;d\xi) = f'(\xi)d\xi$, on écrit aussi $Df = \frac{d}{d\xi} f$.

La prop. 2 et le th.1 donnent, dans ce cas particulier :

Proposition 5. Si f et g sont deux fonctions polynomes d'une variable, à valeurs dans un même espace vectoriel F , et λ un scalaire quelconque , on a $D(f+g) = Df + Dg$, $D(\lambda f) = \lambda Df$.

Autrement dit, l'application $f \to Df$ est une application linéaire de l'espace vectoriel $P(K,F)$ des applications polynomes de K dans F , dans lui-même.

Proposition 6. Soit φ une fonction polynome d'une variable, à valeurs dans E, et f une application polynome de E dans F ; si on pose $g=f\circ\varphi$, on a

$$g'(\xi)=df(\varphi(\xi);\varphi'(\xi)) \tag{15}$$

En particulier :

Corollaire. Si f et g sont deux fonctions polynomes d'une variable, à valeurs dans K, on a

$$D(g\circ f) = (Dg\circ f).Df$$

Le cor.2 du th.1, appliqué à l'application bilinéaire $(\lambda,x)\longrightarrow\lambda x$ de $K\times E$ dans E, donne en particulier :

Proposition 7. Soit φ une fonction polynome d'une variable à valeurs dans K, f une fonction polynome d'une variable à valeurs dans E, on a

$$D(\varphi f) = \varphi Df+(D\varphi)f \tag{16}$$

De même, d'après le cor.3 du th.1 :

Proposition 8. Soient f_i $(1\leqslant i\leqslant p)$ p fonctions polynomes d'une variable, à valeurs dans une algèbre E sur K ; on a

$$D(f_1f_2..f_p) = \sum_{i=1}^{p} f_1..f_{i-1}.Df_i.f_{i+1}..f_p \tag{17}$$

En particulier :

Corollaire. Si f est une fonction polynome d'une variable, à valeurs dans une algèbre commutative E sur K, on a

$$D(f^p) = p.f^{p-1}.Df \tag{18}$$

Cette dernière formule, appliquée à l'application identique de K sur lui-même, donne

$$D(\xi^p) = p\,\xi^{p-1} \tag{19}$$

Par suite, si $f(\xi) = \sum_{k=0}^{n} a_k \xi^k$ est une fonction polynome d'une variable à valeurs dans E, de degré n, on déduit de la formule (19) et des prop.5 et 7 que

$$f'(\xi) = \sum k a_k \xi^{k-1} . \tag{20}$$

La dérivée d'une fonction polynome f de degré n (c'est-à-dire telle que $a_n \neq 0$) est donc de degré n-1 , sauf si $na_n = 0$.

Application : identité d'Euler. Soit f une application polynome homogène de degré m d'un espace vectoriel E dans un espace vectoriel F . On a identiquement $f(\lambda x) = \lambda^m f(x)$ pour tout $\lambda \in K$. Dérivons cette identité en λ (x étant fixe, mais quelconque, dans E) ; d'après la prop.6 et la formule (20), la dérivée de la fonction polynome $\lambda \longrightarrow f(\lambda x)$ est $df(\lambda x; x)$; on a donc identiquement $df(\lambda x; x) = m\lambda^{m-1} f(x)$; d'où, en faisant $\lambda = 1$ dans cette identité en λ et x , l'identité d'Euler

(21) $$df(x;x) = mf(x) .$$

La dérivée première d'une fonction polynome d'une variable f (à valeurs dans F) étant définie, on définit par récurrence la dérivée $p^{ème}$ de f comme la dérivée première de la dérivée $(p-1)^{ème}$ de f ; c'est encore une fonction polynome d'une variable à valeurs dans F , qu'on note $f^{(p)}$ ou $D^p f$; cette dernière notation se justifie en remarquant que D est un endomorphisme de l'espace vectoriel $P(E,F)$, et $f \to D^p f$ est précisément la puissance $p^{ème}$ de cet endomorphisme dans l'anneau $\mathcal{L}(P(E,F))$ des endomorphismes de $P(E,F)$; on a donc identiquement $D^p(f+g) = D^p f + D^p g$, $D^p(\lambda f) = \lambda D^p f$ et

(22) $$D^p(D^q f) = D^{p+q} f$$

On voit immédiatement par récurrence qu'on a $d^p f(\xi ; \lambda_1, .., \lambda_p) = f^{(p)}(\xi)\lambda_1\lambda_2 .. \lambda_p$, d'où, par la différentielle condensée, $d^p f(\xi ; d\xi) = f^{(p)}(\xi)(d\xi)^p$; en raison de cette relation, on écrit aussi $D^p f = \frac{d^p}{d\xi^p} f$.

Si $f(\xi) = \sum_{k=0}^{m} a_k \xi^k$ est une fonction polynome de degré n , à valeurs dans F , on déduit par récurrence de (20) que, pour $p \leqslant n$, on a

(23) $$r^{(p)}(\xi) = \sum_{k=p}^{n} k(k-1)..(k-p+1)a_k \xi^{k-p}$$

et pour $p > n$, $f^{(p)}(\xi) = 0$.

Soit maintenant f une fonction polynome de n variables, à valeurs dans un espace vectoriel F ; comme $d_x f$ est une application linéaire de K^n dans F , on peut écrire

$$df(\xi_1,..,\xi_n;\lambda_1,\lambda_2,..\lambda_n) = \varphi_1(\xi_1,..,\xi_n)\lambda_1 + \varphi_2(\xi_1,..,\xi_n)\lambda_2 + .. \varphi_n(\xi_1,..,\xi_n)\lambda^n$$

où φ_i est une fonction polynome de n variables, à valeurs dans F , pour chaque indice i . Cette fonction est appelée <u>dérivée partielle du premier ordre et d'indice i de f</u> (ou dérivée partielle du premier ordre <u>par rapport à</u> ξ_i) et notée $D_i f$, ou (quand aucune confusion n'en peut résulter) $\frac{\partial f}{\partial \xi_i}$. La différentielle partielle d'indice i de f , restriction de df au sous-espace facteur d'indice i de K^n , est donc $\lambda_i \to D_i f(\xi_1,..,\xi_n)\lambda_i$; par suite $D_i f(\xi_1,..,\xi_n)$ est la valeur pour ξ_i de la dérivée première de la fonction polynome d'une variable $\xi \to f(\xi_1,...,\xi_{i-1},\xi,\xi_{i+1},..,\xi_n)$.

De même, la différentielle partielle d'indices $(j_1,..,j_p)$ de f est de la forme $(\lambda_{1,j},\lambda_{2,j_2},..,\lambda_{p,j_p}) \to \varphi(\xi_1,..,\xi_n)\lambda_{1,j_1}..\lambda_{p,j_p}$; φ est une fonction polynome à valeurs dans F , qu'on appelle <u>dérivée partielle d'ordre</u> p , <u>d'indices</u> $j_1,..,j_p$ <u>de</u> f , et qu'on note $D^p_{j_1 j_2..j_p} f$, ou $\frac{\partial^p f}{\partial \xi_{j_1} \partial \xi_{j_2} .... \partial \xi_{j_p}}$. D'après la définition par récurrence des différentielles partielles, on a $D^p_{j_1 j_2..j_p} f = D_{j_p}(D^{p-1}_{j_1..j_{p-1}} f)$ En d'autres termes, $D^p_{j_1 j_2..j_p}$ est un endomorphisme de l'espace vectoriel $P(K^n,F)$ des fonctions polynomes de n variables à valeurs dans F, et dans l'anneau $\mathcal{L}(P(K^n,F))$ de ces endomorphismes, on peut écrire $D^p_{j_1 j_2..j_p} = D_{j_p} D_{j_{p-1}}..D_{j_1}$. D'après la prop.4, pour toute permutation $\sigma \in \mathfrak{S}_p$, on a $D^p_{j_{\sigma(1)} j_{\sigma(2)}..j_{\sigma(p)}} = D^p_{j_1 j_2..j_p}$; autrement dit,

dans l'anneau $\mathscr{L}(P(K^n,F))$ les n endomorphismes D_i $(1\leqslant i\leqslant n)$ sont permutables ; si, dans la suite $(j_1,\dots,j_p)$, r_k est le nombre de termes égaux à k (pour $1\leqslant k\leqslant n$), on a

$D^p_{j_1 j_2 \dots j_p} = D_1^{r_1} D_2^{r_2} \dots D_n^{r_n}$ $(\sum_{k=1}^{n} r_k = p)$; en raison de cette relation, la dérivée partielle $D^p_{j_1 j_2 \dots j_p} f$ se note aussi $\dfrac{\partial^p f}{\partial \xi_1^{r_1} \partial \xi_2^{r_2} \dots \partial \xi_n^{r_n}}$.

Les D_i étant permutables, à tout polynome $\Phi = \sum_{(r_k)} a_{r_1 r_2 \dots r_n} e_1^{r_1} \dots e_n^{r_n}$ à n indéterminées, à coefficients dans K, correspond l'élément $\Phi(D_1,D_2,\dots,D_n)$ de l'anneau $\mathscr{L}(P(K^n,F))$ (§2,n°1) ; ces éléments sont dits opérateurs polynomes de dérivation sur les fonctions polynomes de n variables, à valeurs dans F. Avec cette notation, on voit aussitôt par récurrence que la différentielle $p^{\text{ème}}$ condensée de f n'est autre que l'application

$$(\lambda_1,\lambda_2,\dots,\lambda_n) \longrightarrow (\lambda_1 D_1 + \lambda_2 D_2 + \dots + \lambda_n D_n)^p f(\xi_1,\dots,\xi_n) .$$

3. La formule de Taylor. Etant donné une fonction polynome d'une variable de degré n $\varphi(\xi) = \sum_{k=0}^{n} a_k \xi^k$, la formule (23) donne en particulier

$$\varphi^{(p)}(0) = p!\,a_p \qquad (0\leqslant p\leqslant n) \tag{24}$$

Nous allons en déduire la proposition suivante :

Proposition 9. Soit f une application polynome de degré n d'un espace vectoriel E dans un espace vectoriel F. Si f_p est la partie homogène de f de degré p de f, on a identiquement

$$p!f_p(x) = d^p f(0;x) \qquad (0\leqslant p\leqslant n) \tag{25}$$

En effet, considérons (pour un $x\in E$ fixe, mais arbitraire), la fonction polynome d'une variable $\varphi(\lambda) = f(\lambda x) = \sum_{p=0}^{n} f_p(x)\lambda^p$; d'après la formule (24), on a $\varphi^{(p)}(0) = p!f_p(x)$; d'autre part, par récurrence sur p, on voit, à l'aide de la définition de la différentielle condensée et de la prop.6, que $\varphi^{(p)}(\lambda) = d^p f(\lambda x;x)$, d'où en faisant $\lambda = 0$ la formule (25).

De (25) on déduit que, si la division par p! est possible dans K (c'est-à-dire si $p!e \neq 0$, e étant l'élément unité de K) , on a $f_p(x) = \frac{1}{p!} d^p f(0;x)$. En particulier :

Proposition 10. Si la division par p! est possible dans K , toute application polynome f , homogène et de degré p , d'un espace vectoriel E sur K , dans un espace vectoriel F sur K , s'obtient en identifiant les p variables dans une application p-linéaire symétrique bien déterminée de E^p dans F (savoir, l'application polarisée de $\frac{1}{p!} f$).

Si g est l'application polarisée de $\frac{1}{p!} f$, on a donc $f(x)=g(x,x,..x)$ si on remplace x par $\lambda_1 x_1 + \lambda_2 x_2 + .. + \lambda_p x_p$, on voit donc, d'après la formule de distributivité, que $g(x_1,x_2,..,x_p)$ peut être définie comme le produit par $\frac{1}{p!}$ du coefficient de $\lambda_1 \lambda_2 .. \lambda_p$ dans l'application polynome $(\lambda_1,..,\lambda_p) \to f(\lambda_1 x_1 + ... + \lambda_p x_p)$.

Z L'exemple donné au n°2 montre que si la division par p! n'est pas possible dans K , la prop.10 est inexacte.

Théorème 3. Soit f une application polynome de degré n de E dans F . Si la division par n! est possible dans K , on a, pour tout élément $a \in E$, l'identité (formule de Taylor en a)

$$(26) \qquad f(a+x) = \sum_{p=0}^{n} \frac{1}{p!} d^p f(a;x)$$

En effet, si on pose $g(x)=f(a+x)$, on a $d^p g(0;x)=d^p f(a;x)$, d'où le théorème en vertu de la prop.9 .

En particulier, pour une fonction polynome de m variables, à valeurs dans un espace vectoriel F, et de degré n, la formule (26) devient, compte tenu de l'expression de la différentielle $p^{ème}$ condensée de f ,

$$(27) \qquad f(a_1+\xi_1,..,a_m+\xi_m) = \sum_{p=0}^{n} \frac{1}{p!} (\xi_1 D_1 + \xi_2 D_2 + ... + \xi_m D_m)^p f(a_1,...,a_m)$$

9. Dérivées des polynomes. La théorie développée dans ce paragraphe repose sur la possibilité de définir des parties homogènes d'une application polynome de E dans F , lorsque E et F sont des espaces vectoriels sur un corps infini K . Or, on peut donner des définitions analogues dans d'autres circonstances, d'où la possibilité de développer alors des théories analogues aux précédentes.

De façon précise, soit A un anneau commutatif quelconque, ayant un élément unité, E l'algèbre $A[e_1,e_2,..,e_n]$ des polynomes à n indéterminées sur A (§ 1). Nous avons déjà remarqué (§ 2,n°4) que, si une fonction polynome de $p \leqslant n$ variables

$$(u_1,\dots,u_p) \longrightarrow \sum \alpha_{\nu_1 \nu_2 \dots \nu_p} u_1^{\nu_1} u_2^{\nu_2} \dots u_p^{\nu_p}$$

définie dans E^p et à valeurs dans E , a ses coefficients $\alpha_{\nu_1 \nu_2 \dots \nu_p}$ dans A , ces coefficients sont déterminés de façon unique, ce qui permet de définir sans ambiguité le degré de chacun des termes de cette fonction par rapport à chacun des u_i ou son degré total, et par suite les parties homogènes de cette fonction polynome.

Soit alors f un polynome à n indéterminées sur A , E l'algèbre $A[e_1,e_2,..,e_{2n}]$ des polynomes à 2n indéterminées sur A ; l'application

(28) $(x_1,\dots,x_n,h_1,\dots,h_n) \longrightarrow f(x_1+h_1,x_2+h_2,\dots,x_n+h_n)$

de E^{2n} dans E est du type que nous venons de considérer ; on peut donc définir encore la différentielle première au point $x=(x_i) \in E^n$ de l'application $(x_1,..,x_n) \longrightarrow f(x_1,..,x_n)$ de E^n dans E , comme étant l'application qui, au point $h=(h_i) \in E^n$, fait correspondre la somme des termes de degré 1 par rapport à l'ensemble des h_i dans l'application (28) ; on peut encore la noter dxf , et noter sa valeur $df(x;h)$. On peut alors refaire sans modification tous les raisonnements qui précèdent, en remplaçant partout la différentielle définie au n°3 par celle que nous venons de définir ; nous laissons au lecteur le soin de faire cette vérification.

Cela étant, la différentielle première du polynome f, qu'on note df, est le polynome (élément de $A[e_1,..,e_{2n}]$) obtenu en remplaçant, dans $df(x;h)$, x par $(e_1,e_2,..,e_n)$, h par $(e_{n+1},...,e_{2n})$. Définitions analogues pour les différentielles partielles et dérivées partielles de f.

Nous nous bornerons seulement à écrire explicitement la dérivée d'un polynome f à une indéterminée

$$f = a_0 + a_1 e + ... + a_n e^n$$

c'est le polynome

$$Df = a_1 + 2a_2 e + ... + n\, a_n e^{n-1}$$

Avec cette définition, il résulte de la prop.5 (étendue comme nous venons de l'expliquer) que D est une application linéaire de $A[e]$ dans lui-même ; si f_i $(1 \leqslant i \leqslant p)$ sont p polynomes de $A[e]$, la formule (17) subsiste sans modification. D^p est la puissance $p^{ème}$ de l'endomorphisme D de $A[e]$, dans l'anneau des endomorphismes de ce module, et $D^p f$ est appelé la dérivée $p^{ème}$ de f ; on a donc

$$D^p f = \sum_{k=p}^{n} k(k-1)..(k-p+1)a_k e^{k-p}$$

pour $p \leqslant n$, et $D^p f = 0$ pour $p > n$. Si, dans A, la division par $n!$ est possible, on a en outre la formule de Taylor

$$f(e_1+e_2) = \sum_{p=0}^{n} \frac{1}{p!} D^p f(e_1) e_2^p \qquad (29)$$

Enfin, si B est une algèbre sur A telle que l'application $f \to \tilde{f}$ de $A[e]$ sur l'anneau $P_1(B)$ des fonctions polynomes d'une variable dans B, à coefficients dans A, soit un isomorphisme, on peut définir la dérivée de la fonction polynome f comme la fonction polynome correspondant au polynome Df par cet isomorphisme. Lorsque $A=B$ est un corps infini, la fonction ainsi définie coïncide avec la dérivée définie au n°7.

Par contre, on ne pourra en général définir de façon cohérente la dérivée d'une fonction polynome de $P_1(B)$ lorsque $f \to \tilde{f}$ n'est pas un isomorphisme. Il se peut en effet alors que, si on pose $f_1=Df$, on ait $\tilde{f}=0$, mais $\tilde{f}_1 \neq 0$. Par exemple, si K est un corps fini de q éléments, le groupe additif de K est d'ordre q, son groupe multiplicatif d'ordre q-1 , donc on a $q\xi=0$ pour tout $\xi \in K$, $\xi^{q-1}=1$ pour tout $\xi \neq 0$, et par suite $\xi^q = \xi$ ~~pour tout ξ^q~~ pour tout $\xi \in K$. Si $f=e^q-e$, on a $f_1=Df=qe^{q-1}-1$, donc $\tilde{f}=0$ et $\tilde{f}_1(\xi)=-1$ pour tout $\xi \in K$.

10. Application : caractérisation des racines multiples d'un polynome. Dans ce qui suit, A est un anneau commutatif quelconque, ayant un élément unité.

Proposition 11. Si $a \in A$ est racine simple du polynome $f \in A[e]$, a n'est pas racine de Df .

En effet, on a par hypothèse $f=(e-a)g$, où g n'est pas divisible par e-a ; en dérivant (formule (17)) cette relation, il vient $Df=g+(e-a)Dg$; si Df était divisible par e-a , il en serait de même de g , contrairement à l'hypothèse.

Plus généralement :

Proposition 12. Si $a \in A$ est racine d'ordre k de f , a est racine d'ordre $\geqslant k-1$ de Df ; a est racine d'ordre k-1 de Df si la division par k est possible dans A .

En effet, on a $f=(e-a)^k g$, où g n'est pas divisible par e-a ; on en tire $Df=k(e-a)^{k-1}g+(e-a)^k Dg$, d'où la première partie de la proposition. Si la division par k est possible, on a $(e-a)^{k-1}g=\frac{1}{k}(Df-(e-a)^k Dg)$; si Df était divisible par $(e-a)^k$, il en serait de même de $(e-a)^{k-1}g$; comme dans $A[e]$, e-a n'est pas un diviseur de 0 , on en conclurait que g est divisible par e-a , contrairement à l'hypothèse.

Si la division par k n'est pas possible dans A , peut être racine d'ordre quelconque $h \geqslant k$ de Df ; il suffit pour le voir de considérer le cas où A est de caractéristique k , et où on prend $g=(e-a)^{h-k+1}+g$, avec $g \neq 0$, $h-k+1$ n'étant pas supposé multiple de k .

Corollaire. Si a A est racine de f , et racine d'ordre p de Df , et si la division par p! est possible dans A , a est racine d'ordre p+1 de f .

En effet, d'après la prop.12, a est racine de f d'ordre k tel que $1 \leqslant k \leqslant p+1$; si on avait $k < p+1$, comme la division par k est possible par hypothèse , a serait racine d'ordre $k-1 < p$ de Df, contrairement à l'hypothèse.

Proposition 13. Si, dans A , la division par p! est possible, pour que $a \in A$ soit racine d'ordre p de f , il faut et il suffit que a soit racine de $f, Df, D^2f, \ldots, D^{p-1}f$, et ne soit pas racine de D^pf.

La condition est nécessaire, car en vertu de la prop.12 appliquée par récurrence, a est racine d'ordre p-k de D^kf pour $1 \leqslant k \leqslant p-1$ et d'après la prop.11, a n'est pas racine de D^pf . La condition est suffisante, en vertu du cor. de la prop.12, appliqué par récurrence.

D'après le cor. de la prop.12, la condition est déjà suffisante si la division par (p-1)! est possible dans A .

Exercices. 1) Soient E et F deux espaces vectoriels sur le corps $\mathbb{Q}$ des nombres rationnels. Montrer que si f est une application de E dans F telle que $\Delta^{n+1}f(x;h)$ soit identiquement nulle, f est une application polynome de degré $\leqslant n$ de E dans F (en utilisant la formule (9), montrer que $(m,n) \to f(mx+ny)$ est une application polynome de $\mathbb{Z}^2$ dans F , quels que soient x et y dans E ; utiliser ensuite l'exerc. 7 du § 2).

2) Soit $(a_i)_{1 \leqslant i \leqslant p}$ une suite de p éléments distincts d'un corps K. Montrer que tout polynome f, de degré $\leqslant p-1$ peut s'écrire d'une seule manière sous la forme

$$f = \lambda_0 + \lambda_1(e-a_1) + \lambda_2(e-a_1)(e-a_2) + \ldots + \lambda_k(e-a_1)\ldots(e-a_k) + \ldots + \lambda_{p-1}(e-a_1)\ldots(e-a_{p-1})$$

(formule d'interpolation de Newton) (déterminer les λ_i par récurrence). En particulier, si $a_i = i-1$ $(1 \leqslant i \leqslant p)$, montrer que $\lambda_0 = f(0)$, $\lambda_i = \frac{1}{i!}\Delta^i \tilde{f}(0;1)$ pour $i > 0$ si la division par $(p-1)!$ est possible dans K.

3) Soit K un corps de caractéristique 0 ; on pose, dans $K[e]$

$$\binom{e}{n} = \frac{1}{n!} e(e-1)(e-2)\ldots(e-n+1) \text{ pour } n > 0, \quad \binom{e}{0} = 1.$$

Démontrer l'identité

$$\binom{e_1+e_2+\ldots+e_p}{n} = \sum \binom{e_1}{\nu_1}\binom{e_2}{\nu_2}\ldots\binom{e_p}{\nu_p}$$

la somme étant étendue aux suites $(\nu_i)_{1 \leqslant i \leqslant p}$ telles que $\sum_i \nu_i = n$ (procéder par récurrence sur p, en utilisant la formule d'interpolation de Newton).

4) Soit K un corps de caractéristique 0, f une fonction polynome de degré $\leqslant p$ de $P_1(K)$. Montrer qu'il existe une fonction polynome g, de degré $\leqslant p+1$, telle que $\Delta g(x;1) = f(x)$ identiquement (formule d'interpolation de Newton). En déduire que si on pose $s_n = f(0)+f(1)+\ldots+f(n-1)$, on a

$$s_n = nf(0) + \binom{n}{2}\Delta f(0;1) + \ldots + \binom{n}{p}\Delta^{p-1} f(0;1) + \binom{n}{p+1}\Delta^p f(0;1).$$

Cas particuliers des fonctions polynomes x, x^2, x^3.

5) Soit $(a_i)_{1 \leqslant i \leqslant p}$ une suite de p éléments distincts d'un corps K. Montrer qu'il existe un polynome et un seul f de degré $\leqslant 2p-1$, tel que $\tilde{f}(a_i) = \beta_i$ et $\tilde{f}'(a_i) = \gamma_i$ pour $1 \leqslant i \leqslant p$, où les β_i et γ_i sont 2p éléments arbitraires de K (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). Généraliser au cas où on se donne, pour chacun des a_i, la valeur de $\tilde{f}$ et d'un certain nombre (dépendant de i) de ses dérivées.

6) Si f et g sont deux polynomes à une indéterminée, on a (formule de Leibniz)

$$D^n(fg)=D^nf.g+\binom{n}{1}D^{n-1}f.Dg+\binom{n}{2}D^{n-2}f.D^2g+\dots+$$
$$+\binom{n}{p}D^{n-p}f.D^pg+\dots+f.D^ng$$

7) Soit f une application polynome d'un espace vectoriel E dans un espace vectoriel F. On définit la différentielle condensée complète d'ordre n de f comme une application de E^{n+1} dans F, notée

$$(x,dx,d^2x,\dots,d^nx) \longrightarrow \overline{d}^nf(x,dx,\dots,d^nx)$$

et satisfaisant aux conditions suivantes : $\overline{d}f(x,dx)=df(x;dx)$, $\overline{d}^nf(x,dx,\dots,d^nx)$ est la valeur de la différentielle de l'application $\overline{d}^{n-1}f$ au point $(x,dx,\dots,d^{n-1}x)$ de E^n, pour la valeur $(dx,d^2x,\dots,d^nx)$ de la variable. Montrer que l'on a

$$\overline{d}^nf(x,dx,d^2x,\dots,d^nx)=\sum c_{a_1a_2\dots a_k}d^kf(x;d^{a_1}x,d^{a_2}x,\dots,d^{a_k}x)$$

la somme étant étendue aux suites (a_i) croissantes d'entiers tels que $\sum a_i=n$, et où $c_{a_1a_2\dots a_k}$ est un entier >0, et en particulier $c_{11\dots1}=c_{00\dots0n}=1$.

Si g est une application polynome de F dans un espace vectoriel G, et $h=g\circ f$, on a

$$\overline{d}^nh(x,dx,\dots,d^nx)=\overline{d}^ng(f(x),\overline{d}f(x,dx),\dots,\overline{d}^nf(x,dx,\dots,d^nx))$$

En déduire que

$$d^nh(x;dx)=\overline{d}^ng(f(x),df(x;dx),\dots,d^nf(x;dx)).$$