N. BOURBAKI

ÉLÉMENTS DE MATHÉMATIQUE

N. BOURBAKI

ÉLÉMENTS DE
MATHÉMATIQUE

ALGÈBRE

Chapitres 4 à 7

Springer

Réimpression inchangée de l'édition originale de 1981
© Masson, Paris, 1981

ISBN-10 3-540-34398-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34398-1 Springer Berlin Heidelberg New York

Springer est membre du Springer Science+Business Media
springer.com

Maquette de couverture: WMXDesign GmbH Heidelberg
Imprimé sur papier non acide SPIN 12062621 41/3180 – 5 4 3 2 1

Mode d'emploi de ce traité

NOUVELLE ÉDITION

1. Le traité prend les mathématiques à leur début, et donne des démonstrations complètes. Sa lecture ne suppose donc, en principe, aucune connaissance mathématique particulière, mais seulement une certaine habitude du raisonnement mathématique et un certain pouvoir d'abstraction. Néanmoins, le traité est destiné plus particulièrement à des lecteurs possédant au moins une bonne connaissance des matières enseignées dans la première ou les deux premières années de l'Université.

2. Le mode d'exposition suivi est axiomatique et procède le plus souvent du général au particulier. Les nécessités de la démonstration exigent que les chapitres se suivent, en principe, dans un ordre logique rigoureusement fixé. L'utilité de certaines considérations n'apparaîtra donc au lecteur qu'au cours de chapitres ultérieurs, à moins qu'il ne possède déjà des connaissances assez étendues.

3. Le traité est divisé en Livres et chaque Livre en chapitres. Les Livres actuellement publiés, en totalité ou en partie, sont les suivants :

Théorie des Ensembles	désigné par	E
Algèbre	—	A
Topologie générale	—	TG
Fonctions d'une variable réelle	—	FVR
Espaces vectoriels topologiques	—	EVT
Intégration	—	INT
Algèbre commutative	—	AC
Variétés différentielles et analytiques	—	VAR
Groupes et algèbres de Lie	—	LIE
Théories spectrales	—	TS

Dans les *six premiers* Livres (pour l'ordre indiqué ci-dessus), chaque énoncé ne fait appel qu'aux définitions et résultats exposés précédemment dans le chapitre

en cours ou dans les chapitres *antérieurs dans l'ordre suivant* : E ; A, chapitres I à III ; TG, chapitres I à III ; A, chapitres IV et suivants ; TG, chapitres IV et suivants ; FVR ; EVT ; INT. A partir du septième Livre, le lecteur trouvera éventuellement, au début de chaque Livre ou chapitre, l'indication précise des autres Livres ou chapitres utilisés (les six premiers Livres étant toujours supposés connus).

4. Cependant, quelques passages font exception aux règles précédentes. Ils sont placés entre deux astérisques : * ... *. Dans certains cas, il s'agit seulement de faciliter la compréhension du texte par des exemples qui se réfèrent à des faits que le lecteur peut déjà connaître par ailleurs. Parfois aussi, on utilise, non seulement les résultats supposés connus dans tout le chapitre en cours, mais des résultats démontrés ailleurs dans le traité. Ces passages seront employés librement dans les parties qui supposent connus les chapitres où ces passages sont insérés et les chapitres auxquels ces passages font appel. Le lecteur pourra, nous l'espérons, vérifier l'absence de tout cercle vicieux.

5. A certains Livres (soit publiés, soit en préparation) sont annexés des *fascicules de résultats*. Ces fascicules contiennent l'essentiel des définitions et des résultats du Livre, mais aucune démonstration.

6. L'armature logique de chaque chapitre est constituée par les *définitions*, les *axiomes* et les *théorèmes* de ce chapitre ; c'est là ce qu'il est principalement nécessaire de retenir en vue de ce qui doit suivre. Les résultats moins importants, ou qui peuvent être facilement retrouvés à partir des théorèmes, figurent sous le nom de « propositions », « lemmes », « corollaires », « remarques », etc. ; ceux qui peuvent être omis en première lecture sont imprimés en petits caractères. Sous le nom de « scholie », on trouvera quelquefois un commentaire d'un théorème particulièrement important.

Pour éviter des répétitions fastidieuses, on convient parfois d'introduire certaines notations ou certaines abréviations qui ne sont valables qu'à l'intérieur d'un seul chapitre ou d'un seul paragraphe (par exemple, dans un chapitre où tous les anneaux considérés sont commutatifs, on peut convenir que le mot « anneau » signifie toujours « anneau commutatif »). De telles conventions sont explicitement mentionnées à la tête du chapitre ou du paragraphe dans lequel elles s'appliquent.

7. Certains passages sont destinés à prémunir le lecteur contre des erreurs graves, où il risquerait de tomber ; ces passages sont signalés en marge par le signe  (« tournant dangereux »).

8. Les exercices sont destinés, d'une part, à permettre au lecteur de vérifier qu'il a bien assimilé le texte ; d'autre part à lui faire connaître des résultats qui n'avaient pas leur place dans le texte ; les plus difficiles sont marqués du signe ¶.

9. La terminologie suivie dans ce traité a fait l'objet d'une attention particulière. *On s'est efforcé de ne jamais s'écarter de la terminologie reçue sans de très sérieuses raisons.*

10. On a cherché à utiliser, sans sacrifier la simplicité de l'exposé, un langage rigoureusement correct. Autant qu'il a été possible, les *abus de langage ou de notation*, sans lesquels tout texte mathématique risque de devenir pédantesque et même illisible, ont été signalés au passage.

11. Le texte étant consacré à l'exposé dogmatique d'une théorie, on n'y trouvera qu'exceptionnellement des références bibliographiques ; celles-ci sont groupées dans des *Notes historiques*. La bibliographie qui suit chacune de ces Notes ne comporte le plus souvent que les livres et mémoires originaux qui ont eu le plus d'importance dans l'évolution de la théorie considérée ; elle ne vise nullement à être complète.

Quant aux exercices, il n'a pas été jugé utile en général d'indiquer leur provenance, qui est très diverse (mémoires originaux, ouvrages didactiques, recueils d'exercices).

12. Dans la nouvelle édition, les renvois à des théorèmes, axiomes, définitions, remarques, etc. sont donnés en principe en indiquant successivement le Livre (par l'abréviation qui lui correspond dans la liste donnée au n° 3), le chapitre et la page où ils se trouvent. A l'intérieur d'un même Livre la mention de ce Livre est supprimée ; par exemple, dans le Livre d'Algèbre,

E, III, p. 32, cor. 3

renvoie au corollaire 3 se trouvant au livre de Théorie des Ensembles, chapitre III, page 32 de ce chapitre ;

II, p. 24, prop. 17

renvoie à la proposition 17 du Livre d'Algèbre, chapitre II, page 24 de ce chapitre.

Les fascicules de résultats sont désignés par la lettre R ; par exemple : EVT, R signifie « fascicule de résultats du Livre sur les Espaces vectoriels topologiques ».

Comme certains Livres doivent seulement être publiés plus tard dans la nouvelle édition, les renvois à ces Livres se font en indiquant successivement le Livre, le chapitre, le paragraphe et le numéro où se trouve le résultat en question ; par exemple :

AC, III, § 4, n° 5, cor. de la prop. 6.

CHAPITRE IV

Polynômes et fractions rationnelles

Dans tout ce chapitre, A *désigne un anneau commutatif.*

§ 1. POLYNÔMES

1. Définition des polynômes

Soit I un ensemble. Rappelons (III, p. 25) que l'algèbre commutative libre de I sur A se note $A[(X_i)_{i\in I}]$ ou $A[X_i]_{i\in I}$. Les éléments de cette algèbre sont appelés *polynômes* par rapport aux indéterminées X_i (ou en les indéterminées X_i) à coefficients dans A. Rappelons que l'indéterminée X_i est l'image canonique de i dans l'algèbre commutative libre de I sur A ; il est parfois commode de désigner cette image par une autre notation, telle que X'_i, Y_i, T_i, etc. On annonce souvent cette convention par une phrase telle que : « Soit $\mathbf{Y} = (Y_i)_{i\in I}$ une famille d'indéterminées » ; lorsqu'il en est ainsi, on note $A[\mathbf{Y}]$ l'algèbre de polynômes considérée. Pour $I = \{1, 2, \ldots, n\}$, on écrit $A[X_1, X_2, \ldots, X_n]$ au lieu de $A[(X_i)_{i\in I}]$.

Pour $\nu \in \mathbf{N}^{(I)}$, posons

$$X^\nu = \prod_{i\in I} X_i^{\nu_i}.$$

Alors $(X^\nu)_{\nu\in\mathbf{N}^{(I)}}$ est une base du A-module $A[(X_i)_{i\in I}]$. Les X^ν s'appellent les *monômes* en les indéterminées X_i. Pour $\nu = 0$, on obtient l'élément unité de $A[(X_i)_{i\in I}]$. Tout polynôme $u \in A[(X_i)_{i\in I}]$ s'écrit d'une façon et d'une seule sous la forme

$$u = \sum_{\nu\in\mathbf{N}^{(I)}} \alpha_\nu X^\nu$$

avec $\alpha_\nu \in A$ et les α_ν nuls sauf pour un nombre fini d'indices ; les α_ν s'appellent les *coefficients* de u ; les $\alpha_\nu X^\nu$ s'appellent les *termes* de u (l'élément $\alpha_\nu X^\nu$ étant souvent appelé le terme en X^ν) ; en particulier le terme $\alpha_0 X^0$, identifié à α_0, s'appelle le *terme constant* de u. Lorsque $\alpha_\nu = 0$, on dit, par abus de langage, que u *ne contient pas de terme en* X^ν ; en particulier, quand $\alpha_0 = 0$, on dit que u est un polynôme *sans terme constant* (III, p. 26). On appelle *polynôme constant* tout multiple scalaire de 1.

Soient B un anneau commutatif, et $\rho : A \to B$ un homomorphisme d'anneaux. Considérons $B[(X_i)_{i\in I}]$ comme une A-algèbre grâce à ρ. Alors l'application σ de $A[(X_i)_{i\in I}]$ dans $B[(X_i)_{i\in I}]$ qui transforme $\sum \alpha_\nu X^\nu$ en $\sum \rho(\alpha_\nu)X^\nu$ est un homomorphisme de A-algèbres ; si $u \in A[(X_i)_{i\in I}]$, on note parfois ${}^\rho u$ l'image de u par cet homomorphisme. L'homomorphisme de $B \otimes_A A[(X_i)_{i\in I}]$ dans $B[(X_i)_{i\in I}]$ défini canoniquement par σ transforme, pour tout $i \in I$, $1 \otimes X_i$ en X_i ; c'est un isomorphisme de B-algèbres (III, p. 22).

Soit M un A-module libre de base $(e_i)_{i\in I}$. Il existe un homomorphisme unifère φ et un seul de l'algèbre symétrique $\mathbf{S}(M)$ dans l'algèbre $A[(X_i)_{i\in I}]$ tel que $\varphi(e_i) = X_i$ pour tout $i \in I$, et cet homomorphisme est un isomorphisme (III, p. 75). Cet isomorphisme est dit *canonique*. Cela permet d'appliquer aux algèbres de polynômes certaines propriétés des algèbres symétriques. Par exemple, soit $(I_\lambda)_{\lambda\in L}$ une partition de I. Soit φ_λ l'homomorphisme de $P_\lambda = A[(X_i)_{i\in I_\lambda}]$ dans $P = A[(X_i)_{i\in I}]$ qui transforme X_i (considéré comme élément de P_λ) en X_i (considéré comme élément de P). Alors les φ_λ définissent un homomorphisme de l'algèbre $\bigotimes_{\lambda\in L} P_\lambda$ dans l'algèbre P, et cet homomorphisme est un isomorphisme (III, p. 73, prop. 9).

Soit E un A-module. On pose $E \otimes_A A[(X_i)_{i\in I}] = E[(X_i)_{i\in I}]$. Les éléments du A-module $E[(X_i)_{i\in I}]$ s'appellent polynômes en les indéterminées X_i à coefficients dans E. Un tel polynôme s'écrit d'une façon et d'une seule $\sum_{\nu\in \mathbf{N}^{(I)}} e_\nu \otimes X^\nu$, où $e_\nu \in E$ et où les e_ν sont nuls sauf pour un nombre fini d'indices ; le plus souvent, on écrira $e_\nu X^\nu$ pour $e_\nu \otimes X^\nu$.

2. Degrés

Soit $P = A[(X_i)_{i\in I}]$ une algèbre de polynômes. Pour tout entier $n \in \mathbf{N}$, soit P_n le sous-module de P engendré par les monômes X^ν tels que $|\nu| = \sum_{i\in I} \nu_i$ soit égal à n. Alors $(P_n)_{n\in\mathbf{N}}$ est une graduation qui fait de $A[(X_i)_{i\in I}]$ une *algèbre graduée de type* N (III, p. 31). Les éléments homogènes de degré n de $A[(X_i)_{i\in I}]$ sont parfois appelés *formes de degré n* par rapport aux indéterminées X_i.

Lorsqu'il sera question de degré de polynômes non homogènes, nous conviendrons généralement d'adjoindre à l'ensemble N des entiers naturels un élément noté $-\infty$ et de prolonger à $\mathbf{N} \cup \{-\infty\}$ la relation d'ordre et l'addition de N par les conventions suivantes, où $n \in \mathbf{N}$,

$$-\infty < n\,, \quad (-\infty) + n = n + (-\infty) = -\infty\,, \quad (-\infty) + (-\infty) = -\infty\,.$$

Soit $u = \sum_{\nu\in\mathbf{N}^{(I)}} \alpha_\nu X^\nu$ un polynôme. La composante homogène u_n de degré n de u (pour la graduation de type N définie ci-dessus) est égale à $\sum_{|\nu|=n} \alpha_\nu X^\nu$, et l'on a évidemment $u = \sum_{n\in\mathbf{N}} u_n$. Lorsque $u \neq 0$, les u_n ne sont pas tous nuls, et l'on appelle

degré (ou *degré total*) de u, et l'on note $\deg u$, le plus grand des entiers n tels que $u_n \neq 0$; autrement dit (III, p. 26), le degré de u est le plus grand des entiers $|\nu|$ pour les multiindices ν tels que $\alpha_\nu \neq 0$. Lorsque $u = 0$, le degré de u est égal par convention à $-\infty$. Pour tout entier $p \in \mathbf{N}$, la relation $\deg u \leqslant p$ équivaut donc à « $\alpha_\nu = 0$ pour tout multiindice ν tel que $|\nu| > p$ » ; l'ensemble des polynômes u tels que $\deg u \leqslant p$ est donc un sous-A-module de $A[(X_i)_{i\in I}]$, égal à $P_0 + P_1 + \cdots + P_p$ avec les notations ci-dessus.

Soit E un A-module. La famille $(E \otimes P_n)_{n\in\mathbf{N}}$ est une graduation de type $\mathbf{N}$ du module $E[(X_i)_{i\in I}] = E \otimes_A A[(X_i)_{i\in I}]$ des polynômes à coefficients dans E. On étend à ce cas les conventions adoptées plus haut pour le degré des polynômes non homogènes.

PROPOSITION 1. — *Soient u et v deux polynômes.*

(i) *Si* $\deg u \neq \deg v$, *on a*

$$u + v \neq 0 \quad \textit{et} \quad \deg(u + v) = \sup(\deg u, \deg v) .$$

Si $\deg u = \deg v$, *on a* $\deg(u + v) \leqslant \deg u$.

(ii) *On a* $\deg(uv) \leqslant \deg u + \deg v$.

Les démonstrations sont immédiates.

Soient $J \subset I$ et $B = A[(X_i)_{i\in I-J}]$. Identifions $A[(X_i)_{i\in I}]$ à $B[(X_i)_{i\in J}]$ (III, p. 26). Le degré de $u \in A[(X_i)_{i\in I}]$, considéré comme élément de $B[(X_i)_{i\in J}]$, s'appelle le degré de u par rapport aux X_i d'indice $i \in J$ (III, p. 27).

Soit $u = \sum_{k=0}^{n} \alpha_k X_k \in A[X]$ un polynôme non nul en une indéterminée, de degré n. Le coefficient α_n, qui est par hypothèse $\neq 0$, s'appelle le *coefficient dominant* de u. Un polynôme $u \neq 0$ dont le coefficient dominant est égal à 1 s'appelle un *polynôme unitaire*.

Dans $A[X_1, X_2, \ldots, X_q]$, le nombre de monômes de degré total p est égal au nombre d'éléments $(n_k)_{1\leqslant k\leqslant q}$ de $\mathbf{N}^q$ tels que $\sum_{k=1}^{q} n_k = p$, c'est-à-dire à $\binom{q+p-1}{p}$ (E, III, p. 44, prop. 15).

Plus généralement, soient Δ un monoïde commutatif et $(\delta_i)_{i\in I}$ une famille d'éléments de Δ. Il existe une unique graduation de type Δ de l'algèbre $A[(X_i)_{i\in I}]$ telle que chaque monôme X^ν soit de degré $\sum_{i\in I} \nu_i \delta_i$ (III, p. 31, exemple 3). Le cas considéré ci-dessus est celui où $\Delta = \mathbf{N}$ et $\delta_i = 1$. Dans le cas général, pour éviter des confusions, nous utiliserons le mot « poids » au lieu de « degré », et le mot « isobare » au lieu de « homogène ». Par exemple, il existe une unique graduation de type $\mathbf{N}$ de l'algèbre $A[(X_i)_{i\geqslant 1}]$ telle que X_i soit de poids i pour tout entier $i \geqslant 1$. Les éléments isobares de poids n sont les polynômes de la forme $\sum_\nu a_\nu X^\nu$ avec $a_\nu = 0$ lorsque $\sum_{i\geqslant 1} i.\nu_i \neq n$.

3. Substitutions

Soient E une algèbre associative unifère sur A, $\mathbf{x} = (x_i)_{i\in I}$ une famille d'éléments de E deux à deux permutables. Soit $\mathbf{X} = (X_i)_{i\in I}$ une famille d'indéterminées. D'après III, p. 22, prop. 7, il existe un unique homomorphisme unifère f de A[**X**] dans E tel que $f(X_i) = x_i$ pour tout $i \in I$. L'image d'un élément u de A[**X**] par f se note $u(\mathbf{x})$ et s'appelle *l'élément de* E *déduit par substitution des* x_i *aux* X_i *dans* u, ou *la valeur de* u *pour les valeurs* x_i *des* X_i, ou encore *la valeur de* u *pour* $X_i = x_i$. En particulier, $u = u((X_i)_{i\in I})$. Si $I = \{1, \ldots, n\}$, on écrit $u(x_1, \ldots, x_n)$ au lieu de $u((x_i)_{i\in I})$. Plus généralement, si M est un A-module et si v est un élément de

$$M[(X_i)_{i\in I}] = M \otimes_A A[(X_i)_{i\in I}],$$

on note $v(\mathbf{x})$ l'image de v dans $M \otimes_A E = M_{(E)}$ par l'application $1_M \otimes f$.

Si l'homomorphisme $u \mapsto u(\mathbf{x})$ de A[**X**] dans E est injectif, on dit que la famille **x** est *algébriquement libre* sur A, ou que les x_i sont *algébriquement indépendants* sur A. Cela signifie aussi que les monômes $\mathbf{x}^\nu$ ($\nu \in \mathbf{N}^{(I)}$) sont linéairement indépendants sur A.

Si λ est un homomorphisme unifère de E dans une A-algèbre associative unifère E′, on a

$$\lambda(u((x_i)_{i\in I})) = u((\lambda(x_i)_{i\in I})), \tag{1}$$

car $\lambda \circ f$ est un homomorphisme de A[**X**] dans E′ qui transforme X_i en $\lambda(x_i)$.

Soit $u \in A[\mathbf{X}]$. Si E est commutative, l'application $\mathbf{x} \mapsto u(\mathbf{x})$ de E^I dans E s'appelle la *fonction polynomiale* définie par u (et l'algèbre E) ; on la note parfois $\tilde{u}$ (ou même simplement u).

Soit $\mathbf{Y} = (Y_j)_{j\in J}$ une autre famille d'indéterminées. Prenons pour E l'algèbre de polynômes A[**Y**]. Soit $u \in A[\mathbf{X}]$; pour $i \in I$, soit $g_i \in A[\mathbf{Y}]$ et posons $\mathbf{g} = (g_i)_{i\in I}$; soit $u(\mathbf{g}) \in A[\mathbf{Y}]$ le polynôme obtenu par substitution des polynômes g_i aux X_i dans le polynôme u. Soit $\mathbf{y} = (y_j)_{j\in J}$ une famille d'éléments deux à deux permutables d'une A-algèbre associative unifère E′ ; appliquons (1) en prenant pour λ l'homomorphisme $g \mapsto g(\mathbf{y})$ de E dans E′ ; on obtient :

$$(u(\mathbf{g}))(\mathbf{y}) = u((g_i(\mathbf{y}))). \tag{2}$$

Si $\mathbf{f} = (f_i)_{i\in I} \in (A[(X_j)_{j\in J}])^I$ et $\mathbf{g} = (g_j)_{j\in J} \in (A[(Y_k)_{k\in K}])^J$, on note $\mathbf{f} \circ \mathbf{g}$, ou $\mathbf{f}(\mathbf{g})$, la famille de polynômes $(f_i(\mathbf{g}))_{i\in I} \in (A[(Y_k)_{k\in K}])^I$. Si l'on désigne par $\tilde{\mathbf{f}}$ l'application $\mathbf{x} \mapsto (f_i(\mathbf{x}))_{i\in I}$ de E'^J dans E'^I (où E′ est une A-algèbre unifère associative et commutative), la relation (2) entraîne

$$(\mathbf{f} \circ \mathbf{g})^{\sim} = \tilde{\mathbf{f}} \circ \tilde{\mathbf{g}}. \tag{3}$$

Si $\mathbf{h} = (h_k)_{k\in K} \in (A[(Z_l)_{l\in L}])^K$, il résulte de (2) que :

$$\mathbf{f} \circ (\mathbf{g} \circ \mathbf{h}) = (\mathbf{f} \circ \mathbf{g}) \circ \mathbf{h}. \tag{4}$$

PROPOSITION 2. — *Soit* $\mathbf{a} = (a_i)_{i\in I}$ *une famille d'éléments de* A *et soit* $u \in A[\mathbf{X}]$. *Soit* v *le polynôme obtenu par substitution de* $X_i + a_i$ *à* X_i *pour tout* $i \in I$. *Le terme constant de* v *est égal à* $u(\mathbf{a})$.

Le terme constant de v est obtenu par la substitution de 0 à X_i dans v pour tout $i \in I$. La proposition résulte donc de la formule (2).

COROLLAIRE 1. — *Soit* $\mathfrak{m}$ *l'idéal des polynômes* $u \in A[\mathbf{X}]$ *tels que* $u(\mathbf{a}) = 0$. *Alors* $\mathfrak{m}$ *est engendré par les polynômes* $X_i - a_i$ *(pour* $i \in I$).

Il est clair qu'on a $X_i - a_i \in \mathfrak{m}$ pour tout $i \in I$. Soit $u \in \mathfrak{m}$ et soit v comme dans la proposition 2. Comme v est sans terme constant, il existe une famille à support fini $(P_i)_{i\in I}$ de polynômes dans $A[\mathbf{X}]$ telle que

$$v(\mathbf{X}) = \sum_{i\in I} X_i . P_i(\mathbf{X}) .$$

Substituons $X_i - a_i$ à X_i pour tout $i \in I$ dans l'égalité précédente ; on trouve alors une relation de la forme $u(\mathbf{X}) = \sum_{i\in I} (X_i - a_i).P'_i(\mathbf{X})$, d'où le corollaire.

COROLLAIRE 2. — *Soient* $\mathbf{X} = (X_i)_{i\in I}$ *et* $\mathbf{Y} = (Y_i)_{i\in I}$ *deux familles d'indéterminées. L'ensemble* $\mathfrak{b}$ *des polynômes* $u \in A[\mathbf{X}, \mathbf{Y}]$ *tels que* $u(\mathbf{X}, \mathbf{X}) = 0$ *est l'idéal de* $A[\mathbf{X}, \mathbf{Y}]$ *engendré par les polynômes* $X_i - Y_i$ *(pour* $i \in I$).

Ce corollaire résulte immédiatement du cor. 1 où l'on remplace A par $A[\mathbf{Y}]$ et a_i par Y_i, en interprétant $A[\mathbf{X}, \mathbf{Y}]$ comme l'anneau des polynômes en les X_i à coefficients dans $A[\mathbf{Y}]$.

PROPOSITION 3. — *Soient* $u \in A[\mathbf{X}]$ *et* $\mathbf{X}.\mathbf{Z}$ *la famille* $(X_i Z)_{i\in I}$ *d'éléments de l'anneau de polynômes* $A[\mathbf{X}][Z]$. *Le coefficient de* Z^k *dans* $u(\mathbf{X}.\mathbf{Z})$ *est la composante homogène de degré* k *de* u, *pour tout entier positif* k.

Il suffit de démontrer la prop. lorsque u est un monôme, auquel cas c'est immédiat.

COROLLAIRE. — *Pour qu'un polynôme* $u \in A[\mathbf{X}]$ *soit homogène de degré* k, *il faut et il suffit que l'on ait* :

$$u(\mathbf{X}.Z) = u(\mathbf{X}).Z^k .$$

Remarque. — Soit $\mathbf{x} \in A^I$. Soit f l'application $u \mapsto u(\mathbf{x})$ de $A[\mathbf{X}]$ dans A. Soit M un A-module. Considérons l'homomorphisme $1 \otimes f$ de $M[\mathbf{X}] = M \otimes_A A[\mathbf{X}]$ dans $M \otimes_A A = M$. Pour tout $v \in M[\mathbf{X}]$, on a $(1 \otimes f)(v) = v(\mathbf{x})$. Si $v = \sum_{\nu\in\mathbf{N}^{(I)}} e_\nu X^\nu$, on a $v(\mathbf{x}) = \sum_{\nu\in\mathbf{N}^{(I)}} \mathbf{x}^\nu e_\nu$.

4. Différentielles et dérivations

Soit $B = A[(X_i)_{i\in I}]$. D'après III, p. 134, il existe, pour tout $i \in I$, une A-dérivation D_i de B et une seule telle que

$$D_iX_i = 1\ ,\quad D_iX_j = 0 \quad \text{pour } j \neq i\ . \tag{5}$$

Le polynôme D_iP s'appelle *la dérivée partielle de* P *par rapport à* X_i ; on le note aussi $D_{X_i}P$, ou $\frac{\partial P}{\partial X_i}$, ou P'_{X_i}. D'après III, p. 123, formule (21), on a, si $\nu = (\nu_j) \in \mathbf{N}^{(I)}$,

$$D_i(X^\nu) = \begin{cases} \nu_i X_i^{\nu_i - 1} \prod_{j\in I-\{i\}} X_j^{\nu_j} & \text{si } \nu_i > 0 \\ 0 & \text{si } \nu_i = 0\ . \end{cases} \tag{6}$$

On déduit de (6) que $D_iD_j = D_jD_i$ quels que soient $i, j \in I$. Pour $\nu = (\nu_i)_{i\in I} \in \mathbf{N}^{(I)}$, on pose $D^\nu = \prod_{i\in I} D_i^{\nu_i}$ et $\nu! = \prod_{i\in I} (\nu_i!)$. Munissons $\mathbf{N}^{(I)}$ de l'ordre produit. On a

$$D^\nu(X^\mu) = \begin{cases} \frac{\mu!}{(\mu-\nu)!} X^{\mu-\nu} & \text{si } \nu \leqslant \mu\ , \\ 0 & \text{sinon}\ . \end{cases}$$

Lorsque P est un polynôme en une seule indéterminée X, l'unique dérivée partielle de P se note DP ou $\frac{dP}{dX}$ ou P', et s'appelle simplement la *dérivée* de P.

Soit à nouveau $B = A[(X_i)_{i\in I}]$. D'après III, p. 134, le B-module $\Omega_A(B)$ des A-différentielles de B admet pour base la famille $(dX_i)_{i\in I}$ des différentielles des X_i. Soit ∂_i la forme coordonnée d'indice i relativement à cette base sur $\Omega_A(B)$. Alors l'application $u \mapsto \langle\, \partial_i, du \,\rangle$ de B dans B est une dérivation de B qui transforme X_i en 1 et X_j en 0 pour $j \neq i$, donc est D_i ; autrement dit, on a

$$du = \sum_{i\in I} (D_iu)\, dX_i \tag{7}$$

pour tout $u \in B$. Si I est fini, $(D_i)_{i\in I}$ est une base du B-module des dérivations de B.

PROPOSITION 4. — *Soient* E *une* A*-algèbre associative, commutative et unifère,* $\mathbf{x} = (x_i)_{i\in I}$ *une famille d'éléments de* E, *u un élément de* $A[(X_i)_{i\in I}]$, *et* $y = u(\mathbf{x})$. *Pour toute dérivation* D *de* E *dans un* E*-module, on a*

$$Dy = \sum_{i\in I} (D_iu)(\mathbf{x}).Dx_i\ .$$

Il suffit de prouver la proposition quand u est un monôme, et elle résulte alors de (6) et de III, p. 123, prop. 6.

COROLLAIRE. — *Soient* $f \in A[X_1, ..., X_p]$ *et* $g_i \in A[Y_1, ..., Y_q]$ *pour* $1 \leqslant i \leqslant p$. *Posons* $h = f(g_1, ..., g_p)$. *Alors, pour* $1 \leqslant j \leqslant q$, *on a*

$$\frac{\partial h}{\partial Y_j} = \sum_{i=1}^{p} D_i f(g_1, ..., g_p) \cdot \frac{\partial g_i}{\partial Y_j}. \tag{8}$$

C'est le cas particulier $E = A[Y_1, ..., Y_q]$, $x_i = g_i$ et $D = \partial/\partial Y_j$ de la prop. 4.

Soient $\mathbf{X} = (X_i)_{i \in I}$, $\mathbf{Y} = (Y_i)_{i \in I}$ deux familles disjointes d'indéterminées. Notons $\mathbf{X} + \mathbf{Y}$ la famille $(X_i + Y_i)_{i \in I}$. Soit $u \in A[\mathbf{X}]$. Considérons l'élément $u(\mathbf{X} + \mathbf{Y})$ de $A[\mathbf{X}, \mathbf{Y}]$. Pour $\nu \in \mathbf{N}^{(I)}$, on note $\Delta^\nu u$ le coefficient de $\mathbf{Y}^\nu$ dans $u(\mathbf{X} + \mathbf{Y})$, considéré comme polynôme en les Y_i à coefficients dans $A[\mathbf{X}]$. On a par définition $\Delta^\nu u \in A[\mathbf{X}]$ et

$$u(\mathbf{X} + \mathbf{Y}) = \sum_{\nu} (\Delta^\nu u)(\mathbf{X})\, \mathbf{Y}^\nu . \tag{9}$$

(Ici et dans la suite de ce numéro, les sommations portent sur l'ensemble d'indices $\mathbf{N}^{(I)}$, sauf mention du contraire.)

Soit $\mathbf{a} \in A^I$. En substituant $\mathbf{a}$ à $\mathbf{X}$ et $\mathbf{X} - \mathbf{a}$ à $\mathbf{Y}$ dans (9), on obtient

$$u(\mathbf{X}) = \sum_{\nu} (\Delta^\nu u)(\mathbf{a})\, (\mathbf{X} - \mathbf{a})^\nu . \tag{10}$$

En particulier, on a

$$u(\mathbf{X}) = \sum_{\nu} (\Delta^\nu u)(0)\, \mathbf{X}^\nu . \tag{11}$$

Si u, $v \in A[\mathbf{X}]$, on a

$$\begin{aligned}(uv)(\mathbf{X} + \mathbf{Y}) &= \Big(\sum_{\nu} (\Delta^\nu u)(\mathbf{X})\, \mathbf{Y}^\nu\Big)\Big(\sum_{\rho} (\Delta^\rho v)(\mathbf{X})\, \mathbf{Y}^\rho\Big) \\ &= \sum_{\sigma} \Big[\sum_{\nu+\rho=\sigma} (\Delta^\nu u)(\mathbf{X})\, (\Delta^\rho v)(\mathbf{X})\Big]\, \mathbf{Y}^\sigma\end{aligned}$$

donc

$$\Delta^\sigma(uv) = \sum_{\nu+\rho=\sigma} (\Delta^\nu u)(\Delta^\rho v) . \tag{12}$$

Soit $\mathbf{Z} = (Z_i)_{i \in I}$ une autre famille d'indéterminées. On a :

$$\begin{aligned}\sum_{\nu} (\Delta^\nu u)(\mathbf{X})\, (\mathbf{Y} + \mathbf{Z})^\nu &= u(\mathbf{X} + \mathbf{Y} + \mathbf{Z}) \\ &= \sum_{\sigma} (\Delta^\sigma u)(\mathbf{X} + \mathbf{Y})\, \mathbf{Z}^\sigma \\ &= \sum_{\rho,\sigma} (\Delta^\rho \Delta^\sigma u)(\mathbf{X})\, \mathbf{Y}^\rho \mathbf{Z}^\sigma ,\end{aligned}$$

donc, d'après I, p. 94, corollaire 2 :

$$\Delta^\rho \Delta^\sigma u = \frac{(\rho + \sigma)!}{\rho!\, \sigma!}\, \Delta^{\rho+\sigma} u . \tag{13}$$

PROPOSITION 5. — *Quels que soient* $u \in A[X]$ *et* $\nu \in \mathbf{N}^{(I)}$, *on a*

$$D^\nu u = \nu! \Delta^\nu u .$$

Supposons d'abord que ν soit de longueur 1 ; il existe alors un élément i de I tel que $\nu = \varepsilon_i$, c'est-à-dire $\nu_i = 1$ et $\nu_j = 0$ pour tout $j \neq i$ dans I. La formule (12) montre que Δ^{ε_i} est une dérivation de la A-algèbre A[X], qui annule évidemment X_j pour $j \neq i$ et prend la valeur 1 sur X_i. On a donc $\Delta^{\varepsilon_i} = D_i$ pour tout $i \in I$.

D'après la formule (13), on a

$$(\rho! \Delta^\rho).(\sigma! \Delta^\sigma) = (\rho + \sigma)! \Delta^{\rho+\sigma} \tag{14}$$

dans l'algèbre des endomorphismes du A-module A[X]. On en déduit $\nu! \Delta^\nu = D^\nu$ par récurrence sur la longueur de ν.

Si A est une **Q**-algèbre, les formules (9), (10), (11) peuvent donc s'écrire

$$u(\mathbf{X} + \mathbf{Y}) = \sum_\nu \frac{1}{\nu!} (D^\nu u)(\mathbf{X}) \mathbf{Y}^\nu \tag{15}$$

$$u(\mathbf{X}) = \sum_\nu \frac{1}{\nu!} (D^\nu u)(\mathbf{a}) (\mathbf{X} - \mathbf{a})^\nu \tag{16}$$

$$u(\mathbf{X}) = \sum_\nu \frac{1}{\nu!} (D^\nu u)(0) \mathbf{X}^\nu . \tag{17}$$

Les formules (15), (16), (17) s'appellent toutes trois « *formule de Taylor* ».

PROPOSITION 6 (« identité d'Euler »). — *Soit* $u \in A[X]$ *un polynôme homogène de degré* r. *On a*

$$\sum_{i \in I} X_i . D_i u = ru .$$

Soit D l'application A-linéaire de A[X] dans lui-même telle que $D(v) = sv$ quand v est homogène de degré s. On sait (III, p. 119, exemple 6) que D est une dérivation de A[X]. La prop. 6 est donc un corollaire de la prop. 4 (IV, p. 6).

5. Diviseurs de zéro dans un anneau de polynômes

PROPOSITION 7. — *Soient* $f \in A[X]$ *un polynôme non nul en une indéterminée,* α *son coefficient dominant. Si* α *est simplifiable dans* A (*en particulier si* f *est unitaire*), *on a, pour tout élément non nul* g *de* A[X],

$$fg \neq 0 \quad et \quad \deg(fg) = \deg f + \deg g .$$

Soient $g \in A[X]$ un polynôme non nul, β son coefficient dominant, $n = \deg f$, $p = \deg g$. Alors le coefficient de X^{n+p} dans fg est $\alpha\beta$ donc est non nul, d'où la proposition.

PROPOSITION 8. — *Si* A *est intègre,* $A[(X_i)_{i\in I}]$ *est intègre.*

Soient u, v deux éléments non nuls de $A[(X_i)_{i\in I}]$. Il s'agit de prouver la relation $uv \neq 0$. Or u et v appartiennent à un même anneau $A[(X_j)_{j\in J}]$ où J est une partie finie de I. On peut donc se borner au cas où I est fini et égal à $\{ 1, 2, \ldots, p \}$. D'autre part, l'anneau $A[X_1, \ldots, X_p]$ est isomorphe à l'anneau des polynômes en X_p à coefficients dans $A[X_1, \ldots, X_{p-1}]$. Par récurrence sur p, on est donc ramené à démontrer la proposition pour A[X], et il suffit alors d'appliquer la proposition 7.

COROLLAIRE 1. — *Si* A *est intègre, et si* u, v *sont des éléments de* $A[(X_i)_{i\in I}]$, *on a* $\deg(uv) = \deg u + \deg v$.

On peut se limiter au cas où u et v sont non nuls. Soient $m = \deg u$, $n = \deg v$. On a

$$u = u_0 + u_1 + \cdots + u_m, \quad v = v_0 + v_1 + \cdots + v_n$$

où u_h (resp. v_h) est la composante homogène de degré h de u (resp. v). Comme $u_m \neq 0$ et $v_n \neq 0$, on a $u_m v_n \neq 0$ (prop. 8). Or $uv = u_m v_n + w$ avec $\deg w < m + n$, d'où le corollaire.

COROLLAIRE 2. — *Si* A *est intègre, les éléments inversibles de* $A[(X_i)_{i\in I}]$ *sont les éléments inversibles de* A.

Cela résulte aussitôt du cor. 1.

PROPOSITION 9. — *Soit* $u \in A[(X_i)_{i\in I}]$. *Pour que* u *soit nilpotent dans l'anneau* $A[(X_i)_{i\in I}]$, *il faut et il suffit que tous ses coefficients soient nilpotents dans l'anneau* A.

Comme dans la démonstration de la prop. 8, on se ramène au cas des polynômes en une variable X. Si tous les coefficients de u sont nilpotents, u est nilpotent (I, p. 95, cor. 3). Supposons u nilpotent non nul, et soit n son degré. Nous raisonnerons par récurrence sur n. Soit α le coefficient dominant de u. Il existe un entier $m > 0$ tel que $u^m = 0$. Le coefficient dominant de u^m est α^m, donc $\alpha^m = 0$. Alors $u - \alpha X^n$ est nilpotent (I, *loc. cit.*), et l'hypothèse de récurrence prouve que tous les coefficients de $u - \alpha X^n$ sont nilpotents. Ainsi, tous les coefficients de u sont nilpotents.

Remarque. — Soient u et v des éléments de $A[(X_i)_{i\in I}]$. On suppose que A est intègre, que v est multiple non nul de u, et que v est homogène. Alors u est homogène. En effet, soit $u' \in A[(X_i)_{i\in I}]$ tel que $v = uu'$; on a $u \neq 0$, $u' \neq 0$; soient

$$u = u_h + u_{h+1} + \cdots + u_k$$
$$u' = u'_{h'} + u'_{h'+1} + \cdots + u'_{k'}$$

les décompositions de u et u' en composantes homogènes, avec $u_h \neq 0$, $u_k \neq 0$, $u'_{h'} \neq 0$, $u'_{k'} \neq 0$. Alors $v = u_h u'_{h'} + u_h u'_{h'+1} + \cdots + u_k u'_{k'}$ et $u_h u'_{h'}$ est homogène non nul de degré $h + h'$, $u_k u'_{k'}$ est homogène non nul de degré $k + k'$ (prop. 8). Comme v est homogène, on a $h + h' = k + k'$, d'où $h = k$, $h' = k'$.

6. Division euclidienne des polynômes à une indéterminée

PROPOSITION 10. — *Soient f et g des éléments non nuls de* A[X] *de degrés respectifs m et n. Soient α_0 le coefficient dominant de f, et $\mu = \sup(n - m + 1, 0)$. Il existe $u, v \in A[X]$ tels que*

$$\alpha_0^\mu g = uf + v\,, \quad \deg v < m\,.$$

Si α_0 est simplifiable dans A, *u et v sont déterminés de manière unique par ces propriétés.*

L'existence de u et v est évidente quand $n < m$ puisqu'on peut alors prendre $u = 0$ et $v = g$. Pour $n \geqslant m$, démontrons-la par récurrence sur n. Soit β le coefficient dominant de g. Si $f = \sum_{k=0}^{m} \alpha_k X^{m-k}$, on peut écrire $\alpha_0^\mu g = \alpha_0^{\mu-1}\beta X^{n-m} f + \alpha_0^{\mu-1} g_1$, où $g_1 \in A[X]$ et $\deg g_1 < n$. D'après l'hypothèse de récurrence, il existe $u_1, v \in A[X]$ tels que $\alpha_0^{\mu-1} g_1 = u_1 f + v$ et $\deg v < m$. Donc

$$\alpha_0^\mu g = (\alpha_0^{\mu-1}\beta X^{n-m} + u_1) f + v$$

et il suffit de poser $u = \alpha_0^{\mu-1}\beta X^{n-m} + u_1$.

Supposons que α_0 soit simplifiable dans A, et prouvons l'unicité de u et v. Soient u, v, u_1, $v_1 \in A[X]$ tels que

$$\alpha_0^\mu g = uf + v = u_1 f + v_1\,, \quad \deg v < m\,, \quad \deg v_1 < m\,.$$

On a $(u - u_1) f = v_1 - v$ et $\deg(v_1 - v) < m$, donc $u - u_1 = 0$ (IV, p. 8, prop. 7) et par suite $v_1 - v = 0$.

COROLLAIRE (« *division euclidienne des polynômes* »). — *Soient f un élément non nul de* A[X] *dont le coefficient dominant est inversible, et $m = \deg f$.*

(i) *Pour tout $g \in A[X]$, il existe $u, v \in A[X]$ tels que*

$$g = uf + v\,, \quad \deg v < m\,.$$

En outre, ces conditions déterminent u et v de manière unique.

(ii) *Les sous-*A*-modules* $A + AX + \cdots + AX^{m-1}$ *et* $fA[X]$ *de* A[X] *sont supplémentaires dans* A[X].

(iii) *Supposons f non constant et considérons* A[X] *comme un* A[T]*-module au moyen de l'homomorphisme $u(T) \mapsto u(f(X))$ de* A[T] *dans* A[X]. *Alors* A[X] *est un* A[T]*-module libre de base* $(1, X, \ldots, X^{m-1})$.

Les assertions (i) et (ii) sont des conséquences immédiates de la prop. 10.

Prouvons (iii). Soit ψ l'homomorphisme $v \mapsto v(f(X), X)$ de A[T, X] dans A[X]. Considérons d'abord A[T, X] comme l'anneau des polynômes en T à coefficients dans A[X] ; le cor. 1 de IV, p. 5, montre que le noyau $\mathfrak{a}$ de ψ est l'idéal $(T - f(X))$ de A[T, X]. Considérons maintenant A[T, X] comme l'anneau des polynômes

en X à coefficients dans A[T] ; alors ψ est une application A[T]-linéaire de A[T] [X] dans A[X]. L'assertion (ii) ci-dessus (appliquée au polynôme $f(X) - T$ en X à coefficients dans A[T]) montre que $(1, X, \ldots, X^{m-1})$ est une base d'un A[T]-sous-module de A[T, X] supplémentaire de $\mathfrak{a}$. Comme on a $\psi(X^i) = X^i$ pour tout entier $i \geqslant 0$, on en déduit aussitôt (iii).

Avec les notations de (i), on dit que u est le *quotient* et v le *reste* de la *division euclidienne* de g par f ; pour que le reste soit nul, il faut et il suffit que f divise g.

7. Divisibilité des polynômes à une indéterminée [1]

PROPOSITION 11. — *Soit* K *un corps commutatif.*

(i) *Pour tout idéal non nul* $\mathfrak{a}$ *de* K[X], *il existe un polynôme unitaire* f *dans* K[X], *et un seul, tel que* $\mathfrak{a} = (f)$.

(ii) *Soient* f_1 *et* f_2 *dans* K[X]. *Pour que* $(f_1) = (f_2)$, *il faut et il suffit qu'il existe un élément non nul* λ *de* K *tel que* $f_2 = \lambda f_1$.

Prouvons (ii), la suffisance de la condition énoncée étant claire. Le cas où f_1 et f_2 engendrent l'idéal nul est trivial. Supposons donc que les polynômes non nuls f_1 et f_2 engendrent le même idéal de K[X]. Il existe donc des polynômes u_1 et u_2 tels que $f_1 = u_1 f_2$ et $f_2 = u_2 f_1$; on en déduit $u_1 u_2 = 1$, d'où $\deg u_1 + \deg u_2 = 0$, et par suite $\deg u_2 = 0$. On a donc prouvé que u_2 est un élément non nul de K.

Prouvons (i). Soit dans $\mathfrak{a}$ un polynôme unitaire f de degré le plus petit possible. Étant donné g dans $\mathfrak{a}$, soient u et v le quotient et le reste de la division euclidienne de g par f ; alors $v = g - uf$ appartient à $\mathfrak{a}$ et l'on a $\deg v < \deg f$; si v était non nul, il existerait un élément non nul λ de K tel que λv soit unitaire, et comme λv appartiendrait à $\mathfrak{a}$, ceci contredirait la définition de f. On a donc $\mathfrak{a} = (f)$. L'unicité d'un polynôme unitaire f tel que $\mathfrak{a} = (f)$ résulte de (ii).

PROPOSITION 12. — *Soient* K *un corps commutatif et* f, g *deux éléments de* K[X]. *Pour tout polynôme* d *dans* K[X], *les propriétés suivantes sont équivalentes* :

(i) *Le polynôme* d *divise* f *et* g, *et tout polynôme qui divise à la fois* f *et* g *divise* d.

(ii) *Le polynôme* d *divise* f *et* g, *et il existe deux polynômes* u *et* v *tels que* $d = uf + vg$.

(iii) *On a la relation* $(d) = (f) + (g)$ *entre idéaux de* K[X].

Le polynôme d *est déterminé par ces propriétés, à la multiplication près par un élément non nul de* K. *Si* f *et* g *ne sont pas tous deux nuls, on a* $d \neq 0$ *et le degré de* d *majore le degré de tout polynôme divisant à la fois* f *et* g.

Lorsque f et g sont nuls, chacune des propriétés (i) à (iii) est satisfaite dans le seul cas où $d = 0$, donc elles sont équivalentes. Nous supposerons désormais que f et g ne sont pas tous deux nuls, et nous noterons $\mathfrak{a}$ l'idéal $(f) + (g)$ de K[X].

[1] Le lecteur notera l'analogie entre les résultats de ce numéro et du suivant et les propriétés de divisibilité dans l'anneau **Z** des entiers (I, p. 106). Ils dépendent essentiellement du fait que, dans les anneaux **Z** et K[X], tout idéal est principal, comme nous le verrons au chapitre VII, § 1.

Remarquons que, quels que soient les polynômes u et v dans K[X], les propriétés $(u) \supset (v)$ et « u divise v » sont équivalentes. L'assertion (ii) équivaut donc à « $(d) \supset (f)$ et $(d) \supset (g)$ et $d \in (f) + (g)$ », c'est-à-dire à (iii). Il est clair que (ii) entraîne (i). Supposons enfin (i) satisfaite ; on a $(d) \supset (f)$ et $(d) \supset (g)$, d'où $(d) \supset \mathfrak{a}$; par ailleurs, d'après la prop. 11 (IV, p. 11), il existe un polynôme d_1 tel que $\mathfrak{a} = (d_1)$; comme le polynôme d_1 divise à la fois f et g, il divise d par hypothèse, d'où $(d) \subset \mathfrak{a}$; finalement, on a $(d) = \mathfrak{a}$, c'est-à-dire (iii).

Les autres assertions de la prop. 12 sont des conséquences immédiates de la prop. 11 appliquée à l'idéal $\mathfrak{a} = (f) + (g)$.

DÉFINITION 1. — *Avec les notations de la prop.* 12, *on dit que d est un* plus grand commun diviseur (en abrégé *pgcd*) *de f et g. On dit que f et g sont étrangers, ou premiers entre eux, ou que f est étranger à g, ou premier à g, lorsque* 1 *est un pgcd de f et g.*

Dire que f et g sont étrangers signifie donc qu'il existe des polynômes u et v dans K[X] tels que $uf + vg = 1$.

COROLLAIRE 1. — *Soient d un pgcd de f et g,* K′ *un corps commutatif contenant* K *comme sous-corps. Alors d est un pgcd de f et g considérés comme éléments de* K′[X].

Cela résulte de la prop. 12, (iii).

COROLLAIRE 2. — *Soit d un pgcd de f et g.*

(i) *Si* $u \in$ K[X], *du est un pgcd de fu et gu.*

(ii) *Si* $v \in$ K[X] *est un diviseur non nul de f et g, d/v est un pgcd de f/v et g/v.*

Cela résulte de la prop. 12, (ii).

COROLLAIRE 3. — *Soit w un diviseur commun de f et g. Pour que w soit un pgcd de f et g, il faut et il suffit que f/w et g/w soient étrangers.*

Cela résulte du cor. 2.

COROLLAIRE 4. — *Soient* $f, g, h \in$ K[X]. *Si f divise gh et est étranger à g, alors f divise h.*

En effet, f divise gh et fh ; donc f divise tout pgcd de gh et fh, en particulier h (cor. 2, (i)).

COROLLAIRE 5. — *Soient* $f, g \in$ K[X]. *Pour que f et g soient étrangers, il faut et il suffit que l'image canonique de g dans* K[X]/(f) *soit inversible.*

En effet, cette condition signifie qu'il existe $u, v \in$ K[X] tels que $uf + vg = 1$.

COROLLAIRE 6. — *Soient* $f, g_1, g_2, \ldots, g_n \in$ K[X]. *Si f est étranger à* $g_1, g_2, \ldots, g_n$, *alors f est étranger à* $g_1 g_2 \ldots g_n$.

* COROLLAIRE 7. — *Pour que f et g soient étrangers, il faut et il suffit qu'ils n'aient de racines communes dans aucune extension de* K.

En effet, si d est un pgcd de f et g, les racines communes à f et g dans une extension K′ de K sont les racines de d dans K′. Le corollaire résulte donc de V, p. 21, prop. 4. *

8. Polynômes irréductibles

DÉFINITION 2. — *Soit* K *un corps commutatif. On dit que* $f \in K[X]$ *est irréductible si* $\deg f \geqslant 1$, *et si* f *n'est divisible par aucun polynôme* g *tel que* $0 < \deg g < \deg f$.

Il revient au même de dire que $\deg f \geqslant 1$ et que les seuls diviseurs de f dans K[X] sont les scalaires $\neq 0$ et les produits de f par les scalaires $\neq 0$. Comme la relation $(f) \subset (g)$ signifie que g divise f, on voit que les polynômes irréductibles de K[X] peuvent encore être définis comme les polynômes f tels que l'idéal (f) soit *maximal* (I, p. 99).

Soient $f, g \in K[X]$. Si f est irréductible, il est clair que ou bien f et g sont étrangers ou bien f divise g. Si f *et* g sont irréductibles, ou bien f et g sont étrangers, ou bien chacun est le produit de l'autre par un scalaire $\neq 0$. En particulier, deux polynômes unitaires irréductibles distincts sont étrangers.

PROPOSITION 13. — *Soit* $\mathscr{I}$ *l'ensemble des polynômes unitaires irréductibles de* K[X]. *Soient* f *un élément non nul de* K[X], α *son coefficient dominant. Il existe une famille* $(v_p)_{p\in\mathscr{I}}$ *à support fini d'entiers positifs, et une seule, telle que l'on ait la décomposition*

$$f = \alpha \prod_{p\in\mathscr{I}} p^{v_p}. \tag{18}$$

Il suffit de prouver la proposition lorsque f est unitaire, c'est-à-dire lorsque $\alpha = 1$. Nous raisonnerons par récurrence sur le degré n de f, le cas $n = 0$ étant trivial. Supposons donc $n \geqslant 1$ et la proposition établie pour tous les polynômes de degré $< n$.

Soit E l'ensemble des polynômes unitaires $\neq 1$ qui divisent f ; on a $f \in E$, donc E n'est pas vide, et il existe dans E un polynôme g de degré minimum. Il est clair que g est irréductible et qu'il existe un polynôme unitaire h de degré $< n$ tel que $f = gh$; d'après l'hypothèse de récurrence, h est produit d'une famille finie de polynômes unitaires irréductibles, donc f a la même propriété. Ceci prouve l'*existence* de la décomposition (18).

Prouvons maintenant l'*unicité* de la décomposition (18). Soit $(w_p)_{p\in\mathscr{I}}$ une famille à support fini d'entiers positifs, telle que $f = \prod_{p\in\mathscr{I}} p^{w_p}$. Comme f est de degré $n \geqslant 1$, il existe p dans $\mathscr{I}$ tel que $w_p > 0$; si l'on avait $v_p = 0$, alors f serait produit d'une famille finie d'éléments de $\mathscr{I}$ distincts de p, donc serait étranger à p (IV, p. 12, cor. 6) contrairement au fait que p divise f. Par l'hypothèse de récurrence, le polynôme f/p admet une unique décomposition du type (18) ; on en déduit aussitôt l'égalité $w_q = v_q$ pour tout $q \in \mathscr{I}$.

Soit f un polynôme non nul dans K[X]. On dit que f est *sans facteur multiple* si les exposants v_p de la décomposition (18) sont tous $\leqslant 1$; il revient au même de dire que f est le produit d'une suite finie de polynômes irréductibles deux à deux distincts, ou encore que f n'est pas divisible par le carré d'un polynôme non constant de K[X].

§ 2. ZÉROS DES POLYNÔMES

1. Racines d'un polynôme à une indéterminée. Multiplicité

Soit $g \in A[(X_i)_{i\in I}]$ et soit E une A-algèbre associative unifère. Soit $\mathbf{x} = (x_i)_{i\in I}$ une famille d'éléments deux à deux permutables de E. On dit que $\mathbf{x}$ est un *zéro* de g dans E^I si $g(\mathbf{x}) = 0$. Si f est un polynôme par rapport à une seule indéterminée, un zéro de f dans E s'appelle encore une *racine* de f dans E.

PROPOSITION 1. — *Soient $f \in A[X]$ et $\alpha \in A$. Le reste de la division de f par $X - \alpha$ est $f(\alpha)$. Pour que α soit racine de f, il faut et il suffit que $X - \alpha$ soit un diviseur de f dans* A[X].

En effet, soient u, $v \in A[X]$ tels que $f = (X - \alpha)u + v$, et $\deg v < 1$. Alors v est un scalaire, et $f(\alpha) = (\alpha - \alpha)u(\alpha) + v = v$. Cela prouve la première assertion. La deuxième résulte de la première.

PROPOSITION 2. — *Soient $f \in A[X]$, $\alpha \in A$, et h un entier $\geqslant 0$. Les conditions suivantes sont équivalentes :*

(i) *f est divisible par $(X - \alpha)^h$ mais non par $(X - \alpha)^{h+1}$;*

(ii) *il existe $g \in A[X]$ tel que $f = (X - \alpha)^h g$ et $g(\alpha) \neq 0$.*

(i) $\Rightarrow$ (ii) : cela résulte aussitôt de la prop. 1.

(ii) $\Rightarrow$ (i) : supposons que $f = (X - \alpha)^h g$, où g n'admet pas la racine α. Alors f est divisible par $(X - \alpha)^h$. Supposons qu'il existe $g_1 \in A[X]$ tel que $f = (X - \alpha)^{h+1} g_1$, où $g_1 \in A[X]$. Comme $(X - \alpha)^h$ n'est pas diviseur de 0 dans A[X] (IV, p. 8, prop. 7), on a $g = (X - \alpha)\, g_1$, donc $g(\alpha) = 0$, ce qui est absurde.

PROPOSITION 3. — *Soient f un élément non nul de* A[X], *et $\alpha \in A$. Il existe un entier $h \geqslant 0$ et un seul qui satisfait aux conditions* (i) *et* (ii) *de la prop.* 2.

C'est évident sur la condition (i), compte tenu du fait que, si f est divisible par $(X - \alpha)^h$, on a $\deg f \geqslant h$ (IV, p. 8, prop. 7).

DÉFINITION 1. — *Avec les notations précédentes, on dit que α est d'ordre h, ou de multiplicité h, relativement à f.*

Si $h > 0$, on dit aussi que α est racine d'ordre h, ou de multiplicité h, de f. Une racine d'ordre 1 est dite racine simple, une racine d'ordre 2 est dite racine double,... Une racine d'ordre > 1 est dite multiple.

Remarques. — 1) Si $f = 0$, on convient de dire que α est d'ordre $\geqslant h$ relativement à f, quels que soient $\alpha \in A$ et l'entier $h \geqslant 0$. Quels que soient $f \in A[X]$ et $\alpha \in A$, dire que α est d'ordre $\geqslant h$ relativement à f signifie que $(X - \alpha)^h$ divise f.

2) Soit B un anneau commutatif contenant A comme sous-anneau. Soient $f \in A[X]$ non nul et $\alpha \in A$. L'ordre de α relativement à f est le même, que l'on considère f comme élément de B[X] ou comme élément de A[X]. C'est évident sur la condition (ii) de la prop. 2.

PROPOSITION 4. — *Soient f et g des éléments non nuls de* A[X]. *Soit* $\alpha \in A$, *et soient p et q les ordres de α relativement à f et g.*

(i) *L'ordre de α relativement à $f + g$ est $\geqslant \inf(p, q)$. Il est égal à $\inf(p, q)$ si $p \neq q$.*

(ii) *L'ordre de α relativement à fg est $\geqslant p + q$. Il est égal à $p + q$ si* A *est intègre.*

En effet, on a $f(X) = (X - \alpha)^p f_1(X)$, $g(X) = (X - \alpha)^q g_1(X)$ avec $f_1(\alpha) \neq 0$, $g_1(\alpha) \neq 0$. Supposons par exemple que $p \leqslant q$; on a alors

$$f(X) + g(X) = (X - \alpha)^p (f_1(X) + (X - \alpha)^{q-p} g_1(X)),$$

et, si $p < q$, α n'est pas racine de $f_1(X) + (X - \alpha)^{q-p} g_1(X)$; cela prouve (i). D'autre part, on a $f(X)\, g(X) = (X - \alpha)^{p+q} f_1(X)\, g_1(X)$, et $f_1(\alpha)\, g_1(\alpha) \neq 0$ si A est intègre ; cela prouve (ii).

PROPOSITION 5. — *Supposons* A *intègre. Soient f un élément non nul de* A[X], $\alpha_1, \ldots, \alpha_p$ *des racines de f dans* A *deux à deux distinctes, d'ordres $k_1, \ldots, k_p$. On a*

$$f(X) = (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \ldots (X - \alpha_p)^{k_p} g(X)$$

où $g \in$ A[X] et où $\alpha_1, \ldots, \alpha_p$ ne sont pas racines de g.

Procédons par récurrence sur p, la proposition étant évidente pour $p = 1$ en vertu de la déf. 1. Supposons donc qu'on ait $f(X) = g_1(X)\, g_2(X)$, où

$$g_1(X) = (X - \alpha_1)^{k_1} \ldots (X - \alpha_{p-1})^{k_{p-1}}, \quad g_2(X) \in A[X].$$

Comme A est intègre et que α_p est distinct de $\alpha_1, \ldots, \alpha_{p-1}$, alors α_p n'est pas racine de $g_1(X)$, donc α_p est racine d'ordre k_p de $g_2(X)$ (prop. 4, (ii)). Par suite, $g_2(X)$ est divisible par $(X - \alpha_p)^{k_p}$, et par conséquent

$$f(X) = (X - \alpha_1)^{k_1} \ldots (X - \alpha_p)^{k_p} g(X)$$

où $g(X) \in$ A[X]. Il est clair que $\alpha_1, \ldots, \alpha_p$ ne sont pas racines de g.

THÉORÈME 1. — *Supposons* A *intègre. Soient f un élément non nul de* A[X], *n son degré. La somme des ordres de toutes les racines de f dans* A *est $\leqslant n$.*

Cela résulte aussitôt de la prop. 5.

COROLLAIRE. — *On suppose* A *intègre. Soient $f, g \in$ A[X], de degrés $\leqslant n$. S'il existe $n + 1$ éléments $x_1, \ldots, x_{n+1}$ de* A, *deux à deux distincts, tels que $f(x_i) = g(x_i)$ pour $1 \leqslant i \leqslant n + 1$, on a $f = g$.*

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

PROPOSITION 6 (formule d'interpolation de Lagrange). — *Soient* K *un corps commutatif, $\alpha_1, \alpha_2, \ldots, \alpha_n$ des éléments distincts de* K, *et $\beta_1, \beta_2, \ldots, \beta_n$ des éléments de* K. *Pour $i = 1, 2, \ldots, n$, posons*

$$f_i(X) = \prod_{j \in U(i)} (X - \alpha_j)/(\alpha_i - \alpha_j),$$

où $U(i)$ *est l'ensemble des entiers* j *tels que* $j \neq i$ *et* $1 \leqslant j \leqslant n$. *Alors* $\beta_1 f_1 + \cdots + \beta_n f_n$ *est l'unique élément* f *de* $K[X]$ *tel que* $\deg f < n$ *et* $f(\alpha_i) = \beta_i$ *pour* $1 \leqslant i \leqslant n$.

L'unicité de f résulte du cor. du th. 1. Soit $f = \beta_1 f_1 + \cdots + \beta_n f_n$. Comme f_i est de degré $n - 1$, on a $\deg f < n$. D'autre part, $f_i(\alpha_j) = 0$ pour $j \neq i$, et $f_i(\alpha_i) = 1$. Donc $f(\alpha_i) = \beta_i$ pour $1 \leqslant i \leqslant n$.

COROLLAIRE. — *Supposons* A *intègre. Soit* $f \in A[X]$, *de degré* $< n$, *et soit* K *un sous-anneau de* A *qui est un corps. S'il existe* n *éléments* $\alpha_1, \ldots, \alpha_n$ *de* A, *distincts, et tels que* $\alpha_i \in K$ *et* $f(\alpha_i) \in K$ *pour* $i = 1, \ldots, n$, *alors* $f \in K[X]$.

2. Critère différentiel pour la multiplicité d'une racine

PROPOSITION 7. — *Soient* $f \in A[X]$, *et* $\alpha \in A$ *une racine de* f. *Pour que* α *soit racine simple de* f, *il faut et il suffit que* α *ne soit pas racine de la dérivée* Df *de* f.

Par hypothèse, on a $f = (X - \alpha)\, g$, où $g \in A[X]$. Pour que α soit racine simple de f, il faut et il suffit que $g(\alpha) \neq 0$. Or, on a $Df = g + (X - \alpha)\, Dg$, d'où $(Df)(\alpha) = g(\alpha)$.

Plus généralement :

PROPOSITION 8. — *Soient* $f \in A[X]$, *et* $\alpha \in A$. *Supposons que* α *soit d'ordre* $k \geqslant 1$ *relativement à* f. *Alors* α *est d'ordre* $\geqslant k - 1$ *relativement à* Df. *Si* $k.1$ *est simplifiable dans* A, *alors* α *est d'ordre* $k - 1$ *relativement à* Df.

Par hypothèse, il existe $g \in A[X]$ tel que $f = (X - \alpha)^k g$ et $g(\alpha) \neq 0$. Alors $Df = k(X - \alpha)^{k-1} g + (X - \alpha)^k\, Dg = (X - \alpha)^{k-1}(kg + (X - \alpha)\, Dg)$, ce qui établit la première partie de la proposition. La valeur de $kg + (X - \alpha)\, Dg$ pour $X = \alpha$ est $kg(\alpha)$, donc est non nulle si $k.1$ est simplifiable dans A ; cela prouve la deuxième partie de la proposition.

> Soit k un entier > 0 tel que $k.1 = 0$ dans A. Soit $f(X) = X^k \in A[X]$. Alors 0 est racine d'ordre k de f, et racine d'ordre arbitrairement grand de Df.

COROLLAIRE. — *Soient* $f \in A[X]$, $\alpha \in A$, *et* p *un entier* $\geqslant 0$. *On suppose que* $p!.1$ *est simplifiable dans* A. *Alors, pour que* α *soit racine d'ordre* p *de* f, *il faut et il suffit que* α *soit racine de* $f, Df, \ldots, D^{p-1}f$, *et ne soit pas racine de* $D^p f$.

Cela résulte de la prop. 8 par récurrence sur p.

3. Fonctions polynomiales sur un anneau intègre infini

PROPOSITION 9. — *On suppose* A *intègre. Soient* I *un ensemble,* $(H_i)_{i \in I}$ *une famille de parties infinies de* A, *et* $H = \prod_{i \in I} H_i \subset A^I$. *Soit* f *un élément non nul de* $A[(X_i)_{i \in I}]$. *Soit* H_f *l'ensemble des* $\mathbf{x} \in H$ *tels que* $f(\mathbf{x}) \neq 0$. *Alors* H *et* H_f *sont équipotents.*

a) Supposons d'abord I fini et soit $n = \mathrm{Card}\, I$. La proposition est évidente pour $n = 0$, et nous la démontrerons par récurrence sur n. Choisissons un élément i_0 de I, et soient $J = I - \{i_0\}$, $B = A[(X_i)_{i \in J}]$. Comme $f \neq 0$, on peut écrire

$f = \sum_{k=0}^{m} g_k X_{i_0}^k$ où $g_0, \ldots, g_m \in B$, et $g_m \neq 0$. D'après l'hypothèse de récurrence, l'ensemble K des $\mathbf{x} \in \prod_{i \in J} H_i$ tels que $g_m(\mathbf{x}) \neq 0$ est équipotent à $\prod_{i \in J} H_i$. Pour $\mathbf{x} \in K$, le polynôme

$$h(X_{i_0}) = \sum_{k=0}^{m} g_k(\mathbf{x})\, X_{i_0}^k \in A[X_{i_0}]$$

est non nul. D'après le th. 1 (IV, p. 15), l'ensemble des $\alpha \in H_{i_0}$ tels que $h(\alpha) \neq 0$ est équipotent à H_{i_0}, d'où

$$\text{Card } H \geqslant \text{Card } H_f \geqslant (\text{Card } K).(\text{Card } H_{i_0}) = \text{Card } H\,,$$

et par suite Card H = Card H_f.

b) Dans le cas général, il existe une partie finie I′ de I telle que $f \in A[(X_i)_{i \in I'}]$. Soit H'_f l'ensemble des $\mathbf{x} \in \prod_{i \in I'} H_i$ tels que $f(\mathbf{x}) \neq 0$. Alors $H_f = H'_f \times (\prod_{i \in I - I'} H_i)$, et il suffit d'appliquer à H'_f la première partie de la démonstration.

COROLLAIRE 1. — *On conserve les hypothèses et les notations de la prop.* 9. *Si* I *est non vide,* H_f *est infini.*

COROLLAIRE 2. — *On suppose que* A *est intègre et infini ou que* A *est une algèbre sur un corps infini. Pour tout* $f \in A[(X_i)_{i \in I}]$, *soit* $\tilde{f} : A^I \to A$ *la fonction polynomiale définie par* f (IV, p. 4). *Alors l'application* $f \mapsto \tilde{f}$ *est injective.*

Lorsque A est intègre infini, le corollaire résulte aussitôt de la prop. 9. Supposons que A soit une algèbre sur un corps infini k. Soit $f = \sum_{\nu \in \mathbf{N}^{(I)}} \alpha_\nu X^\nu$ un élément non nul de $A[(X_i)_{i \in I}]$. Il existe un $\nu_0 \in \mathbf{N}^{(I)}$ tel que $\alpha_{\nu_0} \neq 0$, et une forme k-linéaire φ sur A telle que $\varphi(\alpha_{\nu_0}) \neq 0$. Soit $g = \sum_{\nu \in \mathbf{N}^{(I)}} \varphi(\alpha_\nu) X^\nu \in k[(X_i)_{i \in I}]$. On a $g \neq 0$, donc il existe un $\mathbf{x} \in k^I$ tel que $g(\mathbf{x}) \neq 0$. Alors $\varphi(f(\mathbf{x})) = g(\mathbf{x}) \neq 0$, donc $f(\mathbf{x}) \neq 0$.

Lorsque A est intègre infini, ou lorsque A est une algèbre sur un corps infini, on identifie le plus souvent f à $\tilde{f}$.

Supposons A fini. Soit $f(X) = \prod_{\alpha \in A} (X - \alpha)$. Alors $f \neq 0$ mais $\tilde{f} = 0$. Pour d'autres exemples, cf. IV, p. 84, exerc. 7 et 8.

THÉORÈME 2 (principe du prolongement des identités algébriques). — *Supposons* A *intègre et infini. Soient* $g_1, \ldots, g_m, f$ *des éléments de* $A[(X_i)_{i \in I}]$. *On fait les hypothèses suivantes* :

a) $g_1 \neq 0, \ldots, g_m \neq 0$;

b) *pour tout* $\mathbf{x} \in A^I$ *tel que* $g_1(\mathbf{x}) \neq 0, \ldots, g_m(\mathbf{x}) \neq 0$, *on a* $f(\mathbf{x}) = 0$.

Alors $f = 0$.

En effet, si $f \neq 0$, on a $fg_1 \ldots g_m \neq 0$ (IV, p. 9, prop. 8), donc il existe $\mathbf{x} \in A^I$ tel que $f(\mathbf{x})\, g_1(\mathbf{x}) \ldots g_m(\mathbf{x}) \neq 0$ (IV, p. 17, cor. 2), ce qui contredit l'hypothèse.

Scholie. — Soient A un anneau intègre et $f \in A[(X_i)_{i\in I}]$. Le th. 2 fournit un moyen commode pour prouver que $f = 0$. Il suffit de considérer un anneau intègre infini E contenant A comme sous-anneau ; si l'on démontre que $f((x_i)) = 0$ pour tout $(x_i) \in E^I$ (ou seulement pour les $(x_i) \in E^I$ qui n'annulent pas un nombre fini de polynômes donnés non nuls), il en résulte que $f = 0$. Si A lui-même n'est pas infini, on peut par exemple prendre pour E l'anneau A[X] ou son corps des fractions.

Une fois démontrée la relation $f = 0$, on en déduit évidemment $f((y_i)) = 0$ pour tout $(y_i) \in F^I$, où F est une A-algèbre unifère associative et commutative quelconque ; en particulier, F peut être finie ou non intègre.

En d'autres termes, la démonstration de l'identité $f((x_i)) = 0$ lorsque les x_i parcourent un anneau intègre infini contenant A comme sous-anneau (avec éventuellement la restriction que $g_k((x_i)) \neq 0$ pour $1 \leqslant k \leqslant m$, les g_k étant des polynômes non nuls) entraîne la même identité lorsque les x_i parcourent une A-algèbre unifère associative et commutative quelconque.

En particulier, soit $f \in \mathbf{Z}[(X_i)]$. Si $f((x_i)) = 0$ lorsque les x_i parcourent $\mathbf{Z}$ (avec éventuellement la restriction que $g_k((x_i)) \neq 0$ pour $1 \leqslant k \leqslant m$, les g_k étant des éléments non nuls de $\mathbf{Z}[(X_i)]$), on a la même identité lorsque les x_i parcourent un anneau commutatif quelconque.

§ 3. FRACTIONS RATIONNELLES

1. Définition des fractions rationnelles

DÉFINITION 1. — *Soient* K *un corps commutatif,* I *un ensemble. Le corps des fractions* (I, p. 110) *de l'anneau intègre* $K[(X_i)_{i\in I}]$ *se note* $K((X_i)_{i\in I})$ *ou* $K(X_i)_{i\in I}$. *Ses éléments s'appellent les fractions rationnelles à coefficients dans* K *par rapport aux indéterminées* X_i.

Pour $I = \{1, 2, \ldots, n\}$, on écrit $K(X_1, X_2, \ldots, X_n)$ au lieu de $K((X_i)_{i\in I})$.

Soient A un anneau intègre, K son corps des fractions. L'anneau $A[(X_i)_{i\in I}]$ s'identifie à un sous-anneau de $K[(X_i)_{i\in I}]$, donc de $K((X_i)_{i\in I})$. Pour tout $f \in K[(X_i)_{i\in I}]$, il existe un élément non nul α de A tel que $\alpha f \in A[(X_i)_{i\in I}]$. Donc, tout élément de $K((X_i)_{i\in I})$ peut se mettre sous la forme u/v, où $u, v \in A[(X_i)_{i\in I}]$, $v \neq 0$. Donc $K((X_i)_{i\in I})$ s'identifie au corps des fractions de $A[(X_i)_{i\in I}]$.

Soient maintenant K un corps commutatif, I un ensemble et $J \subset I$. Posons $B = K[(X_i)_{i\in J}]$. Alors $K[(X_i)_{i\in I}] = B[(X_i)_{i\in I-J}]$. D'après ce qui précède, $K((X_i)_{i\in I})$ s'identifie à $K'((X_i)_{i\in I-J})$, où $K' = K((X_i)_{i\in J})$.

2. Degrés

Soit K un corps commutatif. Pour tout élément r de $K((X_i)_{i\in I})$, il existe $u, v \in K[(X_i)_{i\in I}]$ tels que $v \neq 0$ et $r = \frac{u}{v}$. La relation $\frac{u}{v} = \frac{u_1}{v_1}$ où $v \neq 0, v_1 \neq 0$, équi-

vaut à $uv_1 = vu_1$; si $r \neq 0$, on a $u \neq 0$ et $u_1 \neq 0$ et alors $\deg u + \deg v_1 = \deg v + \deg u_1$ (IV, p. 9), ou encore $\deg u - \deg v = \deg u_1 - \deg v_1$. L'entier rationnel $\deg u - \deg v$ ne dépend donc que de r ; on dit que c'est le *degré*, ou le *degré total* de r. On le note $\deg r$. On convient que $\deg 0 = -\infty$. Si $J \subset I$, on définit de même le degré par rapport aux X_j d'indices $j \in J$. Lorsque r est un polynôme, ces notions coïncident avec celles qu'on a définies en IV, p. 3.

PROPOSITION 1. — *Soient r, s deux fractions rationnelles.*

(i) *Si* $\deg r \neq \deg s$, *on a*

$$r + s \neq 0 \quad \textit{et} \quad \deg(r + s) = \sup(\deg r, \deg s) .$$

Si $\deg r = \deg s$, *on a* $\deg(r + s) \leqslant \deg r$.

(ii) *On a* $\deg(rs) = \deg r + \deg s$.

On peut se limiter au cas où r et s sont non nuls.

Écrivons $r = \frac{u}{v}$, $s = \frac{w}{z}$, où u, v, w, z sont des polynômes non nuls. On a $rs = \frac{uw}{vz}$, donc

$$\deg(rs) = \deg(uw) - \deg(vz) = \deg u - \deg v + \deg w - \deg z = \deg r + \deg s .$$

D'autre part, on a $r + s = \frac{uz + vw}{vz}$. Supposons $\deg r \neq \deg s$; autrement dit, $\deg u + \deg z \neq \deg w + \deg v$. Alors $uz + wv \neq 0$, et

$$\begin{aligned} \deg(r + s) &= \deg(uz + wv) - \deg(vz) \\ &= \sup(\deg(uz), \deg(wv)) - \deg(vz) \\ &= \sup(\deg(uz) - \deg(vz), \deg(wv) - \deg(vz)) \\ &= \sup(\deg r, \deg s) . \end{aligned}$$

Supposons $\deg r = \deg s$, c'est-à-dire $\deg u + \deg z = \deg w + \deg v$. Si $r + s \neq 0$, on a

$$\begin{aligned} \deg(r + s) &= \deg(uz + wv) - \deg(vz) \\ &\leqslant \deg(uz) - \deg(vz) = \deg r . \end{aligned}$$

* L'application $r \mapsto -\deg r$ est donc une valuation discrète sur le corps $K((X_i)_{i\in I})$. *

3. Substitutions

Soient K un corps commutatif, E une K-algèbre associative unifère, $\mathbf{x} = (x_i)_{i\in I}$ une famille d'éléments de E deux à deux permutables. Soient $B = K[(X_i)_{i\in I}]$ et $S_{\mathbf{x}}$ l'ensemble des $v \in B$ non nuls tels que $v(\mathbf{x})$ soit inversible dans E. Soient $u \in B$, $v \in S_{\mathbf{x}}$,

et $f = \frac{u}{v} \in K((X_i)_{i\in I})$. L'élément $u(\mathbf{x})\, v(\mathbf{x})^{-1} = v(\mathbf{x})^{-1} u(\mathbf{x})$ est défini dans E ; en outre, si u_1 et v_1 sont deux polynômes tels que $f = \frac{u_1}{v_1}$ et $v_1 \in S_{\mathbf{x}}$, on a $uv_1 = u_1 v$, donc $u(\mathbf{x})\, v_1(\mathbf{x}) = u_1(\mathbf{x})\, v(\mathbf{x})$, donc

$$u(\mathbf{x})\, v(\mathbf{x})^{-1} = u_1(\mathbf{x})\, v_1(\mathbf{x})^{-1} .$$

Soit $f \in K((X_i)_{i\in I})$. S'il existe *au moins un couple* (u, v) tel que $f = \frac{u}{v}$ et $v \in S_{\mathbf{x}}$, on dit que $\mathbf{x}$ est *substituable* dans f ; l'élément $u(\mathbf{x})\, v(\mathbf{x})^{-1}$, qui ne dépend que de f et $\mathbf{x}$, se note alors $f(\mathbf{x})$ ou $f((x_i))$ ou $f((x_i)_{i\in I})$.

PROPOSITION 2. — *Soient* K *un corps commutatif,* E *une* K*-algèbre associative unifère,* $\mathbf{x} = (x_i)_{i\in I}$ *une famille d'éléments de* E *deux à deux permutables. L'ensemble* $S_{\mathbf{x}}^{-1}B$ *des* $f \in K((X_i)_{i\in I})$ *telles que* $\mathbf{x}$ *soit substituable dans* f *est une sous-*K*-algèbre de* $K((X_i)_{i\in I})$. *L'application* $f \mapsto f(\mathbf{x})$ *est un homomorphisme unifère* φ *de* $S_{\mathbf{x}}^{-1}B$ *dans* E. *L'image* $\varphi(S_{\mathbf{x}}^{-1}B)$ *est l'ensemble des* yz^{-1} *où* y *parcourt la sous-algèbre unifère* $K[\mathbf{x}]_E$ *de* E *engendrée par la famille* $\mathbf{x}$ *et où* z *parcourt l'ensemble des éléments inversibles de* $K[\mathbf{x}]_E$.

Soient $f_1 = \frac{u_1}{v_1}$, $f_2 = \frac{u_2}{v_2}$ deux éléments de $K((X_i)_{i\in I})$ tels que $v_1, v_2 \in S_{\mathbf{x}}$. On a $f_1 + f_2 = \frac{u_1 v_2 + u_2 v_1}{v_1 v_2}$, $f_1 f_2 = \frac{u_1 u_2}{v_1 v_2}$, et $v_1 v_2 \in S_{\mathbf{x}}$. Donc $S_{\mathbf{x}}^{-1}B$ est une sous-K-algèbre de $K((X_i)_{i\in I})$. Le reste de la proposition est évident.

COROLLAIRE. — *Soient* L *un corps commutatif,* K *un sous-corps de* L, $\mathbf{x} = (x_i)_{i\in I}$ *une famille d'éléments de* L, M *l'ensemble des* x_i, U *l'ensemble des* $f \in K((X_i)_{i\in I})$ *telles que* $\mathbf{x}$ *soit substituable dans* f, φ *l'homomorphisme* $f \mapsto f(\mathbf{x})$ *de* U *dans* L. *Alors* $\varphi(U)$ *est le sous-corps de* L *engendré par* $K \cup M$.

Soit L′ le sous-corps de L engendré par $K \cup M$. On a

$$K \cup M \subset \varphi(U) \subset L'$$

et $\varphi(U)$ est un sous-anneau de L. La prop. 2 entraîne que $\varphi(U)$ est un sous-corps de L, d'où $\varphi(U) = L'$.

Soit $f \in K((X_i)_{i\in I})$. Soit $(g_i)_{i\in I}$ une famille d'éléments de $K((Y_l)_{l\in L})$. Si (g_i) est substituable dans f, $f((g_i))$ est un élément de $K((Y_l)_{l\in L})$. En particulier, $(X_i)_{i\in I}$ est substituable dans f, et $f = f((X_i)_{i\in I})$.

PROPOSITION 3. — *Soit* E *une algèbre sur* K, *associative, commutative, unifère et non nulle. Soit* $f \in K((X_i)_{i\in I})$. *Pour tout* $i \in I$, *soit* $g_i \in K((Y_l)_{l\in L})$. *Soit* $\mathbf{y} = (y_l)_{l\in L}$ *une famille d'éléments de* E. *On suppose que* $\mathbf{y}$ *est substituable dans chaque* g_i, *et que* $(g_i(\mathbf{y}))_{i\in I}$ *est substituable dans* f. *Alors* :

(i) $(g_i)_{i\in I}$ *est substituable dans* f ;

(ii) *si l'on note* h *l'élément* $f((g_i))$ *de* $K((Y_l)_{l\in L})$, *alors* $\mathbf{y}$ *est substituable dans* h, *et* $h(\mathbf{y}) = f((g_i(\mathbf{y})))$.

On peut supposer I fini. Par hypothèse, pour tout $i \in I$, g_i peut se mettre sous la forme p_i/q_i, où p_i, $q_i \in K[(Y_l)_{l\in L}]$ et $q_i(\mathbf{y})$ est inversible dans E. De même, f peut se mettre sous la forme u/v, où u, $v \in K[(X_i)_{i\in I}]$ et $v((g_i(\mathbf{y})))$ est inversible. Soit $m = \sup(\deg u, \deg v)$. Soient $w = \prod_{i\in I} q_i \in K[(Y_l)_{l\in L}]$, $u_1 = u((g_i))\, w^m$, $v_1 = v((g_i))\, w^m$. Le polynôme u est combinaison K-linéaire de monômes $\prod_{i\in I} X_i^{\nu_i}$ tels que $\sum_{i\in I} \nu_i \leqslant m$. On a $w^m \prod_{i\in I} g_i^{\nu_i} = w^m(\prod_{i\in I} p_i^{\nu_i})(\prod_{i\in I} q_i^{\nu_i})^{-1} \in K[(Y_l)_{l\in L}]$ d'après le choix de m. Donc $u_1 \in K[(Y_l)_{l\in L}]$ et de même $v_1 \in K[(Y_l)_{l\in L}]$. De plus, $v_1(\mathbf{y}) = (w(\mathbf{y}))^m v((g_i(\mathbf{y})))$ est inversible. Donc $v_1 \neq 0$ parce que $E \neq 0$, et par suite $v((g_i)) \neq 0$. La famille (g_i) est donc substituable dans f. En outre on a $f((g_i)) = u_1/v_1$, donc $\mathbf{y}$ est substituable dans $h = f((g_i))$, et $h(\mathbf{y}) = u_1(\mathbf{y})/v_1(\mathbf{y}) = u((g_i(\mathbf{y})))/v((g_i(\mathbf{y}))) = f((g_i(\mathbf{y})))$.

Soient K un corps commutatif, E une K-algèbre commutative, associative et unifère. Soit $f \in K((X_i)_{i\in I})$. Soit T_f l'ensemble des $\mathbf{x} = (x_i)_{i\in I} \in E^I$ qui sont substituables dans f. L'application $\mathbf{x} \mapsto f(\mathbf{x})$ de T_f dans E s'appelle la *fonction rationnelle* associée à f (et à E) ; on la note parfois $\tilde{f}$. Si $g \in K((X_i)_{i\in I})$, on a $T_f \cap T_g \subset T_{f+g}$, $T_f \cap T_g \subset T_{fg}$; la fonction rationnelle associée à $f + g$ (resp. fg) est donc définie sur $T_f \cap T_g$, et a même valeur dans cet ensemble que la fonction $\tilde{f} + \tilde{g}$ (resp. $\tilde{f}\tilde{g}$). Soit T'_f l'ensemble des $\mathbf{x} \in T_f$ tels que $f(\mathbf{x})$ soit inversible ; si $\mathbf{x} \in T'_f$, $\mathbf{x}$ est substituable dans $1/f$, et la fonction rationnelle associée à $1/f$ prend en $\mathbf{x}$ la valeur $f(\mathbf{x})^{-1}$.

Soient K un corps commutatif *infini*, $f \in K((X_i)_{i\in I})$, $g \in K((X_i)_{i\in I})$ et $\tilde{f}$, $\tilde{g}$ les fonctions rationnelles associées à f, g (et à K). Si l'on a $\tilde{f}(\mathbf{x}) = \tilde{g}(\mathbf{x})$ pour tout $\mathbf{x} \in T_f \cap T_g$, alors $f = g$. En effet, si $f = u/v$ et $g = u_1/v_1$, où u, v, u_1, v_1 sont des polynômes, on a $u(\mathbf{x})\, v_1(\mathbf{x}) = u_1(\mathbf{x})\, v(\mathbf{x})$ pour tout $\mathbf{x}$ tel que $v(\mathbf{x})\, v_1(\mathbf{x}) \neq 0$, donc $uv_1 = u_1 v$ (IV, p. 17, th. 2). Par suite, l'application $f \mapsto \tilde{f}$ est injective, et l'on identifie souvent f et $\tilde{f}$.

* En utilisant la factorialité de $K[(X_i)_{i\in I}]$ (AC, VII, § 3, n° 2 et cor. du th. 2), on montre facilement ceci : pour tout $f \in K((X_i)_{i\in I})$, il existe u, $v \in K[(X_i)_{i\in I}]$ tels que :

1) $f = u/v$;

2) pour que $\mathbf{x} \in K^I$ soit substituable dans f, il faut et il suffit que $v(\mathbf{x}) \neq 0$. *

4. Différentielles et dérivations

Soit K un corps commutatif. D'après III, p. 123, prop. 5, toute dérivation D de $K[(X_i)_{i\in I}]$ se prolonge d'une seule manière en une dérivation $\overline{D}$ de $K((X_i)_{i\in I})$. Si D, D′ sont des dérivations permutables de $K[(X_i)_{i\in I}]$, le crochet $[D, D'] = DD' - D'D$ est nul, donc $[\overline{D}, \overline{D}']$, qui est une dérivation de $K((X_i)_{i\in I})$ prolongeant $[D, D']$, est

nul ; autrement dit $\overline{\mathrm{D}}$ et $\overline{\mathrm{D}}'$ sont permutables. En particulier, les dérivations D_i (IV, p. 6) se prolongent en des dérivations de $\mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$ qu'on note encore D_i et qui sont deux à deux permutables. Si $f \in \mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$, $\mathrm{D}_i f$ se note aussi $\mathrm{D}_{\mathrm{X}_i} f$, ou $\dfrac{\partial f}{\partial \mathrm{X}_i}$, ou f'_{X_i}. Lorsqu'il n'y a qu'une seule indéterminée X, on emploie les notations $\mathrm{D}f, \dfrac{df}{d\mathrm{X}}, f'$.

Soient $\mathrm{B} = \mathrm{K}[(\mathrm{X}_i)_{i\in\mathrm{I}}]$, $\mathrm{C} = \mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$. D'après III, p. 138, prop. 23, l'application canonique

$$\Omega_{\mathrm{K}}(\mathrm{B}) \otimes_{\mathrm{B}} \mathrm{C} \to \Omega_{\mathrm{K}}(\mathrm{C})$$

est un isomorphisme de C-espaces vectoriels. Compte tenu de III, p. 134, le C-espace vectoriel $\Omega_{\mathrm{K}}(\mathrm{C})$ admet donc pour base la famille $(d\mathrm{X}_i)_{i\in\mathrm{I}}$ des différentielles des X_i. Soit ∂_i la forme coordonnée d'indice i sur $\Omega_{\mathrm{K}}(\mathrm{C})$, relativement à cette base. Alors l'application $u \mapsto \langle \partial_i, du \rangle$ de C dans C est une dérivation de C qui transforme X_i en 1 et X_j en 0 pour $j \neq i$, donc est égale à D_i ; autrement dit, on a

$$du = \sum_{i\in\mathrm{I}} (\mathrm{D}_i u)\, d\mathrm{X}_i \tag{1}$$

pour tout $u \in \mathrm{C}$. Si I est fini, $(\mathrm{D}_i)_{i\in\mathrm{I}}$ est une base du C-espace vectoriel des dérivations de C.

PROPOSITION 4. — *Soient* E *une* K*-algèbre associative, commutative et unifère,* $\mathbf{x} = (x_i)_{i\in\mathrm{I}}$ *une famille d'éléments de* E, *et* $f \in \mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$. *On suppose que* $\mathbf{x}$ *est substituable dans* f. *Soit* $y = f(\mathbf{x})$.

(i) *Pour toute dérivation* Δ *de* $\mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$ *qui applique* $\mathrm{K}[(\mathrm{X}_i)_{i\in\mathrm{I}}]$ *dans lui-même,* $\mathbf{x}$ *est substituable dans* Δf.

(ii) *Pour toute dérivation* D *de* E *dans un* E*-module, on a*

$$\mathrm{D}y = \sum_{i\in\mathrm{I}} (\mathrm{D}_i f)(\mathbf{x}).\mathrm{D}x_i\ .$$

Soit $f = \dfrac{u}{v}$ avec $u, v \in \mathrm{K}[(\mathrm{X}_i)_{i\in\mathrm{I}}]$ et $v(\mathbf{x})$ inversible dans E. Soit Δ une dérivation de $\mathrm{K}((\mathrm{X}_i)_{i\in\mathrm{I}})$ qui applique $\mathrm{K}[(\mathrm{X}_i)_{i\in\mathrm{I}}]$ dans lui-même. On a

$$\Delta f = \frac{(\Delta u)\, v - u(\Delta v)}{v^2}$$

et $v^2(\mathbf{x})$ est inversible, donc $\mathbf{x}$ est substituable dans Δf. D'autre part, posons $r = u(\mathbf{x})$, $s = v(\mathbf{x})$. On a $y = s^{-1}r$, donc, pour toute dérivation D de E dans un E-module, on a

$$\begin{aligned}\mathrm{D}y &= s^{-2}(s(\mathrm{D}r) - r(\mathrm{D}s)) \\ &= s^{-2}(s \sum_{i\in\mathrm{I}} (\mathrm{D}_i u)(\mathbf{x}).\mathrm{D}x_i - r \sum_{i\in\mathrm{I}} (\mathrm{D}_i v)(\mathbf{x}).\mathrm{D}x_i)\end{aligned}$$

d'après la prop. 4 de IV, p. 6. Ainsi, $Dy = \sum_{i \in I} w_i . Dx_i$, avec

$$w_i = v(\mathbf{x})^{-2}(v(\mathbf{x})\,(D_i u)\,(\mathbf{x}) - u(\mathbf{x})\,(D_i v)\,(\mathbf{x})) = (D_i f)\,(\mathbf{x})\,.$$

§ 4. SÉRIES FORMELLES

1. Définition des séries formelles. Ordre

Soit I un ensemble. Rappelons (III, p. 27 et 28) que l'algèbre large du monoïde $\mathbf{N}^{(I)}$ sur A s'appelle l'*algèbre des séries formelles par rapport aux indéterminées* X_i ($i \in I$) (ou en les indéterminées X_i) *à coefficients dans* A. Elle se note $A[[X_i]]_{i \in I}$ ou $A[[(X_i)_{i \in I}]]$, ou encore $A[[\mathbf{X}]]$ en notant $\mathbf{X}$ la famille $(X_i)_{i \in I}$: dans ce paragraphe, nous utiliserons surtout la notation $A[[I]]$. Il est parfois commode de désigner l'image canonique dans $A[[I]]$ de l'élément i de I par un symbole différent de X_i, par exemple Y_i, Z_i, T_i, ... ; les conventions utilisées dans ce cas sont analogues à celles des polynômes (IV, p. 1). L'algèbre $A[[I]]$ se désigne alors par $A[[Y_i]]_{i \in I}$, ou $A[[\mathbf{Y}]]$, etc.

Lorsque I est un ensemble fini à p éléments, on dit encore que $A[[I]]$ est une algèbre de séries formelles en p indéterminées. Ces algèbres sont toutes isomorphes pour p fixé. Une algèbre de séries formelles à 1, 2, ... indéterminées peut ainsi se noter $A[[X]]$, $A[[U, V]]$, ..., l'ensemble d'indices I étant non spécifié.

Une série formelle u s'écrit conventionnellement $u = \sum_{\nu \in \mathbf{N}^{(I)}} \alpha_\nu X^\nu$ (*cf.* IV, p. 1). Les α_ν sont les *coefficients* de u ; une infinité d'entre eux peuvent être $\neq 0$. Les $\alpha_\nu X^\nu$ s'appellent les *termes* de u ; pour que u soit un polynôme, il faut et il suffit que u ne possède qu'un nombre fini de termes $\neq 0$. Les termes $\alpha_\nu X^\nu$ tels que $|\nu| = p$ s'appellent les termes de degré total p. La série formelle $u_p = \sum_{|\nu| = p} \alpha_\nu X^\nu$ s'appelle la *composante homogène de degré p* de u (c'est un polynôme lorsque I est fini) ; u_0 s'identifie à un élément de A dit encore *terme constant* de u. On dit que u est homogène de degré p si $u = u_p$. Si $u, v \in A[[I]]$ et $w = uv$, on a

$$w_p = \sum_{q+r=p} u_q v_r \tag{1}$$

pour tout entier $p \geqslant 0$.

Rappelons (III, p. 29) que l'*ordre* $\omega(u)$ d'une série formelle $u \neq 0$ est le plus petit des entiers p tels que $u_p \neq 0$. On convient d'adjoindre à $\mathbf{Z}$ un élément noté ∞, et de prolonger la relation d'ordre et l'addition de $\mathbf{Z}$ à $\mathbf{Z} \cup \{\infty\}$ par les conventions

$$n < \infty\,, \quad \infty + \infty = \infty\,, \quad \infty + n = n + \infty = \infty$$

pour tout $n \in \mathbf{Z}$. On pose alors $\omega(0) = \infty$. Avec ces conventions, on a les relations

$$\omega(u + v) \geqslant \inf(\omega(u), \omega(v))$$

$$\omega(u + v) = \inf(\omega(u), \omega(v)) \quad \text{si} \quad \omega(u) \neq \omega(v)$$

$$\omega(uv) \geqslant \omega(u) + \omega(v)$$

quelles que soient les séries formelles u et v dans $A[[I]]$.

Rappelons (III, p. 29) que pour toute partie J de I, on identifie $A[[I]]$ à $A[[I - J]][[J]]$, ce qui permet de définir l'ordre $\omega_J(u)$ d'une série formelle par rapport aux X_j ($j \in J$), la composante homogène de u par rapport aux X_j ($j \in J$), etc.

Soit φ un homomorphisme de A dans un anneau B. On prolonge φ en un homomorphisme $\overline{\varphi}$ de $A[[I]]$ dans $B[[I]]$ en faisant correspondre à toute série formelle $u = \sum_\nu \alpha_\nu X^\nu$ la série formelle $\sum_\nu \varphi(\alpha_\nu) X^\nu$; on dit que cette dernière est obtenue en *appliquant* φ *aux coefficients de la série formelle* u. On écrit parfois ${}^\varphi u$ pour $\overline{\varphi}(u)$.

En particulier, si A est un sous-anneau de B, et si φ est l'injection canonique de A dans B, l'homomorphisme $\overline{\varphi}$ de $A[[I]]$ dans $B[[I]]$ est injectif ; nous identifierons en général $A[[I]]$ par $\overline{\varphi}$ à un sous-anneau de $B[[I]]$.

2. Topologie sur l'ensemble des séries formelles. Familles sommables

Par définition, l'ensemble $A[[I]]$ n'est autre que l'ensemble produit $A^{\mathbf{N}^{(I)}}$. Sauf mention expresse du contraire, on munira A de la topologie discrète et $A[[I]]$ de la topologie prôduit (TG, I, p. 24) qu'on appelle la *topologie canonique*. Muni de l'addition et de la topologie discrète, A est un groupe topologique séparé et complet ; par suite, pour l'addition, $A[[I]]$ est un groupe topologique *séparé et complet* (TG, III, p. 17 et 21 et TG, II, p. 17). De plus, l'algèbre $A[(X_i)_{i\in I}]$ des polynômes est dense dans $A[[I]]$ (TG, III, p. 17, prop. 25), et l'on peut donc considérer $A[[I]]$ comme le *complété* de $A[(X_i)_{i\in I}]$.

Pour tout $\beta \in \mathbf{N}^{(I)}$, soit S_β l'ensemble des multiindices ν tels que $\nu \leqslant \beta$, et soit $\mathfrak{a}_\beta$ l'ensemble des séries formelles $u = \sum_\nu \alpha_\nu X^\nu$ telles que $\alpha_\nu = 0$ pour $\nu \in S_\beta$. Il est clair que S_β est une partie finie de $\mathbf{N}^{(I)}$, et que toute partie finie de $\mathbf{N}^{(I)}$ est contenue dans un ensemble de la forme S_β. Par suite, la famille $(\mathfrak{a}_\beta)_{\beta\in\mathbf{N}^{(I)}}$ est un système fondamental de voisinages de 0 dans $A[[I]]$. Les ensembles $\mathfrak{a}_\beta$ sont des idéaux de $A[[I]]$, donc (TG, III, p. 49) $A[[I]]$ est un *anneau topologique*.

Lemme 1. — *Soient* L *un ensemble infini et* $(u_\lambda)_{\lambda\in L}$ *une famille d'éléments de* $A[[I]]$. *Posons* $u_\lambda = \sum_\nu \alpha_{\lambda,\nu} X^\nu$ *pour* $\lambda \in L$. *Les conditions suivantes sont équivalentes* :

(i) *La famille* $(u_\lambda)_{\lambda\in L}$ *est sommable* (TG, III, p. 37) *dans* $A[[I]]$.

(ii) *On a* $\lim u_\lambda = 0$ *selon le filtre des complémentaires des parties finies de* L.

(iii) *Pour tout* $\nu \in \mathbf{N}^{(I)}$, *on a* $\alpha_{\lambda,\nu} = 0$ *sauf pour un nombre fini d'indices* $\lambda \in L$.