

CHAMBADAL J.L.OVAERT

**COURS DE
MATHÉMATIQUES**

algèbre II



gauthier - villars

COURS DE MATHÉMATIQUES

ALGÈBRE II

Lucien CHAMBADAL

Jean-Louis OVAERT

Anciens élèves de l'École Normale Supérieure
Agrégés de Mathématiques

COURS DE MATHÉMATIQUES

ALGÈBRE II

GAUTHIER-VILLARS ÉDITEUR
55, quai des Grands-Augustins, Paris-6^e
1972

L. CHAMBADAL

J. L. OVAERT

• COURS DE MATHÉMATIQUES

1 | Notions fondamentales d'algèbre et d'analyse

2 | Algèbre II.
Analyse II.

3 | Algèbre III.
Analyse III.

par Gauthier-Villars éditeur

- Algèbre linéaire et algèbre tensorielle (Dunod éditeur).

L. CHAMBADAL

- Exercices et problèmes résolus d'algèbre
- Exercices et problèmes résolus d'analyse

(en préparation) Gauthier-Villars éditeur

- Dictionnaire des mathématiques modernes (Larousse).
- Les ensembles (Bordas).
- Cours de mathématiques CB-BG (Dunod).
- Calcul des probabilités Premier cycle (Dunod).
- Mathématiques pour les enseignements supérieurs économiques et commerciaux (Dunod) :
 1. Éléments d'algèbre.
 2. Éléments d'analyse.
 3. Éléments de calcul des probabilités.
 4. Compléments et exercices.

© GAUTHIER-VILLARS, 1972

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'Article 41, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'Article 40).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les Articles 425 et suivants du Code Pénal.

AVERTISSEMENT

L'évolution de l'enseignement des mathématiques nous a conduits à publier séparément l'algèbre et ses applications à la géométrie d'une part, l'analyse et ses applications à la géométrie d'autre part. Dans ce tome, une référence telle que prop. .I.2.12 renvoie à la proposition 12 du chapitre 2 des *Notions fondamentales d'algèbre et d'analyse*, tandis qu'une référence telle que *Analyse* II., prop. 1.15 renvoie à la proposition 15 du chapitre 1 d'*Analyse* II.

Nous tenons à remercier tous ceux qui ont contribué à la mise au point de ce tome, et en particulier Mme M.-T. BARTHEL, MM. J. CAZALET, J.-P. LAVIGNE, G. MATHIEU, A. RENAUD, B. SKALLI, C. TRINK et P. WROBEL.

Les auteurs.

TABLE DES MATIÈRES

CHAPITRE 1. — Polynômes à une indéterminée

1. Polynômes à une indéterminée	3
2. Fractions rationnelles à une indéterminée	7
3. Fonctions polynomiales et rationnelles.	10
4. Division euclidienne. Idéaux de polynômes	20
5. Décomposition en facteurs irréductibles	23
6. Applications de la théorie de la divisibilité	30
1. Calcul du P. G. C. D. de deux polynômes	30
2. Forme réduite d'une fraction rationnelle	32
3. Parties principales des fractions rationnelles	34
7. Dérivation des polynômes et des fractions rationnelles	40
8. Étude locale des polynômes et des fractions rationnelles.	48
1. Partie principale d'une fraction rationnelle en un point.	48
2. Division suivant les puissances croissantes	51
3. Formule de Taylor	54
9. Corps algébriquement clos	57
1. Corps algébriquement clos	57
2. Théorème fondamental de l'algèbre	61
3. Polynômes et fractions rationnelles à coefficients réels ou complexes	63
10. Séries entières formelles	67
1. Séries entières formelles.	67
2. Exponentielle formelle	82
3. Fonctions d'une variable entière	92
EXERCICES	95

CHAPITRE 2. — Polynômes à plusieurs indéterminées

1. Polynômes à une indéterminée à coefficients dans un anneau	134
1. Polynômes. Fonctions polynomiales	134
2. Idéaux de polynômes	136
3. Décomposition en facteurs irréductibles	138
2. Polynômes et fractions rationnelles à plusieurs indéterminées	146
3. Fonctions polynomiales et rationnelles de plusieurs variables	156

4. Dérivation des polynômes et des fractions rationnelles	165
5. Polynômes et fractions rationnelles symétriques	176
1. Groupe symétrique	176
2. Signature d'une permutation	184
3. Polynômes et fractions rationnelles symétriques	191
6. Séries entières formelles à plusieurs indéterminées	207
1. Séries entières formelles.	207
2. Opérateurs de composition	222
EXERCICES	231

CHAPITRE 3. — Algèbre multilinéaire

1. Applications p -linéaires	258
1. Applications p -linéaires	258
2. Formes p -linéaires	263
3. Développement des applications p -linéaires	267
4. Développement des applications p -linéaires alternées	269
2. Déterminants	274
1. Déterminant de n vecteurs	274
2. Déterminant d'un endomorphisme.	277
3. Calculs de déterminants	282
1. Déterminants de matrices carrées remarquables	282
2. Développement d'un déterminant suivant une colonne, ou une ligne	284
3. Applications de la théorie des polynômes	287
4. Trace d'un endomorphisme	291
5. Notions sur le calcul tensoriel et sur le calcul extérieur.	295
1. Algèbre des formes multilinéaires	295
2. Algèbre des formes multilinéaires alternées	297
6. Algèbre multilinéaire sur un module	299
EXERCICES	303

CHAPITRE 4. — Équations linéaires

1. Rang d'une matrice	326
1. Rang d'une matrice	326
2. Matrices principales	327
3. Matrices équivalentes	329
4. Opérations élémentaires.	331
2. Équations linéaires	334
3. Exemples d'équations linéaires	340
4. Équations linéaires, en dimension finie.	347
5. Résolution des systèmes linéaires	352
1. Emploi des déterminants, dans le cas de Cramer.	352
2. Emploi des déterminants, dans le cas général.	353
3. Systèmes linéaires vectoriels	356
4. Méthode de substitution	358
5. Méthode d'addition	359
6. Recherche de l'inverse d'une matrice carrée	361
EXERCICES	363

CHAPITRE 5. — Réduction des endomorphismes

A. Cas général	389
1. Endomorphismes annulant un polynôme	389
1. Décomposition du noyau d'un polynôme d'un endomorphisme	389
2. Polynôme minimal d'un endomorphisme	393
2. Sous-espaces spectraux	396
3. Réduction des endomorphismes	401
1. Endomorphismes scindés	401
2. Endomorphismes diagonalisables	404
3. Structure des sous-espaces vectoriels stables	407
B. Cas de la dimension finie	409
4. Réduction des endomorphismes, en dimension finie	409
1. Conséquences de la théorie générale	409
2. Polynôme caractéristique d'un endomorphisme	418
3. Endomorphismes trigonalisables	421
4. Réduction d'une famille commutative d'endomorphismes	427
5. Décompositions additive et multiplicative d'un endomorphisme	430
5. Réduction des endomorphismes d'un espace vectoriel sur le corps des réels.	432
1. Extension complexe d'un espace vectoriel sur le corps des réels	432
2. Involution canonique d'une extension complexe	437
3. Réduction des endomorphismes d'un espace vectoriel sur le corps des réels.	440
6. Réduction des matrices	445
7. Réduite de Jordan	452
8. Applications de la théorie de la réduction	463
1. Équations aux différences finies linéaires à coefficients constants	463
2. Équations différentielles linéaires à coefficients constants	470
EXERCICES	477

NOTATIONS

Chapitre 1

$\mathbf{P}(K), K[X]$	algèbre des polynômes à une indéterminée à coefficients dans K .
$K(X)$	corps des fractions rationnelles à une indéterminée à coefficients dans K .
$d^0(P)$	degré du polynôme P .
$d^0(R)$	degré de la fraction rationnelle R .
$v_0(P)$	valuation du polynôme P .
$v_\alpha(P)$	valuation du polynôme P au point α .
$v_\alpha(R)$	valuation de la fraction rationnelle R au point α .
$v_P(A)$	valuation du polynôme A relative à P .
$v_P(R)$	valuation de la fraction rationnelle R relative à P .
\tilde{P}	fonction polynomiale associée au polynôme P .
\tilde{R}	fonction rationnelle associée à la fraction rationnelle R .
$P \circ Q$	polynôme composé des polynômes P et Q .
$R \circ S$	fraction rationnelle composée des fractions rationnelles R et S .
$\text{Pr}_\infty(R)$	partie entière de la fraction rationnelle R .
$\text{Pr}_P(R)$	partie principale de la fraction rationnelle R relative à P .
$\text{Pr}_\alpha(R)$	partie principale de R au point α .
$\text{Res}_\alpha(R)$	résidu de R au point α .
P. G. C. D. (\mathcal{E})	plus grand commun diviseur de la famille \mathcal{E} .
P. P. C. M. (\mathcal{E})	plus petit commun multiple de la famille \mathcal{E} .
D	dérivation canonique de l'algèbre $K[X]$, ou de l'algèbre $K(X)$.
$K_\alpha[X]$	sous-espace vectoriel des fractions rationnelles élémentaires relatives à α de degré strictement négatif.
$K_{\alpha,p}[X]$	sous-espace vectoriel des fractions rationnelles élémentaires relatives à α de degré strictement inférieur à p .
$\text{Pr}_{\alpha,p}(R)$	développement limité à l'ordre p de R au point α .
\bar{P}	conjugué du polynôme P .
\bar{R}	conjugée de la fraction rationnelle R .

$S(K), K[[X]]$	algèbre des séries entières formelles à une indéterminée à coefficients dans K .
$K((X))$	corps des séries entières formelles généralisées.
T_p	troncature à l'ordre p .
$\sum_{i \in I} A_i$	somme d'une famille sommable de séries entières formelles.
\mathfrak{S}_p	idéal des séries entières formelles de valuation strictement supérieure à p .
\mathfrak{M}	idéal des séries entières formelles non inversibles.
\mathfrak{U}	ensemble des séries entières formelles de la forme $1 + N$, où $N \in \mathfrak{M}_1$.
$\exp(A)$	exponentielle formelle de A .
$A(S)$	algèbre de convolution du monoïde S .
$f * g$	produit de convolution de f et de g .

Chapitre 2

$A[X]$	algèbre des polynômes à une indéterminée à coefficients dans A .
a^s	abréviation pour $\prod_{i \in I} a_i^{s(i)}$.
$ s $	abréviation pour $\sum_{i \in I} s(i)$.
$s !$	abréviation pour $\prod_{i \in I} s(i) !$.
$\mathbf{P}_I(A), A[X_i]_{i \in I}$	algèbre des polynômes à coefficients dans A construits sur I .
$A[X_1, X_2, \dots, X_n]$	algèbre des polynômes à n indéterminées à coefficients dans A .
$K(X_i)_{i \in I}$	corps des fractions rationnelles à coefficients dans K construites sur I .
$K(X_1, X_2, \dots, X_n)$	corps des fractions rationnelles à n indéterminées à coefficients dans K .
$d_I^\circ(P)$	degré partiel de P relativement à I .
$d_i^\circ(P)$	degré de P relativement à X_i .
$V(P)$	ensemble des points en lesquels le polynôme P s'annule.
$(T_p(P))$	développement taylorien de P .
dP	différentielle du polynôme P .
$\frac{\partial P}{\partial X_i} D_i(P)$	$i^{\text{ème}}$ dérivée partielle de P .
\mathfrak{D}	algèbre des opérateurs différentiels à coefficients constants.
$[x_1, x_2, \dots, x_p]$	cycle de support $\{x_1, x_2, \dots, x_p\}$.
O'_σ	ensemble des orbites associées à σ .

O_σ	ensemble des orbites associées à σ non réduites à un point.
$\varepsilon(\sigma)$	signature de la permutation σ .
\mathfrak{S}_E	groupe symétrique de E .
\mathfrak{U}_E	groupe alterné de E .
\mathfrak{S}_n	groupe symétrique de degré n .
\mathfrak{U}_n	groupe alterné de degré n .
S_p	polynôme symétrique élémentaire de degré p .
$\pi(P)$	poids du polynôme P .
N_p	polynôme de Newton de degré p .
F_s	polynôme symétrique fondamental associé à s .
$S_I(A), A[[X_i]]_{i \in I}$	algèbre des séries formelles à coefficients dans A construites sur I .
$A[[X_1, X_2, \dots, X_n]]$	algèbre des séries formelles à n indéterminées à coefficients dans A .
$A^p[[X_1, X_2, \dots, X_n]]$	module des séries entières formelles à n indéterminées à coefficients dans A .
$\widehat{\mathfrak{D}}, K[[D]]$	algèbre des opérateurs de composition.
T_α	opérateur de translation défini par α .
B_n	$n^{\text{ième}}$ polynôme de Bernoulli.
β_n	$n^{\text{ième}}$ nombre de Bernoulli.

Chapitre 3

$\mathcal{M}_p(E, F)$	espace vectoriel des applications p -linéaires de E dans F .
$\mathcal{P}_p(E, F)$	espace vectoriel des applications p -linéaires symétriques de E dans F .
$\mathcal{A}_p(E, F)$	espace vectoriel des applications p -linéaires alternées de E dans F .
U_p	extension $p^{\text{ième}}$ de l'application linéaire U .
M	opérateur de symétrisation.
A	opérateur d'antisymétrisation.
$\mathcal{M}_p(E)$	espace vectoriel des formes p -linéaires sur E .
$\mathcal{P}_p(E)$	espace vectoriel des formes p -linéaires symétriques sur E .
$\mathcal{A}_p(E)$	espace vectoriel des formes p -linéaires alternées sur E .
$y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$	produit tensoriel des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$.
$y_1^* \cdot y_2^* \dots y_p^*$	produit symétrique des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$.
$y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*$	produit extérieur des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$.
\mathcal{F}	ensemble des applications de $[1, p]$ dans $[1, n]$.
$(e_\chi)_{\chi \in \mathcal{F}}$	base de $\mathcal{M}_p(E)$ associée à une base de E .
\mathcal{S}	ensemble des applications s de $[1, n]$ dans \mathbf{N} telles que $\sum_{j=1}^n s(j) = p$.

$(e_s)_{s \in \mathcal{P}}$	base de $\mathcal{P}_p(E)$ associée à une base de E .
\mathcal{P}	ensemble des parties de $[1, n]$ à p éléments.
$(e_p)_{p \in \mathcal{P}}$	base de $\mathcal{A}_p(E)$ associée à une base de E .
$\text{Det}_B(x_1, x_2, \dots, x_n)$	déterminant dans la base B des vecteurs x_1, x_2, \dots, x_n .
$\text{Det } U$	déterminant de l'endomorphisme U .
$\text{SL}(E)$	groupe spécial linéaire de E .
$\text{Det } M$	déterminant de la matrice carrée M .
$\text{SL}(n, K)$	groupe spécial linéaire de type n .
\tilde{M}	matrice complémentaire de M .
$U_{a^*, b}$	application linéaire élémentaire associée à (a^*, b) .
$\text{Tr } U$	trace de l'endomorphisme U .
$\text{Tr } M$	trace de la matrice carrée M .
$f \otimes g$	produit tensoriel de f et de g .
$f \cdot g$	produit symétrique de f et de g .
$f \wedge g$	produit extérieur de f et de g .
$\mathcal{M}(E)$	algèbre des formes multilinéaires sur E .
$\mathcal{P}(E)$	algèbre des formes multilinéaires symétriques sur E .
$\mathcal{A}(E)$	algèbre des formes multilinéaires alternées sur E .

Chapitre 4

$\text{rang}(M)$	rang de la matrice M .
A_j^λ	affinité d'axe Ke_j de rapport λ relative à l'hyperplan $\langle e_j^*, x \rangle = 0$.
U_{jk}^λ	transvection d'axe Ke_k de rapport λ relative à l'hyperplan $\langle e_j^*, x \rangle = 0$.
P_b	polynôme d'interpolation de Lagrange associé à b .
H_n	$n^{\text{ième}}$ polynôme de Hilbert.
(S')	système linéaire.
(S)	système homogène associé à (S') .
$M = (\alpha_{ij})$	matrice associée à (S') .
a_j	$j^{\text{ième}}$ vecteur colonne de M .
$a_i'^*$	$i^{\text{ième}}$ vecteur ligne de M .
b	second membre de (S') .

Chapitre 5

π_U, π	polynôme minimal de U .
$E_{\lambda, r}(U), E_{\lambda, r}$	noyau de $(U - \lambda I_E)^r$.
$E_\lambda(U), E_\lambda$	noyau de $U - \lambda I_E$.
$F_\lambda(U), F_\lambda$	réunion des noyaux itérés de $U - \lambda I_E$.
$\text{sp}(U)$	spectre de U .
$n(\lambda)$	indice de la valeur propre λ .
$P_\lambda(U), P_\lambda$	projecteur spectral de U .

δ_M	polynôme caractéristique de la matrice M .
δ_U	polynôme caractéristique de l'endomorphisme U .
$m(\lambda)$	multiplicité de la valeur propre λ .
$\sigma_p(M)$	coefficient du polynôme caractéristique de M .
$\sigma_p(U)$	coefficient du polynôme caractéristique de U .
$F_{\mathbb{C}}$	extension complexe de l'espace vectoriel F .
$U_{\mathbb{C}}$	extension complexe de l'application linéaire U .
\bar{z}	conjugué du vecteur z .
\bar{V}	application linéaire-conjuguée de l'application linéaire V .
\bar{M}	matrice conjuguée de la matrice M .
$\pi_{\mathfrak{x}}$	annulateur du vecteur \mathfrak{x} .
$E_{\mathfrak{x}}$	sous-espace vectoriel de E stable par U engendré par \mathfrak{x} .
$J_{\lambda,n}$	matrice de Jordan de type (λ, n) .
$\exp(XU)$	exponentielle formelle de XU .

CHAPITRE 1

POLYNÔMES À UNE INDÉTERMINÉE

INTRODUCTION

Dans les neuf premiers paragraphes de ce chapitre, nous exposons la théorie des polynômes à une indéterminée à coefficients dans un corps commutatif.

Historiquement, on a d'abord appelé polynômes les fonctions d'une variable réelle de la forme

$$x \mapsto \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n.$$

On s'est ensuite aperçu que bien des propriétés des polynômes sont formelles, c'est-à-dire sont des propriétés des coefficients, et cette remarque a conduit à définir les polynômes comme suites de coefficients; c'est le point de vue maintenant universellement adopté. Les trois premiers paragraphes sont consacrés à la définition et aux propriétés élémentaires des polynômes et des fractions rationnelles à une indéterminée, et des fonctions polynomiales et rationnelles. Les résultats obtenus s'étendront aux polynômes et aux fractions rationnelles à plusieurs indéterminées à coefficients dans un anneau unitaire.

Le plan suivi dans les §§ 4 à 6 est calqué sur celui de l'étude de la divisibilité dans l'anneau \mathbf{Z} (cf. § I.2.3). Dans le § 4, nous exposons la théorie des idéaux de l'anneau des polynômes. Les résultats sont spéciaux au cas des polynômes à une seule indéterminée. C'est pourquoi nous consacrons le § 5 à la décomposition en facteurs irréductibles, qui se généralise au cas des polynômes et des fractions rationnelles à plusieurs indéterminées à coefficients dans un corps.

Dans le § 7, nous appliquons les résultats précédents à la décomposition des fractions rationnelles en parties principales. Dans cette étude, comme dans celle de la décomposition en facteurs irréductibles, nous avons d'abord voulu introduire la notion de partie principale, ou de valuation, d'une fraction rationnelle relativement à un polynôme irréductible donné, et montrer ensuite comment on peut reconstituer une fraction rationnelle à partir de ses parties principales, ou de ses valuations, relativement aux différents polynômes irréductibles.

Dans le § 7, nous exposons une théorie purement algébrique de la dérivation des polynômes et des fractions rationnelles. Pour mettre en évidence le lien entre cette théorie et les autres notions de dérivation (dérivation des séries entières formelles, dérivation des fonctions d'une variable réelle ou complexe), nous introduisons la notion de dérivation d'une algèbre. C'est dans le même esprit qu'est construit le § 8, consacré à l'étude locale des polynômes et des fractions rationnelles, et en particulier au développement limité des fractions rationnelles et à la formule de Taylor.

Dans le § 9, nous étudions les polynômes et fractions rationnelles à coefficients dans un corps algébriquement clos, et nous démontrons le théorème fondamental de l'algèbre (théorème de D'Alembert-Gauss).

La théorie des classes résiduelles dans les anneaux de polynômes, liée de manière très étroite à la théorie des extensions de corps, sera exposée au chapitre III.3.

Enfin, dans le dernier paragraphe, nous exposons la théorie des séries entières formelles à une indéterminée à coefficients dans un corps commutatif. L'utilité de cette notion apparaît dans de très nombreux domaines de l'analyse : séries entières à une variable, fonctions transcendantes élémentaires, équations différentielles; elle apparaît aussi à travers les notions de fonctions d'une variable entière et de série génératrice, dans l'étude de problèmes combinatoires : équations aux différences finies, arithmétique additive. La théorie des séries de Dirichlet formelles, commode pour l'arithmétique multiplicative, est rejetée en exercice.

Dans tout ce chapitre, K désigne un corps commutatif.

§ 1. POLYNÔMES A UNE INDÉTERMINÉE

DÉFINITION 1.1. — **Algèbre des polynômes à une indéterminée à coefficients dans un corps.** — Soient K un corps commutatif, $K^{(\mathbb{N})}$ l'espace vectoriel des suites d'éléments de K à support fini, c'est-à-dire dont les termes sont nuls à partir d'un certain rang (cf. § I.3.4), et $(e_n)_{n \in \mathbb{N}}$ la base canonique de $K^{(\mathbb{N})}$. On considère la structure de K -algèbre définie sur $K^{(\mathbb{N})}$ par la table de multiplication

$$(1) \quad e_i \cdot e_j = e_{i+j},$$

pour tout couple (i, j) d'entiers naturels.

Il résulte immédiatement de la formule (1) et de la proposition I.3.38 que cette algèbre est associative et commutative, et qu'elle admet e_0 pour élément unité. Cette algèbre unitaire se note $\mathbf{P}(K)$.

Ainsi, tout élément P de cette algèbre s'écrit d'une manière et d'une seule sous la forme

$$P = \sum_{n \in \mathbb{N}} \alpha_n e_n,$$

où, pour tout entier naturel n , α_n est un scalaire; ce qu'on écrit encore

$$P = \sum_{n=0}^{+\infty} \alpha_n e_n.$$

Les scalaires α_n s'appellent coefficients de P . Les éléments de $\mathbf{P}(K)$ s'appellent polynômes à coefficients dans K , et l'algèbre unitaire $\mathbf{P}(K)$ s'appelle algèbre des polynômes à coefficients dans K .

Un polynôme dont tous les coefficients sauf au plus un sont nuls est appelé monôme.

L'application qui à tout scalaire α associe le monôme αe_0 est un isomorphisme du corps K sur la sous-algèbre unitaire Ke_0 de $\mathbf{P}(K)$. On identifiera désormais K et Ke_0 . En particulier, e_0 sera noté 1, où 1 désigne l'élément unité du corps K .

Le monôme e_1 s'appelle indéterminée, et se note souvent X . Pour tout entier naturel n ,

$$(2) \quad e_n = X^n.$$

L'algèbre unitaire $P(K)$ se note alors $K[X]$. C'est pourquoi l'algèbre unitaire $P(K)$ s'appelle encore *algèbre des polynômes à une indéterminée à coefficients dans K* .

Avec ces notations, les monômes $1, X, X^2, \dots, X^n, \dots$ constituent la base canonique de l'espace vectoriel $K[X]$. Le produit du polynôme $P = \sum_{p=0}^{+\infty} \alpha_p X^p$ et du polynôme $Q = \sum_{q=0}^{+\infty} \beta_q X^q$ n'est autre que le polynôme $\sum_{n=0}^{+\infty} \gamma_n X^n$, où, pour tout entier naturel n ,

$$\gamma_n = \sum_{p+q=n} \alpha_p \beta_q = \alpha_0 \beta_n + \alpha_1 \beta_{n-1} + \dots + \alpha_p \beta_{n-p} + \dots + \alpha_n \beta_0.$$

PROPOSITION 1.1. — Propriétés de l'algèbre des polynômes. — Soit $K[X]$ l'algèbre des polynômes à coefficients dans un corps K .

1. La sous-algèbre unitaire de $K[X]$ engendrée par X n'est autre que $K[X]$.
2. L'algèbre $K[X]$ possède la propriété universelle suivante :

Pour toute K -algèbre associative unitaire E et pour tout élément a de E , il existe un morphisme f et un seul de l'algèbre unitaire $K[X]$ dans l'algèbre unitaire E tel que

$$(3) \quad f(X) = a.$$

Alors, pour tout polynôme $P = \sum_{n=0}^{+\infty} \alpha_n X^n,$

$$(4) \quad f(P) = \sum_{n=0}^{+\infty} \alpha_n a^n.$$

L'assertion 1 est immédiate.

Assertion 2. — Unicité de f . — Puisque f est un morphisme d'algèbres unitaires, $f(P)$ est nécessairement donné par la formule (4). L'unicité de f en découle.

Existence de f . — L'application f définie par la formule (4) est visiblement linéaire. Pour montrer que f est un morphisme d'algèbres, il suffit donc de prouver que, pour tout couple (p, q) d'entiers naturels,

$$f(X^p X^q) = f(X^p) \cdot f(X^q),$$

ce qui est immédiat.

REMARQUE. — Nous étudierons plus en détail le morphisme f au chapitre III.3.

Pour définir le degré et la valuation d'un polynôme, il est commode d'introduire auparavant la notion suivante : étant donné l'ensemble totalement ordonné \mathbb{N} , nous noterons $\bar{\mathbb{N}}$ l'ensemble totalement ordonné défini au § I.1.5, en adjoignant à \mathbb{N} deux éléments, notés $+\infty$ et $-\infty$. Nous conviendrons de plus que pour tout entier naturel n ,

$$\begin{aligned} n + (+\infty) &= +\infty + n = +\infty \\ n + (-\infty) &= -\infty + n = -\infty, \end{aligned}$$

et que

$$\begin{aligned} +\infty + \infty &= +\infty \\ -\infty - \infty &= -\infty. \end{aligned}$$

Nous pouvons alors poser la

DÉFINITION 1.2. — Degré d'un polynôme. — Soit $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ un élément de $K[X]$.

— Si P est non nul, on appelle degré de P le plus grand des entiers n tels que α_n soit non nul.

— Si P est nul, on appelle degré de P l'élément $-\infty$.

Le degré d'un polynôme P se note $d^0(P)$; c'est un élément de $\bar{\mathbb{N}}$, différent de $+\infty$.

PROPOSITION 1.2. — Degré d'une somme, degré d'un produit. — Soient P et Q deux éléments de $K[X]$, et α un élément de K^* . Alors :

$$d^0(P + Q) \leq \sup [d^0(P), d^0(Q)],$$

avec égalité si $d^0(P) \neq d^0(Q)$;

$$\begin{aligned} d^0(\alpha P) &= d^0(P) \\ d^0(PQ) &= d^0(P) + d^0(Q). \end{aligned}$$

La vérification est immédiate. Évidemment, les conventions concernant le degré du polynôme nul ont été précisément choisies pour que les formules précédentes soient vraies sans aucune restriction sur P et Q .

REMARQUE. — Si $d^0(P) = d^0(Q)$, il se peut que $d^0(P + Q)$ soit strictement inférieur à $\sup [d^0(P), d^0(Q)]$. C'est le cas lorsque $P = X^2$, et $Q = X - X^2$, par exemple.

DÉFINITION 1.3. — Valuation d'un polynôme. — Soit $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ un élément de $K[X]$.

— Si P est non nul, on appelle valuation de P le plus petit des entiers n tels que α_n soit non nul.

— Si P est nul, on appelle valuation de P l'élément $+\infty$.

La valuation d'un polynôme P se note $v_0(P)$; c'est un élément de $\overline{\mathbb{N}}$, différent de $-\infty$.

PROPOSITION 1.3. — **Valuation d'une somme, valuation d'un produit.** — Soient P et Q deux éléments de $K[X]$, et α un élément de K^* . Alors :

$$v_0(P + Q) \geq \inf [v_0(P), v_0(Q)],$$

avec égalité si $v_0(P) \neq v_0(Q)$;

$$\begin{aligned} v_0(\alpha P) &= v_0(P) \\ v_0(PQ) &= v_0(P) + v_0(Q). \end{aligned}$$

Voici une application simple de ces notions :

Pour tout entier naturel n , l'ensemble des polynômes de degré inférieur ou égal à n est un sous-espace vectoriel de $K[X]$; de même pour l'ensemble des polynômes de valuation supérieure ou égale à n .

REMARQUE. — Il n'en est pas de même pour l'ensemble des polynômes de degré égal à n , ou de valuation égale à n : en effet, X^n et $-X^n$ sont de degré n , et de valuation n , tandis que $X^n - X^n = 0$.

PROPOSITION 1.4. — **Familles libres de polynômes.** — Soit $(P_i)_{i \in I}$ une famille d'éléments non nuls de $K[X]$. Si l'application f (resp. g) de I dans \mathbb{N} qui à tout élément i de I associe $d^0(P_i)$ (resp. $v_0(P_i)$) est injective, alors la famille $(P_i)_{i \in I}$ est une famille libre de $K[X]$.

Supposons en effet par l'absurde qu'il existe une relation linéaire non triviale $\sum_{i \in I} \alpha_i P_i = 0$ entre les éléments de la famille $(P_i)_{i \in I}$. L'ensemble J des éléments i de I tels que α_i soit non nul est fini non vide.

Considérons le cas où f est injective. Il existe alors un élément i_0 et un seul de J tel que pour tout élément i de J différent de i_0 , $d^0(P_i) < d^0(P_{i_0})$; il en résulte que $d^0\left(\sum_{i \in J} \alpha_i P_i\right) = d^0(P_{i_0})$, ce qui contredit la relation $\sum_{i \in J} \alpha_i P_i = 0$.

Le cas où g est injective se traite de même.

COROLLAIRE 1. — Soit n un entier naturel. Toute suite (P_0, P_1, \dots, P_n) de $n + 1$ éléments de $K[X]$ tels que pour tout $i \in [0, n]$, $d^0(P_i) = i$, est une base de l'espace vectoriel des éléments de $K[X]$ de degré inférieur ou égal à n .

En effet, la famille $(1, X, \dots, X^n)$ est une base de cet espace vectoriel, qui est donc de dimension $n + 1$. D'après la proposition précédente, la famille (P_0, P_1, \dots, P_n) est libre. Comme elle possède $n + 1$ éléments, c'est une base de l'espace vectoriel considéré (cf. cor. 4 du th. I.3.4).

COROLLAIRE 2. — Soit $(P_i)_{i \in I}$ une famille d'éléments non nuls de $K[X]$. Si l'application $i \mapsto d^0(P_i)$ de I dans \mathbb{N} est surjective (resp. bijective), la famille $(P_i)_{i \in I}$ est génératrice (resp. est une base).

Il suffit de prouver que si cette application est surjective, tout monôme X^n appartient au sous-espace engendré par les polynômes P_i . Considérons pour cela le sous-espace de $K[X]$ constitué des polynômes de degré inférieur ou égal à n ; il résulte aussitôt du corollaire 1 que les polynômes P_i dont le degré est inférieur ou égal à n forment une famille génératrice de cet espace vectoriel, d'où le résultat.

EXEMPLES.

1. Soit (α_n) une suite d'éléments de K . Posons $P_n = (X - \alpha_n)^n$; alors les polynômes $P_0 = 1, P_1, P_2, \dots, P_n, \dots$ forment une base de $K[X]$.

2. Soit (β_n) une suite d'éléments de K . Posons $Q_n = \prod_{p=1}^n (X - \beta_p)$; alors les polynômes $Q_0 = 1, Q_1, Q_2, \dots, Q_n, \dots$ forment une base de $K[X]$.

REMARQUE. — Le corollaire 2 n'est pas vrai dans le cas des valuations; cf. exercice 1.

Exercices conseillés : 2 à 8.

§ 2. FRACTIONS RATIONNELLES A UNE INDÉTERMINÉE

PROPOSITION 1.5. — Intégrité de l'anneau des polynômes.

1. *L'anneau $K[X]$ des polynômes à une indéterminée X à coefficients dans K est intègre.*

2. *Dans cet anneau, les seuls éléments inversibles sont les polynômes de degré 0.*

Assertion 1. — Nous savons déjà que $K[X]$ est un anneau commutatif unitaire. Il reste à montrer que si P et Q sont deux polynômes non nuls, le polynôme PQ est non nul. Cela résulte aussitôt de ce que $d^0(P) \geq 0$ et $d^0(Q) \geq 0$; d'où $d^0(PQ) = d^0(P) + d^0(Q) \geq 0$.

Assertion 2. — Il est évident que les polynômes de degré 0, c'est-à-dire les scalaires non nuls, sont inversibles, puisque K est un corps. Réciproquement, soit P un polynôme inversible; il existe un polynôme Q tel que $PQ = 1$. Donc $d^0(P) + d^0(Q) = 0$, ce qui impose $d^0(P) = d^0(Q) = 0$.

Il en résulte que tout polynôme non nul est un élément régulier de l'anneau $K[X]$, et que l'ensemble $K[X]^*$, constitué des polynômes non nuls, est stable pour la multiplication.

Rappelons que, conformément aux définitions du § I.2.2, un polynôme A divise un polynôme B s'il existe un polynôme Q tel que $B = AQ$, ce qu'on note $A \mid B$. Nous savons qu'on introduit ainsi une relation binaire dans $K[X]$, réflexive et transitive, et que si un polynôme A divise les polynômes B_1, B_2, \dots, B_n , alors A divise le polynôme $\sum_{i=1}^n P_i B_i$, quels que soient les polynômes P_1, P_2, \dots, P_n .

Considérons enfin deux polynômes non nuls A et B , et cherchons une condition nécessaire et suffisante pour que A divise B et B divise A . Nous savons (cf. prop. I.2.23) que cette relation équivaut à l'existence d'un élément inversible Q de $K[X]$ tel que $A = QB$, c'est-à-dire, d'après la proposition 1.5, à l'existence d'un scalaire non nul c tel que $A = cB$.

Pour éviter ces facteurs scalaires, on introduit la notion de polynôme unitaire :

DÉFINITION 1.4. — Polynômes unitaires. — *On appelle coefficient dominant d'un élément non nul P de $K[X]$ le coefficient de son monôme de plus haut degré.*

On dit qu'un polynôme P est unitaire si P est non nul, et si son coefficient dominant est égal à 1.

PROPOSITION 1.6. — Propriétés des polynômes unitaires.

1. *Tout polynôme P non nul s'écrit d'une manière et d'une seule sous la forme $P = \alpha P_1$, où α est un scalaire non nul, et où P_1 est un polynôme unitaire; le polynôme P_1 s'appelle polynôme unitaire associé à P .*

2. *Soient P et Q deux polynômes non nuls, ayant P_1 et Q_1 pour polynômes unitaires associés; alors la relation $P \mid Q$ est équivalente à la relation $P_1 \mid Q_1$.*

3. *Dans l'ensemble des polynômes unitaires, la relation de divisibilité est une relation d'ordre.*

4. *Soient P et Q deux polynômes non nuls; alors le coefficient dominant de PQ est égal au produit des coefficients dominants de P et de Q , et le polynôme unitaire associé à PQ est le produit des polynômes unitaires associés à P et à Q . En particulier, l'ensemble des polynômes unitaires est stable pour la multiplication.*

Nous avons vu (cf. prop. 1.5) que l'anneau des polynômes à une indéterminée à coefficients dans un corps K est un anneau intègre, et n'est pas un corps. Nous allons donc appliquer le théorème d'existence du corps des quotients (cf. th. I.2.7), qui nous a déjà permis de construire le corps \mathbb{Q} des nombres rationnels à partir de l'anneau \mathbb{Z} des entiers rationnels. Nous obtenons ainsi le

THÉORÈME 1.1. — Corps des fractions rationnelles. — *Soit $K[X]$ l'anneau des polynômes à coefficients dans K . Il existe un corps commutatif, appelé corps des fractions rationnelles à coefficients dans K et noté $K(X)$, possédant les propriétés suivantes :*

a) *L'anneau $K[X]$ est un sous-anneau unitaire du corps $K(X)$.*

b) *Le corps $K(X)$ est engendré par l'anneau $K[X]$, c'est-à-dire que tout élément R de $K(X)$ peut s'écrire sous la forme $R = PQ^{-1}$, où P et Q sont des polynômes, Q étant non nul.*

Deux tels corps sont isomorphes.

Comme pour les nombres rationnels, nous noterons aussi les fractions rationnelles par le symbole $R = \frac{P}{Q}$, ce qui ne présente pas d'inconvénient, puisque la multiplication est commutative.

Voici maintenant quelques définitions et propriétés des polynômes qui s'étendent aisément aux fractions rationnelles :

L'application de $K \times K(X)$ dans $K(X)$ qui associe au couple (α, R) la fraction rationnelle αR (α étant considéré comme un polynôme) permet de munir $K(X)$ d'une structure d'algèbre sur le corps K . En particulier, les fractions rationnelles forment un espace vectoriel sur K , et nous pourrions donc parler de fractions rationnelles linéairement indépendantes, de bases dans l'espace des fractions rationnelles, etc.

Pour définir le degré et la valuation d'une fraction rationnelle, on introduit l'ensemble totalement ordonné $\bar{\mathbb{Z}}$ défini au § I.1.5, obtenu en adjoignant à \mathbb{Z} les éléments $+\infty$ et $-\infty$. Nous conviendrons de plus que pour tout entier rationnel, n ,

$$\begin{aligned} n + (+\infty) &= +\infty + n = +\infty \\ n + (-\infty) &= -\infty + n = -\infty, \end{aligned}$$

et que

$$\begin{aligned} +\infty + \infty &= +\infty \\ -\infty - \infty &= -\infty. \end{aligned}$$

Nous pouvons alors énoncer la

PROPOSITION 1.7. — Degré d'une fraction rationnelle.

1. *Il existe une application et une seule, appelée degré, notée d^0 , de $K(X)$ dans $\mathbb{Z} \cup \{-\infty\}$, prolongeant l'application $P \mapsto d^0(P)$ de $K[X]$ dans $\mathbb{N} \cup \{-\infty\}$, et possédant la propriété suivante :*

Pour tout couple (R, R') d'éléments de $K(X)$,

$$(1) \quad d^0(RR') = d^0(R) + d^0(R').$$

2. *Si une fraction rationnelle R est écrite sous la forme $R = \frac{P}{Q}$, où $P \in K[X]$ et où $Q \in K[X]^*$,*

$$(2) \quad d^0(R) = d^0(P) - d^0(Q).$$

3. *Enfin, si R et R' sont deux éléments de $K(X)$,*

$$d^0(R + R') \leq \sup [d^0(R), d^0(R')],$$

avec égalité si $d^0(R) \neq d^0(R')$.

Supposons d'abord qu'une telle application existe, et considérons une fraction rationnelle $R = \frac{P}{Q}$, où $P \in K[X]$, et $Q \in K[X]^*$: il résulte aussitôt de la formule (1) que le degré de R est nécessairement donné par la formule (2), ce qui prouve l'unicité de l'application degré.

Pour voir son existence, nous définissons le degré d'une fraction rationnelle R par la formule (2), ce qui est licite, car le nombre $d^0(P) - d^0(Q)$ ne

dépend que de R : écrivons R sous la forme $R = \frac{P'}{Q'}$, où $P' \in K[X]$, et $Q' \in K[X]^*$; la relation $PQ' = P'Q$ implique la suivante :

$$d^0(P) - d^0(Q) = d^0(P') - d^0(Q').$$

Les propriétés du degré d'une fraction rationnelle s'établissent alors aisément.

REMARQUE. — Nous définirons la valuation d'une fraction rationnelle au § 3.

§ 3. FONCTIONS POLYNOMIALES ET RATIONNELLES

Jusqu'à présent, nous avons développé la théorie des polynômes considérés comme suites de coefficients; nous faisons maintenant le lien avec le point de vue classique des fonctions polynomiales.

DÉFINITION 1.5. — **Substitutions dans un polynôme.** — Soient $K[X]$ l'algèbre des polynômes à une indéterminée à coefficients dans K , E une K -algèbre associative unitaire, et a un élément de E . On sait (cf. prop. 1) qu'il existe un morphisme δ_a et un seul de l'algèbre unitaire $K[X]$ dans l'algèbre unitaire E tel que $\delta_a(X) = a$. Soit P un élément de $K[X]$, écrit sous la forme

$$P = \sum_{n=0}^{+\infty} \alpha_n X^n ;$$

alors

$$\delta_a(P) = \sum_{n=0}^{+\infty} \alpha_n a^n.$$

C'est pourquoi on dit que l'élément $\delta_a(P)$ est obtenu en substituant l'élément a de E à l'indéterminée X dans le polynôme P .

DÉFINITION 1.6. — **Fonctions polynomiales.** — Soit E une K -algèbre associative unitaire. Étant donné un élément $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ de $K[X]$, on note \tilde{P} l'appli-

cation de E dans E qui à tout élément a de E associe l'élément $\delta_a(P) = \sum_{n=0}^{+\infty} \alpha_n a^n$.

Soit maintenant B une partie de E . On dit qu'une application f de B dans E est une fonction polynomiale s'il existe un élément P de $K[X]$ tel que, pour tout élément a de B , $f(a) = \tilde{P}(a)$.

Étant donné un élément P de $K[X]$, la fonction \tilde{P} s'appelle fonction polynomiale sur E associée à P ; pour tout élément a de E , l'élément $\tilde{P}(a)$, valeur au point a de la fonction polynomiale P , s'appelle encore valeur de \tilde{P} en a .

REMARQUE. — Si $E = K$, et si le polynôme P est de la forme $P = \alpha$, où $\alpha \in K$, la fonction polynomiale \tilde{P} associée à P est la fonction constante α ; c'est pourquoi les polynômes de cette forme sont appelés *polynômes constants*.

PROPOSITION 1.8. — **Propriétés des substitutions dans les polynômes.** — Soit E une K -algèbre associative unitaire. Alors l'application de $K[X]$ dans l'algèbre $\mathcal{F}(E)$ des applications de E dans E qui à tout polynôme P associe la fonction polynomiale \tilde{P} est un morphisme d'algèbres unitaires.

EXEMPLES.

1. On prend pour E le corps K lui-même. Lorsque $K = \mathbf{R}$, la notion de fonction polynomiale sur \mathbf{R} définie dans ce paragraphe coïncide avec celle qui a été introduite au § I.4.9.

2. Plus généralement, on peut prendre pour E un corps K' contenant K comme sous-corps. Le cas où $K' = \mathbf{C}$ et $K = \mathbf{R}$ est fréquent dans les applications.

3. On prend pour E l'algèbre $\mathcal{L}(F)$ des endomorphismes d'un espace vectoriel F sur K , ou encore l'algèbre $\mathbf{M}_n(K)$ des matrices carrées d'ordre n à éléments dans K .

4. **Composé de deux polynômes.** — On prend pour E l'algèbre $K[X]$ elle-même. Étant donné un élément Q de $K[X]$, il existe un endomorphisme et un seul de l'algèbre unitaire $K[X]$ transformant X en Q ; cet endomorphisme s'obtient en associant à tout élément $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ de $K[X]$ le polynôme

$\tilde{P}(Q) = \sum_{n=0}^{+\infty} \alpha_n Q^n$. Ce dernier polynôme est donc obtenu en substituant Q à X dans P ; il est encore appelé *composé* du polynôme Q et du polynôme P , et noté $P \circ Q$.

Ainsi, l'application $P \mapsto P \circ Q$ est un endomorphisme de l'algèbre unitaire $K[X]$.

La notation $P \circ Q$ est suggérée par la

PROPOSITION 1.9. — **Propriétés de la composition des polynômes.** — Pour toute K -algèbre associative unitaire E , la fonction polynomiale sur E associée au composé $P \circ Q$ de deux polynômes P et Q n'est autre que l'application composée $\tilde{P} \circ \tilde{Q}$.

Autrement dit, pour tout élément a de E ,

$$(1) \quad (\widetilde{P \circ Q})(a) = \tilde{P}[\tilde{Q}(a)].$$

En effet, d'une part l'application $P \mapsto \tilde{P}[\tilde{Q}(a)]$ est un morphisme d'algèbres unitaires. D'autre part, l'application $P \mapsto P \circ Q$ est un morphisme d'algèbres unitaires; il en est donc de même de l'application $P \mapsto (\widetilde{P \circ Q})(a)$. Par suite, il suffit de prouver la relation (1) lorsque $P = X$, ce qui est trivial.

COROLLAIRE. — **Associativité de la composition des polynômes.** — Pour tout triplet (P, Q, R) d'éléments de $K[X]$,

$$(P \circ Q) \circ R = P \circ (Q \circ R).$$

Il suffit d'appliquer la proposition au cas où $E = K[X]$ et où $a = R$.

REMARQUE 1. — Soient P, Q et Q' trois éléments de $K[X]$; on se gardera de croire que $P \circ (Q + Q') = P \circ Q + P \circ Q'$. (On examinera par exemple le cas où le polynôme P est constant.)

REMARQUE 2. — Pour obtenir le polynôme composé $P \circ Q$, on peut utiliser le procédé mnémotechnique suivant : on écrit le polynôme P en notant Y l'indéterminée, c'est-à-dire en posant $Y = e_1$; ainsi P s'écrit sous la forme $P = \sum_{n=0}^{+\infty} \alpha_n Y^n$. On remplace ensuite Y par Q dans cette expression. C'est pourquoi faire la substitution de Q à X dans P s'appelle encore faire le changement de variable $Y = Q(X)$.

Le polynôme $P \circ Q$ se note encore $P(Q)$. En particulier, lorsque $Q = X$, $P(Q) = \sum_{n=0}^{+\infty} \alpha_n X^n = P$; ainsi, $P(X) = P$.

EXEMPLE. — **Polynômes pairs, polynômes impairs.** — Soit P un polynôme. On note \check{P} le polynôme composé $P(-X)$. On dit que P est *pair* si $\check{P} = P$, *impair* si $\check{P} = -P$.

Si K est de caractéristique différente de 2, les polynômes pairs et les polynômes impairs constituent deux sous-espaces vectoriels supplémentaires dans $K[X]$. Pour que P soit pair (resp. impair), il faut et il suffit que tous ses coefficients d'indice impair (resp. pair) soient nuls.

Dans la suite de ce paragraphe, nous prendrons pour l'algèbre E le corps K lui-même.

DÉFINITION 1.7. — **Racines d'un polynôme.** — On dit qu'un scalaire α est une *racine* d'un élément P de $K[X]$ si la valeur de P au point α est égale à 0, c'est-à-dire si $\tilde{P}(\alpha) = 0$.

PROPOSITION 1.10. — **Caractérisation des racines d'un polynôme.** — Pour qu'un scalaire α soit racine d'un élément P de $K[X]$, il faut et il suffit que P soit divisible par $X - \alpha$.

Cette condition est évidemment suffisante. Pour montrer qu'elle est nécessaire, nous allons prouver que pour tout polynôme P , $X - \alpha$ divise $P - \tilde{P}(\alpha)$. Par linéarité, nous nous ramenons aussitôt à prouver que $X - \alpha$ divise $X^n - \alpha^n$ pour tout entier n strictement positif, ce qui est une conséquence de la proposition I.2.34.

Soient maintenant P un polynôme non nul, et α un scalaire. L'ensemble des entiers naturels m tels que $(X - \alpha)^m$ divise P contient 0, et est majoré par le degré de P . (On rappelle que, par convention, $(X - \alpha)^0 = 1$.) Cet ensemble possède donc un plus grand élément.

DÉFINITION 1.8. — Valuation d'un polynôme en un point. — Soient P un élément de $K[X]$, et α un scalaire.

— Si P est non nul, on appelle valuation de P au point α le plus grand des entiers m tels que $(X - \alpha)^m$ divise P .

— Si P est nul, on appelle valuation de P au point α l'élément $+\infty$. La valuation d'un polynôme P au point α se note $v_\alpha(P)$.

Cette notation est licite, car lorsque $\alpha = 0$, la notion de valuation au point α coïncide avec la notion de valuation donnée dans la définition 1.3.

PROPOSITION 1.11. — Propriétés de la valuation en un point.

1. Soit P un polynôme non nul; pour que $v_\alpha(P)$ soit égal à un entier naturel m , il faut et il suffit qu'il existe un polynôme Q tel que

$$P = (X - \alpha)^m Q \quad \text{et} \quad \tilde{Q}(\alpha) \neq 0.$$

2. Soient P et Q deux éléments de $K[X]$, et β un élément de K^* . Alors, pour tout point α de K :

$$v_\alpha(P + Q) \geq \inf [v_\alpha(P), v_\alpha(Q)],$$

avec égalité si $v_\alpha(P) \neq v_\alpha(Q)$;

$$\begin{aligned} v_\alpha(\beta P) &= v_\alpha(P), & v_\alpha(PQ) &= v_\alpha(P) + v_\alpha(Q), \\ v_\alpha(X - \beta) &= 0 \quad \text{si} \quad \beta \neq \alpha, & \text{et} \quad v_\alpha(X - \alpha) &= 1. \end{aligned}$$

Assertion 1. — Il est immédiat que $v_\alpha(P)$ est égal à m si et seulement s'il existe un polynôme Q non divisible par $X - \alpha$, et tel que $P = (X - \alpha)^m Q$. L'assertion 1 résulte alors de la proposition 1.10.

Assertion 2. — Posons $p = v_\alpha(P)$ et $q = v_\alpha(Q)$. Écartons le cas trivial où l'un des deux polynômes P et Q est nul : il existe alors deux polynômes P_1 et Q_1 tels que

$$\begin{aligned} P &= (X - \alpha)^p P_1, & \text{et} \quad \tilde{P}_1(\alpha) &\neq 0 \\ Q &= (X - \alpha)^q Q_1, & \text{et} \quad \tilde{Q}_1(\alpha) &\neq 0. \end{aligned}$$

L'assertion en découle aisément; calculons par exemple $v_\alpha(PQ)$:

$$PQ = (X - \alpha)^{p+q} R, \quad \text{où} \quad R = P_1 Q_1.$$

Comme K est intègre, $\tilde{R}(\alpha) = \tilde{P}_1(\alpha)\tilde{Q}_1(\alpha) \neq 0$. Donc $v_\alpha(PQ) = p + q$.

DÉFINITION 1.9. — Ordre de multiplicité d'une racine. — Soit P un polynôme non nul. Lorsqu'un scalaire α est racine de P , l'entier $v_\alpha(P)$ s'appelle encore ordre de multiplicité de la racine α . Une racine α de P dont l'ordre de multiplicité est égal à un entier m est appelée plus simplement racine d'ordre m du polynôme P .

Une racine α de P d'ordre 1 est dite simple. Une racine α de P d'ordre strictement supérieur à 1 est dite multiple. Enfin, une racine α de P d'ordre 2 (resp. 3, 4, etc.) est dite double (resp. triple, quadruple, etc.).

Avec cette nouvelle terminologie, l'assertion 1 de la proposition 1.11 peut encore s'énoncer : pour qu'une racine α d'un polynôme P soit d'ordre m , il faut et il suffit qu'il existe un polynôme Q tel que

$$P = (X - \alpha)^m Q, \quad \text{et} \quad \tilde{Q}(\alpha) \neq 0.$$

Ce qui peut se généraliser de la façon suivante :

THÉORÈME 1.2. — Divisibilité par un produit de facteurs du premier degré. — Soient P un polynôme non nul, et $(\alpha_1, \alpha_2, \dots, \alpha_r)$ une suite de r éléments de K distincts deux à deux. Si, pour tout $i \in [1, r]$, le scalaire α_i est racine d'ordre n_i de P , alors P est divisible par le polynôme $Q = \prod_{i=1}^r (X - \alpha_i)^{n_i}$. De manière plus précise, il existe un polynôme R et un seul tel que $P = QR$; alors, pour tout entier $i \in [1, r]$, $\tilde{R}(\alpha_i) \neq 0$.

En particulier, si le nombre $\sum_{i=1}^r n_i$ est égal au degré de P , il existe un scalaire non nul β et un seul tel que $P = \beta Q$.

L'unicité du polynôme R est immédiate, puisque l'anneau $K[X]$ est intègre. Nous allons démontrer l'existence de R par récurrence sur l'entier r . Lorsque $r = 1$, nous venons de l'établir. Soit donc r un entier > 1 ; supposons qu'il existe un polynôme R' tel que $P = Q'R'$, où $Q' = \prod_{i=1}^{r-1} (X - \alpha_i)^{n_i}$, et que, pour tout $i \in [1, r-1]$, $\tilde{R}'(\alpha_i) \neq 0$. Comme α_r est distinct de α_i pour tout $i < r$,

$$v_{\alpha_r}(P) = v_{\alpha_r}(Q') + v_{\alpha_r}(R') = v_{\alpha_r}(R').$$

Donc α_r est racine d'ordre n_r de R' ; il en découle qu'il existe un polynôme R tel que $R' = (X - \alpha_r)^{n_r} R$, et que $R(\alpha_r) \neq 0$. Ce polynôme R convient visiblement.

Nous en déduisons immédiatement le résultat fondamental suivant :

THÉORÈME 1.3. — Propriétés de l'ensemble des racines d'un polynôme. — Soit P un polynôme à coefficients dans K . S'il existe r scalaires $\alpha_1, \alpha_2, \dots, \alpha_r$ distincts deux à deux tels que $\sum_{i=1}^r v_{\alpha_i}(P) > d^0(P)$, alors P est nul.

Autrement dit : si P est un polynôme non nul, de degré inférieur ou égal à n , où $n \in \mathbb{N}$, l'ensemble de ses racines est fini, et la somme des ordres de multiplicité de ces racines est inférieure ou égale à n .

COROLLAIRE 1.

Soit P un polynôme à coefficients dans K . Si P est de degré $n \geq 0$, P a au plus n racines.

En particulier, tout polynôme dont l'ensemble des racines est infini est nul.

COROLLAIRE 2. — Lien entre polynômes et fonctions polynomiales.

1. Soient P et Q deux polynômes à coefficients dans K , de degré inférieur à n , où $n \in \mathbb{N}$. S'il existe $n + 1$ scalaires $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ distincts deux à deux tels que, pour tout entier $i \in [1, n + 1]$, $\tilde{P}(\alpha_i) = \tilde{Q}(\alpha_i)$, alors $P = Q$.

2. Soient K un corps infini, B une partie infinie de K , f et g deux fonctions polynomiales sur K . Si, pour tout élément β de B , $f(\beta) = g(\beta)$, alors $f = g$.

Assertion 1. — Il suffit d'appliquer le corollaire 1 au polynôme $P - Q$.

L'assertion 2 s'en déduit aussitôt.

COROLLAIRE 3. — Injectivité de l'application $P \mapsto \tilde{P}$.

— Si le corps K est infini, le morphisme de l'algèbre unitaire $K[X]$ dans l'algèbre unitaire $\mathcal{F}(K)$ qui associe au polynôme P la fonction polynomiale \tilde{P} est injectif. C'est en particulier le cas lorsque le corps K est de caractéristique 0.

— Si le corps K est fini, et si l'on désigne par $\alpha_1, \alpha_2, \dots, \alpha_p$ ses éléments, alors le noyau du morphisme précédent est l'idéal de $K[X]$ engendré par le poly-

nôme $N = \prod_{i=1}^p (X - \alpha_i)$.

Soit en effet P un élément du noyau de ce morphisme. Cela revient à dire que tout élément de K est racine du polynôme P .

— Si K est infini, le corollaire 1 montre aussitôt que P est nul.

— Si K est fini, le théorème 1.2 montre que P est divisible par N , c'est-à-dire qu'il appartient à l'idéal engendré par N . Réciproquement, il est immédiat que tout polynôme appartenant à cet idéal est dans le noyau du morphisme $P \mapsto \tilde{P}$.

EXEMPLE. — Prenons pour K le corps $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo un nombre premier p . Alors les polynômes P à coefficients dans K tels que $\tilde{P} = 0$ sont les multiples du polynôme $N = X(X - \dot{1}) \dots (X - \dot{p} + \dot{1})$.

REMARQUE 1. — L'étude des fonctions polynomiales sur les corps finis est esquissée dans l'exercice 10.

REMARQUE 2. — Lorsque le corps K est infini, le corollaire 3 montre qu'on peut identifier sans inconvénient un polynôme P à la fonction polynomiale \tilde{P} qu'il définit sur K . La valeur $\tilde{P}(\alpha)$ de P en un point α de K sera désormais notée $P(\alpha)$.

Lorsque aucune erreur n'est à craindre, nous emploierons cette notation même quand le corps K est fini.

REMARQUE 3. — Le polynôme à coefficients réels $X^2 + 1$ n'admet pas de racine. Or le polynôme à coefficients complexes $X^2 + 1$ admet deux racines, à savoir i et $-i$. On voit apparaître sur cet exemple l'intérêt de la définition suivante :

DÉFINITION 1.10. — Extension du corps des scalaires. — Soient K un corps commutatif, et K' un corps commutatif contenant K comme sous-corps. Tout élément de $K[X]$ est un élément de $K'[X]$; l'algèbre $K[X]$ est une sous-algèbre unitaire de la K -algèbre unitaire $K'[X]$.

Soit alors P un polynôme à coefficients dans K . On dit qu'un élément a de K' est une racine de P dans K' si c'est une racine de P , considéré comme polynôme à coefficients dans K' .

Si $P = \sum_{n=0}^{+\infty} \alpha_n X^n$, cela signifie donc que $\sum_{n=0}^{+\infty} \alpha_n a^n = 0$, c'est-à-dire que $\tilde{P}(a) = 0$, où \tilde{P} désigne la fonction polynomiale sur K' associée à P .

De plus, il résulte aussitôt de la proposition 1.11 que pour tout élément α de K , et pour tout élément P de $K[X]$, la valuation de P au point α ne change pas lorsqu'on passe de K à K' . Ainsi, toute racine α d'ordre n de P dans K est encore racine de P dans K' au même ordre n .

En particulier, l'ensemble \mathcal{E} des racines de P dans K est contenu dans l'ensemble \mathcal{E}' des racines de P dans K' ; cette inclusion peut fort bien être stricte, comme le montre l'exemple considéré ci-dessus. Voici cependant un cas où ce phénomène ne se produit pas :

DÉFINITION 1.11. — Polynômes scindés sur K . — On dit qu'un polynôme P à coefficients dans K est scindé sur K si $P = 0$, ou, dans le cas contraire, si

$$\sum_{\alpha \in K} v_{\alpha}(P) = d^0(P).$$

Si P n'est pas constant, cela revient à dire qu'en désignant par $\alpha_1, \alpha_2, \dots, \alpha_r$ les racines de P dans K , par n_1, n_2, \dots, n_r leurs ordres de multiplicité, et par β le coefficient dominant de P ,

$$P = \beta \prod_{i=1}^r (X - \alpha_i)^{n_i}.$$

Si P est un polynôme scindé sur K , alors, pour tout corps K' contenant K comme sous-corps, les seules racines de P dans K' sont les racines de P dans K . Nous verrons (cf. chapitre III.3) que, pour tout élément P de $K[X]$, il existe un corps K' contenant K comme sous-corps, tel que P soit scindé sur K' . C'est pourquoi, par abus de langage, un polynôme scindé sur K est dit aussi avoir toutes ses racines dans K .

Abordons enfin l'étude des fonctions rationnelles.

DÉFINITION 1.12. — Éléments substituables dans une fraction rationnelle. — Soient $K(X)$ le corps des fractions rationnelles à une indéterminée X à coefficients dans un corps K , et E une K -algèbre associative unitaire. Un élément a de E est dit substituable dans une fraction rationnelle $R \in K(X)$ s'il existe un élément (P, Q) de $K[X] \times K[X]^*$ tel que $R = \frac{P}{Q}$, et que $\tilde{Q}(a)$ soit un élément inversible dans E .

Soit a un élément de E substituable dans une fraction rationnelle R ; considérons deux éléments (P, Q) et (P', Q') de $K[X] \times K[X]^*$ tels que $R = \frac{P}{Q} = \frac{P'}{Q'}$ et que $\tilde{Q}(a)$ et $\tilde{Q}'(a)$ soient inversibles dans E . Il est alors immédiat

que $\tilde{P}(a) \cdot [\tilde{Q}(a)]^{-1} = \tilde{P}'(a) \cdot [\tilde{Q}'(a)]^{-1}$. Cet élément de E ne dépend donc que de R ; on l'appelle valeur de R au point a .

DÉFINITION 1.13. — Fonctions rationnelles. — Soit E une K -algèbre associative unitaire. Étant donné un élément R de $K(X)$, on note \tilde{R} l'application qui à tout élément a de E substituable dans R associe la valeur de R au point a .

Soit maintenant B une partie de E . On dit qu'une application f de B dans E est une fonction rationnelle s'il existe un élément R de $K(X)$ satisfaisant aux conditions suivantes :

- a) tout élément de B est substituable dans R ;
- b) pour tout élément a de B , $f(a) = \tilde{R}(a)$.

Étant donné un élément R de $K(X)$, l'application \tilde{R} s'appelle fonction rationnelle associée à R .

EXEMPLES

1. Fonctions rationnelles sur K . — Lorsque $E = K$, une condition nécessaire et suffisante pour qu'un élément α de K soit substituable dans un élément R de $K(X)$ est qu'il existe un élément (P, Q) de $K[X] \times K[X]^*$ tel que $R = \frac{P}{Q}$ et que $\tilde{Q}(\alpha)$ soit non nul. L'ensemble des éléments de K non substituables dans R est donc fini (cf. th. 1.3).

Dans le présent cas, on peut d'ailleurs prolonger la fonction rationnelle \tilde{R} associée à R de la manière suivante :

On introduit l'ensemble $P_1(K)$ obtenu en adjoignant à K un élément, noté ∞ . (Nous verrons au chapitre III.2 que $P_1(K)$ n'est autre que la droite projective construite sur K , l'élément ∞ s'appelant alors point à l'infini.) Lorsqu'un élément α de K n'est pas substituable dans R , on dit que la valeur de R au point α est ∞ . On prolonge donc la fonction rationnelle associée à R aux éléments α de K non substituables dans R en posant $\tilde{R}(\alpha) = \infty$. Enfin, on prolonge cette dernière fonction en une application de $P_1(K)$ dans $P_1(K)$ en définissant $\tilde{R}(\infty)$ de la manière suivante :

- si $d^0(R) < 0$, on pose $\tilde{R}(\infty) = 0$;
- si $d^0(R) > 0$, on pose $\tilde{R}(\infty) = \infty$;
- si $d^0(R) = 0$, on écrit R sous la forme

$$R = \frac{\alpha_p X^p + \alpha_{p-1} X^{p-1} + \dots + \alpha_0}{\beta_p X^p + \beta_{p-1} X^{p-1} + \dots + \beta_0},$$

où $\alpha_p \neq 0$ et $\beta_p \neq 0$, et on pose $\tilde{R}(\infty) = \frac{\alpha_p}{\beta_p}$. (On vérifie aisément que ce scalaire ne dépend que de R .)

Il est immédiat que l'application $\tilde{R} \mapsto R(\infty)$ est un morphisme de l'algèbre des fractions rationnelles de degré négatif ou nul dans K .

L'intérêt de ces considérations apparaît dans les exercices 17 et 18.

2. Lorsque $K = \mathbb{R}$, la notion de fonction rationnelle définie dans ce paragraphe coïncide avec celle qui a été introduite au § I.4.9.

3. Composée de deux fractions rationnelles. — On prend pour E l'algèbre $K(X)$ elle-même. Soit S un élément de $K(X)$ substituable dans un élément R de $K(X)$; la fraction rationnelle obtenue en substituant S à l'indéterminée X dans R s'appelle *composée* de S et de R , et se note $R \circ S$, ou encore $R(S)$. En particulier, $R(X) = R$.

Soient maintenant S un élément de $K(X)$, E une K -algèbre associative unitaire, et a un élément de E substituable dans S . En écrivant S sous la forme d'un quotient de deux polynômes, on voit aussitôt que, pour tout élément P de $K[X]$, a est substituable dans $P \circ S$, et que

$$(1) \quad \widetilde{(P \circ S)}(a) = \tilde{P}[\tilde{S}(a)].$$

Soient ensuite R et S deux éléments de $K(X)$, E une K -algèbre associative unitaire, et a un élément de E . En écrivant R sous la forme d'un quotient de polynômes, et en utilisant la relation (1), on voit que si a est substituable dans S , et si $\tilde{S}(a)$ est substituable dans R , alors S est substituable dans R , a est substituable dans $R \circ S$, et

$$(2) \quad \widetilde{(R \circ S)}(a) = \tilde{R}[\tilde{S}(a)].$$

En appliquant enfin ce dernier résultat au cas où $E = K(X)$, et où a est un élément T de $K(X)$, on obtient l'associativité de la composition des fractions rationnelles.

On prouvera au § 6 que toute fraction rationnelle non constante est substituable dans toute fraction rationnelle. A ce sujet, on pourra aussi consulter l'exercice 12.

EXEMPLE. — **Fractions rationnelles paires, fractions rationnelles impaires.** — Soit R une fraction rationnelle. Le polynôme $-X$ est évidemment substituable dans R . On note \check{R} la fraction rationnelle composée $R(-X)$. On dit que R est *paire* si $\check{R} = R$, *impaire* si $\check{R} = -R$.

Si K est de caractéristique différente de 2, les fractions rationnelles paires et les fractions rationnelles impaires constituent deux sous-espaces vectoriels supplémentaires dans $K(X)$.

Nous pouvons maintenant définir la notion de valuation en un point d'une fraction rationnelle, grâce à la

PROPOSITION 1.12. — **Valuation d'une fraction rationnelle en un point.** — Soient R une fraction rationnelle non nulle à coefficients dans K et α un élément de K . Il existe alors un couple (n, S) , où n est un entier rationnel, et où S est un élément de $K(X)$, satisfaisant aux conditions suivantes :

a)
$$R = (X - \alpha)^n S;$$

b) l'élément α est substituable dans S , et $\tilde{S}(\alpha) \neq 0$.

Un tel couple est unique. L'entier rationnel n s'appelle *valuation* de R au point α , et se note $v_\alpha(R)$. On convient de poser $v_\alpha(0) = +\infty$.

Unicité. — Soit (n', S') un autre couple satisfaisant aux conditions de l'énoncé. Lorsque $n = n'$, il est immédiat que $S = S'$, puisque $K(X)$ est intègre. Supposons par l'absurde que $n \neq n'$; soit par exemple $n > n'$. La relation $(X - \alpha)^n S = (X - \alpha)^{n'} S'$ peut s'écrire $(X - \alpha)^{n-n'} S = S'$. En substituant à X le scalaire α , nous obtenons la relation $\tilde{S}(\alpha) = 0$, d'où la contradiction.

Existence. — Écrivons R sous la forme $R = \frac{P}{Q}$, où P et Q sont deux polynômes non nuls. D'après la proposition 11, il existe des polynômes P_1 et Q_1 et des entiers naturels p et q tels que

$$P = (X - \alpha)^p P_1, \quad \tilde{P}_1(\alpha) \neq 0 \quad \text{et} \quad Q = (X - \alpha)^q Q_1, \quad \tilde{Q}_1(\alpha) \neq 0.$$

Le couple $\left(p - q, \frac{P_1}{Q_1}\right)$ convient visiblement.

REMARQUE 1. — L'assertion 1 de la proposition 1.11 montre que si R est un polynôme, la notion de valuation introduite ci-dessus coïncide avec celle de valuation des polynômes.

REMARQUE 2. — A titre d'exercice, on pourra étendre aux fractions rationnelles les propriétés des valuations des polynômes énoncées dans l'assertion 2 de la proposition 1.11.

DÉFINITION 1.14. — **Pôles et zéros d'une fraction rationnelle.** — Soient R un élément de $K(X)$, et α un scalaire.

On dit que α est un pôle de R si $v_\alpha(R) < 0$; cela revient à dire que α n'est pas substituable dans R . L'entier strictement positif $-v_\alpha(R)$ s'appelle alors ordre de multiplicité du pôle α . Un pôle d'ordre 1 est dit simple, un pôle d'ordre strictement supérieur à 1 est dit multiple.

On dit que α est un zéro de R si $v_\alpha(R) > 0$; si R est un polynôme, la notion de zéro coïncide avec celle de racine. Lorsque $R \neq 0$, l'entier strictement positif $v_\alpha(R)$ s'appelle ordre de multiplicité du zéro α . Un zéro d'ordre 1 est dit simple, un zéro d'ordre strictement supérieur à 1 est dit multiple.

PROPOSITION 1.13. — **Lien entre fractions rationnelles et fonctions rationnelles.** — Soient K un corps infini et B une partie infinie de K .

1. Soient R et R' deux éléments de $K(X)$. Si, pour tout élément α de B substituable à la fois dans R et dans R' , $\tilde{R}(\alpha) = \tilde{R}'(\alpha)$, alors $R = R'$.

2. Soient f et g deux fonctions rationnelles sur K définies sur une même partie de K contenant B . Si, pour tout élément β de B , $f(\beta) = g(\beta)$, alors $f = g$.

Assertion 1. — Écrivons R et R' sous la forme $R = \frac{P}{Q}$, $R' = \frac{P'}{Q'}$, où P et P' sont des éléments de $K[X]$, Q et Q' des éléments non nuls de $K[X]$. Désignons par B_1 (resp. B'_1) l'ensemble des racines de Q (resp. de Q'). Nous savons (cf. th. 1.3) que B_1 et B'_1 sont finis. Il en résulte que $B' = B - (B_1 \cup B'_1)$ est infini. Tout élément α de B' est substituable à la fois dans R et dans R' , et

$$\tilde{R}(\alpha) = \frac{\tilde{P}(\alpha)}{\tilde{Q}(\alpha)}, \quad \tilde{R}'(\alpha) = \frac{\tilde{P}'(\alpha)}{\tilde{Q}'(\alpha)}, \quad \tilde{R}(\alpha) = \tilde{R}'(\alpha).$$

Il s'ensuit que le polynôme $PQ' - QP'$ prend la valeur 0 en tout point de B' ; ce polynôme est donc nul (cf. cor. 2 du th. 1.3), et $R = R'$.

L'assertion 2 s'en déduit aussitôt.

COROLLAIRE. — Soit K un corps infini. Si les fonctions rationnelles sur K associées à deux éléments R et R' de $K(X)$ prennent même valeur en tout point de K où elles sont toutes deux définies, alors $R = R'$.

§ 4. DIVISION EUCLIDIENNE. IDÉAUX DE POLYNÔMES

Pour l'étude de la relation de divisibilité dans l'anneau $K[X]$, nous établirons d'abord le théorème fondamental suivant :

THÉOREME 1. 4. — Division euclidienne des polynômes. — *Soit $K[X]$ l'anneau des polynômes à une indéterminée dans K . Étant donnés deux éléments A et B de $K[X]$, le polynôme B étant supposé unitaire, il existe un couple (Q, R) et un seul d'éléments de $K[X]$ tel que*

$$A = BQ + R \quad \text{et} \quad d^0(R) < d^0(B).$$

Unicité. — Soit (Q', R') un second couple d'éléments de $K[X]$ tel que $A = BQ' + R'$ et $d^0(R') < d^0(B)$. Il en résulte que $B(Q - Q') = R' - R$; d'où la relation :

$$(1) \quad d^0(R' - R) = d^0(B) + d^0(Q' - Q).$$

Nous savons d'autre part que $d^0(R' - R) \leq \sup [d^0(R), d^0(R')]$; donc :

$$(2) \quad d^0(R' - R) < d^0(B).$$

Des relations (1) et (2) nous déduisons que

$$d^0(B) + d^0(Q - Q') < d^0(B).$$

Comme B n'est pas nul, cette dernière relation entraîne $Q = Q'$, et enfin $R = R'$.

Existence. — La démonstration s'effectue par récurrence sur le degré de A ; elle fournit une méthode pratique d'obtention de Q et de R .

Lorsque $d^0(A) < d^0(B)$, le couple $(0, A)$ convient visiblement. Supposons l'existence du couple (Q, R) établie pour tous les polynômes de degré strictement inférieur à n , où n est un entier supérieur ou égal à $d^0(B)$, et considérons un polynôme A de degré n . Écrivons A et B sous la forme suivante :

$$\begin{aligned} A &= \alpha_n X^n + \alpha_{n-1} X^{n-1} + \dots + \alpha_0, & \text{où} \quad \alpha_n \neq 0, \\ B &= X^p + \beta_{p-1} X^{p-1} + \dots + \beta_0. \end{aligned}$$

Comme $n \geq p$, nous pouvons introduire le polynôme $A_1 = A - \alpha_n X^{n-p} B$. Ce polynôme est de degré strictement inférieur à n . Nous pouvons donc lui appliquer l'hypothèse de récurrence : il existe un couple (Q_1, R_1) d'éléments de $K[X]$ tel que

$$A_1 = BQ_1 + R_1 \quad \text{et} \quad d^0(R_1) < d^0(B).$$

Il en résulte que $A = B(Q_1 + \alpha_n X^{n-p}) + R_1$; le couple $(Q_1 + \alpha_n X^{n-p}, R_1)$ convient donc.

COROLLAIRE 1. — Soient A et B deux éléments de $K[X]$, le polynôme B étant supposé non nul. Il existe alors un couple unique (Q, R) d'éléments de $K[X]$ tel que

$$(1) \quad A = BQ + R \quad \text{et} \quad d^0(R) < d^0(B).$$

Les polynômes Q et R s'appellent respectivement quotient et reste de la division euclidienne de A par B .

En effet, le polynôme B peut s'écrire d'une manière et d'une seule sous la forme $B = \beta B_1$, où $\beta \in K^*$ et où B_1 est un polynôme unitaire.

La relation (1) est équivalente à la suivante :

$$\beta^{-1}A = B_1Q + \beta^{-1}R \quad \text{et} \quad d^0(\beta^{-1}R) < d^0(B_1).$$

L'existence et l'unicité du couple (Q, R) en découlent.

REMARQUE. — La pratique de la division s'en déduit :

— On ordonne les polynômes A et B suivant les puissances décroissantes, on place A au dividende, en laissant des vides pour les degrés manquants, et on place B au diviseur.

— Le premier terme du quotient est $\frac{\alpha_n}{\beta_p} X^{n-p}$.

— On écrit le polynôme $\frac{\alpha_n}{\beta_p} X^{n-p} B$ en dessous du polynôme A , et on le retranche de A ; on obtient ainsi A_1 .

— On répète ces opérations jusqu'à obtention au dividende d'un polynôme de degré strictement inférieur au degré de B ; ce polynôme est le reste R , tandis que Q est écrit à l'emplacement traditionnel du quotient.

EXEMPLE. — Division euclidienne de $A = X^4 + 1$ par $B = X^2 + X + 1$.

$$\begin{array}{r|l} X^4 & + 1 \\ X^4 + X^3 + X^2 & \\ \hline - X^3 - X^2 & + 1 \\ - X^3 - X^2 - X & \\ \hline & X + 1 \end{array} \quad \left| \begin{array}{l} X^2 + X + 1 \\ X^2 - X \\ \hline \end{array} \right.$$

Le quotient Q est donc $X^2 - X$, et le reste R est $X + 1$.

COROLLAIRE 2. — **Divisibilité et extension du corps des scalaires.** — Soient K un sous-corps d'un corps commutatif K' , A et B deux polynômes non nuls, à coefficients dans K . Pour que B divise A dans $K[X]$, il faut et il suffit que B divise A dans $K'[X]$.

Il est évident que cette condition est nécessaire. Réciproquement, supposons qu'il existe un élément C de $K'[X]$ tel que $A = BC$. Effectuons la division euclidienne de A par B dans $K[X]$; il existe un couple (Q, R) et un seul d'éléments de $K[X]$ tel que

$$A = BQ + R, \quad d^0(R) < d^0(B).$$

L'unicité du quotient et du reste de la division euclidienne de A par B dans $K'[X]$ montre que $Q = C$ et $R = 0$, ce qui prouve que les coefficients de C appartiennent à K .

PROPOSITION 1.14. — Reste d'une somme, reste d'un produit. — Soient A_1, A_2 et B trois éléments de $K[X]$, le polynôme B étant supposé non nul. On désigne par (Q_1, R_1) et (Q_2, R_2) les couples associés à A_1 et A_2 dans leur division euclidienne par B . Alors le couple associé à $A_1 + A_2$ dans sa division par B est $(Q_1 + Q_2, R_1 + R_2)$. D'autre part, le reste de la division euclidienne de $A_1 A_2$ par B est égal au reste de la division euclidienne de $R_1 R_2$ par B .

Nous étudions maintenant les idéaux de l'anneau $K[X]$: l'ensemble des multiples d'un polynôme A est un idéal de $K[X]$; comme pour l'anneau \mathbb{Z} des entiers rationnels (cf. th. I.2.4), nous allons montrer que tous les idéaux de $K[X]$ sont de ce type.

THÉORÈME 1.5. — Structure des idéaux de l'anneau $K[X]$. — Soit \mathfrak{J} un idéal non réduit à $\{0\}$ de l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans K . Il existe alors dans \mathfrak{J} un polynôme unitaire D et un seul tel que \mathfrak{J} soit l'ensemble des multiples de D . Le polynôme D s'appelle le générateur de l'idéal \mathfrak{J} .

En particulier, tous les idéaux de l'anneau $K[X]$ sont principaux.

Unicité du générateur. — Supposons que D' soit un polynôme unitaire appartenant à \mathfrak{J} et tel que \mathfrak{J} soit l'ensemble des multiples de D' . La relation $D \in \mathfrak{J}$ entraîne $D' \mid D$; de même, la relation $D' \in \mathfrak{J}$ entraîne $D \mid D'$. Puisque D et D' sont unitaires, $D = D'$.

Existence du générateur. — Considérons l'ensemble δ des entiers naturels n tels qu'il existe un élément de \mathfrak{J} de degré n . Puisque \mathfrak{J} est non réduit à $\{0\}$, δ est une partie non vide de \mathbb{N} ; elle possède donc un plus petit élément (cf. th. I.1.3), soit n_0 . Introduisons alors un élément P_0 de \mathfrak{J} ayant pour degré n_0 , et désignons par D le polynôme unitaire associé à P_0 . Le polynôme D convient : en effet, d'une part D appartient à \mathfrak{J} , puisque $D = \alpha P_0$, où $\alpha \in K^*$, et que P_0 appartient à \mathfrak{J} ; soit d'autre part P un élément quelconque de \mathfrak{J} . Effectuons la division euclidienne de P par D (cf. th. 1.4) : il existe un couple (Q, R) d'éléments de $K[X]$ tel que $P = DQ + R$ et $d^0(R) < d^0(D)$. Le polynôme $R = P - DQ$ appartient à \mathfrak{J} , puisque D et P appartiennent à \mathfrak{J} . Or, par définition de $n_0 = d^0(D)$, il n'existe pas de polynôme non nul dans \mathfrak{J} dont le degré soit strictement inférieur à n_0 ; cela montre que $R = 0$, ce qui achève la démonstration.

COROLLAIRE 1. — Caractérisation du générateur de l'idéal engendré par n polynômes non nuls. — Soient A_1, A_2, \dots, A_n des éléments non nuls de $K[X]$. Alors le générateur D de l'idéal \mathfrak{J} engendré par ces polynômes est le seul polynôme unitaire qui divise tous les polynômes A_i et qui puisse s'écrire sous la

forme $\sum_{i=1}^n P_i A_i$, où $P_i \in K[X]$.

En effet le générateur D de \mathfrak{J} satisfait à ces conditions. Réciproquement, soit D' un polynôme unitaire satisfaisant à ces conditions. Puisque D' peut s'écrire sous la forme $\sum_{i=1}^n P_i A_i$, le polynôme D' appartient à l'idéal \mathfrak{J} ; donc D' est un multiple de D . D'autre part, D' divisant tous les polynômes A_i , divise tout élément non nul de \mathfrak{J} , et donc divise D . Comme D et D' sont unitaires, cela entraîne $D' = D$.

COROLLAIRE 2. — Identité de Bezout. — Soient A_1, A_2, \dots, A_n des éléments non nuls de $K[X]$. Il est équivalent de dire :

1. Les seuls diviseurs communs aux polynômes A_i sont les constantes non nulles.
2. Le générateur de l'idéal engendré par A_1, A_2, \dots, A_n est 1.
3. L'idéal engendré par A_1, A_2, \dots, A_n est $K[X]$ tout entier.
4. Il existe une suite (U_1, U_2, \dots, U_n) de polynômes telle que

$$\sum_{i=1}^n A_i U_i = 1 \quad (\text{identité de Bezout}).$$

On dit dans ces conditions que les polynômes A_1, A_2, \dots, A_n sont premiers entre eux dans leur ensemble.

(Lorsque $n = 2$, cette notion coïncide avec celle qui a été introduite dans la définition I.2.27.)

COROLLAIRE 3. — Propriété de Gauss. — Soient A, B, C , trois polynômes non nuls; si A divise BC , et si A et B sont premiers entre eux, alors A divise C .

En effet, le corollaire 2 montre qu'il existe des polynômes U et V tels que $AU + BV = 1$; d'autre part il existe un polynôme Q tel que $BC = AQ$. D'où la relation :

$$C = C(AU + BV) = ACU + BCV = A(CU + QV).$$

REMARQUE. — Les théorèmes 1.4 et 1.5 et les corollaires ci-dessus sont liés à la théorie des anneaux euclidiens (exercice I.2.44) et à celle des anneaux principaux (exercice I.2.45).

Exercices conseillés : 19 à 23.

§ 5. DÉCOMPOSITION EN FACTEURS IRRÉDUCTIBLES

Dans tout ce paragraphe, nous ne retiendrons du § 4 que la propriété de Gauss (cf. cor. 3 du th. 1.5), dont nous rappelons l'énoncé :

Soient A, B, C trois éléments non nuls de $K[X]$; si A divise BC et si A et B sont premiers entre eux, alors A divise C .

Voici une première conséquence, très importante, de cet énoncé :

PROPOSITION 1.15. — *Soient A, B, C trois polynômes non nuls. Si A est premier avec B et C , alors A est premier avec BC .*

Soit en effet P un diviseur commun à A et BC . Les polynômes P et B sont premiers entre eux : en effet, tout diviseur commun à P et B est un diviseur commun à A et B , qui sont premiers entre eux. Puisque P et B sont premiers entre eux, et que P divise BC , la propriété de Gauss montre que P divise C . D'autre part, P divise A , et les polynômes A et C sont premiers entre eux. Par suite, P est constant non nul, ce qu'il fallait prouver.

COROLLAIRE. — *Si un polynôme A est premier avec les polynômes A_1, A_2, \dots, A_n , alors A est premier avec le produit $A_1 A_2 \dots A_n$.*

Cela résulte aussitôt de la proposition 1.15, par récurrence sur n .

DÉFINITION 1.15. — **Polynômes irréductibles sur K .** — *Soit A un polynôme à une indéterminée à coefficients dans un corps K . On dit que A est irréductible sur K (ou, plus simplement, irréductible lorsque aucune confusion n'est à craindre) si A est un élément irréductible (au sens de la définition I.2.27) de l'anneau $K[X]$.*

Plus généralement, si K' est un corps commutatif contenant K comme sous-corps, un polynôme A à coefficients dans K est dit irréductible sur K' si A est un élément irréductible de $K'[X]$.

EXEMPLES.

1. *Tout polynôme à coefficients dans K de degré 1 est irréductible sur K . Un tel polynôme est même irréductible sur K' , pour tout corps K' contenant K comme sous-corps.*

Cependant, un polynôme à coefficients dans K peut fort bien être irréductible sur K , et ne pas l'être sur K' :

2. *Le polynôme à coefficients rationnels $A = X^2 - 2$ est irréductible sur \mathbf{Q} , mais ne l'est pas sur \mathbf{R} .*

Si A n'était pas irréductible sur \mathbf{Q} , il existerait deux éléments q et r de \mathbf{Q} tels que $A = X^2 - 2 = (X - q)(X - r)$. Une telle relation entraîne $r = -q$, et $q^2 = 2$, ce qui est impossible. Au contraire, A n'est pas irréductible sur \mathbf{R} , puisque

$$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}).$$

3. *De même, le polynôme à coefficients réels $X^2 + 1$ est irréductible sur \mathbf{R} , et ne l'est pas sur \mathbf{C} .*

En pratique, l'étude des polynômes irréductibles se ramène aussitôt à celle des polynômes *unitaires* irréductibles : en effet, il est clair qu'un polynôme est irréductible si et seulement si le polynôme unitaire qui lui est associé est irréductible. De plus, pour qu'un polynôme unitaire P soit irréductible, il faut et il suffit que son degré soit strictement positif, et que les seuls polynômes unitaires divisant P soient 1 et P .

Nous sommes en mesure d'aborder le théorème fondamental de décomposition des polynômes en facteurs irréductibles :

THÉOREME 1.6. — Décomposition en facteurs irréductibles. — Soit $K[X]$ l'anneau des polynômes à une indéterminée à coefficients dans K .

1. Soit P un polynôme unitaire irréductible à coefficients dans K . Pour tout élément A non nul de $K[X]$, il existe un couple (n, B) , où n est un entier naturel, et où B est un élément non nul de $K[X]$ premier avec P , tel que $A = P^n B$. Un tel couple est unique.

L'application qui à tout élément A non nul de $K[X]$ associe l'entier naturel n défini ci-dessus s'appelle *valuation relative à P* , et se note v_P . L'entier n est donc noté $v_P(A)$. On convient de poser $v_P(0) = +\infty$.

2. Pour tout élément A non nul de $K[X]$, l'ensemble des polynômes unitaires irréductibles P tels que $v_P(A)$ soit non nul est fini, et

$$(1) \quad A = \alpha \prod_{P \in E} P^{v_P(A)},$$

où α désigne le coefficient dominant du polynôme A , et où E désigne l'ensemble des polynômes unitaires irréductibles à coefficients dans K .

Une telle décomposition est unique, c'est-à-dire que si A peut être écrit sous la forme

$$(2) \quad A = \beta \prod_{P \in E} P^{m_P},$$

où $\beta \in K^*$, et où (m_P) est une famille à support fini d'entiers naturels, alors $\beta = \alpha$ et, pour tout élément P de E , $m_P = v_P(A)$.

Cette décomposition s'appelle *décomposition du polynôme A en facteurs unitaires irréductibles*.

REMARQUE. — Les produits ci-dessus, bien que portant *a priori* sur un ensemble infini d'indices, ont un sens : ce sont de simples notations, qui signifient qu'on effectue le produit des polynômes P^{m_P} où P est tel que $m_P \neq 0$.

Assertion 1. — L'existence du couple (n, B) se prouve par récurrence sur le degré du polynôme A . Si $d^0(A) = 0$, elle est évidente; supposons-la démontrée pour tous les éléments A' de $K[X]$ non nuls et tels que $d^0(A') < r$, et soit A un polynôme de degré r , où $r > 0$. Si A est premier avec P , l'assertion est claire : il suffit de prendre $n = 0$, et $B = A$; sinon, P divise A , puisque P est irréductible. Il existe alors un polynôme non nul A' tel que $A = PA'$. Puisque $d^0(P) > 0$, l'hypothèse de récurrence s'applique à A' , ce qui fournit une décomposition de A .

Pour démontrer l'unicité, considérons deux couples (n, B) et (n', B') satisfaisant aux conditions de l'énoncé : alors $P^n B = P^{n'} B'$. Le polynôme P^n divise $P^{n'} B'$ et est premier avec B' , puisque P est premier avec B' (cf. cor. de la prop. 1.15); il divise donc $P^{n'}$ (propriété de Gauss), d'où $n \leq n'$. De même, $n' \leq n$; finalement, $n' = n$, et donc $B' = B$, puisque $K[X]$ est intègre.

Assertion 2. — Nous allons d'abord démontrer l'existence d'une décomposition du polynôme A sous la forme (2), en procédant par récurrence sur $d^0(A)$. Si $d^0(A) = 0$, c'est évident; de même si $d^0(A) = 1$, puisque tout polynôme unitaire de degré 1 appartient à E . Soit donc r un entier supérieur ou égal à 2; supposons cette existence prouvée pour tous les polynômes de degré strictement inférieur à r . Considérons enfin un polynôme A de degré r . Nous l'écrivons sous la forme $A = \beta A'$, où $\beta \in K^*$, et où A' est unitaire. Deux cas se présentent : ou bien A' est irréductible, et l'assertion est prouvée; ou bien A' n'est pas irréductible, et peut s'écrire $A' = A_1 A_2$, où A_1 et A_2 sont des polynômes unitaires de degré strictement positif. Il en résulte que $d^0(A_1)$ et $d^0(A_2)$ sont strictement inférieurs à r . L'hypothèse de récurrence s'applique donc à A_1 et A_2 , ce qui fournit une décomposition de A .

Ainsi, nous pouvons écrire A sous la forme

$$(2) \quad A = \beta \prod_{P \in E} P^{m_P},$$

où $\beta \in K^*$, l'ensemble des éléments P de E tels que $m_P \neq 0$ étant fini. Pour achever la démonstration de l'assertion 2, il suffit de prouver que $\beta = \alpha$, ce qui est évident, et que pour tout élément P de E , $m_P = v_P(A)$. Écrivons pour cela A sous la forme

$$A = P^{m_P} B, \quad \text{où } B = \beta \prod_{\substack{P' \in E \\ P' \neq P}} P'^{m_{P'}}.$$

Il résulte du corollaire de la proposition 1.15 que B est premier avec P . Nous déduisons alors de l'assertion 1 que $m_P = v_P(A)$.

REMARQUE. — Parmi les polynômes unitaires irréductibles, on trouve en particulier les polynômes de la forme $X - \gamma$, où $\gamma \in K$. Or nous avons défini la valuation v_γ (cf. déf. 1.8). Nous allons montrer que pour tout polynôme non nul A , $v_{X-\gamma}(A) = v_\gamma(A)$. (La notion de valuation relative à un polynôme premier généralise donc celle de valuation en un point.)

D'après la proposition 1.11, il existe un polynôme Q tel que $A = (X - \gamma)^{v_\gamma(A)} Q$, et que $Q(\gamma) \neq 0$. Il en découle que Q n'est pas divisible par $X - \gamma$, donc est premier avec $X - \gamma$. D'après l'assertion 1 du théorème de décomposition en facteurs irréductibles, cela implique que $v_\gamma(A) = v_{X-\gamma}(A)$.

COROLLAIRE 1. — Propriétés des valuations.

1. Pour tout couple (A, B) de polynômes, et pour tout polynôme unitaire irréductible P ,

$$(1) \quad v_P(AB) = v_P(A) + v_P(B);$$

$$(2) \quad v_P(A + B) \geq \inf [v_P(A), v_P(B)],$$

avec égalité si $v_P(A) \neq v_P(B)$.

Il en découle que l'ensemble des éléments A de $K[X]$ tels que $v_P(A)$ soit supérieur à un entier naturel donné, est un idéal de l'algèbre $K[X]$.

2. Pour qu'un polynôme non nul A divise un polynôme non nul B , il faut et il suffit que, pour tout élément P de E ,

$$v_P(A) \leq v_P(B).$$

Assertion 1. — Écartons le cas trivial où l'un au moins des polynômes A et B est nul, et écrivons $A = P^m U$, et $B = P^n V$, où m et n sont des entiers naturels, et où U et V sont des polynômes premiers avec P .

La formule (1) résulte aussitôt de la relation $AB = P^{m+n} UV$.

Pour démontrer la formule (2), supposons par exemple $m \leq n$, et écrivons $A + B$ sous la forme

$$A + B = P^m(U + P^{n-m}V).$$

Si $n \neq m$, il est immédiat que $U + P^{n-m}V$ est premier avec P , d'où la formule (2) dans ce cas. Le cas où $n = m$ est évident.

Assertion 2. — Si pour tout élément P de E , $v_P(A)$ est inférieur à $v_P(B)$, il est évident que A divise B . Réciproquement, si A divise B , il existe un polynôme C non nul tel que $B = AC$. L'assertion 1 montre que pour tout élément P de E ,

$$v_P(B) = v_P(A) + v_P(C) \geq v_P(A).$$

COROLLAIRE 2. — Divisibilité par un produit. — Soit A un polynôme non nul, divisible par des polynômes non nuls A_1, A_2, \dots, A_n premiers entre eux deux à deux. Alors A est divisible par le polynôme $A_1 A_2 \dots A_n$.

Grâce au corollaire de la proposition 1.15, nous nous ramenons, par récurrence sur n , au cas de deux polynômes non nuls B et C , premiers entre eux et divisant A . D'après le corollaire 1, il suffit alors de prouver que pour tout élément P de E , $v_P(BC)$ est inférieur à $v_P(A)$. Cela résulte aussitôt de la formule

$$v_P(BC) = v_P(B) + v_P(C),$$

et des hypothèses, que nous pouvons écrire sous la forme suivante :

$$v_P(B) \leq v_P(A), \quad v_P(C) \leq v_P(A), \quad \text{et} \quad \inf [v_P(B), v_P(C)] = 0.$$

COROLLAIRE 3. — P. G. C. D. d'un ensemble de polynômes. — Soit \mathcal{E} une partie non vide de $K[X]$ constituée de polynômes non tous nuls. Il existe un polynôme unitaire D et un seul satisfaisant aux conditions suivantes :

- a) Le polynôme D divise tout élément de \mathcal{E} .
- b) Le polynôme D est un multiple de tous les diviseurs communs aux éléments de \mathcal{E} .

Ce polynôme s'appelle plus grand commun diviseur des éléments de \mathcal{E} , et se note P. G. C. D. (\mathcal{E}). Pour tout polynôme unitaire irréductible P ,

$$v_P(D) = \inf_{A \in \mathcal{E}} v_P(A).$$

Unicité. — Soient D_1 et D_2 deux polynômes unitaires satisfaisant aux conditions de l'énoncé. Il est clair que D_1 divise D_2 , et que D_2 divise D_1 . Comme D_1 et D_2 sont unitaires, cela implique que $D_1 = D_2$.

Existence. — Pour tout élément P de E , posons

$$n(P) = \inf_{A \in \mathfrak{E}} v_P(A),$$

et considérons le polynôme $D = \prod_{P \in E} P^{n(P)}$.

Il est immédiat que P est un polynôme unitaire, que D divise tout élément de \mathfrak{E} , et que D est un multiple de tous les diviseurs communs aux éléments de \mathfrak{E} (cf. cor. 1).

REMARQUE. — Nous verrons au § 6 des caractérisations du P. G. C. D. de deux polynômes, et un autre moyen de calcul pratique de celui-ci.

Soit maintenant $(A_i)_{i \in I}$ une famille d'éléments non tous nuls de $K[X]$. Le P. G. C. D. de l'ensemble constitué par les polynômes A_i s'appelle P. G. C. D. de la famille $(A_i)_{i \in I}$, et se note P. G. C. D. $((A_i)_{i \in I})$. Lorsque tous les polynômes A_i sont décomposés en facteurs unitaires irréductibles, la décomposition de P. G. C. D. $((A_i)_{i \in I})$ en facteurs unitaires irréductibles s'obtient de la manière suivante : l'exposant de P dans ce polynôme est le plus petit des exposants de P dans la décomposition des polynômes A_i .

En particulier, lorsque $I = [1, n]$, où $n \in \mathbf{N}^$, le P. G. C. D. des polynômes A_1, A_2, \dots, A_n se note P. G. C. D. (A_1, A_2, \dots, A_n) . Pour que les polynômes A_1, A_2, \dots, A_n soient premiers entre eux dans leur ensemble, il faut et il suffit que P. G. C. D. $(A_1, A_2, \dots, A_n) = 1$.*

COROLLAIRE 4. — P. P. C. M. d'un ensemble fini de polynômes. — Soit \mathfrak{E} une partie FINIE non vide de $K[X]$ constituée de polynômes non nuls. Il existe un polynôme unitaire M et un seul satisfaisant aux conditions suivantes :

- a) Le polynôme M est un multiple de tout élément de \mathfrak{E} .
- b) Le polynôme M divise tous les multiples communs aux éléments de \mathfrak{E} .

Ce polynôme s'appelle plus petit commun multiple des éléments de \mathfrak{E} , et se note P. P. C. M. (\mathfrak{E}) . Pour tout polynôme unitaire irréductible P ,

$$v_P(M) = \sup_{A \in \mathfrak{E}} v_P(A).$$

La démonstration est calquée sur celle du corollaire 3.

On définit de même le P. P. C. M. d'une famille finie $(A_i)_{i \in I}$ d'éléments non nuls de $K[X]$; lorsque $I = [1, n]$, ce P. P. C. M. se note

$$\text{P. P. C. M. } (A_1, A_2, \dots, A_n).$$

PROPOSITION 1.16. — Propriétés du P. G. C. D. et du P. P. C. M.

1. Soient A et B deux polynômes non nuls, D leur P. G. C. D., M leur P. P. C. M., α et β leurs coefficients dominants. Alors :

$$AB = \alpha\beta DM.$$

2. Soient A_1, A_2, \dots, A_n des polynômes non nuls, D leur P. G. C. D. et M leur P. P. C. M. Soit d'autre part B un polynôme unitaire. Alors :

$$\text{P. G. C. D. } (BA_1, BA_2, \dots, BA_n) = BD$$

$$\text{P. P. C. M. } (BA_1, BA_2, \dots, BA_n) = BM.$$

Par suite, si C est un polynôme unitaire divisant A_1, A_2, \dots, A_n , et si on pose $A_1 = CA'_1, A_2 = CA'_2, \dots, A_n = CA'_n$, alors :

$$\text{P. G. C. D. } (A'_1, A'_2, \dots, A'_n) = \frac{D}{C}.$$

En particulier, les polynômes $\frac{A_1}{D}, \frac{A_2}{D}, \dots, \frac{A_n}{D}$ sont premiers entre eux dans leur ensemble.

L'assertion 1 découle aussitôt de la formule suivante : pour tout couple (n, n') d'entiers naturels,

$$\sup (n, n') + \inf (n, n') = n + n'.$$

L'assertion 2 découle de même des formules suivantes : pour toute suite (p_1, p_2, \dots, p_n) d'entiers naturels, et pour tout entier naturel p ,

$$\inf_{i \in [1, n]} (p + p_i) = p + \inf_{i \in [1, n]} p_i$$

$$\sup_{i \in [1, n]} (p + p_i) = p + \sup_{i \in [1, n]} p_i.$$

COROLLAIRE. — Caractérisation des couples de polynômes dont le P. G. C. D. est différent de 1. — Soient A et B deux éléments non nuls de $K[X]$, et D leur P. G. C. D.

1. Si D est différent de 1, il existe un couple (U, V) de polynômes premiers entre eux tel que

$$AU + BV = 0 \quad d^0(U) = d^0(B) - d^0(D), \quad d^0(V) = d^0(A) - d^0(D).$$

2. Réciproquement, s'il existe un couple (U, V) de polynômes premiers entre eux tel que

$$AU + BV = 0 \quad d^0(U) < d^0(B) \quad d^0(V) < d^0(A),$$

alors D est différent de 1. Plus précisément,

$$d^0(D) = d^0(B) - d^0(U) = d^0(A) - d^0(V).$$

Assertion 1. — Par hypothèse, il existe deux polynômes A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. Le couple $(B_1, -A_1)$ convient, car A_1 et B_1 sont premiers entre eux.

Assertion 2. — Puisque U divise $AU = -BV$ et que U est premier avec V , U divise B . Il existe donc un polynôme D_1 tel que $B = D_1U$. La relation $AU + BV = 0$ montre alors que $A = -D_1V$. Puisque U et V sont premiers entre eux, il découle des relations $B = D_1U$ et $A = -D_1V$ que le polynôme unitaire associé à D_1 est égal à D . L'assertion en découle.

Exercices conseillés : 26 à 35.

§ 6. APPLICATIONS DE LA THÉORIE DE LA DIVISIBILITÉ

1. CALCUL DU P. G. C. D. DE DEUX POLYNÔMES

Du théorème de structure des idéaux de $K[X]$ (cf. th. 1.5), nous déduisons la

PROPOSITION 1.17. — Caractérisation du P. G. C. D. de n polynômes. — Soient A_1, A_2, \dots, A_n des polynômes non nuls à coefficients dans K . Le P. G. C. D. de ces polynômes n'est autre que le générateur de l'idéal \mathfrak{J} de $K[X]$ engendré par les éléments A_1, A_2, \dots, A_n .

Désignons en effet par D le générateur de l'idéal \mathfrak{J} , et par D' le P. G. C. D. des polynômes A_1, A_2, \dots, A_n . D'après la caractérisation de D (cf. cor. 1 du th. 1.5), D divise tous les polynômes A_i ; donc, par définition du plus grand commun diviseur, D divise D' . D'autre part, D peut s'écrire sous la forme $D = \sum_{i=1}^n A_i U_i$, où, pour tout $i \in [1, n]$, U_i appartient à $K[X]$. Puisque D' divise tous les polynômes A_i , D' divise D . Comme D et D' sont unitaires, il en découle que $D = D'$.

En pratique, pour calculer le P. G. C. D. de A_1, A_2, \dots, A_n , on se ramène par récurrence au cas de deux polynômes; on utilise alors une méthode fondée sur l'existence d'une division euclidienne dans l'anneau $K[X]$ (cf. th. 1.4). Nous nous servons du

LEMME. — Soient A' et B' deux polynômes non nuls et R' le reste de la division euclidienne de A' par B' .

— Si R' est nul, le P. G. C. D. de A' et B' est le polynôme unitaire associé à B' .

— Si R' est non nul, les diviseurs communs à A' et B' sont exactement les diviseurs communs à B' et R' .

Cela résulte aussitôt de la relation $A' = B'Q' + R'$.

Considérons les polynômes donnés A et B , et supposons par exemple que $d^0(A) \geq d^0(B)$. Dans ce cas, on commence par effectuer la division euclidienne de A par B ; on écrit donc $A = BQ_1 + R_1$, où $d^0(R_1) < d^0(B)$.

— Ou bien $R_1 = 0$, et le P. G. C. D. de A et B est alors le polynôme unitaire associé à B .

— Ou bien $R_1 \neq 0$, et le lemme précédent montre que

$$\text{P. G. C. D.}(A, B) = \text{P. G. C. D.}(B, R_1).$$

On est alors ramené au calcul du P. G. C. D. de B et de R_1 , où $d^0(R_1) < d^0(B)$. On répète ces opérations, et, puisque le degré du reste décroît d'au moins une unité à chaque division euclidienne effectuée, on aboutit au bout de n divisions au plus (où $n = d^0(B)$) à l'un des deux cas suivants :

— le dernier reste non nul n'est pas un polynôme constant; dans ce cas, le P. G. C. D. de A et de B est le polynôme unitaire associé à ce polynôme;

— le dernier reste non nul est un polynôme constant; dans ce cas, A et B sont premiers entre eux.

On notera enfin que le P. G. C. D. de deux polynômes n'étant pas changé lorsqu'on multiplie ces polynômes par des scalaires non nuls, on pourra éviter l'écriture de coefficients fractionnaires dans les divisions successives en multipliant le dividende par un scalaire convenable.

La méthode précédente porte le nom d'*algorithme d'Euclide*.

EXEMPLE. — Calculons le P. G. C. D. de $X^3 + 2X + 3$ et de $X^4 - X^3 + 4X^2 - X + 3$. On notera la disposition particulière des quotients, laquelle facilite les calculs.

$X^4 - X^3 + 4X^2 - X + 3$ $X^4 \quad \quad + 2X^2 + 3X$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $- X^3 + 2X^2 - 4X + 3$ $- X^3 \quad \quad - 2X - 3$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $2X^2 - 2X + 6$	$X - 1$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $X^3 \quad \quad + 2X + 3$ $X^3 - X^2 + 3X$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $X^2 - X + 3$ $X^2 - X + 3$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> 0	$X + 1$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $X^2 - X + 3$
---	---	---

Le P. G. C. D. est donc $X^2 - X + 3$.

Nous pouvons préciser l'identité de Bezout de la manière suivante :

PROPOSITION 1.18. — **Identité de Bezout pour deux polynômes.** — Soient A et B deux polynômes non nuls premiers entre eux. Pour tout polynôme P , il existe un couple (U, V) et un seul de polynômes tel que

$$P = AU + BV, \quad d^0(V) < d^0(A).$$

De plus, si $d^0(P) < d^0(A) + d^0(B)$, alors $d^0(U) < d^0(B)$.

En particulier, si A et B ne sont pas constants, il existe un couple (U, V) de polynômes et un seul tel que

$$1 = AU + BV, \quad d^0(V) < d^0(A), \quad d^0(U) < d^0(B)$$

(identité de Bezout avec condition sur les degrés).

Unicité. — Soit (U', V') un autre couple satisfaisant aux conditions de l'énoncé. Il en résulte que $A(U - U') = B(V' - V)$. Supposons par l'absurde que $V' \neq V$: le polynôme A divise $B(V' - V)$, et est premier avec B ; donc A divise $V' - V$, d'après la propriété de Gauss (cf. cor. 3 du th. 1.5), ce qui contredit la relation $d^0(V' - V) < d^0(A)$. Donc $V' = V$, et, par suite, $U' = U$.

Existence. — L'existence d'un couple (U_1, V_1) tel que $P = AU_1 + BV_1$ est immédiate, puisque A et B sont premiers entre eux (cf. cor. 2 du th. 1.5). Effectuons la division euclidienne de V_1 par A :

$$V_1 = AQ + V, \quad d^0(V) < d^0(A).$$

D'où la relation $P = AU + BV$, en posant $U = U_1 + BQ$.

Si nous supposons maintenant que $d^0(P) < d^0(A) + d^0(B)$, alors $d^0(U) < d^0(B)$, comme il résulte aussitôt de la relation $AU = P - BV$.

Une méthode de calcul explicite du couple (U, V) est esquissée dans l'exercice 42.

Exercices conseillés : 24, 25 et 41.

2. FORME RÉDUITE D'UNE FRACTION RATIONNELLE

Nous appliquons maintenant les résultats du § 5 à la théorie des fractions rationnelles.

PROPOSITION 1.19. — Forme réduite d'une fraction rationnelle. — *Soit R une fraction rationnelle non nulle à coefficients dans K . Il existe un couple (P, Q) et un seul de polynômes non nuls et premiers entre eux tel que $R = \frac{P}{Q}$, Q étant unitaire.*

Ce couple s'appelle forme réduite de la fraction rationnelle R . Les polynômes P et Q s'appellent respectivement numérateur et dénominateur de R .

Unicité. — Soient (P, Q) et (P', Q') deux couples de polynômes satisfaisant aux conditions de l'énoncé. Alors $PQ' = P'Q$. Le polynôme Q' divise donc $P'Q$; étant premier avec P' , il divise Q (propriété de Gauss). De même, Q divise Q' . Ces deux polynômes, étant de plus unitaires, sont égaux. L'anneau $K[X]$ étant intègre, il en résulte que $P = P'$, ce qui achève la démonstration.

Existence. — Soit (P_1, Q_1) un couple de polynômes tel que $Q_1 \neq 0$ et que $R = \frac{P_1}{Q_1}$. Puisque $R \neq 0$, $P_1 \neq 0$; désignons donc par D le P. G. C. D. de P_1 et Q_1 , et écrivons P_1 et Q_1 sous la forme $P_1 = DP_2$, et $Q_1 = DQ_2$. Nous savons que P_2 et Q_2 sont premiers entre eux (cf. prop. 16). De plus, $R = \frac{P_2}{Q_2}$, et il suffit maintenant de rendre Q_2 unitaire pour obtenir la décomposition cherchée.

COROLLAIRE. — Soient R et S deux éléments de $K(X)$. Si S est non constante, S est substituable dans R .

Écrivons en effet R sous la forme $R = \frac{U}{V}$, où $U, V \in K[X]$, $V \neq 0$, et S sous la forme réduite $S = \frac{P}{Q}$. Il suffit de prouver que $V \circ \frac{P}{Q}$ n'est pas nulle. Écartons le cas trivial où V est un monôme, et posons

$$V = \alpha_m X^m + \alpha_{m+1} X^{m+1} + \dots + \alpha_n X^n, \quad \text{où} \quad \alpha_m \neq 0, \alpha_n \neq 0.$$

Supposons par l'absurde que $V \circ \frac{P}{Q} = 0$, c'est-à-dire que

$$\alpha_m Q^{n-m} + \alpha_{m+1} Q^{n-m-1} P + \dots + \alpha_n P^{n-m} = 0.$$

Il en découle que P divise Q^{n-m} , comme P est premier avec Q , P est constant. De même, Q est constant, ce qui est impossible, puisque S est non constante.

PROPOSITION 1.20. — Décomposition en facteurs irréductibles. — On désigne encore par E l'ensemble des polynômes unitaires irréductibles à coefficients dans K .

1. Soit P un élément de E . Pour toute fraction rationnelle R non nulle à coefficients dans K , il existe un triplet (n, B, C) , où n est un entier rationnel, où B est un polynôme non nul premier avec P , et où C est un polynôme unitaire premier avec P , tel que $R = P^n \frac{B}{C}$, et que B et C soient premiers entre eux. Un tel triplet est unique.

L'application qui à tout élément non nul R de $K[X]$ associe l'entier rationnel n défini ci-dessus s'appelle valuation relative à P , et se note v_P . L'entier n est donc noté $v_P(R)$. On convient de poser $v_P(0) = +\infty$.

2. Pour tout élément non nul R de $K(X)$, l'ensemble des éléments P de E tels que $v_P(R)$ soit non nul est fini, et :

$$(1) \quad R = \alpha \prod_{P \in E} P^{v_P(R)},$$

ou α est un scalaire non nul.

Une telle décomposition est unique, c'est-à-dire que si R peut être écrite sous la forme

$$(2) \quad R = \beta \prod_{P \in E} P^{m_P},$$

où $\beta \in K^*$, et où (m_P) est une famille à support fini d'entiers naturels, alors $\beta = \alpha$ et, pour tout élément P de E , $m_P = v_P(R)$. Cette décomposition s'appelle *décomposition en facteurs unitaires irréductibles de la fraction rationnelle R* .

Assertion 1. — Pour montrer l'existence d'un tel triplet, nous écrivons R sous forme réduite $R = \frac{B'}{C'}$; il suffit alors d'appliquer l'assertion 1 du théorème 1.6 aux polynômes B' et C' .

Soient (n, B, C) et (n_1, B_1, C_1) deux triplets satisfaisant aux conditions de l'énoncé; alors $P^n \frac{B}{C} = P^{n_1} \frac{B_1}{C_1}$. Supposons par exemple $n_1 \geq n$, et posons $m = n_1 - n$. La relation précédente s'écrit encore $BC_1 = P^m B_1 C$; en prenant les valuations relatives à P des polynômes BC_1 et $P^m B_1 C$, nous obtenons la relation $m = 0$. Donc $n_1 = n$, et $\frac{B_1}{C_1} = \frac{B}{C}$; il découle alors de la proposition 1.19 que $B_1 = B$ et $C_1 = C$.

Assertion 2. — L'existence d'une décomposition de R sous la forme (2) est immédiate: il suffit d'écrire R sous la forme réduite $R = \frac{B'}{C'}$, et de décomposer les polynômes B' et C' en facteurs unitaires irréductibles. Comme dans la démonstration du théorème 1.6, on vérifiera aisément que si R est mise sous la forme (2), nécessairement $m_P = v_P(R)$ pour tout élément P de E .

REMARQUE 1. — Bien entendu, lorsque R est un polynôme, la notion de valuation introduite ci-dessus coïncide avec celle qui a été introduite au théorème 1.6; et lorsque P est de la forme $X - \gamma$, où $\gamma \in K$, elle coïncide avec la notion de valuation d'une fraction rationnelle au point γ , introduite dans la proposition 1.12.

REMARQUE 2. — Comme pour les polynômes, il résulte aisément du théorème précédent que pour tout couple (R, S) d'éléments de $K(X)$ et pour tout élément P de E ,

$$\begin{aligned} v_P(RS) &= v_P(R) + v_P(S); \\ v_P(R + S) &\geq \inf [v_P(R), v_P(S)], \end{aligned}$$

avec égalité si $v_P(R) \neq v_P(S)$.

Il en découle que l'ensemble des éléments R de $K(X)$ tels que $v_P(R)$ soit supérieur à un entier rationnel donné est un sous-espace vectoriel de $K(X)$.

3. PARTIES PRINCIPALES DES FRACTIONS RATIONNELLES

Appliquons maintenant les résultats du § 4.

PROPOSITION 1.21. — Partie entière d'une fraction rationnelle. — Pour tout élément R de $K(X)$, il existe un couple (U, R') constitué d'un polynôme U et d'une fraction rationnelle R' et un seul tel que

$$R = U + R', \quad d^0(R') < 0;$$

Autrement dit, les polynômes, et les fractions rationnelles de degré strictement négatif, constituent deux sous-espaces vectoriels supplémentaires dans l'espace vectoriel $K(X)$.

Le polynôme U ainsi défini s'appelle partie entière de R , ou encore partie principale à l'infini de R , et se note $\text{Pr}_\infty(R)$.

Si R est écrite sous la forme $R = \frac{P}{Q}$, où P et Q sont des polynômes, et où $Q \neq 0$, alors $\text{Pr}_\infty(R)$ est le quotient de la division euclidienne de P par Q .

L'application Pr_∞ qui à tout élément R de $K(X)$ associe sa partie entière $\text{Pr}_\infty(R)$ est donc un projecteur de l'espace vectoriel $K(X)$, dont l'image est le sous-espace vectoriel $K[X]$.

L'unicité du couple (U, R') résulte aussitôt de considérations de degré.

Existence du couple (U, R') . Écrivons R sous la forme $R = \frac{P}{Q}$; il existe (cf. th. 1.4) un couple (U, V) de polynômes tel que

$$P = QU + V, \quad d^0(V) < d^0(Q).$$

Il s'ensuit que

$$R = \frac{P}{Q} = U + \frac{V}{Q}, \quad d^0\left(\frac{V}{Q}\right) < 0.$$

Le couple $\left(U, \frac{Q}{V}\right)$ convient.

REMARQUE. — Pour que la partie principale à l'infini de R soit nulle, il faut et il suffit que $\tilde{R}(\infty)$ appartienne à K , ce qui explique la terminologie employée.

Le résultat suivant est fondamental :

THÉORÈME 1.7. — Décomposition des fractions rationnelles. — *Soit R une fraction rationnelle non nulle à coefficients dans K , écrite sous forme réduite $R = \frac{P}{Q}$. Soit (Q_1, Q_2, \dots, Q_n) une suite de polynômes unitaires, premiers entre eux deux à deux, et telle que*

$$Q = \prod_{i=1}^n Q_i.$$

1. *Il existe une suite (P_1, P_2, \dots, P_n) de polynômes telle que*

$$(1) \quad R = \frac{P}{Q} = \sum_{i=1}^n \frac{P_i}{Q_i}.$$

2. *Si l'on suppose de plus $d^0(P) < d^0(Q)$, il existe une suite (P_1, P_2, \dots, P_n) et une seule de polynômes telle que pour tout $i \in [1, n]$, $d^0(P_i) < d^0(Q_i)$, et qui satisfasse à la relation (1).*

Assertion 1. — Procédons par récurrence sur le nombre n de facteurs. Considérons d'abord le cas où $n = 2$, c'est-à-dire où Q est écrit sous la forme $Q = Q_1 Q_2$, où Q_1 et Q_2 sont unitaires et premiers entre eux. L'idéal engendré par Q_1 et Q_2 est donc $K[X]$ tout entier. En particulier, il existe un couple (P_1, P_2) de polynômes tel que $P = P_1 Q_2 + P_2 Q_1$, d'où il résulte que

$$\frac{P}{Q} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}.$$

Supposons maintenant le résultat établi à l'ordre $n - 1$, et soit (Q_1, Q_2, \dots, Q_n) une suite de polynômes satisfaisant aux conditions de l'énoncé. Le polynôme Q_n est premier avec Q_1, Q_2, \dots, Q_{n-1} , donc est premier avec leur produit Q' (cf. cor. de la prop. 1.15). Comme l'assertion est déjà établie lorsque $n = 2$, nous voyons qu'il existe un couple (P', P_n) de polynômes tel que

$$\frac{P}{Q} = \frac{P}{Q' Q_n} = \frac{P'}{Q'} + \frac{P_n}{Q_n}.$$

En appliquant l'hypothèse de récurrence à $\frac{P'}{Q'}$, nous obtenons la décomposition annoncée.

Assertion 2. — Existence. — Nous procédons encore par récurrence sur n . Lorsque $n = 2$, la proposition 1.18 affirme l'existence d'un couple (P_1, P_2) de polynômes satisfaisant aux conditions suivantes :

$$P = P_1 Q_2 + P_2 Q_1, \quad d^0(P_1) < d^0(Q_1), \quad d^0(P_2) < d^0(Q_2);$$

d'où la décomposition annoncée.

Le cas général s'en déduit exactement comme dans l'assertion 1.

Unicité. — Par différence, nous nous ramenons à prouver que si (P_1, P_2, \dots, P_n) est une suite de polynômes telle que pour tout $i \in [1, n]$, $d^0(P_i) < d^0(Q_i)$, et que

$$(2) \quad \sum_{i=1}^n \frac{P_i}{Q_i} = 0,$$

alors tous les polynômes P_i sont nuls.

Supposons par l'absurde que P_n , par exemple, soit non nul. Il découle aussitôt de la relation (2) qu'il existe un polynôme P' tel que

$$\frac{P_n}{Q_n} = \frac{P'}{Q'}.$$

ce qui signifie encore que $P_n Q' = P' Q_n$. Ainsi Q_n divise $P_n Q'$; comme Q_n est premier avec Q' , il s'ensuit que Q_n divise P_n , ce qui contredit la relation $d^0(P_n) < d^0(Q_n)$.

Le théorème est complètement démontré.

Pour appliquer le théorème précédent à la décomposition en facteurs irréductibles du polynôme Q , nous aurons besoin de la notion suivante :

DÉFINITION 1.16. — Fractions rationnelles P -adiques. — Soit P un polynôme unitaire irréductible à coefficients dans K . On dit qu'une fraction rationnelle R est P -adique s'il existe un entier naturel m tel que RP^m soit un polynôme.

Soit R un élément non nul de $K(X)$; il est immédiat que R est une fraction rationnelle P -adique si et seulement si R peut s'écrire sous la forme $R = P^n B$, où $n \in \mathbb{Z}$, et où B est un polynôme premier avec P . Nous savons d'ailleurs qu'une telle écriture est unique, grâce à la proposition 1.20.

Il est non moins immédiat que les fractions rationnelles P -adiques constituent un sous-espace vectoriel de l'espace vectoriel $K(X)$, et que les fractions rationnelles P -adiques de degré strictement négatif constituent un sous-espace vectoriel du précédent. Ce dernier sous-espace vectoriel est noté $K_p[X]$.

L'étude de l'espace vectoriel $K_p[X]$ est esquissée dans l'exercice 43.

PROPOSITION 1.22. — Partie principale d'une fraction rationnelle. — Soit P un polynôme unitaire irréductible à coefficients dans K . Pour toute fraction rationnelle R , il existe un couple (S, T) de fractions rationnelles et un seul tel que

$$R = S + T, \quad S \in K_p[X], \quad v_P(T) \geq 0.$$

Autrement dit, les fractions rationnelles P -adiques de degré strictement négatif, et les fractions rationnelles dont la valuation relative à P est positive, constituent deux sous-espaces vectoriels supplémentaires dans l'espace vectoriel $K(X)$.

La fraction rationnelle S ainsi définie s'appelle partie principale de R relative à P , et se note $\text{Pr}_P(R)$.

L'application Pr_P qui à tout élément R de $K(X)$ associe sa partie principale relative à P est donc un projecteur de l'espace vectoriel $K(X)$, dont l'image est le sous-espace vectoriel $K_p[X]$.

Unicité du couple (S, T) . — Par différence, tout revient à montrer que si R_1 est une fraction rationnelle P -adique telle que $d^\circ(R_1) < 0$ et que $v_P(R_1) \geq 0$, alors R_1 est nulle. Supposons par l'absurde que R_1 soit non nulle : comme R_1 est P -adique, nous pouvons écrire $R_1 = P^n B$, où $n \in \mathbb{Z}$ et où B est un polynôme premier avec P ; de plus, par définition des valuations, $v_P(R_1) = n$. Comme, par hypothèse, $v_P(R_1) \geq 0$, nous voyons que R_1 est un polynôme non nul, ce qui contredit la relation $d^\circ(R_1) < 0$.

Existence du couple (S, T) . — Si $v_P(R)$ est positif, le couple $(0, R)$ convient. Dans le cas contraire, R peut s'écrire sous la forme $R = P^n \frac{B}{C}$, où n est un entier rationnel strictement négatif, où B et C sont des polynômes premiers entre eux et premiers avec P , C étant unitaire. Posons $m = -n$, et appliquons la proposition 1.18 aux polynômes premiers entre eux P^m et C : il existe des polynômes U et V tels que

$$(1) \quad B = P^m U + CV, \quad d^\circ(V) < d^\circ(P^m).$$

D'où la relation

$$R = P^{-m} \frac{B}{C} = \frac{U}{C} + \frac{V}{P^m}, \quad d^0\left(\frac{V}{P^m}\right) < 0.$$

Le couple $\left(\frac{V}{P^m}, \frac{U}{C}\right)$ convient visiblement.

REMARQUE. — Le calcul effectif de la partie principale d'une fraction R relative à P se ramène à la détermination d'un polynôme V satisfaisant à la relation (1). Un algorithme y conduisant sera trouvé dans l'exercice 42.

THÉORÈME 1.8. — **Décomposition des fractions rationnelles en parties principales.** — *On désigne par E l'ensemble des polynômes unitaires irréductibles à coefficients dans K .*

1. *Soient R un élément de $K(X)$, $\text{Pr}_\infty(R)$ sa partie entière, et $\text{Pr}_P(R)$ sa partie principale relative au polynôme unitaire irréductible P . Alors l'ensemble des éléments P de E tels que $\text{Pr}_P(R) \neq 0$ coïncide avec l'ensemble des éléments P de E tels que $v_P(R) < 0$, donc est fini. De plus,*

$$(1) \quad R = \text{Pr}_\infty(R) + \sum_{P \in E} \text{Pr}_P(R).$$

2. *Une telle décomposition est unique, c'est-à-dire que si R peut être écrite sous la forme*

$$(2) \quad R = U + \sum_{P \in E} R_P,$$

où U est un élément de $K[X]$, et où (R_P) est une famille à support fini d'éléments de $K_P[X]$, alors

$$U = \text{Pr}_\infty(R), \quad \text{et}, \quad \forall P \in E, \quad R_P = \text{Pr}_P(R).$$

On peut donc formuler ce théorème de la manière suivante :

L'espace vectoriel $K(X)$ est somme directe du sous-espace $K[X]$ et de la famille des sous-espaces $K_P[X]$, où P parcourt E ; de plus, la famille constituée de l'application Pr_∞ et des applications Pr_P , où P parcourt E , n'est autre que la famille de projecteurs associée à la décomposition de l'espace vectoriel $K(X)$ en la somme directe précédente.

Nous prouvons d'abord que tout élément R de $K(X)$ peut être écrit sous la forme (2). En effet, d'après la proposition 1.21, R peut s'écrire sous la forme $R = U + R'$, où $U \in K[X]$, et où $d^0(R') < 0$. Si $R' = 0$, l'assertion est évidente; dans le cas contraire, nous écrivons R' sous forme réduite $R' = \frac{A}{B}$. Décomposons le polynôme unitaire B en facteurs unitaires irréductibles

(cf. th. 1.6) : il existe une suite (P_1, P_2, \dots, P_r) d'éléments de E et une suite (n_1, n_2, \dots, n_r) d'entiers strictement positifs telles que

$$B = \prod_{i=1}^r P_i^{n_i}.$$

Posons $B_i = P_i^{n_i}$; les polynômes B_i étant premiers entre eux deux à deux, et R' étant de degré strictement négatif, nous pouvons appliquer l'assertion 2 du théorème 1.7 : il existe une suite (A_1, A_2, \dots, A_r) de polynômes telle que pour tout $i \in [1, r]$, $d^0(A_i) < d^0(B_i)$, et que

$$R' = \frac{A}{B} = \sum_{i=1}^r \frac{A_i}{B_i}.$$

Les fractions rationnelles $\frac{A_i}{B_i}$ appartenant à $K_{P_i}[X]$, la décomposition cherchée en découle.

Il nous reste à montrer que si une fraction rationnelle R est mise sous la forme (2), alors $U = \text{Pr}_\infty(R)$, et, pour tout $P \in E$, $R_P = \text{Pr}_P(R)$.

a) Pour démontrer que $U = \text{Pr}_\infty(R)$, posons $R' = \sum_{P \in E} R_P$. Comme le degré de R_P est strictement négatif pour tout élément P de E , nous voyons qu'il en est de même du degré de R' . Ainsi

$$R = U + R', \quad d^0(R') < 0;$$

d'où la conclusion, par définition même des parties entières (cf. prop. 1.21).

b) Pour démontrer qu'étant donné un élément P de E , $R_P = \text{Pr}_P(R)$, posons $T_P = U + \sum_{\substack{Q \in E \\ Q \neq P}} R_Q$. Il est immédiat que pour tout élément Q de E différent de P , le nombre $v_P(R_Q)$ est positif. Comme il est évident que $v_P(U)$ est positif, la proposition 1.20 montre que $v_P(T_P)$ est positif. Ainsi,

$$R = R_P^\sharp + T_P, \quad R_P \in K_P[X], \quad v_P(T_P) \geq 0;$$

d'où la conclusion, par définition même des parties principales (cf. prop. 1.22).

La preuve du théorème est achevée.

REMARQUE 1. — En pratique, pour obtenir la décomposition d'une fraction rationnelle $R \neq 0$, on procède de la façon suivante :

1. On calcule la partie entière de R (cf. prop. 1.21).
2. On écrit R sous forme réduite $R = \frac{P}{Q}$ (cf. prop. 1.19).
3. On décompose Q en facteurs unitaires irréductibles (cf. th. 1.6).
4. On calcule les parties principales de R relatives à chaque polynôme unitaire irréductible intervenant dans la décomposition de Q (cf. prop. 1.22 et exercice 42).

5. La fraction rationnelle R n'est autre que la somme de sa partie entière et de toutes ses parties principales.

REMARQUE 2. — On peut encore décomposer chaque partie principale en une somme de fractions rationnelles d'un type encore plus particulier, appelées *éléments simples*. La décomposition des fractions rationnelles en éléments simples fera l'objet du § 9 lorsque le corps K est supposé algébriquement clos; dans le cas général, cette théorie fait l'objet de l'exercice 44.

§ 7. DÉRIVATION DES POLYNÔMES ET DES FRACTIONS RATIONNELLES

PROPOSITION 1.23. — **Dérivation des polynômes.** — Soit $K[X]$ l'algèbre des polynômes à une indéterminée à coefficients dans K . Il existe un endomorphisme D et un seul de l'espace vectoriel $K[X]$ tel que

a) pour tout couple (P, Q) d'éléments de $K[X]$,

$$(1) \quad D(PQ) = D(P)Q + PD(Q);$$

$$b) \quad D(X) = 1.$$

De plus, pour tout polynôme $P = \sum_{n=0}^{+\infty} \alpha_n X^n$, le polynôme $D(P)$ est donné par la formule

$$(2) \quad D(P) = \sum_{n=1}^{+\infty} n\alpha_n X^{n-1}.$$

Le polynôme $D(P)$ s'appelle polynôme dérivé du polynôme P ; on dit encore que $D(P)$ est la *dérivée* de P . L'endomorphisme D s'appelle *dérivation canonique* de l'algèbre $K[X]$. Plus généralement, pour tout entier naturel non nul n , le polynôme $D^n(P)$ s'appelle *dérivée $n^{\text{ième}}$* du polynôme P , et se note aussi $P^{(n)}$. Lorsque $n = 1$, $D(P)$ s'appelle encore dérivée première de P , et se note P' ; lorsque $n = 2$, $D^2(P)$ s'appelle dérivée seconde de P , et se note P'' , etc.

Unicité de D . — Soit D un endomorphisme de l'espace vectoriel $K[X]$ satisfaisant aux conditions a) et b). Alors, pour tout entier naturel non nul n ,

$$D(X^n) = nX^{n-1}.$$

Cette formule s'établit par récurrence sur n . Lorsque $n = 1$, il s'agit d'une évidence; supposons donc la formule démontrée pour l'entier $n - 1$, où $n \geq 2$, et calculons $D(X^n)$:

$$D(X^n) = D(XX^{n-1}) = D(X)X^{n-1} + XD(X^{n-1}) = nX^{n-1}D(X),$$

ce qu'il fallait prouver.

D'autre part, la condition *a*) appliquée au couple (1, 1) montre que $D(1) = 0$. La formule (2) en résulte par linéarité, ce qui prouve l'unicité de D .

Existence de D . — Associons à tout polynôme P le polynôme $D(P)$ défini par la formule (2), et prouvons que D convient. Il est évident que D est linéaire, et que $D(X) = 1$. Pour démontrer que la condition *a*) est satisfaite, considérons les applications $(P, Q) \mapsto D(PQ)$ et $(P, Q) \mapsto D(P)Q + PD(Q)$. Comme ces deux applications sont bilinéaires, et que les monômes X^n , $n \in \mathbb{N}$, constituent une base de l'espace vectoriel $K[X]$, il suffit, pour vérifier l'égalité de ces deux applications, de montrer qu'elles prennent même valeur sur les couples de la forme (X^p, X^q) , où p et q appartiennent à \mathbb{N} . Il suffit donc de vérifier que

$$D(X^{p+q}) = D(X^p)X^q + X^pD(X^q),$$

ce qui est immédiat.

REMARQUE. — Dans la suite de ce chapitre, nous allons rencontrer d'autres cas (cf. dérivation des fractions rationnelles et des séries entières formelles) d'endomorphismes satisfaisant aux conditions *a*) et *b*). Nous sommes ainsi conduit à poser la

DÉFINITION 1.17. — Dérivations d'une algèbre. — Soit E une K -algèbre. On appelle dérivation de E tout endomorphisme D de E tel que, pour tout couple (a, b) d'éléments de E ,

$$(1) \quad D(ab) = D(a)b + aD(b).$$

PROPOSITION 1.24. — Propriétés des dérivations. — Soit D une dérivation d'une K -algèbre associative commutative unitaire E .

1. Soit e l'élément unité de E . Alors

$$(2) \quad D(e) = 0.$$

Pour tout couple (a, b) d'éléments de E tel que b soit inversible,

$$(3) \quad D\left(\frac{a}{b}\right) = \frac{D(a)b - aD(b)}{b^2}.$$

2. Pour tout élément a de E et pour tout entier naturel non nul m ,

$$(4) \quad D(a^m) = ma^{m-1}D(a).$$

De plus, lorsque l'élément a est inversible, la formule (4) est valable pour tout entier rationnel m .

3. Pour toute suite (a_1, a_2, \dots, a_n) d'éléments de E ,

$$(5) \quad D(a_1 a_2 \dots a_n) = \sum_{i=1}^n a_1 a_2 \dots a_{i-1} D(a_i) a_{i+1} \dots a_n.$$

4. Pour tout couple (a, b) d'éléments de E et pour tout entier naturel non nul n ,

$$(6) \quad D^n(ab) = C_n^0 D^n(a)b + C_n^1 D^{n-1}(a)D(b) + \dots + C_n^p D^{n-p}(a)D^p(b) + \dots + C_n^n aD^n(b)$$

(formule de Leibniz).

Assertion 1. — La formule (2) s'obtient en appliquant la relation (1) au couple (e, e) .

Pour démontrer la formule (3), on montre d'abord que, pour tout élément inversible b de E ,

$$(7) \quad D\left(\frac{1}{b}\right) = -\frac{D(b)}{b^2},$$

en appliquant la relation (1) au couple $\left(b, \frac{1}{b}\right)$. La formule (3) s'obtient alors en appliquant la relation (1) au couple $\left(a, \frac{1}{b}\right)$.

Assertion 2. — La formule (4) se démontre par récurrence sur l'entier m . Lorsque $m = 1$, elle est évidente; supposons-la établie à l'ordre $m - 1$, où $m \geq 2$, et calculons $D(a^m)$:

$$D(a^m) = D(aa^{m-1}) = D(a)a^{m-1} + aD(a^{m-1}) = ma^{m-1}D(a).$$

Supposons maintenant que a soit inversible et que m soit négatif. Le cas où m est strictement négatif se ramène au cas précédent, en posant $m' = -m$ et en tenant compte de la relation (7). Enfin, le cas où $m = 0$ se réduit à la formule (2).

Assertion 3. — La formule (5) se déduit aussitôt de la formule (1) par récurrence sur l'entier n .

Assertion 4. — Pour $n = 1$, la formule de Leibniz se réduit à la relation (1). Supposons-la démontrée à l'ordre $n - 1$, où $n \geq 2$, et calculons $D^n(ab)$:

$$(8) \quad D^n(ab) = D[D^{n-1}(ab)].$$

Or, d'après l'hypothèse de récurrence,

$$(9) \quad D^{n-1}(ab) = \sum_{p=0}^{n-1} C_{n-1}^p a_p b_p,$$

où, pour tout $p \in [0, n - 1]$, $a_p = D^{n-p-1}(a)$ et $b_p = D^p(b)$.

Des relations (8) et (9), nous déduisons que

$$(10) \quad D^n(ab) = \sum_{p=0}^{n-1} C_{n-1}^p D(a_p b_p).$$

D'autre part,

$$D(a_p b_p) = D(a_p) b_p + a_p D(b_p) = D^{n-p}(a) D^p(b) + D^{n-p-1}(a) D^{p+1}(b).$$

D'où la relation

$$D^n(ab) = \sum_{k=0}^n \alpha_k D^{n-k}(a) D^k(b).$$

où les scalaires α_k sont définis par les relations suivantes :

$$\alpha_0 = 1, \quad \alpha_k = C_{n-1}^k + C_{n-1}^{k-1} \quad \text{si} \quad k \in [1, n-1], \quad \text{et} \quad \alpha_n = 1.$$

La formule de Leibniz en découle, puisque

$$C_n^0 = 1, \quad C_n^k = C_{n-1}^k + C_{n-1}^{k-1} \quad \text{si} \quad k \in [1, n-1], \quad \text{et} \quad C_n^n = 1.$$

COROLLAIRE. — Propriétés de la dérivation des polynômes.

1. Pour tout élément P de $K[X]$ et pour tout entier naturel non nul m ,

$$(4') \quad D(P^m) = m P^{m-1} D(P).$$

2. Pour toute suite (P_1, P_2, \dots, P_n) d'éléments de $K[X]$,

$$(5') \quad D(P_1 P_2 \dots P_n) = \sum_{i=1}^n P_1 P_2 \dots P_{i-1} D(P_i) P_{i+1} \dots P_n.$$

3. Pour tout couple (P, Q) d'éléments de $K[X]$ et pour tout entier naturel non nul n ,

$$(6') \quad D^n(PQ) = C_n^0 D^n(P) Q + C_n^1 D^{n-1}(P) D(Q) + \dots \\ + C_n^p D^{n-p}(P) D^p(Q) + \dots + C_n^n P D^n(Q)$$

(formule de Leibniz).

4. Soient m et n deux entiers naturels non nuls et α un scalaire.

$$\text{Si } n \geq m, \quad D^m(X - \alpha)^n = \frac{n!}{(n-m)!} (X - \alpha)^{n-m}.$$

$$\text{Si } n < m, \quad D^m(X - \alpha)^n = 0.$$

PROPOSITION 1.25. — Dérivée d'un polynôme composé. — Pour tout couple (P, Q) d'éléments de $K[X]$, la dérivée du polynôme composé $P \circ Q$ est donnée par la formule

$$(11) \quad D(P \circ Q) = [D(P) \circ Q] \cdot D(Q).$$

Les applications $P \mapsto D(P \circ Q)$ et $P \mapsto [D(P) \circ Q] \cdot D(Q)$ étant linéaires, il suffit de vérifier la formule (11) lorsque P est un monôme, auquel cas elle se réduit à la formule (4').

Nous abordons maintenant l'étude de l'injectivité et de la surjectivité de l'application D . Nous posons à cet effet la

DÉFINITION 1.18. — Primitives d'un polynôme. — *On dit qu'un polynôme P est une primitive d'un polynôme Q si la dérivée de P est égale à Q .*

Évidemment, si P est une primitive de Q , alors, pour tout scalaire β , $P + \beta$ est encore une primitive de Q . Plus précisément :

PROPOSITION 1.26. — Existence et unicité des primitives. — *Soit K un corps de caractéristique nulle.*

1. *Les constantes sont les seuls polynômes P tels que $D(P) = 0$. Si P_1 et P_2 sont deux primitives d'un même polynôme Q , $P_1 - P_2$ est une constante.*

2. *Étant donné un scalaire α et un polynôme Q , il existe une primitive P de Q et une seule telle que $P(\alpha) = 0$. Autrement dit, l'application linéaire $P \mapsto D(P)$ induit un isomorphisme de l'espace vectoriel des polynômes s'annulant au point α sur l'espace vectoriel $K[X]$.*

Assertion 1. — Puisque l'application D est linéaire, tout revient à montrer qu'un polynôme $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ tel que $D(P) = 0$ est constant. Or $D(P) = \sum_{n=1}^{+\infty} n\alpha_n X^{n-1}$; donc, pour tout entier $n \geq 1$, $n\alpha_n = 0$, et, puisque le corps K est de caractéristique nulle, $\alpha_n = 0$.

Assertion 2. — L'unicité de P résulte aussitôt de l'assertion 1. Montrons ensuite l'existence d'une primitive de $Q = \sum_{n=0}^{+\infty} \beta_n X^n$. Puisque K est de caractéristique nulle, il existe pour tout entier naturel n un scalaire γ_n tel que $(n+1)\gamma_n = \beta_n$, et γ_n est nul si n est strictement supérieur à $\deg(Q)$. Il est alors évident que le polynôme $P_0 = \sum_{n=0}^{+\infty} \gamma_n X^{n+1}$ est une primitive de Q telle que $P_0(0) = 0$.

Soit maintenant α un scalaire quelconque; le polynôme $P_\alpha = P_0 - P_0(\alpha)$ est une primitive de Q qui s'annule au point α .

REMARQUE. — Lorsque le corps K est de caractéristique p différente de zéro, la proposition précédente n'est pas valable : pour que le monôme X^n admette une primitive, il faut et il suffit que n ne soit pas congru à -1 modulo p , auquel cas $n+1$ est inversible dans K , et $\frac{X^{n+1}}{n+1}$ est une primitive de X^n .

PROPOSITION 1.27. — Dérivation des fractions rationnelles. — *Soit $K(X)$ le corps des fractions rationnelles à une indéterminée à coefficients dans K . Il existe une dérivation D et une seule de l'algèbre $K(X)$ telle que*

$$D(X) = 1.$$

Pour toute fraction rationnelle R , la fraction rationnelle $D(R)$ s'appelle *dérivée de R* . L'endomorphisme D s'appelle *dérivation canonique de l'algèbre $K(X)$* ; cet endomorphisme prolonge la dérivation canonique de l'algèbre $K[X]$.

De plus, pour tout élément R de $K(X)$, mis sous la forme $R = \frac{P}{Q}$, où P et Q sont des polynômes, Q étant non nul,

$$(1) \quad D(R) = \frac{D(P)Q - PD(Q)}{Q^2}.$$

Pour effectuer la démonstration, nous noterons D_1 la dérivation canonique de l'algèbre des polynômes.

Unicité de D . — Par hypothèse, pour tout couple (R, S) d'éléments de $K(X)$,

$$(2) \quad D(RS) = D(R)S + RD(S).$$

Le raisonnement utilisé dans le cas des polynômes (cf. prop. 1.23) montre que, pour tout élément P de $K[X]$, $D(P) = D_1(P)$.

Considérons alors un polynôme non nul Q , et appliquons la formule (2) au couple $\left(Q, \frac{1}{Q}\right)$:

$$D\left(Q \frac{1}{Q}\right) = D(Q) \frac{1}{Q} + QD\left(\frac{1}{Q}\right).$$

Nous en déduisons que

$$D\left(\frac{1}{Q}\right) = -\frac{D_1(Q)}{Q^2},$$

car

$$D\left(Q \frac{1}{Q}\right) = D(1) = D_1(1) = 0 \quad \text{et} \quad D(Q) = D_1(Q).$$

Soit maintenant R un élément de $K(X)$, écrit sous la forme $R = \frac{P}{Q}$, où P et Q sont des polynômes, Q étant non nul. En appliquant la formule (1) au couple $\left(P, \frac{1}{Q}\right)$, nous obtenons la formule

$$(3) \quad D(R) = \frac{D_1(P)Q - PD_1(Q)}{Q^2},$$

ce qui montre l'unicité de D .

Existence de D . — Définissons $D(R)$ par la formule (3), ce qui est licite : en effet, on vérifie facilement que si R est écrite sous la forme $R = \frac{P'}{Q'}$, où P' et Q' sont des polynômes, Q' étant non nul,

$$\frac{D_1(P)Q - PD_1(Q)}{Q^2} = \frac{D_1(P')Q' - P'D_1(Q')}{Q'^2}.$$

On vérifie ensuite que l'application D ainsi définie convient.

PROPOSITION 1.28. — **Propriétés de la dérivation des fractions rationnelles.**

1. Pour tout couple (R, S) d'éléments de $K(X)$, S étant non nul,

$$(1') \quad D\left(\frac{R}{S}\right) = \frac{D(R)S - RD(S)}{S^2}.$$

2. Pour tout élément non nul R de $K(X)$ et pour tout entier rationnel m ,

$$(4) \quad D(R^m) = mR^{m-1}D(R).$$

3. Pour toute suite (R_1, R_2, \dots, R_n) d'éléments de $K(X)$,

$$(5) \quad D(R_1 R_2 \dots R_n) = \sum_{i=1}^n R_1 R_2 \dots R_{i-1} D(R_i) R_{i+1} \dots R_n.$$

4. Pour tout couple (R, S) d'éléments de $K(X)$ et pour tout entier naturel non nul n ,

$$(6) \quad D^n(RS) = C_n^0 D^n(R)S + C_n^1 D^{n-1}(R)D(S) + \dots \\ + C_n^p D^{n-p}(R)D^p(S) + \dots + C_n^n R D^n(S)$$

(formule de Leibniz).

5. Pour tout entier naturel non nul m , pour tout entier rationnel n et pour tout scalaire α ,

$$(7) \quad D^m[(X - \alpha)^n] = n(n-1) \dots (n-m+1)(X - \alpha)^{n-m}.$$

6. Pour tout couple (R, S) d'éléments de $K(X)$ tel que $S \notin K$,

$$(8) \quad D(R \circ S) = [D(R) \circ S]D(S).$$

Les assertions 1 à 4 résultent des propriétés générales des dérivations (cf. prop. 1.24).

L'assertion 5 se démontre par récurrence sur l'entier m .

Assertion 6. — Lorsque R est un monôme, la formule (8) se réduit à la formule (4). Les applications $R \mapsto D(R \circ S)$ et $R \mapsto [D(R) \circ S]D(S)$ étant linéaires, la formule (8) en découle lorsque R est un polynôme. Lorsque R est de la forme $\frac{1}{Q}$, où Q est un polynôme non nul, écrivons que

$$D(R \circ S) = D\left(\frac{1}{Q \circ S}\right) = -\frac{D(Q \circ S)}{(Q \circ S)^2} = -\frac{D(Q) \circ S}{(Q \circ S)^2} D(S) = -\left(\frac{D(Q)}{Q^2} \circ S\right) D(S) \\ = [D(R) \circ S]D(S).$$

Enfin, si la formule (8) est vraie pour deux fractions rationnelles R_1 et R_2 , il est immédiat qu'elle est vraie pour leur produit $R_1 R_2$. Par suite, la formule (8) est vraie pour toute fraction rationnelle R .

REMARQUE 1. — Tout scalaire substituable dans R est encore substituable dans $D(R)$. (Cela résulte aussitôt de la formule (2).)

REMARQUE 2. — **Degré et valuations de la dérivée d'une fraction rationnelle.** Soit R une fraction rationnelle à éléments dans K .

Le degré de R' est inférieur ou égal à $d^0(R) - 1$, avec égalité si $d^0(R) \neq 0$. Lorsque $d^0(R) = 0$, on écrit $R = \beta + R_1$, où $d^0(R_1) < 0$; alors $d^0(R') = d^0(R_1) - 1$.

La valuation de R' en un point α de K est supérieure ou égale à $v_\alpha(R) - 1$, avec égalité si $v_\alpha(R) \neq 0$. Lorsque $v_\alpha(R) = 0$, on écrit $R = R(\alpha) + R_1$, où $v_\alpha(R_1) > 0$; alors $v_\alpha(R') = v_\alpha(R_1) - 1$.

La première assertion résulte facilement de la formule (1). Pour démontrer la deuxième assertion, on prouvera d'abord, grâce à la formule (1), que si la valuation $v_\alpha(R_1)$ d'une fraction rationnelle R_1 est nulle, alors $v_\alpha(R'_1)$ est positive. En supposant maintenant que $n = v_\alpha(R) \neq 0$, on écrira R sous la forme $R = (X - \alpha)^n R_1$, où $v_\alpha(R_1) = 0$. D'où $R' = (X - \alpha)^{n-1} [nR_1 + (X - \alpha)R'_1]$. Il suffit alors de tenir compte des propriétés classiques des valuations.

REMARQUE 3. — On dit qu'une fraction rationnelle R est une primitive d'une fraction rationnelle S si $D(R) = S$. Le problème de l'existence des primitives fait l'objet de l'exercice 67. Nous nous bornerons ici au résultat suivant :

PROPOSITION 1.29. — **Primitives d'une fraction rationnelle.** — Soit K un corps de caractéristique nulle. Alors les seules fractions rationnelles R telles que $D(R) = 0$ sont les constantes. Si R_1 et R_2 sont deux primitives d'une même fraction rationnelle S , $R_1 - R_2$ est une constante.

Soit en effet R un élément de $K(X)$ tel que $D(R) = 0$. Si $R \neq 0$, écrivons R sous forme réduite $R = \frac{P}{Q}$ (cf. prop. 1.19). La relation $D(R) = 0$ entraîne la relation $PD(Q) = QD(P)$. Supposons par l'absurde P non constant; il en résulte que $D(P) \neq 0$ (cf. prop. 1.26); donc $QD(P) \neq 0$, et, par suite, $D(Q) \neq 0$. Le polynôme Q divise $PD(Q)$, et est premier avec P ; il divise donc $D(Q)$, ce qui contredit la relation $d^0(Q) = d^0[D(Q)] + 1$. Le polynôme P est donc constant. La relation $PD(Q) = 0$ montre alors que Q est constant.

Pour calculer la dérivée d'un produit de plusieurs polynômes ou fractions rationnelles, on est amené à introduire la notion suivante :

DÉFINITION 1.19. — **Dérivée logarithmique d'une fraction rationnelle.** — Étant donnée une fraction rationnelle R non nulle, on appelle dérivée logarithmique de R la fraction rationnelle $\frac{D(R)}{R}$.

(Cette terminologie sera justifiée au § 10 ; cf. prop. 1.42.)

PROPOSITION 1.30. — Propriétés des dérivées logarithmiques.

1. Soient (R_1, R_2, \dots, R_r) une suite d'éléments non nuls de $K(X)$, et (n_1, n_2, \dots, n_r) une suite d'entiers rationnels. Alors la dérivée logarithmique de la fraction rationnelle $R = \prod_{p=1}^r R_p^{n_p}$ est donnée par la formule

$$\frac{D(R)}{R} = \sum_{p=1}^r n_p \frac{D(R_p)}{R_p}.$$

2. Soient R et S deux éléments non nuls de $K(X)$. S'il existe un scalaire non nul α tel que $S = \alpha R$, alors R et S ont même dérivée logarithmique. La réciproque est vraie lorsque le corps K est de caractéristique nulle.

Assertion 1. — La démonstration s'effectue par récurrence sur l'entier r , en utilisant les formules (1) et (4).

Assertion 2. — La première partie est évidente. Réciproquement, supposons que $\frac{D(R)}{R} = \frac{D(S)}{S}$; cette relation entraîne que la dérivée de la fraction rationnelle $T = \frac{S}{R}$ est nulle. Comme le corps K est de caractéristique nulle, la proposition 1.29 s'applique, ce qui prouve que T est une constante, évidemment non nulle.

Exercices conseillés : 58 à 69.

§ 8. ÉTUDE LOCALE DES POLYNÔMES ET DES FRACTIONS RATIONNELLES

1. PARTIE PRINCIPALE D'UNE FRACTION RATIONNELLE EN UN POINT

Nous allons appliquer la théorie des parties principales des fractions rationnelles (cf. § 6) relatives au polynôme $P = X - \alpha$, où $\alpha \in K$.

DÉFINITION 1.20. — Fractions rationnelles élémentaires. — Soit α un élément de K . On dit qu'une fraction rationnelle R à coefficients dans K est élémentaire relativement à α si R est $(X - \alpha)$ -adique, c'est-à-dire s'il existe un entier naturel m tel que $(X - \alpha)^m R$ soit un polynôme.

Toute fraction rationnelle R élémentaire relativement à α peut s'écrire sous la forme $R = (X - \alpha)^n \cdot B$, où $n \in \mathbb{Z}$, et où B est un polynôme premier avec $X - \alpha$, c'est-à-dire tel que $B(\alpha) \neq 0$; une telle écriture est unique.

Un polynôme P est élémentaire relativement à α . Nous savons d'ailleurs (cf. cor. 1 de la prop. 1.4) que P peut s'écrire d'une manière et d'une seule sous la forme $P = \sum_{n=0}^{+\infty} \gamma_n (X - \alpha)^n$. Plus généralement :

PROPOSITION 1.31. — Structure des fractions rationnelles élémentaires. — Soit α un élément de K .

1. Les fractions rationnelles élémentaires relativement à α constituent un sous-espace vectoriel de $K(X)$, et les fractions rationnelles $(X - \alpha)^n$, où n parcourt \mathbf{Z} , forment une base de ce sous-espace.

2. Les fractions rationnelles élémentaires relativement à α de degré strictement négatif constituent un sous-espace vectoriel du précédent. Ce dernier sous-espace vectoriel est noté $K_\alpha[X]$; les fractions rationnelles $(X - \alpha)^n$, où $n < 0$, en forment une base.

La proposition 1.22 se spécialise en la suivante :

PROPOSITION 1.32. — Partie principale d'une fraction rationnelle en un point. Soit α un élément de K . Pour toute fraction rationnelle R , il existe un couple (S, T) de fractions rationnelles et un seul tel que

$$R = S + T, \quad S \in K_\alpha[X], \quad v_\alpha(T) \geq 0.$$

La fraction rationnelle S ainsi définie est la partie principale de R relative à $X - \alpha$; on l'appelle plus simplement partie principale de R au point α , et on la note $\text{Pr}_\alpha(R)$.

Cette partie principale s'écrit donc d'une manière et d'une seule sous la forme

$$\text{Pr}_\alpha(R) = \sum_{r \in \mathbf{N}^*} \gamma_{-r} \frac{1}{(X - \alpha)^r}.$$

Le scalaire γ_{-1} s'appelle résidu de R au point α , et se note $\text{Res}_\alpha(R)$.

Pour tout élément α de K , l'application Res_α est une forme linéaire sur l'espace vectoriel $K(X)$.

REMARQUE. — Les résidus jouent un rôle important dans de nombreuses questions (cf. par exemple exercice 67). Dans ces mêmes questions, on utilise parfois la notion de résidu à l'infini d'une fraction rationnelle. On est amené (cf. exercice 73) à la définition suivante :

On appelle résidu à l'infini d'une fraction rationnelle R , et on note $\text{Res}_\infty(R)$, le résidu à l'origine de la fraction rationnelle

$$R_1(Y) = - \frac{1}{Y^2} R\left(\frac{1}{Y}\right).$$

L'application Res_∞ est une forme linéaire sur l'espace vectoriel $K(X)$.

On notera que $\text{Res}_\infty(R)$ est encore le terme constant de la partie entière de la fraction rationnelle $-XR(X)$. En particulier, lorsque R est de degré

strictement inférieur à -1 , son résidu à l'infini est nul; lorsque R est de degré égal à -1 , son résidu à l'infini est la valeur au point ∞ de $-XR(X)$; enfin, le résidu à l'infini d'un polynôme est nul.

La notion de partie principale peut se généraliser de la manière suivante :

PROPOSITION 1.33. — Développement limité d'une fraction rationnelle en un point. — Soient α un élément de K , et p un entier rationnel. Pour toute fraction rationnelle R , il existe un couple (S_p, T_p) de fractions rationnelles et un seul tel que

$$R = S_p + (X - \alpha)^{p+1}T_p, \quad S_p \in K_{\alpha,p}[X], \quad v_{\alpha}(T_p) \geq 0,$$

où $K_{\alpha,p}[X]$ désigne le sous-espace vectoriel de $K(X)$ constitué des fractions rationnelles élémentaires relativement à α de degré inférieur ou égal à p . La fraction rationnelle S_p ainsi définie s'appelle développement limité à l'ordre p de R au point α , et se note $\text{Pr}_{\alpha,p}(R)$.

L'application $\text{Pr}_{\alpha,p}$ est un projecteur de $K(X)$, dont l'image est le sous-espace vectoriel $K_{\alpha,p}[X]$.

(Lorsque $p = -1$, on retrouve la proposition précédente.)

Unicité du couple (S_p, T_p) . — Par différence, tout revient à montrer que si R_1 est une fraction rationnelle élémentaire relativement à α telle que $d^0(R_1) \leq p$, et que $v_{\alpha}(R_1) \geq p+1$, alors R_1 est nulle. Supposons par l'absurde que R_1 soit non nulle : comme R_1 est élémentaire relativement à α , nous pouvons écrire $R_1 = (X - \alpha)^n B$, où $n \in \mathbb{Z}$, et où B est un polynôme tel que $B(\alpha) \neq 0$; il en découle que $v_{\alpha}(R_1) = n \geq p+1$. Donc $d^0(R_1) = n + d^0(B) \geq p+1$, d'où la contradiction.

Existence du couple (S_p, T_p) . — Si $v_{\alpha}(R) \geq p+1$, le couple $(0, R(X - \alpha)^{-p-1})$ convient. Dans le cas contraire, posons $q = v_{\alpha}(R)$, et écrivons R sous la forme $R = (X - \alpha)^q \frac{A}{B}$, où A et B sont des polynômes premiers entre eux, et tels que $A(\alpha) \neq 0$ et $B(\alpha) \neq 0$. D'après l'identité de Bezout (cf. prop. 1.18), il existe des polynômes U et V tels que

$$(1) \quad A = (X - \alpha)^{p+1-q}U + BV, \quad d^0(V) < p+1-q.$$

D'où la relation

$$R = (X - \alpha)^{p+1} \frac{U}{B} + V(X - \alpha)^q, \quad d^0(V(X - \alpha)^q) \leq p.$$

Le couple $\left(V(X - \alpha)^q, \frac{U}{B}\right)$ convient visiblement.

REMARQUE 1. — Calcul des développements limités — Le calcul effectif de la partie principale d'une fraction rationnelle R en un point α , ou, plus généralement, du développement limité à l'ordre p de R au point α , se ramène à la détermination d'un couple (U, V) de polynômes satisfaisant à la relation (1). Par la substitution $X = \alpha + Y$, on voit qu'il suffit de traiter le cas où $\alpha = 0$, ce qui fait l'objet du sous-paragraphe 2. Le développement limité de R au point α est aussi donné par la formule de Taylor, qui fait l'objet du sous-paragraphe 3.

REMARQUE 2. — **Opérations sur les développements limités.** — On trouvera dans l'exercice 56 des règles permettant de calculer les développements limités de produits, quotients, composées et dérivées de fractions rationnelles. Ces règles peuvent souvent être utilisées pour le calcul pratique des développements limités.

2. DIVISION SUIVANT LES PUISSANCES CROISSANTES

PROPOSITION 1.34. — **Division suivant les puissances croissantes.** — Soient p un entier naturel, A et B deux polynômes à coefficients dans K , B étant tel que $B(0) = 1$. Il existe alors un couple (Q, R) et un seul d'éléments de $K[X]$ tel que

$$A = BQ + X^{p+1}R, \quad d^0(Q) \leq p.$$

Cela résulte aussitôt de l'identité de Bezout (cf. prop. 1.18), mais nous préférons donner une démonstration directe, applicable dans un cadre plus général, et fournissant une méthode pratique d'obtention du couple (Q, R) .

Unicité du couple (Q, R) . — Soit (Q', R') un second couple d'éléments de $K[X]$, tel que $A = BQ' + X^{p+1}R'$, et $d^0(Q') \leq p$. Il en résulte que $B(Q' - Q) = X^{p+1}(R - R')$; d'où la relation :

$$v_0(B) + v_0(Q' - Q) = p + 1 + v_0(R - R').$$

Comme $v_0(B) = 0$, cela implique que $v_0(Q' - Q) \geq p + 1$, ce qui impose $Q = Q'$, car, dans le cas contraire, $v_0(Q' - Q) \leq d^0(Q' - Q) \leq p$. Ainsi, $X^{p+1}R = X^{p+1}R'$, et enfin $R = R'$, puisque $K[X]$ est un anneau intègre.

Existence du couple (Q, R) . — La démonstration se fait par récurrence descendante sur la valuation de A ; elle fournit une méthode pratique d'obtention de Q et de R .

Lorsque $v_0(A) \geq p + 1$, nous écrivons $A = X^{p+1}C$, et le couple $(0, C)$ convient visiblement. Soit donc n un entier naturel inférieur ou égal à p ; supposons l'existence de (Q, R) établie pour tous les polynômes de valuation strictement supérieure à n , et considérons un polynôme A de valuation n .

Écrivons A et B sous la forme suivante :

$$\begin{aligned} A &= \alpha_n X^n + \alpha_{n+1} X^{n+1} + \dots + \alpha_m X^m, & \text{où } \alpha_n \neq 0, \\ B &= 1 + \beta_1 X + \dots + \beta_q X^q. \end{aligned}$$

Nous voyons que le polynôme $A_1 = A - \alpha_n X^n B$ est de valuation strictement supérieure à n , et nous pouvons donc lui appliquer l'hypothèse de récurrence : il existe un couple (Q_1, R_1) d'éléments de $K[X]$ tel que

$$A_1 = BQ_1 + X^{p+1}R_1, \quad \text{et} \quad d^0(Q_1) \leq p.$$

Il en résulte que $A = B(Q_1 + \alpha_n X^n) + X^{p+1}R_1$; le couple $(Q_1 + \alpha_n X^n, R_1)$ convient donc.

COROLLAIRE. — Soient p un entier naturel, A et B deux éléments de $K[X]$, B étant de valuation nulle. Il existe alors un couple (Q, R) et un seul d'éléments de $K[X]$ tel que

$$(1) \quad A = BQ + X^{p+1}R, \quad \text{et} \quad d^0(Q) \leq p.$$

Les polynômes Q et R s'appellent respectivement quotient et reste à l'ordre p de la division de A par B suivant les puissances croissantes.

REMARQUE 1. — Soient A et B deux polynômes, B étant de valuation nulle. Si p et n sont deux entiers naturels tels que $p > n$, on obtient le quotient Q_n de A par B à l'ordre n en supprimant dans le quotient Q_p de A par B à l'ordre p les termes de degré strictement supérieur à n .

Divisons en effet A par B à l'ordre p :

$$A = BQ_p + X^{p+1}R_p, \quad d^0(Q_p) \leq p,$$

et écrivons Q_p sous la forme $Q_p = Q'_n + X^{n+1}R'_n$. Nous obtenons la relation

$$A = BQ'_n + X^{n+1}(BR'_n + X^{p-n}R_p), \quad d^0(Q'_n) \leq n;$$

par unicité, le polynôme Q'_n est donc égal à Q_n .

REMARQUE 2. — De la même façon, on montre qu'on ne change pas le quotient de A par B à l'ordre p en ajoutant à A , ou à B , un polynôme de valuation strictement supérieur à p . Il en découle que pour calculer ce quotient, on peut supprimer dans A et B les termes de degré strictement supérieur à p .

REMARQUE 3. — La pratique de la division suivant les puissances croissantes s'en déduit :

— On ordonne A et B suivant les puissances croissantes, on place A au dividende, en laissant des vides pour les degrés manquants inférieurs ou égaux à p , et on place B au diviseur.

— Le premier terme du quotient est $\frac{\alpha_n}{\beta_0} X^n$.

— On écrit le polynôme $\frac{\alpha_n}{\beta_0} X^n B$ en dessous du polynôme A , et on le retranche de A ; on obtient ainsi A_1 .

— On répète ces opérations jusqu'à obtention au dividende d'un polynôme de valuation strictement supérieure à p ; mettant X^{p+1} en facteur dans ce polynôme, on obtient le reste à l'ordre p , tandis que le quotient est écrit à son emplacement traditionnel.

EXEMPLE. — Division suivant les puissances croissantes de $A = 1 + X$ par $B = 1 + X + X^2$ à l'ordre 4.

$$\begin{array}{r|l}
 \begin{array}{r}
 1 + X \\
 1 + X + X^2 \\
 \hline
 - X^2 \\
 - X^2 - X^3 - X^4 \\
 \hline
 X^3 + X^4 \\
 X^3 + X^4 + X^5 \\
 \hline
 - X^5
 \end{array}
 &
 \begin{array}{r}
 1 + X + X^2 \\
 \hline
 1 - X^2 + X^3
 \end{array}
 \end{array}$$

Le quotient Q_4 est donc $1 - X^2 + X^3$, et le reste R_4 est -1 .

REMARQUE 4. — **Calcul des parties principales d'une fraction rationnelle.** — Comme il a été annoncé, on peut déduire du théorème de division suivant les puissances croissantes une méthode pratique de recherche des parties principales d'une fraction rationnelle :

Soient R une fraction rationnelle, et α un pôle d'ordre n de R .

— *On effectue dans la fraction $R(X)$ la substitution $X = \alpha + Y$. On obtient ainsi une fraction rationnelle $R_1(Y)$, écrite sous la forme*

$$R_1(Y) = \frac{P(Y)}{Y^n Q(Y)}, \quad \text{où} \quad P(0) \neq 0 \quad \text{et} \quad Q(0) \neq 0.$$

— *On procède à la division de P par Q suivant les puissances croissantes de Y jusqu'à l'ordre $n - 1$; on obtient donc des polynômes U et V tels que*

$$P = QV + Y^n U, \quad \text{d}^\circ(V) \leq n - 1.$$

— *Le polynôme V peut s'écrire sous la forme*

$$V = \beta_n + \beta_{n-1} Y + \dots + \beta_1 Y^{n-1}.$$

Dans ces conditions, la partie principale $\text{Pr}_\alpha(R)$ de R au point α est donnée par la formule

$$\text{Pr}_\alpha(R) = \frac{\beta_n}{(X - \alpha)^n} + \frac{\beta_{n-1}}{(X - \alpha)^{n-1}} + \dots + \frac{\beta_1}{X - \alpha}.$$

EXEMPLE. — Recherche de la partie principale au point 1 de la fraction rationnelle à coefficients complexes

$$R(X) = \frac{1}{(X - 1)^3(X + 1)X}.$$

— Substituons $1 + Y$ à X :

$$R_1(Y) = R(1 + Y) = \frac{1}{Y^3(2 + Y)(1 + Y)}.$$

— Divisons 1 par $(2 + Y)(1 + Y) = 2 + 3Y + Y^2$ suivant les puissances croissantes de Y à l'ordre 2; le quotient V est donné par la formule

$$V = \frac{1}{2} - \frac{3}{4} Y + \frac{7}{8} Y^2.$$

La partie principale cherchée s'écrit donc :

$$\text{Pr}_1(R) = \frac{1}{2} \cdot \frac{1}{(X - 1)^3} - \frac{3}{4} \cdot \frac{1}{(X - 1)^2} + \frac{7}{8} \cdot \frac{1}{X - 1}.$$

REMARQUE 5. — **Cas d'un pôle simple.** — Lorsque α est un pôle simple de R , le procédé précédent fournit la règle qui suit :

Soit R une fraction rationnelle admettant α pour pôle simple, écrite sous la

forme $R = \frac{P}{(X - \alpha)Q}$, où $P(\alpha) \neq 0$, $Q(\alpha) \neq 0$. La partie principale de R au point α est donnée par la formule

$$\text{Pr}_\alpha(R) = \frac{P(\alpha)}{Q(\alpha)} \cdot \frac{1}{X - \alpha}.$$

REMARQUE 6. — En pratique, la méthode de recherche de la partie principale d'une fraction rationnelle R en un point α que nous venons d'exposer est recommandable lorsque le pôle α est mis en évidence, c'est-à-dire lorsqu'il est très simple d'écrire R sous la forme

$$R = \frac{P}{(X - \alpha)^n Q}, \quad P(\alpha) \neq 0, \quad Q(\alpha) \neq 0.$$

Dans le cas contraire, on utilisera plutôt une méthode déduite de la formule de Taylor, qui fait l'objet du sous-paragraphe suivant.

3. FORMULE DE TAYLOR

THÉORÈME 1.9. — **Formule de Taylor pour un polynôme à une indéterminée.** Soient K un corps de caractéristique zéro, P un élément de $K[X]$, et α un élément de K . Alors :

$$P = \sum_{p=0}^{+\infty} [D^p(P)](\alpha) \cdot \frac{(X - \alpha)^p}{p!} \quad (\text{formule de Taylor}).$$

Bien entendu, le second membre a un sens, puisque $[D^p(P)](\alpha)$ est nul dès que p est strictement supérieur à $n = d^\circ(P)$.

Nous savons déjà que les polynômes $1, X - \alpha, \dots, (X - \alpha)^p, \dots$, forment une base de l'espace vectoriel $K[X]$. Le polynôme P s'écrit donc de manière unique sous la forme

$$(1) \quad P = \sum_{p=0}^{+\infty} \beta_p \cdot (X - \alpha)^p, \quad \text{où, pour tout } p \in \mathbb{N}, \beta_p \in K.$$

Ainsi, tout revient à calculer les scalaires β_p . Pour calculer β_q , où q est un entier naturel donné, dérivons q fois l'égalité (1) en tenant compte des formules suivantes :

$$\begin{aligned} \text{si} \quad & q > p, & D^q[(X - \alpha)^p] &= 0 \\ \text{si} \quad & q \leq p, & D^q[(X - \alpha)^p] &= \frac{p!}{(p - q)!} \cdot (X - \alpha)^{p - q}. \end{aligned}$$

D'où la relation

$$D^q(P) = \sum_{p=q}^{+\infty} \beta_p \cdot \frac{p!}{(p - q)!} \cdot (X - \alpha)^{p - q}.$$

En substituant dans cette égalité le scalaire α à l'indéterminée X , nous obtenons la relation

$$[D^q(P)](\alpha) = \beta_q \cdot q !$$

Le corps K étant de caractéristique zéro, il en découle que

$$\beta_q = \frac{1}{q !} [D^q(P)](\alpha),$$

ce qu'il fallait démontrer.

COROLLAIRE 1. — Formule de Maclaurin. — *Pour tout élément P de $K[X]$,*

$$P = P(0) + [D(P)](0) \cdot \frac{X}{1 !} + \dots + [D^p(P)](0) \cdot \frac{X^p}{p !} + \dots + [D^n(P)](0) \cdot \frac{X^n}{n !},$$

où n désigne le degré de P .

COROLLAIRE 2. — Critère de multiplicité d'une racine d'un polynôme. — *Soient K un corps de caractéristique zéro, P un élément non nul de $K[X]$, α un élément de K , et m un entier strictement positif. Pour que α soit racine d'ordre m du polynôme P , il faut et il suffit que*

$$P(\alpha) = 0, \quad [D(P)](\alpha) = 0, \dots, \quad [D^{m-1}(P)](\alpha) = 0, \quad \text{et} \quad [D^m(P)](\alpha) \neq 0.$$

Puisque P est non nul, la formule de Taylor montre qu'il existe un entier p tel que $[D^p(P)](\alpha) \neq 0$. Désignons par r le plus petit des entiers p tels que $[D^p(P)](\alpha) \neq 0$. La formule de Taylor appliquée au polynôme P montre aussitôt que P est de la forme

$$P = (X - \alpha)^r Q, \quad \text{où} \quad Q(\alpha) \neq 0.$$

L'entier r est donc égal à la valuation $v_\alpha(P)$ de P au point α . Par définition de l'ordre de multiplicité d'une racine, pour que α soit racine d'ordre m de P , il faut et il suffit que $v_\alpha(P) = m$, donc que $m = r$, ce qu'il fallait démontrer.

La formule de Taylor fournit le développement limité d'un polynôme P en un point α à tout ordre. Une formule analogue fournit le développement limité d'une fraction rationnelle en un point :

THÉORÈME 1.10. — Formule de Taylor pour une fraction rationnelle à une indéterminée. — *Soient K un corps de caractéristique zéro, R un élément de $K(X)$, α un élément de K substituable dans R , et p un entier naturel. Alors le développement limité $\text{Pr}_{\alpha,p}(R)$ à l'ordre p de la fraction rationnelle R au point α est donné par la formule suivante :*

$$\text{Pr}_{\alpha,p}(R) = \sum_{r=0}^p [D^r(R)](\alpha) \cdot \frac{(X - \alpha)^r}{r !}.$$

Autrement dit, il existe une fraction rationnelle T_p telle que

$$R = \sum_{r=0}^p [D^r(R)](\alpha) \cdot \frac{(X - \alpha)^r}{r!} + (X - \alpha)^{p+1} T_p, \quad v_\alpha(T_p) \geq 0.$$

Cette dernière formule s'appelle *formule de Taylor à l'ordre p appliquée à la fraction rationnelle R au point α* .

Nous savons déjà (cf. prop. 1.33) que R peut s'écrire d'une manière et d'une seule sous la forme

$$(1) \quad R = \sum_{r=0}^p \beta_r (X - \alpha)^r + (X - \alpha)^{p+1} T_p,$$

où $v_\alpha(T_p) \geq 0$, et où, pour tout $r \in [0, p]$, $\beta_r \in K$.

Pour calculer β_q , où q est un entier donné, $q \in [0, p]$, on dérive q fois l'égalité (1), et l'on substitue ensuite le scalaire α à l'indéterminée X . On obtient la formule

$$[D^q(R)](\alpha) = \beta_q q !$$

Le théorème s'en déduit, puisque K est de caractéristique zéro.

COROLLAIRE. — Calcul du développement limité à l'ordre p d'une fraction rationnelle en un point. — Soient K un corps de caractéristique zéro, R un élément de $K(X)$, α un pôle de R d'ordre n , et p un entier rationnel supérieur ou égal à $-n$. Soit enfin $\text{Pr}_{\alpha,p}(R) = \sum_{r=-n}^p \gamma_r (X - \alpha)^r$ le développement limité à l'ordre p de la fraction R au point α . Alors, pour tout entier $r \in [-n, p]$, le scalaire γ_r est donné par la formule suivante :

$$\gamma_r = \frac{1}{(n+r)!} [D^{n+r}((X - \alpha)^n R)](\alpha).$$

En particulier, le résidu de R au point α est donné par la formule

$$\text{Res}_\alpha(R) = \gamma_{-1} = \frac{1}{(n-1)!} [D^{n-1}((X - \alpha)^n R)](\alpha).$$

Il suffit d'appliquer le théorème à la fraction rationnelle $R_1 = (X - \alpha)^n R$. Lorsque $p = -1$, le corollaire précédent fournit une méthode de calcul de la partie principale d'une fraction rationnelle en un point. Le problème pratique qui se pose alors est d'expliciter les dérivées successives de $(X - \alpha)^n R$; c'est ce que nous allons faire maintenant dans quelques cas particuliers :

EXEMPLE 1. — Calcul de γ_{-n} . — Soit R une fraction rationnelle admettant α pour pôle d'ordre n , écrite sous la forme $R = \frac{P}{Q}$, où $P(\alpha) \neq 0$. Le coefficient γ_{-n}

de $\frac{1}{(X - \alpha)^n}$ dans la partie principale de R au point α est donné par la formule suivante :

$$\gamma_{-n} = n! \frac{P(\alpha)}{[D^n(Q)](\alpha)}.$$

En effet, $\gamma_{-n} = [R(X - \alpha)^n](\alpha)$. Or, α étant une racine d'ordre n de Q , la formule de Taylor au point α appliquée au polynôme Q montre que Q peut s'écrire sous la forme $Q = (X - \alpha)^n Q_1$, où Q_1 est un polynôme tel que $Q_1(\alpha) = \frac{1}{n!} [D^n(Q)](\alpha)$. Le résultat annoncé en découle aussitôt.

En particulier, si α est un pôle simple de R , la partie principale de R au point α est donnée par la formule suivante :

$$\text{Pr}_\alpha(R) = \frac{P(\alpha)}{Q'(\alpha)} \cdot \frac{1}{X - \alpha};$$

le résidu de R au point α est donc égal à $\frac{P(\alpha)}{Q'(\alpha)}$.

En pratique, la formule précédente est à recommander lorsque le facteur $X - \alpha$ n'est pas en évidence dans le dénominateur Q de R . A titre d'exemple, on pourra calculer les parties principales de la fraction rationnelle à coefficients complexes $\frac{1}{X^n - 1}$.

EXEMPLE 2. — Cas d'un pôle double. — On pourra, à titre d'exercice, démontrer que si α est un pôle double d'une fraction rationnelle R , écrite sous la forme $R = \frac{P}{Q}$, où $P(\alpha) \neq 0$, alors

$$\gamma_{-2} = 2 \frac{P(\alpha)}{Q''(\alpha)} \quad \text{et} \quad \gamma_{-1} = \frac{2}{3} \cdot \frac{3P'(\alpha)Q''(\alpha) - P(\alpha)Q'''(\alpha)}{Q''(\alpha)^2}.$$

Exercices conseillés : 70 à 73.

§ 9. CORPS ALGÈBRIQUEMENT CLOS

1. CORPS ALGÈBRIQUEMENT CLOS

Comme nous l'avons déjà constaté, les propriétés de divisibilité pour un polynôme P se simplifient considérablement lorsque P est scindé sur K . Nous sommes ainsi amené à poser la

DÉFINITION 1.21. — Corps algébriquement clos. — *On dit qu'un corps commutatif K est algébriquement clos si tout polynôme non constant à coefficients dans K admet au moins une racine dans K .*

REMARQUE. — *Tout corps algébriquement clos est infini.* — En effet, pour tout corps fini K ayant q éléments $\alpha_1, \alpha_2, \dots, \alpha_q$, le polynôme $\prod_{i=1}^q (X - \alpha_i) + 1$ n'a pas de racine dans K .

L'intérêt de la notion de corps algébriquement clos apparaît dans les deux propositions suivantes :

PROPOSITION 1.35. — Polynômes irréductibles à coefficients dans un corps algébriquement clos. — *Les seuls polynômes irréductibles à coefficients dans un corps algébriquement clos sont les polynômes de degré 1.*

Nous savons déjà que, pour tout corps K , un polynôme de degré 1 est irréductible. Supposons maintenant K algébriquement clos, et montrons qu'un polynôme P de degré $n > 1$ n'est pas irréductible : P étant non constant, il existe un élément α de K tel que $P(\alpha) = 0$; le polynôme P est donc divisible par $X - \alpha$, c'est-à-dire qu'il existe un polynôme Q tel que $P = (X - \alpha)Q$. Puisque $d^0(Q) = n - 1 > 0$, le polynôme P n'est pas irréductible.

REMARQUE. — Réciproquement, si tout polynôme à coefficients dans un corps K irréductible sur K est de degré 1, alors K est algébriquement clos.

Cela résulte aussitôt du théorème 1.6 (décomposition en facteurs irréductibles).

PROPOSITION 1.36. — Décomposition en facteurs irréductibles pour un polynôme à coefficients dans un corps algébriquement clos. — *Soit K un corps algébriquement clos. Alors tout polynôme à coefficients dans K est scindé sur K .*

Autrement dit : soient A un polynôme non constant à coefficients dans K , $\alpha_1, \alpha_2, \dots, \alpha_r$ les racines de A dans K , n_1, n_2, \dots, n_r leurs ordres de multiplicité, et β le coefficient dominant de A . Alors

$$A = \beta \prod_{p=1}^r (X - \alpha_p)^{n_p}.$$

Cette décomposition n'est autre que l'unique décomposition en facteurs irréductibles de A , c'est-à-dire que pour tout $p \in [1, r]$, n_p est égal à la valuation de A au point α_p .

Cette proposition résulte aussitôt de la précédente et du théorème 1.6.

COROLLAIRE. — Critère de divisibilité. — *Soient K un sous-corps d'un corps K' algébriquement clos, A et B deux polynômes non nuls à coefficients dans K . Pour que B divise A dans $K[X]$, il faut et il suffit que, A et B étant considérés comme éléments de $K'[X]$, toute racine d'ordre p de B soit racine de A avec un ordre de multiplicité supérieur ou égal à p .*

En effet, pour que B divise A dans $K[X]$, il faut et il suffit que B divise A dans $K'[X]$ (cf. cor. 2 du th. 1.4). L'assertion résulte alors du corollaire 1 du théorème 1.6.

Nous étudions maintenant les fractions rationnelles à coefficients dans un corps algébriquement clos.

DÉFINITION 1.22. — Éléments simples. — *Soit K un corps algébriquement clos. On appelle éléments simples (à coefficients dans K) les fractions rationnelles à coefficients dans K des types suivants :*

- a) les monômes X^p , où $p \in \mathbb{N}$;
- b) les fractions rationnelles $\frac{1}{(X - \alpha)^n}$, où $\alpha \in K$, et $n \in \mathbb{N}^*$.

THÉORÈME 1.11. — Décomposition des fractions rationnelles en éléments simples (cas d'un corps algébriquement clos). — *Soit K un corps algébriquement clos. Alors les éléments simples à coefficients dans K forment une base de l'espace vectoriel $K(X)$ des fractions rationnelles à coefficients dans K .*

Autrement dit : tout élément R de $K(X)$ peut s'écrire d'une manière et d'une seule sous la forme

$$R = \sum_{p=0}^{+\infty} \gamma_p X^p + \sum_{\alpha \in K, n \in \mathbb{N}^*} \beta_{\alpha, n} \frac{1}{(X - \alpha)^n},$$

où, pour tout $p \in \mathbb{N}$, $\gamma_p \in K$, et où pour tout $\alpha \in K$ et pour tout $n \in \mathbb{N}^*$, $\beta_{\alpha, n} \in K$. Cette décomposition s'appelle décomposition sur K de R en éléments simples.

De plus, le polynôme $\sum_{p=0}^{+\infty} \gamma_p X^p$ n'est autre que la partie entière $\text{Pr}_\infty(R)$ de la fraction rationnelle R , tandis que pour tout élément α de K , la fraction rationnelle $\sum_{n \in \mathbb{N}^*} \beta_{\alpha, n} \frac{1}{(X - \alpha)^n}$ n'est autre que la partie principale $\text{Pr}_\alpha(R)$ de la fraction rationnelle R au point α .

Ainsi,

$$R = \text{Pr}_\infty(R) + \sum_{\alpha \in K} \text{Pr}_\alpha(R).$$

Explicitons d'abord le théorème 1.8 dans le cas des corps algébriquement clos : l'espace vectoriel $K(X)$ est somme directe du sous-espace $K[X]$ et de la famille des sous-espaces $K_\alpha[X]$, où α parcourt K . (Rappelons que $K_\alpha[X]$ désigne l'ensemble des fractions rationnelles élémentaires relativement à α de degré strictement négatif.) De plus, la famille constituée de l'application Pr_∞ et des applications Pr_α , où α parcourt K , n'est autre que la famille des projecteurs associée à la décomposition de $K(X)$ en la somme directe précédente.

Or, les monômes X^p , où p parcourt \mathbb{N} , forment une base de l'espace vectoriel $K[X]$, tandis que pour tout élément α de K , les fractions ration-

nelles $\frac{1}{(X - \alpha)^n}$, où n parcourt \mathbf{N}^* , forment une base de l'espace vectoriel $K_\alpha[X]$. Le théorème s'en déduit aussitôt.

COROLLAIRE. — Formule des résidus. — *Soit K un corps algébriquement clos. Alors, pour toute fraction rationnelle R à coefficients dans K ,*

$$(1) \quad \text{Res}_\infty(R) + \sum_{\alpha \in K} \text{Res}_\alpha(R) = 0.$$

Grâce à la linéarité des applications Res_α et Res_∞ , il suffit de prouver la formule (1) d'une part lorsque R est un polynôme, cas où elle est évidente, d'autre part lorsque R est de degré strictement négatif; alors

$$R = \sum_{\alpha \in K} \text{Pr}_\alpha(R).$$

Il en découle que le degré de la fraction rationnelle

$$S = R - \sum_{\alpha \in K} \text{Res}_\alpha(R) \frac{1}{X - \alpha}$$

est strictement inférieur à -1 . Le résidu à l'infini de S est donc nul; or,

$$\text{Res}_\infty(S) = \text{Res}_\infty(R) - \sum_{\alpha \in K} \text{Res}_\alpha(R) \text{Res}_\infty\left(\frac{1}{X - \alpha}\right) = \text{Res}_\infty(R) + \sum_{\alpha \in K} \text{Res}_\alpha(R),$$

ce qui achève la démonstration.

EXEMPLE. — *Soit R une fraction rationnelle à coefficients dans un corps algébriquement clos. On suppose R non constante, et décomposée en facteurs irréductibles :*

$$R = \beta \prod_{\alpha \in K} (X - \alpha)^{v_\alpha(R)}.$$

La décomposition en éléments simples de $\frac{R'}{R}$ est alors donnée par la formule :

$$\frac{R'}{R} = \sum_{\alpha \in K} v_\alpha(R) \frac{1}{X - \alpha}.$$

Pratique de la décomposition en éléments simples. — Pour décomposer une fraction rationnelle R en éléments simples, on cherche d'abord les pôles de R et leurs ordres de multiplicité, et l'on écrit *a priori* la décomposition de R avec des coefficients indéterminés. Étant assuré de l'existence et de l'unicité de ces coefficients, on les calculera par toute méthode semblant avantageuse. Une méthode générale consiste à calculer la partie entière de R et la partie principale de R en chacun de ses pôles, comme il a été expliqué plus haut. On peut

aussi substituer à l'indéterminée X des scalaires convenablement choisis. Cette dernière méthode ne présente un intérêt que lorsqu'on a déjà calculé tous les coefficients sauf un ou deux. (Sinon, on est conduit à des systèmes d'équations linéaires inextricables.) On notera enfin que la formule des résidus (cf. cor. du th. 1.11) fournit une relation linéaire liant les coefficients en question.

Lorsque R est une fraction paire, ou impaire, les coefficients de la partie principale de R au pôle $-\alpha$ sont liés simplement aux coefficients de la partie principale de R au pôle α : il suffit d'écrire la décomposition de R en éléments simples, de substituer $-X$ à X dans cette formule, et d'utiliser l'unicité de la dite décomposition.

Lorsque R est de la forme $P \cdot (S \circ T)$, où $P \in K[X]$ et où S et T sont deux éléments non constants de $K(X)$, il peut être commode, pour décomposer R en éléments simples, de décomposer d'abord S en éléments simples. On est alors ramené à décomposer en éléments simples des fractions rationnelles des types suivants : PT^n , où $n \in \mathbb{N}$, et $\frac{P}{(T - \alpha)^p}$ où α est un pôle d'ordre p de S .

Cette méthode est utilisée dans les développements eulériens; cf. exercice 54.

2. THÉORÈME FONDAMENTAL DE L'ALGÈBRE

THÉORÈME 1.12. — Théorème fondamental de l'algèbre (d'Alembert-Gauss).
Le corps des nombres complexes est algébriquement clos.

Autrement dit : pour tout polynôme P à coefficients complexes non constant, il existe un nombre complexe α tel que $P(\alpha) = 0$.

Ce résultat fondamental a été énoncé par d'Alembert. Beaucoup plus tard, Gauss donna plusieurs démonstrations de ce théorème, toutes de grand intérêt mathématique. Celle que nous exposons ici lui est due, ainsi que celles qui utilisent la théorie des extensions algébriques (cf. Algèbre III), et celle qui utilise la théorie des fonctions holomorphes (cf. Analyse III). Les autres démonstrations restent en dehors du cadre de cet ouvrage.

Soit en effet P un polynôme à coefficients complexes, de degré $n \geq 1$. Nous pouvons nous ramener au cas où P est unitaire :

$$P = X^n + \alpha_{n-1}X^{n-1} + \dots + \alpha_0.$$

Nous écartons enfin le cas trivial où $\alpha_0 = 0$.

La démonstration comporte alors deux étapes :

1. On prouve qu'il existe un nombre complexe α tel que pour tout nombre complexe z , $|P(z)| \geq |P(\alpha)|$.
2. On prouve qu'un tel élément α est une racine de P .

1. *Existence d'un minimum pour la fonction $z \mapsto |P(z)|$.* Considérons l'application f de \mathbb{C} dans \mathbb{R}_+ qui à tout nombre complexe z associe $|P(z)|$. Cette application est continue sur \mathbb{C} , comme module d'une fonction polynomiale (cf. § I.5.5).

a) En utilisant l'inégalité triangulaire, nous voyons que pour tout nombre complexe z ,

$$f(z) \geq |z|^n - \sum_{p=0}^{n-1} |\alpha_p| \cdot |z|^p.$$

Introduisons donc l'application g de \mathbf{R}_+ dans \mathbf{R} qui à tout nombre réel positif x associe le nombre réel

$$g(x) = x^n - \sum_{p=0}^{n-1} |\alpha_p| \cdot x^p.$$

Ainsi, pour tout nombre complexe z , $f(z) \geq g(|z|)$.

D'autre part, il est immédiat que g est une fonction numérique tendant vers $+\infty$ lorsque x tend vers $+\infty$. Il existe donc un nombre réel strictement positif a tel que, pour tout nombre réel $x > a$, $g(x) > |\alpha_0|$. En résumé, la relation $|z| > a$ implique la relation

$$(1) \quad f(z) > |\alpha_0|.$$

b) Le disque fermé $B'_0(a)$ de centre 0 et de rayon a est une partie compacte de \mathbf{C} (théorème de Borel-Lebesgue; cf. th. I.5.4). Par suite, sur cette partie, la fonction f admet une borne inférieure, qu'elle atteigne en un point α de ce compact (cf. cor. 2 du th. I.5.10). Il est clair que

$$(2) \quad f(\alpha) = \inf_{z \in B'_0(a)} f(z) \leq f(0) = |\alpha_0|.$$

c) Il découle aussitôt des relations (1) et (2) que pour tout nombre complexe z , $f(z) \geq f(\alpha)$. Autrement dit : pour tout nombre complexe z , $|P(z)| \geq |P(\alpha)|$.

2. *Un tel élément α est une racine de P .* Supposons par l'absurde que $P(\alpha)$ soit non nul.

a) Considérons le polynôme Q défini par la formule

$$Q(X) = \frac{1}{P(\alpha)} P(X + \alpha).$$

Le polynôme Q est de degré n , $Q(0) = 1$, et, pour tout nombre complexe z , $|Q(z)| \geq 1$. Le polynôme Q s'écrit donc sous la forme

$$Q(X) = 1 + \beta_1 X + \dots + \beta_n X^n,$$

où, pour tout $p \in [1, n]$, $\beta_p \in \mathbf{C}$, et où $\beta_n \neq 0$.

Désignons par m le plus petit des entiers p tels que $\beta_p \neq 0$. Puisque $\beta_m \neq 0$, il existe un nombre complexe γ non nul tel que $\gamma^m = -\beta_m$ (cf. cor. du th. I.6.13).

b) Considérons alors le polynôme R défini par la formule

$$R(X) = Q\left(\frac{X}{\gamma}\right).$$

Le polynôme R est de degré n , $R(0) = 1$, et, pour tout nombre complexe z , $|R(z)| \geq 1$. De plus, le polynôme R s'écrit sous la forme

$$R(X) = 1 - X^m[1 + S(X)],$$

où S est un polynôme tel que $S(0) = 0$.

c) En utilisant l'inégalité triangulaire, nous voyons que, pour tout nombre réel $x \in [0, 1]$,

$$|R(x)| \leq 1 - x^m + x^m |S(x)|.$$

Puisque $S(0) = 0$, il existe un nombre réel strictement positif r tel que, pour tout point x de $[0, r]$, $|S(x)| \leq \frac{1}{2}$.

Ainsi, pour tout point x de $]0, r']$, où $r' = \inf(1, r)$,

$$|R(x)| \leq 1 - \frac{x^m}{2} < 1,$$

ce qui contredit l'hypothèse.

COROLLAIRE 1. — *Les seuls polynômes irréductibles à coefficients complexes sont les polynômes de degré 1.*

COROLLAIRE 2. — *Tout polynôme à coefficients complexes est scindé sur \mathbb{C} .*

3. POLYNÔMES ET FRACTIONS RATIONNELLES À COEFFICIENTS RÉELS OU COMPLEXES

Nous allons d'abord montrer que l'involution canonique $z \mapsto \bar{z}$ de \mathbb{C} permet de définir une involution sur $\mathbb{C}[X]$, et sur $\mathbb{C}(X)$.

PROPOSITION 1.37. — **Involution canonique de $\mathbb{C}[X]$, et de $\mathbb{C}(X)$.**

1. L'application φ qui à tout polynôme à coefficients complexes $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ associe le polynôme $\bar{P} = \sum_{n=0}^{+\infty} \bar{\alpha}_n X^n$ est un automorphisme involutif de l'anneau unitaire $\mathbb{C}[X]$. On dit que les polynômes P et \bar{P} sont conjugués.

2. L'automorphisme φ se prolonge d'une manière et d'une seule en un automorphisme ψ du corps $\mathbb{C}(X)$. L'automorphisme ψ est involutif, et laisse invariante toute fraction rationnelle à coefficients réels.

Si un élément R de $\mathbb{C}(X)$ est mis sous la forme $R = \frac{P}{Q}$, où P et $Q \in \mathbb{C}[X]$, $Q \neq 0$, l'élément $\psi(R)$, noté encore \bar{R} , est donné par la formule

$$(1) \quad \bar{R} = \frac{\bar{P}}{\bar{Q}}.$$

On dit que les fractions rationnelles R et \bar{R} sont conjuguées.

3. Pour tout élément R de $\mathbf{C}(X)$, $d^0(\bar{R}) = d^0(R)$, et pour tout nombre complexe α , la valuation au point $\bar{\alpha}$ de \bar{R} est égale à la valuation au point α de R . Ainsi, lorsque R admet α pour racine (resp. pour pôle), \bar{R} admet $\bar{\alpha}$ pour racine (resp. pour pôle), avec le même ordre de multiplicité.

4. Soient R un élément de $\mathbf{C}(X)$, α un nombre complexe, et p un entier rationnel. Alors les développements limités à l'ordre p de R au point α et de \bar{R} au point $\bar{\alpha}$ sont liés par la formule

$$\text{Pr}_{\bar{\alpha}, p}(\bar{R}) = \overline{\text{Pr}_{\alpha, p}(R)}.$$

5. Pour tout élément R de $\mathbf{C}(X)$,

$$D(\bar{R}) = \overline{D(R)}.$$

Assertion 1. — Il est évident que $\varphi(P + Q) = \varphi(P) + \varphi(Q)$, et que $\varphi(PQ) = \varphi(P) \cdot \varphi(Q)$ lorsque P et Q sont des monômes. Nous en déduisons que cette dernière formule est valable lorsque P et Q sont des polynômes quelconques. L'application φ est donc un endomorphisme de l'anneau $\mathbf{C}[X]$; comme φ est involutif, c'est même un automorphisme de cet anneau.

Assertion 2. — L'unicité de ψ est immédiate : écrivons en effet un élément R de $\mathbf{C}(X)$ sous la forme $R = \frac{P}{Q}$, où P et $Q \in \mathbf{C}[X]$, $Q \neq 0$. Alors $\psi(R)$ est nécessairement donné par la formule

$$\psi(R) = \frac{\psi(P)}{\psi(Q)} = \frac{\varphi(P)}{\varphi(Q)}.$$

Existence de ψ . — Considérons un autre couple (P', Q') d'éléments de $\mathbf{C}[X]$ tel que $Q' \neq 0$, et que $R = \frac{P'}{Q'}$. De la relation $PQ' = P'Q$ nous déduisons que $\overline{PQ'} = \overline{P'Q}$, et donc que

$$\frac{\varphi(P)}{\varphi(Q)} = \frac{\varphi(P')}{\varphi(Q')}.$$

La fraction rationnelle $\frac{\varphi(P)}{\varphi(Q)}$ ne dépend donc que de R ; nous pouvons donc définir ψ par la formule (1) :

$$\psi(R) = \frac{\varphi(P)}{\varphi(Q)}.$$

Nous laissons au lecteur le soin de vérifier que ψ est un automorphisme involutif du corps $\mathbf{C}(X)$ qui prolonge φ .

Assertion 3. — Il est évident que $d^0(\bar{R}) = d^0(R)$. Soit maintenant α un nombre complexe; par définition de $v_\alpha(R)$, il existe des polynômes P et Q , $Q \neq 0$, tels que

$$R = (X - \alpha)^{v_\alpha(R)} \frac{P}{Q}, \quad P(\alpha) \neq 0, Q(\alpha) \neq 0.$$

Il en résulte que

$$\bar{R} = (X - \bar{\alpha})^{v_{\alpha}(R)} \frac{\bar{P}}{\bar{Q}},$$

et que $\bar{P}(\bar{\alpha}) = \overline{P(\alpha)} \neq 0$, $\bar{Q}(\bar{\alpha}) = \overline{Q(\alpha)} \neq 0$.

Par définition de la valuation de \bar{R} au point $\bar{\alpha}$,

$$v_{\bar{\alpha}}(\bar{R}) = v_{\alpha}(R).$$

Assertion 4. — Il suffit d'écrire la relation de définition du développement limité à l'ordre p de R au point α (cf. prop. 1.33), de conjuguer cette relation, et d'utiliser l'unicité du développement limité de \bar{R} au point $\bar{\alpha}$.

Assertion 5. — Il est immédiat que pour tout élément P de $\mathbb{C}[X]$,

$$D(\bar{P}) = \overline{D(P)}.$$

Considérons alors un élément R de $\mathbb{C}(X)$, et écrivons-le sous la forme $R = \frac{P}{Q}$, P et $Q \in \mathbb{C}[X]$, $Q \neq 0$. La relation cherchée découle aussitôt de la formule

$$D(R) = \frac{D(P)Q - PD(Q)}{Q^2}.$$

COROLLAIRE. — **Cas où les coefficients sont réels.** — *Soit R une fraction rationnelle à coefficients réels.*

1. *Lorsque R admet un nombre complexe α pour racine (resp. pour pôle), R admet $\bar{\alpha}$ pour racine (resp. pour pôle) avec le même ordre de multiplicité.*
2. *Les pôles complexes de R sont conjugués deux à deux, et la partie principale de R au point $\bar{\alpha}$ est la conjuguée de la partie principale de R au point α .*

REMARQUE. — Cette dernière assertion permet de réduire les calculs intervenant dans la recherche de la décomposition sur \mathbb{C} d'une fraction rationnelle à coefficients réels en éléments simples.

Voici un exemple de décomposition sur \mathbb{C} en éléments simples qui utilise les diverses remarques précédentes :

EXEMPLE. — *Décomposition sur \mathbb{C} en éléments simples de la fraction rationnelle*

$$R = \frac{X^4 + 1}{(X^2 + X + 1)^2(X^2 - X + 1)^2}.$$

Le degré de R est égal à -4 , donc la partie entière est nulle. La fraction R admet quatre pôles doubles, à savoir j , $-j$, j^2 et $-j^2$.

On écrit *a priori* la décomposition de R en éléments simples :

$$R = \frac{a}{(X-j)^2} + \frac{a'}{X-j} + \frac{b}{(X+j)^2} + \frac{b'}{X+j} + \frac{c}{(X-j^2)^2} + \frac{c'}{X-j^2} + \frac{d}{(X+j^2)^2} + \frac{d'}{X+j^2}.$$

La remarque précédente montre que $c = \bar{a}$, $c' = \bar{a}'$, $d = \bar{b}$, $d' = \bar{b}'$.

En utilisant le fait que R est une fraction paire, on voit que $b = a$, et que $b' = -a'$.

Il reste donc à calculer a et a' .

Le scalaire a s'obtient en multipliant R par $(X - j)^2$, et en substituant j à X : on trouve ainsi que $a = \frac{1}{12}$.

Pour calculer $a' = \alpha + i\beta$, où $\alpha, \beta \in \mathbf{R}$, on substitue d'abord 0 à X dans R , ce qui fournit la relation $-2a'j^2 - 2\bar{a}'j = \frac{7}{6}$, ou encore

$$\alpha - \beta\sqrt{3} = \frac{7}{12}.$$

Pour trouver une deuxième relation liant α et β , on peut calculer la valeur à l'infini de la fraction X^2R : on voit ainsi que $2a'j + 2a'j^2 = -\frac{1}{3}$, soit

$$\alpha + \beta\sqrt{3} = \frac{1}{6}.$$

On en déduit que $a' = \frac{3}{8} - \frac{5\sqrt{3}}{72}i$.

Exercices conseillés : 46 à 55.

Nous examinons enfin les conséquences du théorème fondamental de l'algèbre relatives aux polynômes et fractions rationnelles à coefficients réels :

PROPOSITION 1.38. — Polynômes irréductibles sur \mathbf{R} . — *Les seuls polynômes à coefficients réels irréductibles sur \mathbf{R} sont :*

- a) *les polynômes de degré 1 ;*
- b) *les polynômes du second degré dont le discriminant est strictement négatif.*

(On appelle *discriminant* d'un polynôme du second degré $\alpha X^2 + \beta X + \gamma$ le scalaire $\beta^2 - 4\alpha\gamma$.)

Il est clair que les polynômes du type précédent sont irréductibles sur \mathbf{R} (cf. prop. I.4.74). Considérons, réciproquement, un élément P de $\mathbf{R}[X]$ irréductible sur \mathbf{R} , de degré $n \geq 2$. Ce polynôme, considéré comme élément de $\mathbf{C}[X]$, admet une racine complexe α . Le nombre α n'est pas réel : sinon, P serait divisible par $X - \alpha$, et ne serait donc pas irréductible. D'après le corollaire de la proposition 1.37, P est divisible par $X - \bar{\alpha}$ dans $\mathbf{C}[X]$; les deux polynômes $X - \alpha$ et $X - \bar{\alpha}$ étant premiers entre eux, $(X - \alpha)(X - \bar{\alpha})$ divise P dans $\mathbf{C}[X]$ (cf. cor. 2 du th. 1.6). Le polynôme $(X - \alpha)(X - \bar{\alpha})$, étant à coefficients réels, divise donc P dans $\mathbf{R}[X]$ (cf. cor. 2 du th. 1.4). Comme P est irréductible sur \mathbf{R} , il existe un nombre réel β tel que $P = \beta(X - \alpha)(X - \bar{\alpha})$, ce qu'il fallait prouver.

COROLLAIRE. — Décomposition en facteurs irréductibles sur \mathbf{R} . — *Soient P un polynôme non nul à coefficients réels, $\alpha_1, \alpha_2, \dots, \alpha_r$ les racines réelles de P , m_1, m_2, \dots, m_r leurs ordres de multiplicité, $\beta_1, \beta_2, \dots, \beta_s, \bar{\beta}_1, \bar{\beta}_2, \dots, \bar{\beta}_s$ les racines complexes non réelles de P , n_1, n_2, \dots, n_s leur ordre de multiplicité, et γ le coefficient dominant de P . Alors*

$$P = \gamma \prod_{p=1}^r (X - \alpha_p)^{m_p} \prod_{q=1}^s (X^2 - 2\operatorname{Re}(\beta_q)X + |\beta_q|^2)^{n_q}.$$

Cette décomposition n'est autre que la décomposition de P en facteurs irréductibles sur \mathbf{R} .

En particulier, tout polynôme à coefficients réels est produit d'une famille finie de polynômes à coefficients réels de degré inférieur ou égal à 2.

REMARQUE. — La proposition précédente permet aussi de définir les éléments simples sur le corps des réels, et de traiter complètement le problème de la décomposition sur \mathbf{R} des fractions rationnelles à coefficients réels en éléments simples; on pourra se reporter à l'exercice 44.

Exercices conseillés : 37 et 38.

§ 10. SÉRIES ENTIÈRES FORMELLES

1. SÉRIES ENTIÈRES FORMELLES

DÉFINITION 1.23. — **Algèbre des séries entières formelles.** — Soient K un corps commutatif, et $K^{\mathbf{N}}$ l'espace vectoriel des suites d'éléments de K . L'application bilinéaire de $K^{\mathbf{N}} \times K^{\mathbf{N}}$ dans $K^{\mathbf{N}}$ qui aux suites (α_n) et (β_n) associe la suite (γ_n) déterminée par la formule

$$\gamma_n = \sum_{p+q=n} \alpha_p \beta_q$$

définit sur $K^{\mathbf{N}}$ une structure de K -algèbre. Cette algèbre s'appelle algèbre des séries entières formelles à une indéterminée à coefficients dans K , et se note $S(K)$.

Soit $A = (\alpha_n)$ une série entière formelle. Les scalaires α_n s'appellent coefficients de A .

L'algèbre $S(K)$ est évidemment commutative, et elle admet pour élément unité le polynôme 1. L'algèbre $\mathbf{P}(K)$ des polynômes à coefficients dans K est une sous-algèbre unitaire de $S(K)$, différente de $S(K)$. C'est pourquoi $S(K)$ se note $K[[X]]$ lorsque $\mathbf{P}(K)$ se note $K[X]$.

DÉFINITION 1.24. — **Valuation d'une série entière formelle.** — Soit $A = (\alpha_n)$ un élément de $K[[X]]$.

— Si A est non nul, on appelle valuation de A le plus petit des entiers n tels que α_n soit non nul.

— Si A est nul, on appelle valuation de A l'élément $+\infty$.

La valuation d'une série entière formelle A se note $v_0(A)$; c'est un élément de $\overline{\mathbf{N}}$, différent de $-\infty$.

PROPOSITION 1.39. — **Valuation d'une somme, valuation d'un produit.** — Soient A et B deux éléments de $K[[X]]$, et α un élément de K^* . Alors

$$v_0(A + B) \geq \inf [v_0(A), v_0(B)],$$

avec égalité si $v_0(A) \neq v_0(B)$;

$$v_0(\alpha A) = v_0(A)$$

$$v_0(AB) = v_0(A) + v_0(B).$$

COROLLAIRE. — Soit n un entier naturel. L'ensemble des séries entières formelles de valuation supérieure ou égale à n est un idéal de l'algèbre $K[[X]]$, admettant pour sous-espace vectoriel supplémentaire l'ensemble des polynômes de degré strictement inférieur à n .

DÉFINITION 1.25. — Troncatures d'une série entière formelle. — Soit p un entier naturel. On appelle troncature à l'ordre p l'application T_p qui à tout élément $A = (\alpha_n)$ de $K[[X]]$ associe le polynôme $\sum_{n=0}^p \alpha_n X^n$.

PROPOSITION 1.40. — Propriétés de la troncature. — Soit p un entier naturel. La troncature T_p est un endomorphisme de l'espace vectoriel $K[[X]]$, dont l'image est contenue dans $K[X]$, et dont le noyau est l'idéal \mathfrak{I}_p de $K[[X]]$ constitué des séries entières formelles de valuation strictement supérieure à p .

Ainsi, l'intersection des noyaux des endomorphismes T_p , où p parcourt \mathbb{N} , est réduite à $\{0\}$. Autrement dit, pour que deux éléments A et B de $K[[X]]$ soient égaux, il faut et il suffit que, pour tout entier naturel p , $T_p(A) = T_p(B)$.

COROLLAIRE 1. — Critère d'égalité de deux endomorphismes de l'espace vectoriel des séries entières formelles. — Soient U et V deux endomorphismes de l'espace vectoriel $K[[X]]$ satisfaisant à la condition suivante ; pour toute suite (A_n) d'éléments de $K[[X]]$ telle que $v_0(A_n)$ tende vers $+\infty$, $v_0[U(A_n)]$ et $v_0[V(A_n)]$ tendent vers $+\infty$ avec n . Alors, pour que $U = V$, il faut et il suffit que, pour tout entier naturel n , $U(X^n) = V(X^n)$.

Cette dernière condition est évidemment nécessaire. Réciproquement, si elle est vérifiée, alors, puisque U et V sont linéaires, pour tout élément P de $K[X]$, $U(P) = V(P)$. Autrement dit, $W = U - V$ est un endomorphisme de $K[[X]]$ qui s'annule sur tous les polynômes. De plus, pour toute suite (A_n) d'éléments de $K[[X]]$ telle que $v_0(A_n)$ tende vers $+\infty$ avec n , $v_0[W(A_n)]$ tend vers $+\infty$. Considérons maintenant une série entière formelle A ; pour tout entier naturel p , notons A_p la tronquée de A à l'ordre p . Puisque $v_0(A - A_p)$ tend vers $+\infty$, $v_0[W(A - A_p)]$ tend vers $+\infty$ avec p . Or,

$$W(A) = W(A_p) + W(A - A_p) = W(A - A_p),$$

puisque A_p est un polynôme. Par suite, $v_0[W(A)]$ tend vers $+\infty$ avec p , ce qui implique que $v_0[W(A)] = +\infty$, c'est-à-dire que $W(A) = 0$.

COROLLAIRE 2. — Critère d'égalité de deux applications multilinéaires sur l'espace vectoriel des séries entières formelles. — Soient r un entier naturel non nul, S et T deux applications multilinéaires de $K[[X]]^r$ dans $K[[X]]$ satisfaisant à

la condition suivante : pour tout élément j de $[1, r]$, pour toute suite $(B_1, \dots, B_{j-1}, B_{j+1}, \dots, B_r)$ d'éléments de $K[[X]]$ et pour toute suite (A_n) d'éléments de $K[[X]]$ telle que $v_0(A_n)$ tende vers $+\infty$, $v_0[S(B_1, \dots, B_{j-1}, A_n, B_{j+1}, \dots, B_r)]$ et $v_0[T(B_1, \dots, B_{j-1}, A_n, B_{j+1}, \dots, B_r)]$ tendent vers $+\infty$ avec n . Alors, pour que $S = T$, il faut et il suffit que, pour toute suite (n_1, n_2, \dots, n_r) d'entiers naturels

$$S(X^{n_1}, X^{n_2}, \dots, X^{n_r}) = T(X^{n_1}, X^{n_2}, \dots, X^{n_r}).$$

Lorsque $r = 1$, ce corollaire se réduit au précédent. Le cas général s'en déduit par récurrence sur r , en appliquant à chaque pas le corollaire 1 à l'application linéaire

$$A \mapsto S(B_1, \dots, B_{j-1}, A, X^{n_{j+1}}, \dots, X^{n_r}).$$

COROLLAIRE 3. — Propriétés de la multiplication des séries entières formelles.

1. L'application $(A, B) \mapsto AB$ est la seule application bilinéaire symétrique M de $K[[X]] \times K[[X]]$ dans $K[[X]]$ prolongeant la multiplication des polynômes et satisfaisant à la condition suivante : pour toute série entière formelle B et pour toute suite (A_n) de séries entières formelles telle que $v_0(A_n)$ tende vers $+\infty$, $v_0[M(A_n, B)]$ tende vers $+\infty$.

2. L'algèbre $K[[X]]$ est associative.

L'assertion 1 découle aussitôt du corollaire 2, que l'on spécialise aux applications bilinéaires $(A, B) \mapsto AB$ et $(A, B) \mapsto M(A, B)$.

L'assertion 2 découle encore de ce corollaire, que l'on spécialise aux applications trilinéaires $(A, B, C) \mapsto A(BC)$ et $(A, B, C) \mapsto (AB)C$.

DÉFINITION 1.26. — Familles sommables de séries entières formelles. — Soient I un ensemble non vide et $(A_i)_{i \in I}$ une famille d'éléments de $K[[X]]$. On dit que cette famille est sommable si, pour tout entier naturel p , l'ensemble I_p des éléments i de I tels que $v_0(A_i) \leq p$ est fini. Alors, pour tout entier naturel p , la famille (α_{pi}) des $p^{\text{ièmes}}$ coefficients des séries entières formelles A_i est à support fini. On appelle somme de la famille $(A_i)_{i \in I}$ la série entière formelle $A = (\alpha_p)$ définie par la formule

$$\alpha_p = \sum_{i \in I} \alpha_{pi}.$$

REMARQUE. — Toute famille $(A_i)_{i \in I}$ à support fini est sommable, et sa somme n'est autre que $\sum_{i \in I} A_i$. C'est pourquoi, dans le cas général, la somme d'une

famille sommable $(A_i)_{i \in I}$ de séries entières formelles se note encore $\sum_{i \in I} A_i$.

Lorsque $I = \mathbb{N}$, cette somme se note $\sum_{n=0}^{+\infty} A_n$. Lorsque $I = \mathbb{Z}$, elle se note $\sum_{n=-\infty}^{+\infty} A_n$.

EXEMPLE. — Soit $A = (\alpha_n)$ un élément de $K[[X]]$. La famille des séries entières formelles $(\alpha_n X^n)_{n \in \mathbb{N}}$ est évidemment sommable, et sa somme n'est autre que A . C'est pourquoi nous noterons désormais A sous la forme

$$A = \sum_{n=0}^{+\infty} \alpha_n X^n.$$

Lorsque A est un polynôme, cette notation est compatible avec celle qui a été introduite au § 1, puisque la famille $(\alpha_n X^n)_{n \in \mathbb{N}}$ est alors à support fini.

PROPOSITION 1.41. — **Valuation et troncatures de la somme d'une famille sommable.** — Soit $(A_i)_{i \in I}$ une famille sommable d'éléments de $K[[X]]$. Alors

$$v_0\left(\sum_{i \in I} A_i\right) \geq \inf_{i \in I} v_0(A_i),$$

avec égalité s'il existe un élément i de I tel que, pour tout élément j de I différent de i , $v_0(A_i) < v_0(A_j)$. De plus, pour tout entier naturel p , la famille $(T_p(A_i))_{i \in I}$ est une famille à support fini de polynômes, et

$$T_p\left(\sum_{i \in I} A_i\right) = \sum_{i \in I} T_p(A_i).$$

En effet, l'ensemble des éléments i de I tels que $v_0(A_i) \leq p$ est fini.

COROLLAIRE. — Soient $(A_i)_{i \in I}$ et $(B_i)_{i \in I}$ deux familles sommables d'éléments de $K[[X]]$, et p un entier naturel. Si, pour tout élément i de I ,

$$A_i \equiv B_i \pmod{\mathfrak{F}_p},$$

alors

$$\sum_{i \in I} A_i \equiv \sum_{i \in I} B_i \pmod{\mathfrak{F}_p}.$$

PROPOSITION 1.42. — **Propriétés de la sommation des séries entières formelles.** — Soient I un ensemble non vide, et $(A_i)_{i \in I}$ une famille d'éléments de $K[[X]]$.

1. Soit σ une permutation de I . Si $(A_i)_{i \in I}$ est sommable, il en est de même de $(A_{\sigma(i)})_{i \in I}$, et

$$(1) \quad \sum_{i \in I} A_{\sigma(i)} = \sum_{i \in I} A_i$$

(formule de réindexation).

2. Soit J une partie de I . Si $(A_i)_{i \in I}$ est sommable, il en est de même de $(A_i)_{i \in J}$. (On convient que si $J = \emptyset$, $\sum_{i \in J} A_i = 0$.)

3. Soit $(I_h)_{h \in H}$ une famille de parties de I disjointes deux à deux et telles que $I = \bigcup_{h \in H} I_h$. Si la famille $(A_i)_{i \in I}$ est sommable, alors, pour tout élément h de H ,

la famille $(A_i)_{i \in I_h}$ est sommable, et la famille $(B_h)_{h \in H}$, où $B_h = \sum_{i \in I_h} A_i$, l'est aussi.

De plus,

$$(2) \quad \sum_{i \in I} A_i = \sum_{h \in H} \left(\sum_{i \in I_h} A_i \right)$$

(formule de sommation par paquets).

Assertion 1. — Soit p un entier naturel. L'ensemble J_p des éléments i de I tels que $v_0(A_i) \leq p$ est fini. La famille $(A_{\sigma(i)})_{i \in I}$ est donc sommable, puisque l'ensemble des éléments i de I tels que $v_0(A_{\sigma(i)}) \leq p$ n'est autre que $\sigma^{-1}(J_p)$.

Pour vérifier la relation (1), il suffit de prouver que, pour tout entier p , les deux membres sont congrus modulo \mathfrak{F}_p , ce qui est immédiat, puisque, pour tout élément i de I n'appartenant pas à $J_p \cup \sigma^{-1}(J_p)$, A_i et $A_{\sigma(i)}$ sont congrus à 0 modulo \mathfrak{F}_p .

L'assertion 2 est évidente.

Assertion 3. — Si $(A_i)_{i \in I}$ est sommable, $(B_h)_{h \in H}$ est évidemment sommable. Pour vérifier la relation (2), on prouve comme dans l'assertion 1 que, pour tout entier p , les deux membres sont congrus modulo \mathfrak{F}_p .

REMARQUE 1. — Soit $(A_i)_{i \in I}$ une famille sommable de séries entières formelles. Alors l'ensemble P des éléments i de I tels que $A_i \neq 0$ est dénombrable, puisque $P = \bigcup_{p=0}^{+\infty} J_p$.

REMARQUE 2. — La réciproque de l'assertion 3 est fautive, comme le montre l'exemple où $I = \mathbb{Z}^*$, où $H = \mathbb{N}^*$, où, pour tout $h \in \mathbb{N}^*$, $I_h = \{-h, h\}$, et où, pour tout $i \in \mathbb{Z}^*$, $A_i = 1$ si $i > 0$, $A_i = -1$ si $i < 0$.

PROPOSITION 1.43. — Distributivité de la sommation. — Soient I et J deux ensembles non vides, $(A_i)_{i \in I}$ et $(B_j)_{j \in J}$ deux familles sommables d'éléments de $K[[X]]$. Alors la famille $(A_i B_j)_{(i,j) \in I \times J}$ est sommable, et

$$(1) \quad \left(\sum_{i \in I} A_i \right) \left(\sum_{j \in J} B_j \right) = \sum_{(i,j) \in I \times J} A_i B_j.$$

En effet, pour tout entier naturel p , l'ensemble I_p (resp. J_p) des éléments i de I (resp. j de J) tels que $v_0(A_i) \leq p$ (resp. $v_0(B_j) \leq p$) est fini. Comme $v_0(A_i B_j) = v_0(A_i) + v_0(B_j)$, l'ensemble des couples (i, j) tels que $v_0(A_i B_j) \leq p$ est contenu dans $I_p \times J_p$. La famille $(A_i B_j)_{(i,j) \in I \times J}$ est donc sommable.

Pour démontrer la relation (1), écrivons que, pour tout entier naturel p ,

$$A_i B_j \equiv T_p(A_i) T_p(B_j). \quad (\text{mod. } \mathfrak{F}_p)$$

Par suite,

$$(2) \quad \sum_{i,j} A_i B_j \equiv \sum_{i,j} T_p(A_i) T_p(B_j). \quad (\text{mod. } \mathfrak{F}_p)$$

D'autre part,

$$\sum_{i \in I} A_i \equiv \sum_{i \in I} T_p(A_i), \quad (\text{mod. } \mathfrak{I}_p)$$

$$\sum_{j \in J} B_j \equiv \sum_{j \in J} T_p(B_j). \quad (\text{mod. } \mathfrak{I}_p)$$

Donc

$$(3) \quad \left(\sum_{i \in I} A_i \right) \left(\sum_{j \in J} B_j \right) \equiv \left(\sum_{i \in I} T_p(A_i) \right) \left(\sum_{j \in J} T_p(B_j) \right) \quad (\text{mod. } \mathfrak{I}_p)$$

Les seconds membres des congruences (2) et (3) sont égaux, puisque les familles $(T_p(A_i))_{i \in I}$ et $(T_p(B_j))_{j \in J}$ sont à support fini.

Ainsi, pour tout entier naturel p ,

$$(4) \quad \sum_{i,j} A_i B_j \equiv \left(\sum_{i \in I} A_i \right) \left(\sum_{j \in J} B_j \right). \quad (\text{mod. } \mathfrak{I}_p)$$

La formule (1) en résulte, car l'intersection des idéaux \mathfrak{I}_p est réduite à $\{0\}$.

PROPOSITION 1.44. — Substitution d'une série entière formelle dans une autre.

1. Soient $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ et B deux séries entières formelles. Si $v_0(B)$ est strictement positif, la famille $(\alpha_n B^n)_{n \in \mathbb{N}}$ est sommable. La somme de cette famille s'appelle composée de A et de B , et se note $A \circ B$; elle est dite obtenue par substitution de B à X dans A . De plus,

$$(5) \quad v_0(A \circ B) = v_0(A) \cdot v_0(B).$$

En particulier, pour tout entier strictement positif p ,

$$A \in \mathfrak{I}_p \Rightarrow A \circ B \in \mathfrak{I}_p.$$

2. Soit B un élément de $K[[X]]$ tel que $v_0(B)$ soit strictement positif. L'application $A \mapsto A \circ B$ est un endomorphisme de l'algèbre unitaire $K[[X]]$. Autrement dit,

$$(6) \quad (A_1 + A_2) \circ B = A_1 \circ B + A_2 \circ B$$

$$(7) \quad (\alpha A) \circ B = \alpha(A \circ B)$$

$$(8) \quad (A_1 A_2) \circ B = (A_1 \circ B) \cdot (A_2 \circ B).$$

De plus, pour toute famille sommable $(A_i)_{i \in I}$ d'éléments de $K[[X]]$,

$$(9) \quad \left(\sum_{i \in I} A_i \right) \circ B = \sum_{i \in I} A_i \circ B.$$

3. Soient A , B et C trois éléments de $K[[X]]$. Si $v_0(B)$ et $v_0(C)$ sont strictement positifs, alors

$$(10) \quad (A \circ B) \circ C = A \circ (B \circ C)$$

(associativité de la substitution).

Assertion 1. — Il est immédiat que la famille $(\alpha_n B^n)$ est sommable, puisque, pour tout entier naturel n , $v_0(\alpha_n B^n) \geq nv_0(B) \geq n$.

Posons $p = v_0(A)$. Alors

$$A = \sum_{n=p}^{+\infty} \alpha_n X^n,$$

où $\alpha_p \neq 0$. Donc

$$A \circ B = \sum_{n=p}^{+\infty} \alpha_n B^n,$$

et

$$v_0(A \circ B) = \inf_{n \in \mathbb{N}} v_0(\alpha_n B^n) = v_0(\alpha_p B^p) = pv_0(B).$$

Assertion 2. — Il est immédiat que l'application $A \mapsto A \circ B$ est un endomorphisme de l'espace vectoriel $K[[X]]$, qui transforme 1 en 1. Il reste donc à prouver que, pour tout couple (A_1, A_2) d'éléments de $K[[X]]$ et pour tout élément B de $K[[X]]$,

$$(A_1 A_2) \circ B = (A_1 \circ B) \cdot (A_2 \circ B).$$

Lorsque $A_1 = X^p$ et $A_2 = X^q$, où p et q appartiennent à \mathbb{N} , cette relation est vérifiée, car elle se réduit à $B^{p+q} = B^p B^q$. D'autre part, les applications $(A_1, A_2) \mapsto (A_1 A_2) \circ B$ et $(A_1, A_2) \mapsto (A_1 \circ B) \cdot (A_2 \circ B)$ sont bilinéaires, et elles satisfont aux hypothèses du corollaire 2 de la proposition 1.40, puisque $v_0(A \circ B) = v_0(A) \cdot v_0(B)$. Par suite, ces applications bilinéaires sont égales, ce qui démontre la formule (8).

La formule (9) résulte aussitôt de la formule (6) lorsque la famille $(A_i)_{i \in I}$ est à support fini. Dans le cas général, on prouve que, pour tout entier strictement positif p , les deux membres de cette formule sont congrus modulo \mathfrak{F}_p .

Assertion 3. — Lorsque $A = X^n$, la formule (10) se réduit à la suivante :

$$(11) \quad B^n \circ C = (B \circ C)^n,$$

laquelle s'établit par récurrence sur l'entier n , grâce à la formule (8). Lorsque

$A = \sum_{n=0}^{+\infty} \alpha_n X^n$, la formule (9) montre que

$$(12) \quad (A \circ B) \circ C = \left(\sum_{n=0}^{+\infty} \alpha_n B^n \right) \circ C = \sum_{n=0}^{+\infty} \alpha_n (B^n \circ C)$$

et que

$$(13) \quad A \circ (B \circ C) = \sum_{n=0}^{+\infty} \alpha_n (B \circ C)^n.$$

La formule (10) résulte alors des formules (11) à (13).

REMARQUE. — Lorsque A et B sont des polynômes, $v_0(B)$ étant strictement positif, $A \circ B$ coïncide évidemment avec le composé des deux polynômes A et B , ce qui justifie la notation employée.

EXEMPLE. — Séries entières formelles paires, impaires. — On dit qu'une série entière formelle A est paire si $A(-X) = A(X)$; on dit que A est impaire si $A(-X) = -A(X)$.

Si la caractéristique de K est différente de 2, les séries entières formelles paires et les séries entières formelles impaires constituent deux sous-espaces vectoriels supplémentaires dans $K[[X]]$, notés respectivement \mathfrak{P} et \mathfrak{I} ; les projecteurs associés à cette décomposition en somme directe sont les applications

$$A \mapsto \frac{1}{2} [A(X) + A(-X)] \quad \text{et} \quad A \mapsto \frac{1}{2} [A(X) - A(-X)].$$

De plus, pour que A soit paire (resp. impaire), il faut et il suffit que tous ses coefficients d'indice impair (resp. pair) soient nuls.

PROPOSITION 1.45. — Détermination d'un endomorphisme de l'espace vectoriel des séries entières formelles. — Soit $(B_n)_{n \in \mathbb{N}}$ une famille sommable d'éléments de $K[[X]]$. Il existe un endomorphisme U et un seul de l'espace vectoriel $K[[X]]$ satisfaisant aux deux conditions suivantes :

- a) Pour tout entier naturel n , $U(X^n) = B_n$.
- b) Pour toute suite (A_n) d'éléments de $K[[X]]$ telle que $v_0(A_n)$ tende vers $+\infty$, $v_0[U(A_n)]$ tend vers $+\infty$ avec n .

De plus, la valeur de U sur une série entière formelle $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ est donnée par la formule

$$(1) \quad U(A) = \sum_{n=0}^{+\infty} \alpha_n B_n.$$

L'unicité de U a déjà été démontrée (cf. cor. 1 de la prop. 1.40). Puisque la famille (B_n) est sommable, il en est de même de la famille $(\alpha_n B_n)$, pour toute suite (α_n) de scalaires. Il est alors immédiat que l'application U définie par la formule (1) convient, car $v_0(B_n)$ tend vers $+\infty$ avec n .

REMARQUE. — On laisse au lecteur le soin d'étendre cette proposition au cas des applications multilinéaires de $K[[X]]^r$ dans $K[[X]]$.

THÉORÈME 1.13. — Intégrité de l'anneau des séries entières formelles.

1. L'anneau $K[[X]]$ des séries entières formelles à une indéterminée à coefficients dans K est intègre.

2. Pour qu'un élément A de cet anneau soit inversible, il faut et il suffit que $v_0(A) = 0$, autrement dit, que le terme constant de A soit non nul. Dans ces conditions, on peut écrire A sous la forme $A = \alpha(1 + N)$, où $\alpha \in K^*$ et où $v_0(N) \geq 1$. Alors

$$A^{-1} = \alpha^{-1}(1 - N + N^2 + \dots + (-1)^n N^n + \dots).$$

L'assertion 1 résulte aussitôt de la formule $v_0(AB) = v_0(A) + v_0(B)$.

Assertion 2. — Notons d'abord que $1 + X$ est inversible dans $K[[X]]$, et admet pour inverse $U = \sum_{n=0}^{+\infty} (-1)^n X^n$, car $(1 + X)U = 1$.

Soit maintenant A un élément de $K[[X]]$ admettant un inverse B . La relation $AB = 1$ montre que $v_0(A) + v_0(B) = 0$, ce qui impose $v_0(A) = v_0(B) = 0$.

Réciproquement, tout élément A de $K[[X]]$ tel que $v_0(A) = 0$ se met d'une manière et d'une seule sous la forme $A = \alpha(1 + N)$, où $\alpha \in K^*$ et où $v_0(N) \geq 1$. Cette dernière relation montre que N est substituable dans la série entière formelle U . De plus,

$$(1 + N) \cdot (U \circ N) = [(1 + X)U] \circ N = 1 \circ N = 1.$$

Par suite, $\alpha^{-1}U \circ N$ est inverse de A , ce qu'il fallait prouver.

COROLLAIRE 1. — *L'ensemble \mathfrak{U} des séries entières formelles de la forme $U = 1 + N$, où $v_0(N) > 0$, est un sous-groupe du groupe multiplicatif des éléments inversibles de $K[[X]]$.*

Il est immédiat que \mathfrak{U} est stable pour la multiplication et que 1 appartient à \mathfrak{U} . D'autre part, tout élément $U = 1 + N$ de \mathfrak{U} est inversible dans $K[[X]]$, et $U^{-1} = 1 - N + N^2 + \dots + (-1)^n N^n + \dots$, ce qui montre que U^{-1} appartient encore à \mathfrak{U} .

COROLLAIRE 2. — **Structure des idéaux de l'algèbre $K[[X]]$.**

1. *Pour tout entier naturel p , l'ensemble \mathfrak{M}_p des séries entières formelles de valuation supérieure ou égale à p est un idéal de l'algèbre $K[[X]]$, qui n'est autre que l'idéal principal engendré par X^p . La suite des idéaux \mathfrak{M}_p est strictement décroissante, et l'intersection de ces idéaux est réduite à $\{0\}$.*

2. *Tout idéal non réduit à $\{0\}$ de $K[[X]]$ est de la forme précédente. En particulier, $K[[X]]$ admet un plus grand idéal strict, à savoir \mathfrak{M}_1 .*

L'assertion 1 est immédiate.

Assertion 2. — Soient \mathfrak{J} un idéal non réduit à $\{0\}$ de $K[[X]]$, p le plus petit des entiers $v_0(B)$, où B parcourt \mathfrak{J} , et A un élément de \mathfrak{J} tel que $v_0(A) = p$. Nous pouvons écrire A sous la forme $A = \alpha X^p(1 + N)$, où $\alpha \in K^*$ et où $v_0(N) \geq 1$. Comme $\alpha(1 + N)$ est inversible, X^p appartient à \mathfrak{J} , ce qui prouve que \mathfrak{M}_p est contenu dans \mathfrak{J} . D'autre part, pour tout élément B de \mathfrak{J} , $v_0(B) \geq p$, ce qui montre que B est divisible par X^p . L'idéal \mathfrak{J} est donc contenu dans \mathfrak{M}_p , ce qui achève la démonstration.

Pour tout entier naturel non nul n , X^n est non inversible dans $K[[X]]$, ce qui conduit à la

DÉFINITION 1.27. — **Algèbre des séries entières formelles généralisées.** — *Soit E le sous-espace vectoriel de $K^{\mathbb{Z}}$ constitué des suites $(\alpha_n)_{n \in \mathbb{Z}}$ à support minoré, c'est-à-dire telles que l'ensemble des entiers n tels que $\alpha_n \neq 0$ soit minoré. L'application de $E \times E$ dans E qui aux suites (α_n) et (β_n) associe la suite (γ_n) déterminée par la formule*

$$\gamma_n = \sum_{p+q=n} \alpha_p \beta_q$$

définit sur E une structure de K -algèbre. Cette algèbre s'appelle algèbre des séries entières formelles généralisées à une indéterminée à coefficients dans K , et se note $K((X))$; elle est évidemment commutative, et elle admet pour élément unité le polynôme 1. L'algèbre $K[[X]]$ des séries entières formelles est une sous-algèbre unitaire de l'algèbre unitaire $K((X))$.

DÉFINITION 1.28. — Valuation d'une série entière formelle généralisée. — Soit $A = (\alpha_n)_{n \in \mathbb{Z}}$ un élément de $K((X))$.

— Si A est non nul, on appelle valuation de A le plus petit des entiers rationnels n tels que α_n soit non nul.

— Si A est nul, on appelle valuation de A l'élément $+\infty$.

La valuation d'une série entière formelle généralisée A se note $v_0(A)$; c'est un élément de $\overline{\mathbb{Z}}$, différent de $-\infty$.

Les propriétés de la valuation des séries entières formelles (cf. prop. 1.39) s'étendent aussitôt à ce cas.

DÉFINITION 1.29. — Troncatures d'une série entière formelle généralisée. — Soit p un entier rationnel. On appelle troncature à l'ordre p l'application T_p qui

à tout élément $A = (\alpha_n)_{n \in \mathbb{Z}}$ de $K((X))$ associe l'élément $\sum_{n=-\infty}^p \alpha_n X^n$.

La troncature T_p est un endomorphisme de l'espace vectoriel $K((X))$, dont l'image est le sous-espace vectoriel engendré par la famille $(X^n)_{n \leq p}$, et dont le noyau est le sous-espace vectoriel \mathfrak{F}_p de $K((X))$ constitué des séries entières formelles généralisées de valuation strictement supérieure à p .

REMARQUE 1. — Cette fois \mathfrak{F}_p n'est pas un idéal de $K((X))$, mais, pour tout couple (p, q) d'entiers rationnels, $\mathfrak{F}_p \mathfrak{F}_q \subset \mathfrak{F}_{p+q}$.

REMARQUE 2. — Les deux premiers corollaires de la proposition 1.40 s'étendent aussitôt au cas des séries entières formelles généralisées. Exactement comme au corollaire 3 de la proposition 1.40, on en déduit que l'algèbre des séries entières formelles généralisées est associative.

DÉFINITION 1.30. — Forme canonique d'une série entière formelle généralisée. — Soit $A = (\alpha_n)_{n \in \mathbb{Z}}$ un élément non nul de $K((X))$. Il existe un couple (p, B) et un seul constitué d'un entier rationnel p et d'une série entière formelle B tel que $A = X^p B$ et que $v_0(B) = 0$. L'entier p n'est autre que $v_0(A)$.

THÉORÈME 1.14. — Corps des séries entières formelles généralisées. — L'algèbre $K((X))$ des séries entières formelles généralisées est un corps commutatif, possédant les propriétés suivantes :

1. L'anneau $K[[X]]$ est un sous-anneau unitaire du corps $K((X))$.
2. Le corps $K((X))$ est engendré par l'anneau $K[[X]]$.

Autrement dit, $K((X))$ est isomorphe au corps des quotients de l'anneau intègre $K[[X]]$.

Nous savons déjà que la multiplication est associative dans $K[[X]]$; nous en déduisons qu'elle l'est encore dans $K((X))$, en utilisant les formes canoniques.

Considérons un élément non nul A de $K((X))$, écrit sous la forme canonique $A = X^p B$, où $p = v_0(A)$ et $v_0(B) = 0$. D'après le théorème 1.13,

B est inversible dans $K[[X]]$ et, *a fortiori*, dans $K((X))$. Par suite, A est inversible dans $K((X))$, et $A^{-1} = X^{-p}B^{-1}$.

Le reste du théorème est immédiat.

REMARQUE 1. — En particulier, tout élément de $K(X)$ est un élément de $K((X))$. On trouvera dans l'exercice 74 une condition nécessaire et suffisante portant sur les coefficients d'une série entière formelle généralisée A pour que A appartienne à $K(X)$.

REMARQUE 2. — Les familles sommables de séries entières formelles généralisées se définissent comme dans le cas des séries entières formelles. Toute série entière formelle généralisée $A = (\alpha_n)_{n \in \mathbb{Z}}$ s'écrit alors sous la forme $A = \sum_{n=-\infty}^{+\infty} \alpha_n X^n$. Les propositions 1.41, 1.42 et 1.43 s'étendent aussitôt.

REMARQUE 3. — Soient $A = \sum_{n=-\infty}^{+\infty} \alpha_n X^n$ une série entière formelle généralisée et B une série entière formelle. Si $v_0(B) > 0$, la famille $(\alpha_n B^n)_{n \in \mathbb{Z}}$ est sommable. La somme de cette famille s'appelle composée de A et de B , et se note $A \circ B$. La proposition 1.44 s'étend aussitôt.

THÉORÈME 1.15. — Dérivation des séries entières formelles généralisées. — Soit $K((X))$ l'algèbre des séries entières formelles généralisées à une indéterminée à coefficients dans K .

1. Il existe un endomorphisme D et un seul de l'espace vectoriel $K((X))$ tel que

a) pour tout couple (A, B) d'éléments de $K((X))$.

$$(1) \quad D(AB) = D(A)B + AD(B);$$

$$b) \quad D(X) = 1;$$

c) pour toute suite (A_n) de séries entières formelles généralisées telle que $v_0(A_n)$ tende vers $+\infty$ lorsque n tend vers $+\infty$, $v_0(D(A_n))$ tende vers $+\infty$.

De plus, pour toute série entière formelle généralisée $A = \sum_{n=-\infty}^{+\infty} \alpha_n X^n$,

$$(2) \quad D(A) = \sum_{n=-\infty}^{+\infty} n\alpha_n X^{n-1}$$

et

$$(3) \quad v_0(D(A)) \geq v_0(A) - 1,$$

avec égalité si $v_0(A) \neq 0$.

La série entière formelle généralisée $D(A)$ s'appelle dérivée de A , et l'endomorphisme D s'appelle dérivation canonique de l'algèbre $K((X))$.

2. L'application $A \mapsto D(A)$ est la seule dérivation de l'algèbre $K[[X]]$ telle que $D(X) = 1$.

3. Pour toute famille sommable $(A_i)_{i \in I}$ de séries formelles généralisées, la famille $(D(A_i))_{i \in I}$ est sommable, et

$$(4) \quad D\left(\sum_{i \in I} A_i\right) = \sum_{i \in I} D(A_i).$$

4. Pour tout couple (A, B) d'éléments de $K((X))$ tel que $B \neq 0$,

$$(5) \quad D\left(\frac{A}{B}\right) = \frac{D(A)B - AD(B)}{B^2}.$$

De plus, la dérivation canonique de $K((X))$ prolonge celle de $K(X)$.

5. Pour tout élément non nul A de $K((X))$ et pour tout entier rationnel m ,

$$(6) \quad D(A^m) = mA^{m-1}D(A).$$

6. Pour toute suite (A_1, A_2, \dots, A_n) d'éléments de $K((X))$,

$$(7) \quad D(A_1 A_2 \dots A_n) = \sum_{i=1}^n A_1 A_2 \dots A_{i-1} D(A_i) A_{i+1} \dots A_n.$$

7. Pour tout couple (A, B) d'éléments de $K((X))$ et pour tout entier naturel non nul n ,

$$(8) \quad D^n(AB) = C_n^0 D^n(A)B + C_n^1 D^{n-1}(A)D(B) + \dots \\ + C_n^p D^{n-p}(A)D^p(B) + \dots + C_n^n AD^n(B)$$

(formule de Leibniz).

8. Pour tout couple (A, B) d'éléments de $K((X))$ tel que $v_0(B) > 0$,

$$(9) \quad D(A \circ B) = [D(A) \circ B]D(B).$$

Assertion 1. — Existence de D . — Il est clair que l'application $A \mapsto D(A)$ définie par la formule (2) est un endomorphisme de l'espace vectoriel $K((X))$ et que D satisfait à la formule (3) et, par suite, à la condition c). D'autre part, les applications $(A, B) \mapsto D(AB)$ et $(A, B) \mapsto D(A)B + AD(B)$ sont bilinéaires, et elles prennent la même valeur lorsque $A = X^p$ et $B = X^q$, où p et q sont deux entiers rationnels. La formule (3) montre que ces deux applications bilinéaires satisfont aux hypothèses du corollaire 2 de la proposition 1.40 (valable pour les séries entières formelles généralisées); elles sont donc égales. Ainsi, D satisfait aux conditions a), b) et c).

Unicité de D . — Considérons un endomorphisme D' de l'espace vectoriel $K((X))$ satisfaisant à ces conditions. Comme dans la proposition 1.23, on démontre que $D'(1) = 0$ et, par récurrence, que, pour tout entier naturel non nul n , $D'(X^n) = nX^{n-1}$. Par suite, pour tout entier naturel n , $D'(X^n) = D(X^n)$. Il en découle que $D' = D$, d'après le corollaire 1 de la proposition 1.40 (valable pour les séries entières formelles généralisées).

Assertion 2. — Soit D' une dérivation de $K[[X]]$ telle que $D'(X) = 1$. Il est immédiat que, pour tout entier naturel n , $D'(X^n) = D(X^n)$. Soit maintenant A un élément non nul de $K[[X]]$, de valuation $p > 0$. Alors A peut s'écrire sous la forme $A = X^p B$, où $B \in K[[X]]$. Par suite,

$$D'(A) = D'(X^p)B + X^p D'(B) = pX^{p-1}B + X^p D'(B).$$

Ainsi, $v_0[D'(A)] \geq p - 1 = v_0(A) - 1$. Les endomorphismes D et D' satisfont donc aux hypothèses du corollaire 1 de la proposition 1.40. Il en résulte que $D' = D$.

Assertion 3. — Soit $(A_i)_{i \in I}$ une famille sommable de séries entières formelles généralisées. Puisque, pour tout élément i de I ,

$$v_0(D(A_i)) \geq v_0(A_i) - 1,$$

la famille $(D(A_i))_{i \in I}$ est sommable.

Soit p un entier naturel non nul. Il existe une partie finie J de I telle que, pour tout élément i de I n'appartenant pas à J , $v_0(A_i) > p + 1$. Alors

$$\sum_{i \in I} A_i \equiv \sum_{i \in J} A_i \pmod{\mathfrak{F}_{p+1}}$$

Donc

$$(10) \quad D\left(\sum_{i \in I} A_i\right) \equiv D\left(\sum_{i \in J} A_i\right) \pmod{\mathfrak{F}_p}$$

Comme, pour tout élément i de $I - J$, $v_0(D(A_i)) \geq v_0(A_i) - 1 \geq p + 1$,

$$(11) \quad \sum_{i \in I} D(A_i) \equiv \sum_{i \in J} D(A_i) \pmod{\mathfrak{F}_p}$$

L'ensemble J étant fini, les seconds membres de (10) et de (11) sont égaux. Ainsi, pour tout entier naturel p ,

$$D\left(\sum_{i \in I} A_i\right) \equiv \sum_{i \in I} D(A_i) \pmod{\mathfrak{F}_p}$$

ce qui prouve la formule (4).

Assertions 4 à 7. — Les formules (5) à (8) découlent des propriétés générales des dérivations d'une algèbre (cf. prop. 1.24).

Il reste à prouver que la dérivation canonique de $K((X))$ prolonge celle de $K(X)$. D'après la formule (2), elle prolonge celle de $K[X]$. Soit maintenant R un élément de $K(X)$, mis sous la forme $R = \frac{P}{Q}$, où $P, Q \in K[X]$, $Q \neq 0$. Il découle de la formule (5) que

$$D(R) = \frac{D(P)Q - QD(P)}{Q^2},$$

ce qu'il fallait prouver.

Assertion 8. — Lorsque $A = X^p$, où $p \in \mathbb{Z}$, la formule (9) se réduit à la formule (6). D'autre part, les applications $A \mapsto D(A \circ B)$ et $A \mapsto [D(A) \circ B]D(B)$ sont linéaires, et

$$\begin{aligned} v_0[D(A \circ B)] &\geq v_0(A)v_0(B) - 1 \geq v_0(A) - 1 \\ v_0([D(A) \circ B]D(B)) &\geq [v_0(A) - 1]v_0(B) + v_0(B) - 1 \geq v_0(A) - 1. \end{aligned}$$

Le corollaire 1 de la proposition 1.40 montre alors que les deux applications linéaires considérées sont égales, ce qui prouve la formule (9).

COROLLAIRE. — Formule de Maclaurin. — Soit K un corps de caractéristique 0. Soit δ le morphisme de l'algèbre unitaire $K[[X]]$ dans K qui à toute série entière formelle $A = (\alpha_n)$ associe son terme constant α_0 . (Par analogie avec le cas des polynômes, $\delta(A)$ se note encore $A(0)$.)

1. Soit $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ une série entière formelle. Alors, pour tout entier naturel p ,

$$\alpha_p = \frac{[D^p(A)](0)}{p!}.$$

Autrement dit,

$$(1) \quad A = \sum_{n=0}^{+\infty} \frac{[D^n(A)](0)}{n!} X^n$$

(formule de Maclaurin pour les séries entières formelles).

2. Soit A une série entière formelle généralisée non nulle, de valuation q , écrite sous la forme $A = \sum_{n=q}^{+\infty} \alpha_n X^n$. Alors, pour tout entier p supérieur ou égal à q ,

$$(2) \quad \alpha_p = \frac{[D^{p+q}(X^q A)](0)}{(p+q)!}.$$

Autrement dit,

$$A = \sum_{n=q}^{+\infty} \frac{[D^{n+q}(X^q A)](0)}{(n+q)!} X^n.$$

Assertion 1. — Il est immédiat que, pour tout entier p ,

$$D^p(A) = \sum_{n=p}^{+\infty} \frac{n!}{(n-p)!} \alpha_n X^{n-p}.$$

La formule (1) s'en déduit.

Assertion 2. — Il est immédiat que, pour tout entier p supérieur ou égal à q ,

$$D^{p+q}(X^q A) = \sum_{n=p}^{+\infty} \frac{(n+q)!}{(n-p)!} \alpha_n X^{n-p}.$$

La formule (2) s'en déduit.

DÉFINITION 1.31. — Primitives d'une série entière formelle généralisée. — On dit qu'une série entière formelle généralisée A est une primitive d'une série entière formelle généralisée B si la dérivée de A est égale à B .

PROPOSITION 1.46. — Existence et unicité des primitives d'une série entière formelle généralisée. — Soit K un corps de caractéristique zéro. Pour tout entier naturel p , on note $K_p((X))$ l'hyperplan de $K((X))$ noyau de la forme linéaire $(\alpha_n) \mapsto \alpha_p$.

1. Si A_1 et A_2 sont deux primitives d'une même série entière formelle généralisée, $A_1 - A_2$ est constante.

2. Pour qu'une série entière formelle généralisée B admette une primitive, il faut et il suffit que B appartienne à $K_{-1}((X))$. Il existe alors une primitive A de B et une seule appartenant à $K_0((X))$. L'application P_0 qui à tout élément de $K_{-1}((X))$ associe cette primitive est un isomorphisme de $K_{-1}((X))$ sur $K_0((X))$, dont l'isomorphisme réciproque coïncide avec D .

La démonstration est calquée sur le cas des polynômes (cf. prop. 1.26).

REMARQUE. — Dérivée logarithmique d'une série entière formelle généralisée. On appelle dérivée logarithmique d'un élément non nul A de $K((X))$ la série entière formelle généralisée $\frac{D(A)}{A}$. La proposition 1.30 s'étend aussitôt à ce cas.

THÉORÈME 1.16. — Séries entières formelles réciproques. — Soit \mathfrak{M} l'idéal de $K[[X]]$ constitué des séries entières formelles de valuation strictement positive.

1. L'application $(A, B) \mapsto A \circ B$ définit sur \mathfrak{M} une structure de K -algèbre associative, dont l'élément unité est X .

2. Pour qu'un élément A de l'algèbre \mathfrak{M} soit inversible, il faut et il suffit que $v_0(A) = 1$. L'unique élément B de \mathfrak{M} tel que $A \circ B = B \circ A = X$ s'appelle série entière formelle réciproque de A .

De plus,

$$(1) \quad D(B) = \frac{1}{D(A) \circ B}.$$

L'assertion 1 résulte aussitôt de la relation

$$v_0(A \circ B) = v_0(A)v_0(B).$$

Assertion 2. — Soient d'abord A et B deux éléments de \mathfrak{M} tels que

$$B \circ A = X.$$

Alors $v_0(B)v_0(A) = v_0(B \circ A) = 1$. Par suite, $v_0(A)$ et $v_0(B)$ sont égaux à 1.

Réciproquement, soit $A = \sum_{n=1}^{+\infty} \alpha_n X^n$ un élément de \mathfrak{M} tel que $v_0(A) = 1$.

Pour qu'un élément $B = \sum_{n=1}^{+\infty} \beta_n X^n$ de \mathfrak{M} satisfasse à la relation $B \circ A = X$, il faut et il suffit que

$$(2) \quad \sum_{n=1}^{+\infty} \beta_n A^n = X.$$

Or,

$$\sum_{n=1}^{+\infty} \beta_n A^n = \sum_{n=1}^{+\infty} \gamma_n X^n,$$

où, pour tout entier n , γ_n est de la forme

$$\gamma_n = \beta_n \alpha_1^n + \sum_{j=1}^{n-1} \lambda_{jn} \beta_j.$$

La relation (2) équivaut donc à la conjonction des suivantes :

$$\begin{aligned} \beta_1 \alpha_1 &= 1 \\ \beta_n \alpha_1^n + \sum_{j=1}^{n-1} \lambda_{jn} \beta_j &= 0 \quad \text{si } n > 1. \end{aligned}$$

Puisque α_1 n'est pas nul, il existe une suite $(\beta_n)_{n \geq 1}$ et une seule satisfaisant à ces relations, ce qui prouve l'existence et l'unicité d'un élément B de \mathfrak{M} tel que $B \circ A = X$. De plus, $v_0(B) = 1$. Par suite, il existe un élément C de \mathfrak{M} tel que $C \circ B = X$. Ainsi, B admet un inverse à gauche et un inverse à droite dans l'algèbre \mathfrak{M} , et admet donc A pour inverse (cf. prop. I.1.8).

Enfin, la formule (1) s'obtient par dérivation de la formule $A \circ B = X$.

Exercice conseillé : 75.

2. EXPONENTIELLE FORMELLE

Dans ce qui suit, on suppose que la caractéristique de K est nulle.

THÉORÈME 1.17. — Exponentielle formelle.

1. Il existe un élément $E = \sum_{n=0}^{+\infty} \alpha_n X^n$ de $K[[X]]$ et un seul tel que $D(E) = E$

et que $E(0) = 1$. On l'appelle *exponentielle formelle de X* , et on le note $\exp X$. De plus,

$$(1) \quad \exp X = 1 + \frac{X}{1!} + \frac{X^2}{2!} + \dots + \frac{X^n}{n!} + \dots$$

Plus généralement, pour tout élément A de \mathfrak{M} , la composée $(\exp X) \circ A$ s'appelle *exponentielle formelle de A* , et se note $\exp A$. Ainsi,

$$(2) \quad \exp A = 1 + \frac{A}{1!} + \frac{A^2}{2!} + \dots + \frac{A^n}{n!} + \dots$$

De plus,

$$(3) \quad D(\exp A) = (\exp A)D(A).$$

2. Pour tout couple (A, B) d'éléments de \mathfrak{M} ,

$$(4) \quad \exp(A + B) = (\exp A)(\exp B).$$

De plus,

$$(5) \quad \exp 0 = 1.$$

Enfin, pour tout élément A de \mathfrak{M} , $\exp A$ est inversible, et, pour tout entier rationnel n ,

$$(6) \quad \exp(nA) = (\exp A)^n.$$

3. L'application $A \mapsto \exp A$ est un isomorphisme du groupe additif \mathfrak{M} sur le groupe multiplicatif \mathfrak{U} , dont l'isomorphisme réciproque est l'application qui à tout élément $U = 1 + N$ de \mathfrak{U} associe l'élément de \mathfrak{M} , noté $\log U$, défini par la relation

$$(7) \quad \log U = N - \frac{N^2}{2} + \dots + (-1)^{n+1} \frac{N^n}{n} + \dots$$

En particulier, pour tout couple (U, V) d'éléments de \mathfrak{U} ,

$$(8) \quad \log(UV) = \log U + \log V.$$

De plus, pour tout élément U de \mathfrak{U} , $\log U$ est le seul élément de \mathfrak{M} satisfaisant à la relation

$$(9) \quad D(\log U) = \frac{D(U)}{U}.$$

En particulier, $\log(1 + X)$ est la seule primitive de $\frac{1}{1+X}$ s'annulant à l'origine.

Assertion 1. — Soit $E = \sum_{n=0}^{+\infty} \alpha_n X^n$ une série entière formelle telle que $D(E) = E$ et que $E(0) = 1$. Par récurrence, on voit aussitôt que, pour tout entier naturel p , $D^p(E) = E$. Par suite, $D^p(E)(0) = 1$. La formule de Maclaurin (cf. cor. du th. 1.15) montre alors que $E = \sum_{n=0}^{+\infty} \frac{X^n}{n!}$.

Réciproquement, il est immédiat que la série ainsi définie satisfait aux conditions de l'énoncé.

Assertion 2. — Il résulte de la définition de $\exp A$ et de $\exp B$ et de la distributivité de la sommation (cf. prop. 1.43) que la famille $\left(\frac{A^p B^q}{p! q!} \right)$, où (p, q) parcourt \mathbb{N}^2 , est sommable, et que

$$(10) \quad (\exp A)(\exp B) = \sum_{p,q} \frac{A^p B^q}{p! q!}.$$

Pour tout entier naturel n , considérons la partie I_n de \mathbb{N}^2 constituée des couples (p, q) tels que $p + q = n$. La famille $(I_n)_{n \in \mathbb{N}}$ constitue une partition de \mathbb{N}^2 . Appliquons alors la formule de sommation par paquets des séries entières formelles (cf. prop. 1.42) :

$$(11) \quad \sum_{p,q} \frac{A^p B^q}{p! q!} = \sum_{n=0}^{+\infty} \left(\sum_{p+q=n} \frac{A^p B^q}{p! q!} \right).$$

Or, la formule du binôme montre que, pour tout entier n ,

$$(12) \quad \sum_{p+q=n} \frac{A^p B^q}{p! q!} = \frac{(A + B)^n}{n!}.$$

La relation (4) découle des relations (10) (11) et (12).

La relation (5) est évidente. En appliquant la relation (4) au couple $(A, -A)$, nous voyons que $\exp A$ est inversible, et qu'elle admet pour inverse $\exp(-A)$. L'application $A \mapsto \exp A$ est donc un morphisme du groupe additif \mathfrak{M} dans le groupe multiplicatif \mathfrak{U} . La formule (6) en découle.

Assertion 3. — Pour montrer la bijectivité de l'exponentielle, notons que l'équation $\exp A = 1 + N$, où N et A appartiennent à \mathfrak{M} , peut encore s'écrire

$$(13) \quad (\exp X - 1) \circ A = N.$$

Puisque $\exp X - 1$ appartient à \mathfrak{M} et que sa valuation est égale à 1, nous savons que cette série entière formelle est inversible dans l'algèbre \mathfrak{M} (munie de la loi de composition des séries entières formelles) et que, par suite, l'équation (13) admet une solution et une seule. Ainsi, pour tout élément $U = 1 + N$ de \mathfrak{U} , il existe un élément A de \mathfrak{M} et un seul tel que $\exp A = U$, ce qu'il fallait prouver.

Enfin, en dérivant la relation $\exp A = 1 + N$, nous voyons que $(\exp A)D(A) = D(N)$, c'est-à-dire que $D(A) = \frac{D(N)}{1 + N}$. Or,

$$\frac{D(N)}{1 + N} = \left(\sum_{n=0}^{+\infty} (-1)^n N^n \right) D(N) = D \left(\sum_{n=0}^{+\infty} (-1)^n \frac{N^{n+1}}{n+1} \right) = D[\log(1 + N)].$$

Ainsi, A et $\log(1 + N)$ ont la même dérivée; elles sont donc égales, puisque leurs termes constants sont nuls. Ce raisonnement montre de plus que, pour tout élément U de \mathfrak{U} , $\log U$ est le seul élément A de \mathfrak{M} satisfaisant à la relation $D(A) = \frac{D(U)}{U}$, ce qui prouve la formule (9).

REMARQUE. — La formule (9) justifie le nom de dérivée logarithmique donné à la série entière formelle $\frac{D(A)}{A}$, pour tout élément non nul A de $K((X))$. Néanmoins, $\frac{D(A)}{A}$ n'admet de primitive dans $K((X))$ que si $v_0(A) = 0$. Dans ce cas, A s'écrit sous la forme $A = \alpha U$, où $\alpha \in K^*$ et $U \in \mathfrak{U}$, et $\log U$ est l'unique primitive de $\frac{D(A)}{A}$ s'annulant à l'origine.

Écrivons en effet A sous la forme $A = \alpha X^p U$, où $\alpha \in K^*$, $p \in \mathbb{Z}$ et $U \in \mathfrak{U}$. Alors

$$\frac{D(A)}{A} = \frac{p}{X} + \frac{D(U)}{U}.$$

Comme $\frac{D(U)}{U}$ appartient à $K[[X]]$, $\frac{D(A)}{A}$ admet une primitive si et seulement si $p = 0$ (cf. prop. 1.46). Alors

$$\frac{D(A)}{A} = \frac{D(U)}{U} = D(\log U).$$

CORROLLAIRE. — Caractérisation des exponentielles formelles. — Soit α un élément de K . Il existe un élément B de $K[[X]]$ et un seul satisfaisant aux conditions suivantes :

$$(14) \quad D(B) = \alpha B$$

$$(15) \quad B(O) = 1.$$

De plus,

$$(16) \quad B = \exp(\alpha X).$$

La formule (3) montre aussitôt que la série entière formelle $\exp(\alpha X)$ satisfait aux conditions (14) et (15). Réciproquement, considérons une série entière formelle B satisfaisant à ces conditions, et introduisons la série entière formelle $C = \exp(-\alpha X)B$. Alors

$$D(C) = -\alpha \exp(-\alpha X)B + \exp(-\alpha X)D(B) = 0.$$

De plus, $C(O) = 1$. Il en découle que $C = 1$, et, d'après la formule (6), que $B = \exp(\alpha X)$, ce qui achève la démonstration.

THÉORÈME 1.18. — Série formelle du binôme.

1. Pour tout élément α de K , il existe un élément B_α de $K[[X]]$ et un seul tel que

$$(1) \quad (1 + X)D(B_\alpha) = \alpha B_\alpha$$

et que $B_\alpha(0) = 1$. De plus,

$$(2) \quad B_\alpha = 1 + \alpha X + \frac{\alpha(\alpha-1)}{2!} X^2 + \dots + \frac{\alpha(\alpha-1) \dots (\alpha-n+1)}{n!} X^n + \dots$$

2. Pour tout élément α de K ,

$$(3) \quad B_\alpha = \exp[\alpha \log(1 + X)].$$

En particulier, pour tout entier rationnel n ,

$$(4) \quad B_n = (1 + X)^n.$$

C'est pourquoi, dans le cas général, B_α se note $(1 + X)^\alpha$, et s'appelle série formelle du binôme.

3. L'application $\alpha \mapsto B_\alpha$ est un morphisme du groupe additif K dans le groupe multiplicatif \mathfrak{U} . En particulier, pour tout couple (α, β) de scalaires,

$$(5) \quad (1 + X)^\alpha (1 + X)^\beta = (1 + X)^{\alpha+\beta}.$$

4. Plus généralement, pour tout élément U de \mathfrak{U} , écrit sous la forme $U = 1 + N$, on pose

$$(6) \quad U^\alpha = (1 + N)^\alpha = B_\alpha \circ N = 1 + \alpha N + \frac{\alpha(\alpha-1)}{2!} N^2 + \dots \\ + \frac{\alpha(\alpha-1) \dots (\alpha-n+1)}{n!} N^n + \dots$$

L'application $\alpha \mapsto U^\alpha$ est un morphisme du groupe additif K dans le groupe multiplicatif \mathfrak{U} , et, pour tout scalaire α ,

$$(7) \quad D(U^\alpha) = \alpha U^{\alpha-1} D(U).$$

De plus,

$$(8) \quad U^\alpha = \exp(\alpha \log U).$$

En particulier, pour tout élément N de \mathfrak{M} ,

$$(9) \quad (\exp N)^\alpha = \exp(\alpha N).$$

Pour tout élément U de \mathfrak{U} ,

$$(10) \quad \log(U^\alpha) = \alpha \log U.$$

Enfin, pour tout élément U de \mathfrak{U} et pour tout couple (α, β) d'éléments de K ,

$$(11) \quad (U^\alpha)^\beta = U^{\beta\alpha}.$$

5. L'application $P_\alpha : U \mapsto U^\alpha$ est un automorphisme de \mathfrak{U} , dont l'isomorphisme réciproque n'est autre que $P_{\alpha^{-1}}$.

En particulier, pour tout élément V de \mathfrak{U} et pour tout entier rationnel n , il existe un élément U de \mathfrak{U} et un seul tel que $U^n = V$, à savoir $U = V^{\frac{1}{n}}$.

Assertion 1. — Soit $B_\alpha = \sum_{n=0}^{+\infty} \alpha_n X^n$ une série entière formelle satisfaisant aux conditions de l'énoncé. En utilisant la formule de Leibniz, on voit aussitôt que, pour tout entier naturel p ,

$$(1 + X) D^{p+1}(B_\alpha) = (\alpha - p) D^p(B_\alpha).$$

Par suite,

$$[D^p(B_\alpha)](0) = \alpha(\alpha-1) \dots (\alpha-p+1).$$

La formule de Maclaurin (cf. cor. du th. 1.15) montre alors que B_α satisfait à la formule (2).

Réciproquement, il est immédiat que la série entière formelle ainsi définie satisfait aux conditions de l'énoncé.

Assertion 2. — Posons $C_\alpha = \exp [\alpha \log (1 + X)]$. D'une part, $C_\alpha(0) = 1$. D'autre part, d'après le théorème 1.17,

$$D(C_\alpha) = C_\alpha D[\alpha \log (1 + X)] = \alpha \frac{C_\alpha}{1 + X}.$$

Autrement dit,

$$(1 + X)D(C_\alpha) = \alpha C_\alpha.$$

Par unicité de la série formelle du binôme, nous en déduisons que $C_\alpha = B_\alpha$, ce qu'il fallait prouver.

En particulier, si α est un entier rationnel n ,

$$B_\alpha = \exp [n \log (1 + X)] = (\exp [\log (1 + X)])^n = (1 + X)^n.$$

L'assertion 3 se déduit de la formule (3), compte tenu des propriétés de l'exponentielle formelle.

Assertion 4. — En composant les deux membres de la formule (5) avec N , on voit aussitôt que l'application $\alpha \mapsto U^\alpha$ est un morphisme du groupe additif K dans \mathfrak{U} . De plus,

$$(12) \quad D(U^\alpha) = D(B_\alpha \circ N) = [D(B_\alpha) \circ N]D(N).$$

Or,

$$(13) \quad D(B_\alpha) \circ N = \left(\alpha \frac{B_\alpha}{1 + X} \right) \circ N = \alpha \frac{B_\alpha \circ N}{1 + N} = \alpha U^{\alpha-1}.$$

La formule (7) découle des formules (12) et (13), puisque $D(U) = D(N)$.

Pour démontrer la formule (8), nous écrivons que

$$\begin{aligned} U^\alpha &= B_\alpha \circ N = (\exp \circ \alpha \log (1 + X)) \circ N = \exp \circ (\alpha \log (1 + X) \circ N) \\ &= \exp [\alpha \log (1 + N)] = \exp (\alpha \log U). \end{aligned}$$

En particulier, pour tout élément N de \mathfrak{M} ,

$$(\exp N)^\alpha = \exp [\alpha \log (\exp N)] = \exp (\alpha N).$$

De même, pour tout élément U de \mathfrak{U} ,

$$(U^\alpha)^\beta = \exp [\beta \log (U^\alpha)] = \exp (\beta \alpha \log U) = U^{\beta \alpha}.$$

Assertion 5. — Soient U et V deux éléments de \mathfrak{U} et α un scalaire. Alors

$$\begin{aligned} P_\alpha(UV) &= (UV)^\alpha = \exp [\alpha \log (UV)] = \exp [\alpha(\log U + \log V)] \\ &= [\exp (\alpha \log U)] \cdot [\exp (\alpha \log V)] = U^\alpha V^\alpha = P_\alpha(U)P_\alpha(V). \end{aligned}$$

Ainsi, P_α est un endomorphisme du groupe multiplicatif \mathfrak{U} . De plus, d'après la formule (11), $P_\beta \circ P_\alpha = P_{\beta \alpha}$. Comme P_1 est l'application identique de \mathfrak{U} , nous en déduisons que P_α est un automorphisme de \mathfrak{U} , admettant $P_{\alpha^{-1}}$ pour application réciproque.

Nous terminons en traitant des séries entières formelles correspondant aux fonctions trigonométriques. Nous supposons à cet effet que le corps K est égal à \mathbf{R} ou à \mathbf{C} .

Nous allons d'abord montrer que l'involution canonique $z \mapsto \bar{z}$ de \mathbf{C} se prolonge en une involution de $\mathbf{C}((X))$.

PROPOSITION 1.47. — Involution canonique de $\mathbf{C}((X))$.

1. L'application φ qui à toute série entière formelle généralisée à coefficients complexes $A = \sum_{n=-\infty}^{+\infty} \alpha_n X^n$ associe la série entière formelle généralisée $\bar{A} = \sum_{n=-\infty}^{+\infty} \bar{\alpha}_n X^n$ est un automorphisme involutif de l'anneau unitaire $\mathbf{C}((X))$.

On dit que les séries entières formelles généralisées A et \bar{A} sont conjuguées.

2. Pour tout élément A de $\mathbf{C}((X))$, $v_0(A) = v_0(\bar{A})$, et, pour tout élément p de \mathbf{Z} , $T_p(\bar{A}) = \overline{T_p(A)}$.

3. Pour que $\bar{A} = A$, il faut et il suffit que les coefficients de A soient réels. On dit alors que A est réelle.

Les séries entières formelles généralisées réelles constituent un sous-espace vectoriel, noté \mathcal{R} , du \mathbf{R} -espace vectoriel $\mathbf{C}((X))$, et ce \mathbf{R} -espace vectoriel est somme directe de \mathcal{R} et de $i\mathcal{R}$. Les projecteurs associés à cette décomposition en somme directe sont les applications, notées Re et Im , définies par les formules

$$\text{Re}(A) = \frac{A + \bar{A}}{2} \quad \text{et} \quad \text{Im}(A) = \frac{A - \bar{A}}{2i}.$$

DÉFINITION 1.32. — Séries entières formelles hyperboliques. — On appelle cosinus hyperbolique formel et sinus hyperbolique formel de X , et on note $\text{ch } X$ et $\text{sh } X$, les parties paire et impaire de la série entière formelle $\exp X$. Ainsi,

$$(1) \quad \text{ch } X = \frac{1}{2} [\exp X + \exp(-X)] = 1 + \frac{X^2}{2!} + \dots + \frac{X^{2r}}{(2r)!} + \dots$$

$$(2) \quad \text{sh } X = \frac{1}{2} [\exp X - \exp(-X)] = X + \frac{X^3}{3!} + \dots + \frac{X^{2r+1}}{(2r+1)!} + \dots$$

Enfin, on appelle tangente hyperbolique formelle de X , et on note $\text{th } X$, la série entière formelle définie par la formule

$$(3) \quad \text{th } X = \frac{\text{sh } X}{\text{ch } X} = \frac{\exp X - \exp(-X)}{\exp X + \exp(-X)} = \frac{1 - \exp(-2X)}{1 + \exp(-2X)} = \frac{\exp(2X) - 1}{\exp(2X) + 1}.$$

PROPOSITION 1.48. — Propriétés des séries entières formelles hyperboliques.

1. Les séries entières formelles $\text{ch } X$ et $\text{sh } X$ satisfont aux relations suivantes :

$$(4) \quad \exp X = \text{ch } X + \text{sh } X$$

$$(5) \quad \exp(-X) = \text{ch } X - \text{sh } X$$

$$(6) \quad \text{ch}^2 X - \text{sh}^2 X = 1.$$

Plus précisément,

$$(7) \quad \operatorname{ch} X = (1 + \operatorname{sh}^2 X)^{\frac{1}{2}}.$$

En outre,

$$(8) \quad D(\operatorname{ch} X) = \operatorname{sh} X$$

$$(9) \quad D(\operatorname{sh} X) = \operatorname{ch} X$$

$$(10) \quad D(\operatorname{th} X) = 1 - \operatorname{th}^2 X = \frac{1}{\operatorname{ch}^2 X}.$$

2. Les séries entières formelles $\operatorname{sh} X$ et $\operatorname{th} X$ admettent des séries entières formelles réciproques, appelées argument sinus hyperbolique formel et argument tangente hyperbolique formel de X , et notées $\operatorname{Arg} \operatorname{sh} X$ et $\operatorname{Arg} \operatorname{th} X$. De plus,

$$(11) \quad D(\operatorname{Arg} \operatorname{sh} X) = (1 + X^2)^{-\frac{1}{2}}$$

$$(12) \quad D(\operatorname{Arg} \operatorname{th} X) = \frac{1}{1 - X^2}.$$

Par suite,

$$(13) \quad \operatorname{Arg} \operatorname{sh} X = X - \frac{X^3}{6} + \frac{3}{40} X^5 + \dots + (-1)^r \frac{(2r)!}{2^{2r}(r!)^2} \frac{X^{2r+1}}{2r+1} + \dots$$

$$(14) \quad \operatorname{Arg} \operatorname{th} X = X + \frac{X^3}{3} + \frac{X^5}{5} + \dots + \frac{X^{2r+1}}{2r+1} + \dots$$

3. L'application $A \mapsto \operatorname{sh} A$ est une bijection de \mathfrak{M} sur lui-même, appelée sinus hyperbolique formel, dont la bijection réciproque n'est autre que l'application $A \mapsto \operatorname{Arg} \operatorname{sh} A$.

De même, l'application $A \mapsto \operatorname{th} A$ est une bijection de \mathfrak{M} sur lui-même, appelée tangente hyperbolique formelle, dont la bijection réciproque n'est autre que l'application $A \mapsto \operatorname{Arg} \operatorname{th} A$.

Enfin, l'application $A \mapsto \operatorname{ch} A$ est une application de \mathfrak{M} dans \mathfrak{A} . Pour que deux éléments A et A' de \mathfrak{M} satisfassent à la relation $\operatorname{ch} A' = \operatorname{ch} A$, il faut et il suffit que $A' = \pm A$.

Assertion 1. — Les formules (4) et (5) s'obtiennent en ajoutant les égalités (1) et (2), et la formule (6) s'obtient en multipliant les égalités (4) et (5). La formule (7) s'en déduit, puisque $(1 + \operatorname{sh}^2 X)^{\frac{1}{2}}$ et $\operatorname{ch} X$ appartiennent à \mathfrak{U} (cf. th. 1.18). Les formules (8) et (9) résultent des formules (1) et (2) et des relations

$$D(\exp X) = \exp X \quad \text{et} \quad D(\exp(-X)) = -\exp X.$$

La formule (10) s'en déduit, grâce à la formule donnant la dérivée d'un quotient de séries entières formelles.

Assertion 2. — Les séries entières formelles $\text{sh } X$ et $\text{th } X$ ont des valuations égales à 1; elles admettent donc des séries entières formelles réciproques (cf. th. 1.16), que nous notons B et C . Alors

$$D(B) = \frac{1}{[D(\text{sh } X)] \circ B} \quad \text{et} \quad D(C) = \frac{1}{[D(\text{th } X)] \circ C}.$$

Or, d'après les formules (8) et (7),

$$D(\text{sh } X) = \text{ch } X = (1 + \text{sh}^2 X)^{\frac{1}{2}} = (1 + X^2)^{\frac{1}{2}} \circ \text{sh } X.$$

Donc

$$[D(\text{sh } X)] \circ B = (1 + X^2)^{\frac{1}{2}} \circ [(\text{sh } X) \circ B] = (1 + X^2)^{\frac{1}{2}}.$$

La formule (11) en résulte.

De même, d'après la formule (10),

$$D(\text{th } X) = 1 - \text{th}^2 X.$$

Donc

$$[D(\text{th } X)] \circ C = (1 - \text{th}^2 X) \circ C = 1 - [(\text{th } X) \circ C]^2 = 1 - X^2.$$

La formule (12) en découle.

Les formules (13) et (14) résultent alors des propriétés de la série entière formelle du binôme (cf. th. 1.18).

Assertion 3. — Les applications $A \mapsto \text{sh } A$ et $A \mapsto \text{th } A$ sont bijectives, puisque

$$\text{sh } A = (\text{sh } X) \circ A \quad \text{et} \quad \text{th } A = (\text{th } X) \circ A.$$

Pour étudier l'application $A \mapsto \text{ch } A$, introduisons la série entière formelle

$$H = \frac{X}{2!} + \frac{X^2}{4!} + \dots + \frac{X^n}{(2n)!} + \dots$$

Cette série entière formelle admet une série entière formelle réciproque; donc l'application $B \mapsto H \circ B$ est une bijection de \mathfrak{M} sur lui-même. D'autre part, pour tout élément A de \mathfrak{M} ,

$$\text{ch } A = 1 + H \circ A^2.$$

La relation $\text{ch } A' = \text{ch } A$ équivaut donc à la relation $A'^2 = A^2$, ou encore à la relation $A' = \pm A$.

REMARQUE 1. — Le calcul explicite des coefficients de la série entière formelle $\text{th } X$ sera effectué au § 2.6.

REMARQUE 2. — Les formules d'addition des fonctions hyperboliques et leurs conséquences (cf. prop. I.6.19 à I.6.22) subsistent sans aucun changement pour les séries entières formelles hyperboliques.

DÉFINITION 1.33. — **Séries entières formelles trigonométriques.** — On appelle *cosinus formel* et *sinus formel* de X , et on note $\cos X$ et $\sin X$, les parties réelle et imaginaire de la série entière formelle $\exp(iX)$. Ainsi,

$$(1') \quad \cos X = \frac{1}{2} [\exp(iX) + \exp(-iX)] = 1 - \frac{X^2}{2!} + \dots + (-1)^r \frac{X^{2r}}{(2r)!} + \dots$$

$$(2') \quad \sin X = \frac{1}{2i} [\exp(iX) - \exp(-iX)] = X - \frac{X^3}{3!} + \dots + (-1)^r \frac{X^{2r+1}}{(2r+1)!} + \dots$$

Enfin, on appelle *tangente formelle* de X , et on note $\operatorname{tg} X$, la série entière formelle définie par la formule

$$(3') \quad \operatorname{tg} X = \frac{\sin X}{\cos X} = i \frac{\exp(-iX) - \exp(iX)}{\exp(-iX) + \exp(iX)} = i \frac{\exp(-2iX) - 1}{\exp(-2iX) + 1} \\ = i \frac{1 - \exp(2iX)}{1 + \exp(2iX)}.$$

Par suite,

$$(15) \quad \cos X = \operatorname{ch}(iX) \quad \operatorname{ch} X = \cos(iX)$$

$$(16) \quad i \sin X = \operatorname{sh}(iX) \quad i \operatorname{sh} X = \sin(iX)$$

$$(17) \quad i \operatorname{tg} X = \operatorname{th}(iX) \quad i \operatorname{th} X = \operatorname{tg}(iX).$$

PROPOSITION 1.49. — **Propriétés des séries entières formelles trigonométriques.**

1. Les séries entières formelles $\cos X$ et $\sin X$ satisfont aux relations suivantes :

$$(4') \quad \exp(iX) = \cos X + i \sin X$$

$$(5') \quad \exp(-iX) = \cos X - i \sin X$$

$$(6') \quad \cos^2 X + \sin^2 X = 1.$$

Plus précisément,

$$(7') \quad \cos X = (1 - \sin^2 X)^{\frac{1}{2}}$$

En outre,

$$(8') \quad D(\cos X) = -\sin X$$

$$(9') \quad D(\sin X) = \cos X$$

$$(10') \quad D(\operatorname{tg} X) = 1 + \operatorname{tg}^2 X = \frac{1}{\cos^2 X}.$$

2. Les séries entières formelles $\sin X$ et $\operatorname{tg} X$ admettent des séries entières formelles réciproques, appelées *arc sinus formel* et *arc tangente formel* de X , et notées $\operatorname{Arc} \sin X$ et $\operatorname{Arc} \operatorname{tg} X$. Par suite,

$$(18) \quad i \operatorname{Arc} \sin X = \operatorname{Arg} \operatorname{sh}(iX) \quad i \operatorname{Arg} \operatorname{sh} X = \operatorname{Arc} \sin(iX)$$

$$(19) \quad i \operatorname{Arc} \operatorname{tg} X = \operatorname{Arg} \operatorname{th}(iX) \quad i \operatorname{Arg} \operatorname{th} X = \operatorname{Arc} \operatorname{tg}(iX).$$

De plus,

$$(11') \quad D(\text{Arc sin } X) = (1 - X^2)^{-\frac{1}{2}}$$

$$(12') \quad D(\text{Arc tg } X) = \frac{1}{1 + X^2}.$$

Par suite,

$$(13') \quad \text{Arc sin } X = X + \frac{X^3}{6} + \frac{3}{40} X^5 + \dots + \frac{(2r)!}{2^{2r}(r!)^2} X^{2r+1} + \dots$$

$$(14') \quad \text{Arc tg } X = X - \frac{X^3}{3} + \frac{X^5}{5} + \dots + (-1)^r \frac{X^{2r+1}}{2r+1} + \dots$$

3. L'application $A \mapsto \sin A$ est une bijection de \mathfrak{M} sur lui-même, appelée *sinus formel*, dont la bijection réciproque n'est autre que l'application $A \mapsto \text{Arc sin } A$.

De même, l'application $A \mapsto \text{tg } A$ est une bijection de \mathfrak{M} sur lui-même, appelée *tangente formelle*, dont la bijection réciproque n'est autre que l'application $A \mapsto \text{Arc tg } A$.

Enfin, l'application $A \mapsto \cos A$ est une application de \mathfrak{M} dans \mathfrak{U} . Pour que deux éléments A et A' de \mathfrak{M} satisfassent à la relation $\cos A' = \cos A$, il faut et il suffit que $A' = \pm A$.

Pour démontrer cette proposition, on peut s'inspirer du cas des séries entières formelles hyperboliques, ou, plus simplement, utiliser les formules (15), (16) et (17).

REMARQUE 1. — Le calcul explicite des coefficients de la série entière formelle $\text{tg } X$ sera effectué au § 2.6.

REMARQUE 2. — Les propositions I.6.29 à I.6.31 subsistent pour les séries entières formelles trigonométriques ; en outre, elles sont valables sans aucune restriction.

Exercices conseillés : 76, 80 à 82.

3. FONCTIONS D'UNE VARIABLE ENTIÈRE

DÉFINITION 1.34. — **Algèbre de convolution d'un monoïde.** — Soit S un monoïde, c'est-à-dire un ensemble muni d'une loi de composition interne associative, notée multiplicativement, admettant un élément neutre e . On suppose que, pour tout élément s de S , l'ensemble des couples (t, u) d'éléments de S tels que $tu = s$ est fini.

On appelle *produit de convolution* de deux éléments f et g de l'espace vectoriel $\mathcal{F}(S, K)$ l'élément, noté $f * g$, de $\mathcal{F}(S, K)$, défini par la formule

$$(f * g)(s) = \sum_{tu=s} f(t)g(u).$$

L'application $(f, g) \mapsto f * g$ est une application bilinéaire de $\mathcal{F}(S, K) \times \mathcal{F}(S, K)$ dans $\mathcal{F}(S, K)$, qui définit sur cet espace vectoriel une structure de K -algèbre. La K -algèbre ainsi construite s'appelle algèbre de convolution du monoïde S , et se note $A_K(S)$, ou, plus simplement, $A(S)$.

PROPOSITION 1.50. — Propriétés de l'algèbre de convolution d'un monoïde. L'algèbre de convolution d'un monoïde S est associative et unitaire. Son élément neutre n'est autre que la fonction δ définie par la relation $\delta(s) = \delta_{es}$. Si le monoïde S est commutatif, l'algèbre $A(S)$ est commutative.

REMARQUE 1. — Lorsque S est le monoïde additif \mathbb{N} et que K est le corps des nombres complexes, $A(S)$ n'est autre que la \mathbb{C} -algèbre des séries entières formelles à une indéterminée. Lorsque cette indéterminée est notée X , pour tout élément f de $\mathcal{F}(\mathbb{N}, \mathbb{C})$, la série entière formelle $\sum_{n=0}^{+\infty} f(n)X^n$ s'appelle *série génératrice* de f . Alors la série génératrice du produit de convolution de deux fonctions définies sur \mathbb{N} à valeurs complexes n'est autre que le produit des séries génératrices associées à ces deux fonctions. De ce point de vue, les propriétés des séries entières formelles sont liées à celles du monoïde additif \mathbb{N} .

Voici des applications de cette méthode aux problèmes additifs de l'arithmétique :

EXEMPLE. — Partitions d'un entier. — Soit p un entier naturel non nul. On appelle partition d'un entier naturel n en p entiers une suite (n_1, n_2, \dots, n_p) d'entiers naturels telle que $\sum_{j=1}^p n_j = n$. Pour calculer le nombre $P(n)$ des partitions de n , considérons la série génératrice B de la fonction P :

$$B = \sum_{n=0}^{+\infty} P(n)X^n.$$

Considérons d'autre part la série

$$C = \sum_{n=0}^{+\infty} X^n.$$

On démontre par récurrence sur l'entier p que $B = C^p$. Or, $C = \frac{1}{1-X}$; donc

$$B = \frac{1}{(1-X)^p} = (1-X)^{-p} = \sum_{n=0}^{+\infty} C_{n+p-1}^n X^n.$$

Par suite, pour tout entier naturel n ,

$$P(n) = C_{n+p-1}^n = \frac{(n+p-1)!}{n!(p-1)!}$$

(formule des partitions).

(On retrouve ainsi de façon plus simple le résultat de l'exercice I.1.35.) On trouvera une généralisation de ce résultat dans l'exercice 79.

REMARQUE 2. — Lorsque S est le monoïde multiplicatif \mathbb{N}^* et que K est le corps des nombres complexes, $A(S)$ s'appelle algèbre des séries de Dirichlet formelles à une indéterminée. Son étude est esquissée dans l'exercice 84. Les propriétés des séries de Dirichlet formelles sont liées aux propriétés du monoïde multiplicatif \mathbb{N}^* . On trouvera de nombreuses applications de cette méthode aux problèmes multiplicatifs de l'arithmétique dans les exercices 86 et 87.

Exercices conseillés : 77 et 83.

EXERCICES

PROBLÈMES LINÉAIRES

- 1 A. On considère la suite des polynômes P_n , $n \geq 0$, à coefficients dans un corps K , définis par la formule

$$P_n = X^n + X^{n+1}.$$

Montrer que l'application $n \mapsto v_0(P_n)$ est une bijection de \mathbb{N} , et que, cependant, les polynômes P_n ne forment pas une base de $K[X]$.

- 2 A. 1. Soient α et β deux éléments distincts d'un corps K , et n un entier naturel. Montrer que les polynômes $P_r = (X - \alpha)^r(X - \beta)^{n-r}$, où r parcourt l'intervalle $[0, n]$, forment une base de l'espace vectoriel E_n des éléments de $K[X]$ de degré inférieur ou égal à n .

2. Montrer, plus généralement, que si U et V sont deux polynômes linéairement indépendants, alors, pour tout entier naturel n , les polynômes $P_r = U^r V^{n-r}$, où r parcourt $[0, n]$, sont linéairement indépendants.

3. Soient n un entier strictement positif, p un entier strictement supérieur à 2, et $\alpha_1, \alpha_2, \dots, \alpha_p$ des scalaires distincts deux à deux. Montrer que les polynômes

$$\prod_{i=1}^p (X - \alpha_i)^{\beta_i}, \quad \text{où, } \forall i \in [1, p], \quad \beta_i \in \mathbb{N}, \quad \text{et où } \sum_{i=1}^p \beta_i = n,$$

ne sont pas linéairement indépendants.

3. Soient α et β deux nombres complexes. On considère la famille S d'éléments de $\mathbb{C}[X]$ définie par les formules suivantes :

$$\begin{aligned} P_1 &= X^3 - 2\beta^2 X \\ P_2 &= 2X^5 + \beta X^4 - \beta^4 X \\ P_3 &= X^5 - \beta^2 X^3 \\ P_4 &= 3X^4 + 3\alpha^3 X \\ P_5 &= X^8 - \beta^2 X^6 + 2\beta^2 \alpha^2 X^4 \\ P_6 &= 3X^6 - 2\beta X^5 + \beta^5 X. \end{aligned}$$

1. Trouver le rang de la famille S , en discutant suivant les valeurs de α et β . Expliquer une famille libre L extraite de S ayant ce rang.

2. Compléter L en une base B de l'espace vectoriel E_8 des éléments de $\mathbb{C}[X]$ de degré inférieur ou égal à 8. Évaluer les monômes $1, X, X^2, \dots, X^8$ dans cette base.

- 4 A. Soient A et B deux polynômes à coefficients dans un corps K de caractéristique 0. On suppose que A est unitaire, et que A et B sont premiers entre eux. Soit enfin $A = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$ la décomposition en facteurs irréductibles du polynôme A .

On considère l'application U_B qui à tout élément R de $K(X)$ associe la fraction rationnelle $AR' - BR$.

1. Montrer que U_B est un endomorphisme de l'espace vectoriel $K(X)$.

Dans la suite de cet exercice, on se propose de déterminer le noyau de cet endomorphisme.

2. Montrer que si R est un élément non nul du noyau de U_B , tout facteur irréductible de R est un facteur irréductible de A , et réciproquement.

3. En déduire que si l'un au moins des entiers α_i est strictement supérieur à 1, le noyau de U_B est réduit à $\{0\}$.

4. On suppose donc désormais que, pour tout i , $\alpha_i = 1$. Pour tout $i \in [1, n]$, on considère le polynôme $A_i = P_1 P_2 \dots P_{i-1} P'_i P_{i+1} \dots P_n$. Montrer que ces n polynômes sont linéairement indépendants. Prouver que le noyau de U_B n'est pas réduit à $\{0\}$ si et seulement si le polynôme B est de la forme $B = \sum_{i=1}^n \beta_i A_i$, où, pour tout $i \in [1, n]$, $\beta_i \in \mathbb{Z}^*$,

et montrer qu'alors le noyau de U_B est la droite engendrée par $S = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n}$.

5. Montrer que si B et C sont deux éléments distincts de $K[X]$, premiers avec A , l'intersection des noyaux de U_B et U_C est réduite à $\{0\}$.

5. Soit E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n à coefficients dans un corps K de caractéristique nulle.

1. Soit α un scalaire. Montrer que l'application U_α qui à tout élément P de E_n associe $P(X + \alpha)$ est un endomorphisme de E_n .

2. Montrer que l'ensemble G des endomorphismes U_α , où α parcourt K , est un sous-groupe commutatif du groupe linéaire $\text{GL}(E_n)$, et que l'application $\alpha \mapsto U_\alpha$ est un isomorphisme du groupe additif K sur G .

3. Écrire la matrice M_α associée à U_α dans la base canonique de E_n .

4. De la relation $M_{\alpha+\beta} = M_\alpha M_\beta$ déduire des formules d'analyse combinatoire.

6. Soit $K[X]$ l'espace vectoriel des polynômes à coefficients dans K .

1. On considère un entier n strictement positif, une famille libre (P_1, P_2, \dots, P_n) d'éléments de $K[X]$, et deux polynômes Q et R premiers entre eux, R étant non constant.

Prouver que, pour tout $p \in \mathbb{N}^*$, les $n + p$ polynômes $Q, RQ, \dots, R^{p-1}Q, R^p P_1, R^p P_2, \dots, R^p P_n$ sont linéairement indépendants.

2. En déduire le résultat suivant :

Soient a_1, a_2, \dots, a_n des éléments de K distincts deux à deux, et $\alpha_1, \alpha_2, \dots, \alpha_n$ des entiers strictement positifs. Alors les polynômes

$$\frac{\prod_{i=1}^n (X - a_i)^{\alpha_i}}{(X - a_j)^{\beta_j}},$$

où j parcourt l'intervalle $[1, n]$, et où, pour tout j , β_j parcourt l'intervalle $[1, \alpha_j]$, sont linéairement indépendants.

3. Retrouver à l'aide de la question 2 l'unicité de la décomposition en éléments simples d'une fraction rationnelle à coefficients dans un corps algébriquement clos.

7. Soit E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n , $n \in \mathbb{N}^*$, à coefficients dans un corps K de caractéristique 0.

1. Montrer que les polynômes $P_p(X) = X^p(1 - X)^{n-p}$, où $p \in [0, n]$, forment une base B de E_n .

Écrire la matrice de passage de la base canonique de E_n à la base B , ainsi que la matrice inverse.

2. A tout élément P de $K[X]$ on associe le polynôme $U_n(P)$ défini par

$$U_n(P) = \sum_{p=0}^n P\left(\frac{p}{n}\right) C_n^p X^p (1 - X)^{n-p}.$$

a) Calculer $U_n(P)$ lorsque $P = 1$, $P = X$. Vérifier la relation

$$U_n(XP) = \frac{1}{n} X(1 - X) D[U_n(P)] + XU_n(P).$$

En déduire $U_n(P)$ lorsque $P = X^2$. Démontrer la relation

$$\sum_{p=0}^n (p - nX)^2 C_n^p X^p (1 - X)^{n-p} = nX(1 - X).$$

b) Montrer que, pour tout entier naturel m , le sous-espace vectoriel E_m est stable par U_n et que, si $m \leq n$, U_n induit un automorphisme de E_m .

- 8 A. Soient n un entier strictement positif, et E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n , à coefficients dans un corps K de caractéristique zéro. On considère l'application U qui à tout élément P de $K[X]$ associe le polynôme

$$P(X + 1) + P(X - 1) - 2P(X).$$

1. Montrer que U est un endomorphisme de l'espace vectoriel $K[X]$ qui laisse stable E_n .

2. Calculer $U(X^p)$, où p parcourt \mathbb{N} .

3. Déterminer le noyau et l'image de U .

4. Montrer enfin que pour tout élément Q de $K[X]$, il existe un élément P de $K[X]$ et un seul tel que

$$U(P) = Q, \quad \text{et} \quad P(0) = P'(0) = 0.$$

(On trouvera dans l'exercice 4.33 une méthode permettant le calcul explicite de P .)

9 A. Fonctions polynomiales sur un corps fini.

I. — *Sous-groupes finis du groupe multiplicatif d'un corps commutatif.* — Soient K un corps commutatif, G un sous-groupe fini de K^* , n l'ordre de G , d le plus grand des ordres des éléments de G et x un élément de G d'ordre d . Prouver que tout élément y de G dont l'ordre divise d est une racine du polynôme $X^d - 1$. En déduire que $d = n$.

(On pourra raisonner par l'absurde, en montrant qu'il existe alors un élément z de G dont l'ordre c ne divise pas d . On prouvera qu'il existe un élément du sous-groupe engendré par x et z dont l'ordre est égal au P. P. C. M. de c et d , ce qui contredit la définition de d .)

Ainsi, tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. En particulier, le groupe multiplicatif d'un corps fini est cyclique.

II. — *Polynômes réduits à coefficients dans un corps fini.* — Soient K un corps commutatif fini, $\alpha_1, \alpha_2, \dots, \alpha_q$ ses éléments.

On dit qu'un élément P de $K[X]$ est *réduit* si son degré est strictement inférieur à q . On note f le morphisme de l'algèbre unitaire $K[X]$ dans l'algèbre unitaire $\mathcal{F}(K)$ qui à tout polynôme P associe la fonction polynomiale \tilde{P} .

1. Prouver que si P est réduit et si $\tilde{P} = 0$, alors P est nul.

2. Prouver que, pour tout élément P de $K[X]$, le reste de la division euclidienne de P par $X^q - X = \prod_{i=1}^q (X - \alpha_i)$ est le seul polynôme réduit ayant même fonction polynomiale associée que P .

3. Montrer que l'application f définit un isomorphisme du sous-espace vectoriel de $K[X]$ constitué des polynômes réduits sur l'espace vectoriel $\mathcal{F}(K)$. (On pourra utiliser le polynôme d'interpolation de Lagrange; cf. th. 4.5.)

10 A. Racines rationnelles des équations algébriques.

Soit

$$P = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \dots + \alpha_0$$

un polynôme à coefficients entiers rationnels premiers entre eux dans leur ensemble. Montrer que, pour toute racine rationnelle r de P , écrite sous forme canonique $r = \frac{p}{q}$, p divise α_0 et q divise α_n .

Application. — Trouver les racines rationnelles des polynômes suivants :

$$\begin{aligned} &4X^3 - 8X^2 + 5X - 3 \\ &2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10 \\ &45X^4 - 168X^3 - 55X^2 + 26X + 8 \\ &X^6 - X^5 - 19X^4 - 10X^3 + 29X^2 - 17X - 15 \\ &8X^6 - 34X^5 - 11X^4 + 152X^3 - 76X^2 - 39X + 18. \end{aligned}$$

11. Caractérisation des fractions rationnelles paires, ou impaires.

Soit K un corps de caractéristique différente de 2. Soit R une fraction rationnelle non nulle à coefficients dans K , écrite sous la forme irréductible $R = \frac{P}{Q}$.

1. Prouver que R est paire si et seulement si P et Q sont pairs.

2. Prouver que si R est impaire, 0 est soit un pôle, soit un zéro de R . Prouver que R est impaire et admet 0 pour pôle si et seulement si P est pair et Q impair; prouver que R est impaire et admet 0 pour zéro si et seulement si P est impair et Q pair.

12. Composée de deux fractions rationnelles.

1. Soient P et Q deux éléments de $K[X]$, $P \neq 0$.

Montrer que la relation $P \circ Q = 0$ implique que Q est un scalaire.

Prouver que si $d^\circ(Q) > 0$, alors $d^\circ(P \circ Q) = d^\circ(P) \cdot d^\circ(Q)$.

2. Soient P un élément de $K[X]$, écrit sous la forme

$$P = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \dots + \alpha_m X^m, \quad \alpha_m \neq 0, \alpha_n \neq 0,$$

et R un élément de $K(X)$. Montrer que

— si $d^\circ(R) > 0$, $d^\circ(P \circ R) = n d^\circ(R)$;

— si $d^\circ(R) < 0$, $d^\circ(P \circ R) = m d^\circ(R)$;

— si $d^\circ(R) = 0$, la relation $P \circ R = 0$ implique que R est un scalaire. (On pourra écrire R sous la forme $R = \beta + R_1$, où $d^\circ(R_1) < 0$.)

3. En déduire que si R est une fraction rationnelle non constante, R est substituable dans toute fraction rationnelle.

4. Soient R une fraction rationnelle de degré strictement positif et S une fraction rationnelle. Prouver que $d^\circ(S \circ R) = d^\circ(S) \cdot d^\circ(R)$.

5. Prouver que si R et S sont non constantes, il en est de même de $S \circ R$. (On pourra raisonner par l'absurde, en supposant que $S \circ R = \alpha$, où $\alpha \in K$, et poser $S_1 = S - \alpha$.)

13 A. Endomorphismes de $K[X]$.

1. Pour tout élément P de $K[X]$, il existe un endomorphisme U_P et un seul de la K -algèbre unitaire $K[X]$ tel que $U_P(X) = P$. Prouver que l'application j qui à tout élément P de $K[X]$ associe U_P est une bijection de $K[X]$ sur l'ensemble des endomorphismes de la K -algèbre unitaire $K[X]$.

2. Montrer que, pour tout couple (P, Q) d'éléments de $K[X]$, $U_{Q \circ P} = U_P \circ U_Q$.

14 A. Endomorphismes de $K(X)$.

1. Prouver que, pour tout élément R non constant de $K(X)$, il existe un endomorphisme U_R et un seul de la K -algèbre unitaire $K(X)$ tel que $U_R(X) = R$. Montrer que l'application j qui à tout élément R non constant de $K(X)$ associe U_R est une bijection de $K(X) - K$ sur l'ensemble des endomorphismes de la K -algèbre unitaire $K(X)$ dont l'image n'est pas contenue dans K .

2. Montrer que, pour tout couple (R, S) d'éléments non constants de $K(X)$,

$$U_{S \circ R} = U_R \circ U_S.$$

15 B. Automorphismes de $K[X]$ et de $K(X)$.

1. Soient (α, β) un couple d'éléments de K tel que $\beta \neq 0$, et $U_{\alpha\beta}$ l'endomorphisme de la K -algèbre unitaire $K[X]$ défini par la relation

$$U_{\alpha\beta}(X) = \beta(X - \alpha).$$

Montrer que $U_{\alpha\beta}$ est un automorphisme et que, réciproquement, tout automorphisme U de la K -algèbre unitaire $K[X]$ est de la forme précédente. (On pourra considérer l'unique polynôme P tel que $U(P) = X$.)

2. Soient $(\alpha, \beta, \gamma, \delta)$ un quadruplet d'éléments de K tel que $\alpha\delta - \beta\gamma \neq 0$, et $U_{\alpha\beta\gamma\delta}$ l'endomorphisme de la K -algèbre unitaire $K(X)$ défini par la relation

$$U_{\alpha\beta\gamma\delta}(X) = \frac{\alpha X + \beta}{\gamma X + \delta}.$$

Montrer que $U_{\alpha\beta\gamma\delta}$ est un automorphisme et que, réciproquement, tout automorphisme U de la K -algèbre unitaire $K(X)$ est de la forme précédente. (On pourra considérer la fraction rationnelle $R = U(X)$ et l'unique fraction rationnelle S telle que $U(S) = X$. On prouvera que le degré p de R est nécessairement égal à 1, 0 ou -1 . On traitera d'abord le cas où $p = 1$ en écrivant R sous la forme $R = \beta(X - \alpha) + R_1$, où $\alpha \in K$, $\beta \in K^*$ et $d^\circ(R_1) < 0$, et l'on prouvera que R_1 est nulle, en considérant un facteur irréductible éventuel du dénominateur de R . On ramènera le cas où $p = -1$ au cas où $p = 1$ à l'aide de l'automorphisme transformant X en $\frac{1}{X}$. Enfin, on ramènera le cas où $p = 0$ au cas où $p = -1$ en écrivant R sous la forme $R = \alpha + R_1$, où $\alpha \in K$ et $d^\circ(R_1) < 0$, et en utilisant l'automorphisme transformant X en $X - \alpha$.)

16 A. Automorphismes réels de $C[X]$ et de $C(X)$.

1. Trouver tous les automorphismes de l'anneau $C[X]$ qui laissent fixes les polynômes constants réels. (On prouvera qu'un élément α de C se transforme en α ou $\bar{\alpha}$; on appliquera ensuite l'exercice précédent.)

2. Chercher de même tous les automorphismes du corps $C(X)$ qui laissent fixes les constantes réelles.

17 B. Automorphismes de la droite et de la droite projective.

Soit K un corps infini.

I. — Automorphismes de la droite.

1. Prouver que, pour tout couple (α, β) d'éléments de K tel que $\beta \neq 0$, l'application $f_{\alpha\beta} : x \mapsto \beta(x - \alpha)$ est une fonction polynomiale sur K bijective, et que la bijection réciproque est encore une fonction polynomiale.

Réciproquement, montrer que tout automorphisme de la droite K , c'est-à-dire toute fonction polynomiale f sur K , bijective et dont la bijection réciproque g est polynomiale, est affine, c'est-à-dire de la forme $f_{\alpha\beta}$. (On montrera que la relation $(g \circ f)(x) = x$ pour tout point x de K implique que f et g sont de degré 1.)

2. Retrouver le résultat précédent en utilisant la question 1 de l'exercice 15.

3. On suppose que K est algébriquement clos. Soit f une fonction polynomiale sur K , satisfaisant à la condition suivante : il existe une partie finie E de K telle que la restriction de f à $K - E$ soit injective. Prouver que f est de la forme $f_{\alpha\beta}$. (En composant f avec des applications $f_{\alpha\beta}$ convenablement choisies, on se ramènera au cas où $0 \notin E$ et où $f(0) = 0$.)

Prouver que ce résultat ne s'étend pas lorsque K n'est pas algébriquement clos, en construisant une fonction polynomiale sur \mathbb{R} , bijective, et dont la bijection réciproque n'est pas polynomiale.

II. — Automorphismes de la droite projective.

1. Prouver que, pour tout quadruplet $(\alpha, \beta, \gamma, \delta)$ d'éléments de K tel que $\alpha\delta - \beta\gamma \neq 0$, l'application $f_{\alpha\beta\gamma\delta} : x \mapsto \frac{\alpha x + \beta}{\gamma x + \delta}$ est une fonction rationnelle sur $P_1(K)$ bijective, et que la bijection réciproque est encore une fonction rationnelle.

Réciproquement, montrer que tout automorphisme de la droite projective $P_1(K)$, c'est-à-dire toute fonction rationnelle sur $P_1(K)$, bijective et dont la bijection réciproque g est rationnelle, est homographique, c'est-à-dire de la forme $f_{\alpha\beta\gamma\delta}$. (On considérera la relation $(g \circ f)(x) = x$ pour tout point x de $P_1(K)$. On prouvera que le degré de f est nécessairement égal à 1, 0 ou -1 . On utilisera alors la même méthode que dans la question 2 de l'exercice 15.)

2. Retrouver le résultat précédent en utilisant la question 2 de l'exercice 15.

3. On suppose que K est algébriquement clos. Soit f une fonction rationnelle sur $P_1(K)$, satisfaisant à la condition suivante : il existe une partie finie E de $P_1(K)$ telle que la restriction de f à $P_1(K) - E$ soit injective. Prouver que f est de la forme $f_{\alpha\beta\gamma\delta}$. (En composant f avec des applications $f_{\alpha\beta\gamma\delta}$ convenablement choisies, on se ramènera au cas où $\infty \notin E$ et où $f(\infty) = \infty$. On prouvera alors que f est polynomiale, et l'on appliquera les résultats de la question I.3.)

18 A. 1. Soit α un nombre complexe. Déterminer tous les éléments P de $\mathbb{C}[X]$ tels que $P(\alpha X) = P(X)$. Plus généralement, déterminer tous les couples (P, β) , où $P \in \mathbb{C}[X]$ et $\beta \in \mathbb{C}$, tels que $P(\alpha X) = \beta P(X)$.

2. Soient α et β deux nombres complexes. Déterminer tous les éléments R de $\mathbb{C}(X)$ tels que $R(\alpha X + \beta) = R(X)$.

*3. Soient $\alpha, \beta, \gamma, \delta$ quatre nombres complexes tels que $\alpha\delta - \beta\gamma \neq 0$. Déterminer tous les éléments R de $\mathbb{C}(X)$ tels que

$$R\left(\frac{\alpha X + \beta}{\gamma X + \delta}\right) = R(X).$$

(On pourra introduire les points fixes z_0 et z_1 de l'application qui à tout élément z de $P_1(\mathbb{C})$ associe $\frac{\alpha z + \beta}{\gamma z + \delta}$. On traitera d'abord le cas où l'un au moins de ces points fixes est l'élément ∞ de $P_1(\mathbb{C})$, puis le cas où $z_0 = z_1$, et enfin le cas où $z_0 \in \mathbb{C}$, $z_1 \in \mathbb{C}$, $z_0 \neq z_1$.)

Dans ces deux derniers cas, on utilisera la forme réduite de la transformation homographique précédente.)_{*}

4. Déterminer en particulier tous les éléments R de $\mathbb{C}(X)$ tels que

$$R\left(\frac{1}{X}\right) = R(X).$$

DIVISION EUCLIDIENNE

19. *Calculs de restes de divisions euclidiennes.*

Tous les polynômes intervenant dans cet exercice seront considérés comme polynômes à coefficients complexes.

1. Soient p et q deux entiers naturels. Calculer le reste de la division euclidienne de $X^p + X^q + 1$ par $X^2 + X + 1$.

En déduire une condition nécessaire et suffisante portant sur p et q pour que $X^p + X^q + 1$ soit divisible par $X^2 + X + 1$.

2. Soient n un entier strictement positif et α un nombre réel. Calculer le reste de la division euclidienne de $X^{n+1} \cos(n-1)\alpha - X^n \cos n\alpha - X \cos \alpha + 1$ par $X^2 - 2X \cos \alpha + 1$.

3. Soit n un entier naturel. Calculer le reste de la division euclidienne de

$$(X-1)^{n+2} + X^{2n+1}$$

par $X^2 - X + 1$.

4. Soient α un nombre réel et n un entier naturel. Calculer le reste de la division euclidienne de $(X \sin \alpha + \cos \alpha)^n$ par $X^2 + 1$.

20 A. *Reste d'une division euclidienne par un produit.*

1. Soient α et β deux éléments distincts de K , et P un élément de $K[X]$. Déterminer le reste de la division euclidienne de P par $(X - \alpha)(X - \beta)$, connaissant les restes de la division euclidienne de P par $X - \alpha$, et par $X - \beta$.

2. Plus généralement, soient $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une famille d'éléments de K distincts deux à deux, et P un élément de $K[X]$. Déterminer, grâce à la formule d'interpolation de Lagrange, le reste de la division euclidienne de P par $(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$, connaissant, pour tout $i \in [1, n]$, le reste de la division euclidienne de P par $X - \alpha_i$._{}

3. Soient a un élément d'un corps de caractéristique zéro, et P un élément de $K[X]$. Déterminer le reste de la division euclidienne de P par $(X - a)^2$ connaissant le reste de la division euclidienne de P par $X - a$, et celui de la division euclidienne de P' par $X - a$.

4. Soient enfin A un polynôme scindé sur un corps K de caractéristique zéro, et P un élément de $K[X]$. Déterminer le reste de la division euclidienne de P par A , connaissant, pour toute racine α de A d'ordre p , les restes des divisions euclidiennes de $P, D(P), \dots, D^{p-1}(P)$ par $X - \alpha$._{}

21 A. *Reste de la division par $X^p - \alpha$.*

Soit p un entier strictement positif. Montrer que tout élément P de $K[X]$ peut s'écrire d'une manière et d'une seule sous la forme

$$P = Q_0(X^p) + XQ_1(X^p) + \dots + X^{p-1}Q_{p-1}(X^p),$$

où $Q_0, Q_1, \dots, Q_{p-1} \in K[X]$.

Application. — Soit α un élément de K . Trouver le reste de la division de P par $X^p - \alpha$.

DIVISIBILITÉ

22 A. Soit K un corps de caractéristique zéro. Trouver tous les éléments de $K[X]$ divisibles par leur dérivée.

23. *Conditions de divisibilité.*

Tous les polynômes intervenant dans cet exercice seront considérés comme polynômes à coefficients complexes.

1. Montrer que $(X + 1)^n - X^n - 1$ est divisible par

$$\begin{array}{ll} X(X + 1)(X^2 + X + 1) & \text{si } n \text{ est de la forme } 6p - 1 \\ X(X + 1)(X^2 + X + 1)^2 & \text{si } n \text{ est de la forme } 6p + 1. \end{array}$$

2. Trouver une condition nécessaire et suffisante portant sur des nombres complexes α et β pour que $\alpha X^{n+1} + \beta X^n + 1$ soit divisible par $(X - 1)^2$.

3. Pour quelles valeurs de l'entier naturel n le polynôme $X^{4n} - X^{3n} + X^{2n} - X^n + 1$ est-il divisible par $X^4 - X^3 + X^2 - X + 1$?

4. Soient α et β deux nombres complexes. Trouver une condition nécessaire et suffisante portant sur α et β pour que $X^4 + 3X^2 + \alpha X + \beta$ soit divisible par $X^2 + \alpha X + 2$.

5. Soient $\alpha, \beta, \gamma, \lambda, \mu, \nu$ des nombres complexes. Trouver une condition nécessaire et suffisante portant sur ces nombres pour que le polynôme $\lambda X^8 + \mu X^4 + \nu$ soit divisible par le polynôme $\alpha X^2 + \beta X + \gamma$.

6. Trouver une condition nécessaire et suffisante portant sur des nombres complexes α et β pour que $X^{2n} + X^n + 1$ soit divisible par $X^3 + \alpha X + \beta$.

24 A. P. G. C. D. de $X^p - 1$ et $X^q - 1$.

Soit K un corps de caractéristique zéro.

1. Soient p et q deux entiers strictement positifs, et d leur P. G. C. D. Prouver que le P. G. C. D. des deux polynômes $X^p - 1$ et $X^q - 1$ est $X^d - 1$.

2. Plus généralement, étant donnés des entiers strictement positifs p_1, p_2, \dots, p_n , déterminer le P. G. C. D. des polynômes $X^{p_r} - 1$, où r parcourt l'intervalle $[1, n]$.

3. Soient n, p et q trois entiers strictement positifs. Déterminer le P. G. C. D. des deux polynômes suivants :

$$\begin{aligned} P &= X^{n(p-1)} + X^{n(p-2)} + \dots + X^n + 1. \\ Q &= X^{n(q-1)} + X^{n(q-2)} + \dots + X^n + 1. \end{aligned}$$

4. Lorsque $K = \mathbb{C}$, retrouver les résultats des questions précédentes à l'aide de la théorie des racines de l'unité.

25. *Calculs de P. G. C. D.*

Tous les polynômes intervenant dans cet exercice seront considérés comme polynômes à coefficients complexes.

1. Calculer le P. G. C. D. de

$$X^4 - 3X^3 - 12X^2 + 17X - 3 \quad \text{et} \quad 2X^3 + 5X^2 - 4X - 3.$$

2. Calculer le P. G. C. D. de

$$X^6 - 2X^5 + X^4 - X^2 + 2X - 1 \quad \text{et} \quad X^5 - 3X^3 + X^2 + 2X - 1.$$

3. Calculer le P. G. C. D. du polynôme $4X^4 + 4X^3 - 3X^2 - 2X + 1$ et de sa dérivée.
 4. Soit a un nombre complexe. Déterminer, suivant les valeurs de a , le P. G. C. D. de

$$X^6 - X^5 - X^4 + 2X^3 - X^2 - X + a \quad \text{et de} \quad X^4 + X^3 - 3X^2 - X + 2.$$

26. Soit n un entier naturel non nul. Déterminer les nombres complexes α tels que les polynômes $(X + \alpha)^n - 1$ et $(X - \alpha)^n - 1$ ne soient pas premiers entre eux.
 27. Trouver tous les couples (A, B) de polynômes à coefficients complexes tels que

$$A = B'B'' \quad \text{et} \quad B = A'A''.$$

Expliciter les racines de A et B .

28. Trouver tous les triplets (A, B, C) de polynômes unitaires à coefficients dans K tels que

$$A \mid BC, \quad B \mid CA, \quad C \mid AB.$$

(On pourra se ramener au cas où P. G. C. D. $(A, B, C) = 1$, et montrer que la solution générale est alors :

$$A = VW, \quad B = WU, \quad C = UV,$$

où U, V, W sont trois polynômes unitaires premiers entre eux deux à deux.)

29. On se propose de déterminer les triplets (A, B, C) de polynômes à coefficients complexes premiers entre eux deux à deux et tels que

$$A^2 + B^2 = C^2.$$

1. Montrer que les polynômes $C + B$ et $C - B$ sont des carrés parfaits dans l'anneau $\mathbb{C}[X]$. En déduire tous les triplets (A, B, C) satisfaisant au problème.

2. Déterminer A et B lorsque $C = X^2 + \alpha^2$, où $\alpha \in \mathbb{C}$. Lorsque α est réel, montrer que les seuls polynômes A et B à coefficients réels tels que $A^2 + B^2 = X^2 + \alpha^2$ sont de la forme

$$\begin{aligned} A &= (X^2 - \alpha^2) \sin \beta + 2\alpha X \cos \beta \\ B &= (X^2 - \alpha^2) \cos (\beta + k\pi) - 2\alpha X \sin (\beta + k\pi), \end{aligned}$$

où $\beta \in \mathbb{R}$ et $k \in \mathbb{N}$.

30. 1. Déterminer tous les couples (P_1, Q_1) de polynômes à coefficients complexes, premiers entre eux, et tels que

$$P_1^2 + Q_1^2 = X^2 + 1.$$

Expliciter les couples (P_1, Q_1) de polynômes à coefficients réels satisfaisant à ces conditions.

2. Déterminer tous les couples (P_n, Q_n) de polynômes à coefficients complexes, premiers entre eux, et tels que

$$P_n^2 + Q_n^2 = (X^2 + 1)^n, \quad \text{où } n \in \mathbb{N}^*.$$

Expliciter les couples (P_n, Q_n) de polynômes à coefficients réels satisfaisant à ces conditions.

(On pourra employer une méthode directe, ou se ramener au cas où $n = 1$ en introduisant des primitives de P_1 et Q_1 .)

31. Soient K un corps de caractéristique zéro, n un entier strictement positif, p et q deux entiers naturels tels que $p + q = n + 1$, α et β deux scalaires distincts, $\beta \neq 0$. Trouver les éléments P de $K[X]$ de degré n tels que $P + \alpha$ soit divisible par $(X - \beta)^p$, et que $P - \alpha$ soit divisible par $(X + \beta)^q$.

Application. — Expliciter le cas où $p = q = 3$, et $\alpha = \beta = 1$.

32. Étant donnés deux polynômes A et B à coefficients dans un corps K , premiers entre eux, et deux scalaires distincts α et β , déterminer tous les éléments P de $K[X]$ dont le reste de la division euclidienne par A soit α , et le reste de la division euclidienne par B soit β .

Comparer avec l'exercice précédent.

33. Étant donnés trois polynômes A , B et C à coefficients complexes, B et C premiers entre eux, déterminer tous les éléments P de $C[X]$ tels que $A + PB$ soit divisible par C .

Examiner le cas où C a toutes ses racines simples, et où $B = C'$.

34. 1. Soient α et β deux éléments non nuls d'un corps K . Trouver le P. G. C. D. de deux éléments A et B de $K[X]$, sachant que $\alpha A + \beta B$ divise A et B .

2. Trouver tous les éléments P de $K[X]$ tels qu'il existe un couple (U, V) d'éléments de $K[X]$ dont $U - V$ soit le P. G. C. D., et P le P. P. C. M.

Application. — Montrer que l'élément $P = 2X^3 - 3X^2 - 5X + 6$ de $C[X]$ répond à la question, et déterminer alors tous les couples (U, V) .

35. Soient n un entier naturel strictement supérieur à 1 et P un élément non nul de $C[X]$.

1. On suppose que $P(X)$ divise $P(X^n)$. Soit α une racine non nulle de P . Prouver qu'il existe deux entiers naturels distincts r et s tels que $\alpha^{(n^r)} = \alpha^{(n^s)}$. En déduire qu'il existe un entier naturel k tel que $\alpha^k = 1$. On note $m(\alpha)$ le plus petit des entiers k satisfaisant à cette condition.

Soit p le P. P. C. M. des nombres $m(\alpha)$, où α parcourt l'ensemble E des racines non nulles de P , et β une racine primitive $p^{\text{ième}}$ de l'unité. Prouver que, pour tout élément α de E , il existe un entier q tel que $\alpha = \beta^q$.

2. On suppose en outre que $P(X + 1)$ divise $P(X^n)$. Montrer que pour toute racine α de P différente de 0 et de 1, $(\alpha - 1)^n$ appartient à E . En déduire que α et $\alpha - 1$ sont des racines $np^{\text{ièmes}}$ de l'unité, et que α est nécessairement égal à $-j$ ou à $-j^2$.

On suppose que n n'est pas multiple de 3, et que $P(X)$ et $P(X + 1)$ divisent $P(X^n)$. Montrer que les seules racines de P sont nécessairement égales à 0 ou 1. Prouver que les seuls polynômes non nuls satisfaisant aux conditions précédentes sont les polynômes constants si n est impair, et les polynômes de la forme $\gamma X^p(X - 1)^q$, où $\gamma \in C^*$ et $p \leq q \leq np$, si n est pair.

On suppose maintenant que n est multiple de 3. Prouver que les seuls polynômes non nuls tels que $P(X)$ et $P(X + 1)$ divisent $P(X^n)$ sont les polynômes constants si n est impair, et les polynômes de la forme $\gamma X^p(X - 1)^q(X + j)^r(X + j^2)^s$, où $\gamma \in C^*$, $p \leq q \leq np$, $r \leq q$, $s \leq q$, si n est pair.

36. 1. Soient K un corps algébriquement clos de caractéristique différente de 2, P et Q deux éléments de $K[X]$ premiers entre eux. Montrer que si un élément α de K est racine double de $P^2 + Q^2$, α est racine de $P'^2 + Q'^2$.

* Étendre ce résultat au cas où K est un corps de caractéristique différente de 2. (On pourra considérer une extension convenable de K .) Trouver un contre-exemple lorsque K est de caractéristique 2.*

2. Soit P un polynôme de degré 4 à coefficients dans un corps K de caractéristique zéro. Montrer que pour que P soit un carré parfait, il faut et il suffit que $PP'' - \frac{3}{4}P'^2$ soit proportionnel à P .

DÉCOMPOSITION EN FACTEURS IRRÉDUCTIBLES

37. *Décompositions en facteurs irréductibles.*

1. Décomposer le polynôme $X^5 - 1$ en facteurs irréductibles sur \mathbf{C} , sur \mathbf{R} , sur \mathbf{Q} .
 2. Soient α un nombre réel, et n un entier strictement positif. Décomposer le polynôme $X^{2n} - 2 \cos \alpha X^n + 1$ en facteurs irréductibles sur \mathbf{C} , et sur \mathbf{R} .
 3. Soit n un entier strictement positif. Décomposer le polynôme $X^{2n} - 1$ en facteurs irréductibles sur \mathbf{C} , et sur \mathbf{R} .
- En déduire la valeur de

$$\sin \frac{\pi}{2n} \cdot \sin \frac{2\pi}{2n} \cdots \sin \frac{(n-1)\pi}{2n}.$$

4. Soient p et q deux nombres réels. Décomposer le polynôme

$$X^4 + pX^3 + qX^2 - pX + 1$$

en facteurs irréductibles sur \mathbf{R} .

5. Soient n un entier naturel non nul et α un nombre réel. Décomposer en facteurs irréductibles les polynômes

$$\frac{1}{2} [(X + e^{i\alpha})^n + (X + e^{-i\alpha})^n]$$

$$\frac{1}{2i} [(X + e^{i\alpha})^n - (X + e^{-i\alpha})^n]$$

dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.

- *38.** Décomposer en facteurs irréductibles dans $\mathbf{C}[X, Y]$, puis dans $\mathbf{R}[X, Y]$, les polynômes suivants :

$$\begin{array}{ccc} X^n - Y^n & X^n + Y^n & n \in \mathbf{N}^* \\ (X + Y)^7 - X^7 - Y^7. \end{array}$$

39. Soit \mathbf{F}_3 le corps $\mathbf{Z}/3\mathbf{Z}$.

1. Le polynôme $X^3 + X^2 - X + 1$ est-il un élément irréductible de $\mathbf{F}_3[X]$?
2. Déterminer tous les polynômes unitaires irréductibles de degré 2 dans $\mathbf{F}_3[X]$.

- 40.** Soient K un sous-corps d'un corps K' , P et Q deux éléments de $K[X]$. Montrer que P et Q ont même P. G. C. D. dans $K[X]$ et dans $K'[X]$. En particulier, si P et Q sont premiers entre eux dans $K[X]$, P et Q sont premiers entre eux dans $K'[X]$.

41 A. *Décomposition de Lagrange.*

Soit K un corps de caractéristique nulle. On dit qu'un élément P de $K[X]$ est un polynôme simple (sur K) si P est non constant et si P. G. C. D. $(P, P') = 1$.

1. Prouver que toutes les racines d'un polynôme simple sont simples.
2. Soient K' un corps contenant K comme sous-corps, et P un élément de $K[X]$. Prouver que si P est simple sur K , P est encore simple sur K' .
3. Déterminer les polynômes simples lorsque K est algébriquement clos, et lorsque $K = \mathbf{R}$.

4. Montrer que si K est algébriquement clos, tout élément Q non nul de $K[X]$ peut s'écrire d'une manière et d'une seule sous la forme

$$(1) \quad Q = \beta P_1^{p_1} P_2^{p_2} \dots P_r^{p_r}$$

où $\beta \in K^*$, où P_1, P_2, \dots, P_r sont des polynômes unitaires simples et premiers entre eux deux à deux, et où $p_1 < p_2 < \dots < p_r$.

5. Soient P un polynôme unitaire à coefficients dans K , n un nombre entier strictement positif, R un élément non nul de $K[X]$ premier avec P , et $Q = P^\alpha R$. Prouver que P. G. C. D. $(Q, Q') = P^{\alpha-1}$ P. G. C. D. (R, R') .

6. En déduire que le résultat de la question 4 est encore valable lorsque le corps K n'est pas algébriquement clos. (Pour prouver l'unicité de la décomposition (1), on calculera

$$Q_1 = \text{P. G. C. D. } (Q, Q'), \dots, Q_r = \text{P. G. C. D. } (Q_{r-1}, Q'_{r-1}).$$

et on explicitera les polynômes P_i en fonction des polynômes Q_i . On en déduira ensuite l'existence de la décomposition (1).)

En déduire que le nombre de racines distinctes d'un polynôme est la différence entre le degré de ce polynôme et le degré du P. G. C. D. de ce polynôme et du polynôme dérivé.

7. *Application.* — Décomposer en facteurs irréductibles sur \mathbb{C} , puis sur \mathbb{R} , les polynômes suivants :

$$\begin{aligned} X^3 + 4X^2 + 5X + 2 & \quad X^4 - 7X^3 + 18X^2 - 20X + 8 \\ X^6 - 3X^2 - 2 & \quad X^6 + X^4 + 3X^2 - 2X + 2 \\ X^9 + X^8 - 5X^7 - 7X^6 + 6X^5 + 14X^4 + 3X^3 - 7X^2 - 5X - 1. \end{aligned}$$

DÉCOMPOSITION EN ÉLÉMENTS SIMPLES

42 A. Compléments sur l'identité de Bezout.

Soient K un corps commutatif, A et B deux éléments non nuls de $K[X]$ premiers entre eux, et (U_0, V_0) l'unique couple d'éléments de $K[X]$ tels que

$$1 = AU_0 + BV_0, \quad d^\circ(V_0) < d^\circ(A), \quad d^\circ(U_0) < d^\circ(B).$$

1. Déterminer tous les couples (U, V) d'éléments de $K[X]$ tels que

$$1 = AU + BV.$$

2. Montrer comment l'algorithme d'Euclide permet d'expliciter le couple (U_0, V_0) .

*3. On suppose que le polynôme A est de degré n , où $n \in \mathbb{N}$, et possède n racines simples $\alpha_1, \alpha_2, \dots, \alpha_n$ dans K . Expliciter alors le polynôme V_0 . (On pourra utiliser la formule d'interpolation de Lagrange.)

Même question lorsque A est supposé seulement scindé sur K , le corps K étant de caractéristique zéro.*

4. Reprendre les questions précédentes dans le cas du problème suivant : étant donné un élément P de $K[X]$, déterminer tous les couples (U, V) de $K[X]$ tels que

$$P = AU + BV.$$

5. *Applications.* — (On suppose que $K = \mathbb{C}$). Déterminer tous les couples (U, V) d'éléments de $\mathbb{C}[X]$ tels que

- a) $1 = (X^2 + 1)U + (X^5 + 1)V$;
 b) $1 = (X^3 + X + 1)U + (X^3 - X + 1)V$;
 c) $1 = (X - \alpha)U + (X^p - 1)V$, où $p \in \mathbb{N}^*$, $\alpha \in \mathbb{C}$, et $\alpha^p \neq 1$;
 $1 = (X - \alpha)^2 U + (X^p - 1)V$, sous les mêmes hypothèses ;
 $X - \alpha = (X - \alpha)^2 U + (X^p - 1)V$, où $p \in \mathbb{N}^*$, $\alpha \in \mathbb{C}$, et $\alpha^p = 1$;
 d) $X - 1 = (X^p - 1)U + (X^q - 1)V$,

où p et q sont deux entiers strictement positifs premiers entre eux ;

- e) $1 = (X - \alpha)^p U + (X - \beta)^q V$, où p et $q \in \mathbb{N}^*$, α et $\beta \in \mathbb{C}$, $\alpha \neq \beta$;
 f) $1 = (X^2 + \alpha^2)U + (X - \alpha)^n V$, où $n \in \mathbb{N}^*$, et $\alpha \in \mathbb{C}^*$.

6. *Application à la recherche des parties principales.* — Soient R un élément de $K[X]$ et P un polynôme unitaire irréductible tels que $v_P(R) < 0$. Appliquer la question 4 à la détermination de la partie principale $\text{Pr}_P(R)$.

Exemples. — Déterminer les parties principales des éléments suivants de $\mathbb{R}[X]$:

$$\frac{X^2 + 1}{(X + 1)(X^2 + X + 1)^n}, \quad n \in \mathbb{N} \quad \frac{X^3}{(X - 1)^3(X^2 - X + 1)^2}$$

$$\frac{1}{(X^4 - 1)^3} \quad \frac{1}{X^4 + X^2 + 1}.$$

43 A. Étude des fractions rationnelles P -adiques.

Soient P un polynôme unitaire irréductible à coefficients dans K , de degré p , et $K_P[X]$ l'espace vectoriel des fractions rationnelles P -adiques de degré strictement négatif.

1. Montrer que la famille des fractions rationnelles $X^r P^n$, où $r \in [0, p - 1]$ et $n \in \mathbb{Z}$, constitue une base de l'espace vectoriel des fractions rationnelles P -adiques. Trouver une méthode de calcul explicite des composantes d'une fraction rationnelle P -adique dans cette base.

2. Prouver que la famille des fractions rationnelles $X^r P^n$, où $r \in [0, p - 1]$ et où n parcourt l'ensemble des entiers strictement négatifs, est une base de l'espace vectoriel $K_P[X]$.

44 A. Décomposition en éléments simples sur un corps quelconque.

On appelle éléments simples à coefficients dans K les éléments de $K(X)$ des types suivants :

a) les monômes X^p , où $p \in \mathbb{N}$;

b) les fractions rationnelles $\frac{X^r}{P^n}$, où P est un polynôme unitaire irréductible, n un

entier naturel non nul et r un entier naturel strictement inférieur au degré de P .

On note I l'ensemble des triplets (P, n, r) satisfaisant à la condition précédente.

1. Prouver que, les éléments simples constituent une base de l'espace vectoriel $K(X)$, autrement dit, que tout élément R de $K(X)$ peut s'écrire d'une manière et d'une seule sous la forme

$$R = \sum_{p=0}^{+\infty} \beta_p X^p + \sum_{(P,n,r) \in I} \alpha_{P,n,r} \frac{X^r}{P^n}.$$

Prouver en outre que

$$\sum_{p=0}^{+\infty} \beta_p X^p = \text{Pr}_\infty(R)$$

et que, pour tout polynôme unitaire irréductible P ,

$$\sum_{n,r} \alpha_{P,n,r} \frac{X^r}{P^n} = \text{Pr}_P(R).$$

2. *Application.* — Soit R un élément non constant de $K(X)$, décomposé en facteurs irréductibles :

$$R = \beta \prod_{P \in E} P^{v_P(R)}.$$

Écrire la décomposition en éléments simples de $\frac{R'}{R}$.

3. *Cas du corps des réels.* — Prouver que les éléments simples à coefficients dans \mathbf{R} sont les éléments de $\mathbf{R}(X)$ des types suivants :

- a) les monômes X^p , où $p \in \mathbf{N}$;
- b) les fractions rationnelles $\frac{1}{(X - \alpha)^n}$, où $\alpha \in \mathbf{R}$ et $n \in \mathbf{N}^*$ (éléments simples de première espèce);
- c) les fractions rationnelles $\frac{X}{(X^2 + \beta X + \gamma)^n}$ et $\frac{1}{(X^2 + \beta X + \gamma)^n}$, où $n \in \mathbf{N}^*$, $(\beta, \gamma) \in \mathbf{R}^2$, $\beta^2 - 4\gamma < 0$ (éléments simples de seconde espèce).

Exemples. — Décomposer en éléments simples les fractions rationnelles données dans la question 6 de l'exercice 42. (On pourra comparer la méthode utilisée dans cet exercice et celle qui consiste à décomposer ces fractions rationnelles en éléments simples dans $\mathbf{C}(X)$ et à regrouper les éléments simples conjugués.)

45. *Exemples de divisions suivant les puissances croissantes.*

On considère l'algèbre $\mathbf{R}[X]$. Soient α et β deux nombres réels; diviser suivant les puissances croissantes à l'ordre n

$$\begin{array}{ll} 1 & \text{par } 1 - 2X \cos \alpha + X^2 \\ \cos \beta - X \cos(\alpha - \beta) & \text{par } 1 - 2X \cos \alpha + X^2. \end{array}$$

46. *Exemples de décompositions en éléments simples (pôles simples).*

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{array}{lll} \frac{1}{X^3 + 1} & \frac{1}{X^4 - 1} & \frac{1}{X^5 + 1} \\ \frac{1}{(X^2 + 1)^2 + 1} & \frac{X^4 - 2X^2 + 1}{X(X + 1)(X^2 + 1)} & \frac{1}{(X^2 + 1)^2 - X^2}. \end{array}$$

47. *Exemples de décomposition en éléments simples (pôles doubles).*

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{array}{lll} \frac{X^6}{(X^5 + 1)^2} & \frac{4X^3}{(X^4 - 1)^2} & \frac{X^4 + 3X^3 + 1}{(X + 1)^2(X^2 + X + 1)} \\ \frac{X^6}{(X^2 + 1)^2(X + 1)^2} & \frac{9}{(X^3 + 1)^2} & \frac{1}{(1X - 1)(X^3 - 1)} \\ \frac{X^2 + 1}{X^2(X^3 - 1)} & \frac{X}{(X + 1)(X^2 + 1)^2} & \end{array}$$

48. Exemples de décompositions en éléments simples (pôles triples).

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{array}{ccc} \frac{1}{(X^3 - 1)^3} & \frac{X^3}{(X^3 - 1)^3} & \frac{1}{X(X^2 - 1)^3} \\ \frac{X^2 + 1}{X^2(X - 1)^3} & \frac{1}{X^2(X + 1)^3(X^2 + 1)} & \frac{X^2 + 2X + 5}{(X + 3)^3(X - 1)^3} \\ \frac{X^7}{(X^2 - 1)^3} & \frac{X^5 + 4X^4 + 7X^3 + 9X^2 + 5X + 3}{(X^2 + X + 1)(X + 1)^3} & \end{array}$$

49. Exemples divers de décomposition en éléments simples.

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{array}{ccc} \frac{X^4}{(X + 1)^5 - X^5} & \frac{7}{(X + 1)^7 - X^7 - 1} & \frac{1}{(X + i)^6 + (X - i)^6} \\ \frac{X^3 - X}{(X^4 + 1)(X^2 + 1)^4} & \frac{X^2 + 2X}{X^4 + X^2 + 1} & \frac{X^2 - 4}{X^4 + X^3 - X - 1} \end{array}$$

50. Exemples de décompositions en éléments simples (avec paramètres).

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{array}{ccc} \frac{1}{X^n(1 - X)^n}, \text{ où } n \in \mathbb{N}^* & \frac{X}{(X + 1)^n(X^2 + X + 1)}, \text{ où } n \in \mathbb{N} & \\ \frac{1}{X^n + 1}, \frac{1}{(X^n + 1)^2}, \frac{1}{(X^n + 1)^3}, \text{ où } n \in \mathbb{N}^* & & \\ \frac{X^m}{X^n + 1}, \text{ où } m \in \mathbb{N}, \text{ et } n \in \mathbb{N}^* & \frac{X^{2n}}{(X^2 + 1)^n}, \text{ où } n \in \mathbb{N}^* & \\ \frac{1}{(X - 1)(X^n - 1)}, \text{ où } n \in \mathbb{N}^* & \frac{X^5 - X + 1}{(X^2 + 1)^n}, \text{ où } n \in \mathbb{N}^*. & \end{array}$$

51 A. Calculs de sommes classiques.

Soient P et Q deux polynômes à coefficients complexes, où Q est non nul et a toutes ses racines simples, et où $\text{d}^\circ(P) \leq \text{d}^\circ(Q) - 2$.

1. Décomposer en éléments simples la fraction rationnelle $R = \frac{P}{Q}$.

2. On suppose de plus que toutes les racines de Q sont des nombres entiers rationnels négatifs. Pour tout entier n strictement positif, calculer la somme

$$S_n = \sum_{p=1}^n R(p).$$

3. Expliciter la valeur de S_n dans les cas suivants :

$$\begin{array}{l} R = \frac{1}{X(X + 1)(X + 3)} \quad R = \frac{X}{(X + 1)(X + 2)(X + 3)} \\ R = \frac{1}{X(X + 1)(X + 2) \dots (X + r)}, \text{ où } r \in \mathbb{N}^* \\ R = \frac{1}{X(X + 2)(X + 4) \dots (X + 2r)}, \text{ où } r \in \mathbb{N}^*. \end{array}$$

52. Soient P un polynôme unitaire de degré n à coefficients complexes ayant toutes ses racines distinctes, $\alpha_1, \alpha_2, \dots, \alpha_n$ ces racines, et Q un élément de $\mathbb{C}[X]$ de degré $n - 1$. Montrer que

$$\frac{Q(\alpha_1)}{P'(\alpha_1)} + \frac{Q(\alpha_2)}{P'(\alpha_2)} + \dots + \frac{Q(\alpha_n)}{P'(\alpha_n)} = \beta,$$

où β est le coefficient dominant de Q .

53. *Décompositions en éléments simples par changements d'indéterminée.*

Décomposer en éléments simples les fractions rationnelles à coefficients complexes suivantes :

$$\begin{aligned} & \frac{X^6}{(X^4 - 1)^2} && \text{(on pourra poser } T = X^2) \\ & \frac{X^6}{(X^2 + X - 1)^3(X^3 - 1)^3} && \left(\text{on pourra poser } T = X - \frac{1}{X} \right) \\ & \frac{X^n}{(X^2 + 1)^n - 2X^n} \quad \frac{X^{2n}}{[(X^2 + 1)^n - 2X^n]^2} \quad n \in \mathbb{N}^* && \left(\text{on pourra poser } T = X + \frac{1}{X} \right). \end{aligned}$$

- 54 A. *Développements eulériens.*

Toutes les fractions rationnelles intervenant dans cet exercice seront considérées comme des fractions rationnelles à coefficients complexes.

1. Soit n un entier strictement positif. Montrer qu'il existe un élément A de $\mathbb{C}[X]$ et un seul tel que

$$X^n + \frac{1}{X^n} = A \left(X + \frac{1}{X} \right).$$

Décomposer en éléments simples la fraction rationnelle $R = \frac{1}{A}$.

2. Soit n un entier strictement positif. Montrer qu'il existe un élément P de $\mathbb{C}[X]$ et un seul tel que, pour tout nombre réel t ,

$$\cos nt = P(\cos t).$$

Décomposer en éléments simples les fractions rationnelles $\frac{1}{P}$ et $\frac{1}{P^2}$. Pour tout nombre complexe α , décomposer en éléments simples la fraction rationnelle

$$\frac{1}{P(X) - P(\alpha)}.$$

3. Soit n un entier strictement positif.

— Montrer que si n est impair, il existe un élément P de $\mathbb{C}[X]$ et un seul tel que, pour tout nombre réel t ,

$$\sin nt = P(\sin t).$$

— Montrer que si n est pair, il existe un élément Q de $\mathbb{C}[X]$ et un seul tel que, pour tout nombre réel t ,

$$\sin nt = \sin t Q(\cos t).$$

Décomposer en éléments simples les fractions rationnelles $\frac{1}{P}$, $\frac{1}{P^2}$, $\frac{1}{Q}$ et $\frac{1}{Q^2}$.

Pour tout nombre complexe α , décomposer en éléments simples les fractions rationnelles

$$\frac{1}{P(X) - P(\alpha)} \quad \text{et} \quad \frac{1}{Q(X) - Q(\alpha)}.$$

4. Soit n un entier strictement positif. Montrer qu'il existe un élément R de $C(X)$ et un seul tel que, pour tout nombre réel t non de la forme $\frac{\pi}{2n} + \frac{k\pi}{n}$, où $k \in \mathbb{Z}$,

$$\operatorname{tg} nt = R(\operatorname{tg} t).$$

Décomposer en éléments simples les fractions rationnelles R , R^2 , $\frac{1}{R}$ et $\frac{1}{R^2}$.

Pour tout nombre complexe α substituable dans R , décomposer en éléments simples la fraction rationnelle

$$\frac{1}{R(X) - R(\alpha)}.$$

5. Reformuler et traiter à nouveau les questions 2, 3 et 4 en remplaçant les fonctions \cos , \sin et tg par les fonctions ch , sh et th .

Les formules obtenues en substituant à l'indéterminée X dans les décompositions en éléments simples précédentes les nombres réels $\cos t$, $\sin t$, $\operatorname{tg} t$, $\operatorname{ch} t$, $\operatorname{sh} t$, et $\operatorname{th} t$, s'appellent *développements eulériens* des fonctions $\frac{1}{\cos nt}$, $\frac{1}{\cos^2 nt}$, etc.

55. Soient p un entier naturel non nul et E_p le sous-espace vectoriel de $C(X)$ constitué des fractions rationnelles de degré inférieur ou égal à $-p$ et dont les pôles sont d'ordre inférieur ou égal à p . Montrer que les fractions rationnelles de la forme $\frac{1}{P}$, où P est un polynôme de degré p , engendrent l'espace vectoriel E_p .

56 A. *Opérations sur les développements limités.*

Soit α un élément de K . Pour tout entier rationnel p , on désigne par L_p le projecteur de $K(X)$ qui à toute fraction rationnelle associe son développement limité à l'ordre p au point α .

1. *Troncature.* — Soit (p, q) un couple d'entiers rationnels tel que $p \geq q$. Montrer que

$$L_q = L_q \circ L_p.$$

2. *Produit.* — Soient R et S deux éléments de $K(X)$, $r = v_\alpha(R)$ et $s = v_\alpha(S)$. Prouver que, pour tout entier rationnel n supérieur ou égal à $\sup(r, s)$,

$$L_n(RS) = L_n[L_{n-r}(R) \cdot L_{n-s}(S)].$$

3. *Puissance.* — Soient R un élément de $K(X)$, $r = v_\alpha(R)$, et m un entier strictement supérieur à 1. Prouver que, pour tout entier rationnel n supérieur ou égal à rm ,

$$L_n(R^m) = L_n([L_{n-r(m-1)}(R)]^m).$$

4. *Inverse.* — Soit R un élément de $K(X)$ tel que $v_\alpha(R) = 0$, écrit sous la forme $R = R(\alpha)(1 - H)$. Prouver que, pour tout entier naturel non nul n ,

$$L_n\left(\frac{1}{R}\right) = \frac{1}{R(\alpha)} \sum_0^n L_n(H^r).$$

5. *Composée.* — Dédurre des questions 3 et 4 une règle permettant d'obtenir le développement limité de la composée de deux fractions rationnelles.

6. *Dérivée.* — On suppose que le corps K est de caractéristique zéro. Soit R un élément de $K(X)$. Prouver que, pour tout entier naturel non nul n ,

$$L_{n-1}[D(R)] = D[L_n(R)].$$

57 A. Développements limités des fractions rationnelles relativement à un polynôme irréductible.

1. Soient P un polynôme unitaire irréductible à coefficients dans K , et p un entier rationnel. Prouver que, pour toute fraction rationnelle R , il existe un couple (S_p, T_p) de fractions rationnelles et un seul tel que

$$K = S_p + P^{p+1}T_p, \quad S_p \in K_{P,p}[X], \quad v_P(T_p) \geq 0,$$

où $K_{P,p}[X]$ désigne le sous-espace vectoriel de $K(X)$ constitué des fractions rationnelles P -adiques de degré strictement inférieur à $(p+1) \deg(P)$. La fraction rationnelle S_p ainsi définie s'appelle développement limité à l'ordre p de R relativement à P , et se note $\text{Pr}_{P,p}(R)$. Prouver que l'application $\text{Pr}_{P,p}$ est un projecteur de $K(X)$, dont l'image est le sous-espace vectoriel $K_{P,p}[X]$.

(Lorsque $p = -1$, on retrouve la notion de partie principale d'une fraction rationnelle relativement à P .)

2. A l'aide de l'exercice 42, donner une méthode de calcul explicite de S_p et T_p .

3. Étendre à ce cas les résultats de l'exercice 56, concernant les opérations sur les développements limités.

DÉRIVATION

58 A. Dérivations de $K[X]$ et de $K(X)$.

1. Montrer que, pour tout élément A de $K[X]$, il existe une dérivation U de l'algèbre $K[X]$ et une seule telle que $U(X) = A$. Prouver que $U = AD$.

2. Montrer de même que, pour tout élément B de $K(X)$, il existe une dérivation V de l'algèbre $K(X)$ et une seule telle que $V(X) = B$.

59 A. Formule de Leibniz généralisée.

Montrer que, pour tout entier $r > 0$ et pour toute suite (R_1, R_2, \dots, R_p) d'éléments de $K(X)$,

$$D^r(R_1 R_2 \dots R_p) = \sum_{r_1 + r_2 + \dots + r_p = r} \frac{r!}{r_1! r_2! \dots r_p!} D^{r_1}(R_1) D^{r_2}(R_2) \dots D^{r_p}(R_p).$$

60. Calculs de dérivées $n^{\text{ièmes}}$.

1. Soient α un nombre complexe, et p un entier strictement positif. Calculer la dérivée $n^{\text{ième}}$ de la fraction rationnelle

$$\frac{1}{X(X + \alpha)(X + 2\alpha) \dots (X + p\alpha)}.$$

2. Calculer les dérivées $n^{\text{ièmes}}$ des éléments suivants de $\mathbb{C}(X)$:

$$\frac{1}{X^2 - 1} \text{ et } \frac{1}{X^2 + 1},$$

et déterminer tous les zéros de ces dérivées $n^{\text{ièmes}}$.

3. Soit α un nombre réel. Calculer les dérivées $n^{\text{ièmes}}$ des éléments suivants de $\mathbb{C}(X)$:

$$\begin{array}{cc} \frac{1}{X^2 - 2X \cos \alpha + 1} & \frac{1}{X^2 - 2iX \sin \alpha - 1} \\ \frac{1}{X^2 - 2X \operatorname{ch} \alpha + 1} & \frac{1}{X^2 - 2X \operatorname{sh} \alpha - 1} \end{array},$$

et déterminer tous les zéros de ces dérivées $n^{\text{ièmes}}$.

4. Calculer les dérivées $n^{\text{ièmes}}$ des fractions rationnelles suivantes :

$$\frac{X^2 + 1}{(X + 1)^3} \quad \frac{3X + 2}{X^2 - 4} \quad \frac{X - 1}{X + 1}.$$

61 A. Soient K un corps de caractéristique zéro, n un entier naturel non nul, et E_n le sous-espace vectoriel de $K[X]$ constitué des polynômes de degré inférieur ou égal à n .

1. Soient A un élément de $K[X]$, et D l'endomorphisme de E_n qui à tout polynôme associe sa dérivée. Prouver que l'endomorphisme $P \mapsto A(D)(P)$ est un automorphisme de l'espace vectoriel E_n si et seulement si $A(0) \neq 0$. Montrer que, dans ces conditions, il existe un polynôme B de degré inférieur ou égal à n et un seul tel que AB soit congru à 1 modulo X^{n+1} dans $K[X]$, et que $B(D)$ est l'automorphisme réciproque de $A(D)$.

2. Applications.

a) Prouver que, pour tout élément α de K , l'application $P \mapsto P - \alpha D(P)$ est un automorphisme de l'espace vectoriel E_n , et déterminer l'automorphisme réciproque. En déduire que, pour tout élément Q de E_n , il existe un élément P de E_n et un seul tel que

$$P + \alpha D(P) + \alpha^2 D^2(P) + \dots + \alpha^n D^n(P) = Q.$$

Expliciter P lorsque $Q = X^p$, $p \in [0, n]$.

b) Prouver que, pour tout élément α de K , l'application

$$P \mapsto P + \alpha \frac{D(P)}{1!} + \alpha^2 \frac{D^2(P)}{2!} + \dots + \alpha^n \frac{D^n(P)}{n!}.$$

est un automorphisme de l'espace vectoriel E_n , et déterminer l'automorphisme réciproque.

62 A. *Équations différentielles linéaires à coefficients constants.*

Soient K un corps de caractéristique zéro, et A un élément de $K[X]$ de degré $n > 0$ tel que $A(0) \neq 0$. On note A^* le polynôme $X^n A\left(\frac{1}{X}\right)$.

1. Prouver que l'endomorphisme L de l'espace vectoriel $K[X]$ défini par les relations $L(X^p) = p! X^p$ pour tout entier naturel p , est un automorphisme de $K[X]$, dont on déterminera l'automorphisme réciproque.

2. Pour tout entier naturel p , on note δ_p l'endomorphisme de l'espace vectoriel $K[X]$ qui à tout polynôme P associe la valeur à l'origine de sa dérivée $p^{\text{ième}}$. Soit S l'endomorphisme de $K[X]$ défini par la relation $S(P) = XP$. Prouver que

$$SLD = L - \delta_0.$$

Prouver plus généralement que, pour tout entier naturel non nul p ,

$$S^p L D^p = L - \delta_0 - S\delta_1 - S^2\delta_2 - \dots - S^{p-1}\delta_{p-1}.$$

En déduire que, pour tout élément P de $K[X]$ et pour tout élément p de $[0, n]$, le degré de $X^n L(D^p P) - X^{n-p} L(P)$ est strictement inférieur à n , et qu'il en est de même du degré de $X^n L[A(D)(P)] - A^*(X) L(P)$.

3. Soit Q un élément de $K[X]$. Prouver que s'il existe un élément P de $K[X]$ satisfaisant à l'équation différentielle $A(D)(P) = Q$, $L(P)$ est nécessairement le quotient de la division euclidienne de $X^n L(Q)$ par $A^*(X)$. Réciproquement, soit U le quotient de cette division euclidienne; prouver que $L^{-1}(U)$ est solution de l'équation différentielle considérée.

4. Prouver que l'unique solution P de l'équation $A(D)(P) = Q$ satisfait aux relations $P(0) = DP(0) = \dots = D^{n-1}P(0) = 0$ si et seulement si $A^*(X)$ divise $L(Q)$.

5. Étudier de même l'équation différentielle $A(D)(P) = Q$ lorsque A est de la forme $X^r A'$, où $r > 0$ et $A'(0) \neq 0$.

6. *Applications.* — Résoudre les équations différentielles suivantes :

$$\begin{aligned}(D^2 + I)(P) &= X^r \quad r \in \mathbb{N} \\ (D^4 + D^2 + I)(P) &= X^2 + X + 1 \\ (D - I)^3(P) &= X^3.\end{aligned}$$

63. On suppose que la caractéristique de K est nulle.

I. — Soient n un entier naturel non nul, et E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n à coefficients dans K . Pour tout couple (α, β) d'entiers naturels, on considère l'application $U_{\alpha, \beta}$ qui à tout élément P de $K[X]$ associe le polynôme

$$X^2 P'' - (\alpha + \beta - 1) X P' + \alpha \beta P.$$

1. Montrer que $U_{\alpha, \beta}$ est un endomorphisme de l'espace vectoriel $K[X]$, qui laisse stable E_n .

2. Calculer $U_{\alpha, \beta}(X^p)$, où p parcourt \mathbb{N} .

3. Déterminer le noyau et l'image de $U_{\alpha, \beta}$, en discutant suivant les valeurs de α et β .

4. *Application.* — Déterminer tous les éléments P de $K[X]$ tels que

$$X^2 P'' - 2 X P' + 2 P = Q,$$

où Q est un élément donné de $K[X]$.

II. — Soient n un entier naturel non nul et Q un élément de $K[X]$ de degré n .

1. Prouver que l'application U qui à tout polynôme P associe le polynôme

$$U(P) = D^n(P)Q - D^{n-1}(P)D(Q) + \dots + (-1)^n P D^n(Q)$$

est un endomorphisme de $K[X]$.

2. Déterminer le noyau de $D \circ U$, et en déduire que le noyau de U est contenu dans le sous-espace vectoriel E_n de $K[X]$ constitué des polynômes de degré inférieur ou égal à n . Soit V la restriction de U à E_n . Déterminer l'image de V , et en déduire que le noyau de U est de dimension n .

3. On suppose que le polynôme Q est scindé, et écrit sous la forme

$$Q = \beta \prod_{j=1}^p (X - \alpha_j)^{n_j}.$$

Prouver que le noyau de U a pour base la famille des polynômes $(X - \alpha_j)^s$, où $j \in [1, p]$ et où, pour tout j , $n - n_j < s \leq n$.

4. Déterminer une base du noyau de U lorsque $K = \mathbb{R}$. (On pourra d'abord considérer Q comme un polynôme à coefficients complexes.)

64. Soient n un entier strictement positif, et E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n , à coefficients dans un corps K de caractéristique zéro. Soient enfin P, Q, R trois éléments de E_n , Q et R étant de degré n . Connaissant le développement de P dans la base $(Q, D(Q), D^2(Q), \dots, D^n(Q))$, et celui de Q dans la base

$$(R, D(R), D^2(R), \dots, D^n(R)),$$

expliciter le développement de P dans cette dernière base.

65 A. Interpolation et dualité.

Soit E_n l'espace vectoriel des polynômes de degré inférieur ou égal à n , $n \in \mathbb{N}$, à coefficients dans un corps K de caractéristique zéro.

1. Soit α un élément de K ; montrer que l'application qui à tout élément P de E_n associe le scalaire $P(\alpha)$ est une forme linéaire sur E_n , qu'on notera δ_α .

2. Soient $\alpha_0, \alpha_1, \dots, \alpha_n$ des scalaires distincts deux à deux. Montrer que les formes linéaires δ_{α_i} , où i parcourt $[0, n]$, constituent une base B^* du dual de E_n .

Prouver que les polynômes

$$P_i = \frac{\prod_{j \neq i} (X - \alpha_j)}{\prod_{j \neq i} (\alpha_i - \alpha_j)}, \quad \text{où } i \in [0, n],$$

forment une base de E_n , dont B^* est la base duale.

3. Montrer que, pour tout entier $p \in [0, n]$, et pour tout élément α de K , l'application $P \mapsto [D^p(P)](\alpha)$ est une forme linéaire sur E_n , qu'on notera $\delta_{\alpha, p}$. Prouver que, α étant fixé, les formes linéaires $\delta_{\alpha, p}$, où p parcourt $[0, n]$, forment une base B'^* du dual de E_n . Déterminer la base de E dont B'^* est la base duale.

4. Écrire le développement de $\delta_{\alpha, p}$ dans la base B^* ; on prouvera que

$$\delta_{\alpha, p} = \sum_{i=0}^n [D^p(P_i)](\alpha) \cdot \delta_{\alpha_i}.$$

66 A. Soit P un élément de $\mathbb{Z}[X]$, unitaire, de degré n et tel que $P(0) \neq 0$. On suppose que les racines $\alpha_1, \alpha_2, \dots, \alpha_n$ de P dans \mathbb{C} sont simples.

1. Décomposer en éléments simples sur \mathbb{C} la fraction rationnelle

$$R = \frac{1}{XP\left(\frac{1}{X}\right)}.$$

2. Prouver que

$$\sum_{i=1}^n \frac{\alpha_i^k}{P'(\alpha_i)} = 0 \quad \text{si } k \in [0, n-2]$$

$$\sum_{i=1}^n \frac{\alpha_i^{n-1}}{P'(\alpha_i)} = 1.$$

3. Soit $M = (\beta_{jk})$ l'élément de $\mathbf{M}_n(\mathbb{C})$ défini par les relations

$$\beta_{jk} = \sum_{i=1}^n \frac{\alpha_i^{j+k-2}}{P'(\alpha_i)}.$$

Prouver que M appartient à $\mathbf{M}_n(\mathbb{Z})$ et que M est inversible dans $\mathbf{M}_n(\mathbb{Z})$.

*4. Pour tout $i \in [1, n]$, on désigne par E_i l'ensemble des éléments z_i de \mathbb{C} qui sont de la forme

$$z_i = \sum_{k=1}^n y_k \frac{\alpha_i^{k-1}}{P'(\alpha_i)}, \quad \text{où } (y_1, y_2, \dots, y_n) \in \mathbb{Z}^n.$$

Prouver que, pour tout $i \in [1, n]$, $Z(\alpha_i)$ est contenu dans E_i , et que l'application $x \mapsto \frac{x}{P'(\alpha_i)}$ est une bijection de $Z[\alpha_i]$ sur E_i .

5. Appliquer les résultats précédents au cas où $P = X^2 + 1$.

67 A. Existence des primitives des fractions rationnelles, en caractéristique zéro.

Soit K un corps de caractéristique zéro.

I. — Cas où le corps K est algébriquement clos.

1. Soit R un élément de $K(X)$. Prouver que, pour tout pôle α de R , le résidu de $D(R)$ au point α est nul.

2. Réciproquement, soit S un élément de $K(X)$ dont tous les résidus sont nuls. Prouver que S admet une primitive dans $K(X)$.

On trouvera des exemples dans l'exercice 69.

II. — Cas général.

1. Soient P un polynôme unitaire irréductible, p son degré, R un élément de $K(X)$ et $n = v_P(R)$. Montrer que si n n'est pas nul,

$$v_P[D(R)] = v_P(R) - 1.$$

Si $n = 0$, prouver que $v_P[D(R)] \geq 0$.

2. Soient P un polynôme unitaire irréductible et S une fraction rationnelle P -adique, de la forme $S = \frac{Q}{P^m}$, où $Q \in K[X]$ et $m \geq 1$. Montrer que si S admet une primitive R dans $K(X)$, R est une fraction rationnelle P -adique, et que $v_P(R) = m - 1$.

En déduire que si $m = 1$, S n'admet pas de primitive, et que si $m > 1$, S admet une primitive si et seulement si S est de la forme $S = \alpha \frac{D(P)}{P^m}$, où $\alpha \in K$.

3. Soit S un élément de $K(X)$. En utilisant la décomposition de S en éléments simples (cf. exercice 44), établir une condition nécessaire et suffisante pour que S admette une primitive dans $K(X)$. Expliciter cette condition lorsque $K = \mathbf{R}$.

On notera que, pour que S admette une primitive, il est nécessaire que, pour tout élément P de E tel que $v_P(R) < 0$, $v_P(R)$ soit inférieur ou égal à -2 .

On trouvera un exemple dans l'exercice 68.

68 A. Primitives des fractions rationnelles de la forme $\frac{A}{B^2}$.

Soit K un corps de caractéristique zéro. On note E_q l'espace vectoriel des polynômes à coefficients dans K de degré inférieur ou égal à un entier q . On considère enfin un polynôme unitaire B à coefficients dans K , dont le degré est noté p .

1. On considère l'espace vectoriel G des polynômes A à coefficients dans K tels que la fraction rationnelle $\frac{A}{B^2}$ admette une primitive dans $K(X)$, et le sous-espace F de G constitué des éléments A de G tels que $d^0(A) < 2 d^0(B)$. Montrer que G est somme directe de F et de $K[X] \cdot B^2$.

2. Dans cette question, on suppose que pour tout polynôme irréductible P , $v_P(B) \leq 1$. Soit $B = P_1 P_2 \dots P_n$ la décomposition en facteurs irréductibles de B .

Montrer que si R est une primitive dans $K(X)$ de $\frac{A}{B^2}$, où A appartient à l'espace vectoriel F , R peut être mise sous la forme $R = \frac{C}{B}$, où C est un élément de $K[X]$ de degré inférieur ou égal à p .

Montrer que l'application U qui à tout élément Q de $K[X]$ associe $BQ' - B'Q$ est un endomorphisme de l'espace vectoriel $K[X]$, et déterminer son noyau. En déduire le rang de la restriction U_q de U au sous-espace vectoriel E_q . En conclure que U_{p-1} définit un isomorphisme de l'espace vectoriel E_{p-1} sur l'espace vectoriel F . La dimension de F est donc égale à $p = d^\circ(B)$. Expliciter une base de F .

3. On suppose seulement que le polynôme B n'est pas constant. Soit

$$B = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}$$

la décomposition en facteurs irréductibles de B . On désigne par B_0 le polynôme $P_1 P_2 \dots P_n$, et par B_1 le polynôme

$$B_1 = B_0 \sum_{i=1}^n (2\alpha_i - 1) \frac{P'_i}{P_i}.$$

Montrer que si R est une primitive dans $K(X)$ de $\frac{A}{B^2}$, où A appartient à l'espace vectoriel F , R peut être mise sous la forme $R = \frac{CB_0}{B^2}$, où C est un élément de $K[X]$ de degré inférieur ou égal à $2 d^\circ(B) - d^\circ(B_0)$.

Montrer que l'application V qui à tout élément Q de $K[X]$ associe le polynôme $B_0 Q' - B_1 Q$ est un endomorphisme de l'espace vectoriel $K[X]$, et déterminer son noyau. En déduire le rang de la restriction V_q de V au sous-espace vectoriel E_q . En conclure qu'en désignant par r l'entier $2 d^\circ(B) - d^\circ(B_0)$, V_{r-1} définit un isomorphisme de l'espace vectoriel E_{r-1} sur l'espace vectoriel F . La dimension de F est donc égale à r . Expliciter une base de F .

4. Expliciter le résultat précédent lorsque K est un corps algébriquement clos. Retrouver alors ce résultat en utilisant la décomposition en éléments simples sur K de $\frac{A}{B^2}$.

5. Expliciter une base de F lorsque $K = \mathbf{R}$.

69. Exemples de fractions rationnelles admettant des primitives.

Toutes les fractions rationnelles intervenant dans cet exercice seront considérées comme fractions rationnelles à coefficients complexes.

1. Soient α , λ et μ trois nombres complexes. Trouver une condition nécessaire et suffisante portant sur α , λ et μ pour que la fraction rationnelle

$$\frac{X^2 + \lambda X + \mu}{X^2(X + \alpha)^2}$$

admette une primitive dans $\mathbf{C}(X)$.

Même question pour la fraction rationnelle

$$\frac{X^2 + \lambda X + \mu}{(X^2 + \alpha^2)^2}.$$

2. Soient α , β , γ , δ quatre nombres complexes. Trouver une condition nécessaire et suffisante portant sur ces nombres pour que la fraction rationnelle

$$\frac{(X - \alpha)(X - \beta)}{(X - \gamma)^2(X - \delta)^2}$$

admette une primitive dans $\mathbf{C}(X)$.

Même question pour la fraction rationnelle

$$\frac{\alpha X + \beta}{(X - \gamma)^2(X - \delta)^2}$$

3. Soient α, β, γ trois nombres complexes. Trouver une condition nécessaire et suffisante portant sur ces nombres pour que la fraction rationnelle

$$\frac{X^5 + 3X^4 + \alpha X^3 + X^2 - 3X + \beta}{X^4 - 2X^3 + \gamma X^2 - 2X + 1}$$

admette une primitive dans $\mathbb{C}(X)$.

4. Soient α, β, γ trois nombres complexes. Trouver tous les triplets (λ, μ, ν) de nombres complexes tels que la fraction rationnelle

$$\left(\frac{\lambda}{X - \alpha} + \frac{\mu}{X - \beta} + \frac{\nu}{X - \gamma} \right)^2$$

admette une primitive dans $\mathbb{C}(X)$.

70 A. Soient P un polynôme à coefficients complexes de degré $n > 0$, dont les racines $\alpha_1, \alpha_2, \dots, \alpha_n$ sont distinctes, et R un élément de $\mathbb{C}(X)$ tel que, pour tout $i \in [1, n]$, $v_{\alpha_i}(R) = 0$.

1. Soit i un élément de $[1, n]$. Montrer qu'une condition nécessaire et suffisante pour que $\text{Res}_{\alpha_i} \left(\frac{R}{P^2} \right) = 0$ est que

$$R'(\alpha_i)P'(\alpha_i) = R(\alpha_i)P''(\alpha_i).$$

2. On suppose que $R = (X - \alpha)^p$, où $\alpha \in \mathbb{C}$ et $p \in \mathbb{N}$. Montrer que si tous les résidus de $\frac{R}{P^2}$ sont nuls, P satisfait nécessairement à l'équation différentielle

$$pP' = (X - \alpha)P''.$$

Déterminer tous les polynômes P ayant toutes leurs racines simples et différentes de α tels que $\frac{(X - \alpha)^p}{P^2}$ admette une primitive dans $\mathbb{C}(X)$.

3. On suppose que $R = (X^2 + \alpha X + \beta)^n$, où α et β sont deux nombres complexes tels que $\alpha^2 - 4\beta \neq 0$. Montrer que si tous les résidus de $\frac{R}{P^2}$ sont nuls, P satisfait nécessairement à l'équation différentielle

$$(X^2 + \alpha X + \beta)P'' - n(2X + \alpha)P' + n(n + 1)P = 0.$$

Réciproquement, prouver qu'il existe un polynôme unitaire P de degré n et un seul satisfaisant à cette équation différentielle, que les racines de P sont simples et distinctes des racines de R , et que les résidus de $\frac{R}{P^2}$ sont nuls.

***71 B.** Soit A un polynôme unitaire à coefficients complexes. On se propose d'étudier les valeurs propres et les vecteurs propres de l'endomorphisme $U : R \mapsto AR''$ de l'espace vectoriel $\mathbb{C}(X)$.

1. Soit R un élément non nul de $\mathbb{C}(X)$. Déterminer les pôles de $\frac{D(R)}{R}$ et de $\frac{D^2(R)}{R}$ avec leurs multiplicités, et calculer les parties principales relatives à ces pôles (On pourra introduire l'ensemble des racines simples de R qui sont racines de $D^2(R)$).

2. Déterminer les valeurs propres et les vecteurs propres de U lorsque $A = (X - \alpha)^n$, $\alpha \in \mathbb{C}$, $n \in \mathbb{N}^*$. On écartera ce cas dans la suite.

3. Déterminer les valeurs propres et les vecteurs propres de U lorsque $A = (X - \alpha)(X - \beta)$, où α et β sont deux nombres complexes distincts. (On pourra se ramener au cas où $\alpha = 0$ et $\beta = 1$.)

4. Examiner le cas où A a au moins une racine de multiplicité strictement supérieure à 2.

5. Examiner le cas où toutes les racines de A sont simples.

6. On suppose que A a une racine double α , toutes ses autres racines étant simples.

Prouver que tout vecteur propre R de U peut s'écrire sous la forme $R = \frac{P}{(X - \alpha)^n}$, où $n \in \mathbb{N}^*$, $P \in \mathbb{C}[X]$, le degré de P étant égal à n ou $n + 1$.

Déterminer les valeurs propres et les vecteurs propres de U lorsque

$$A = (X - \alpha)^2(X - \beta), \quad \text{où } \alpha \neq \beta.$$

72 B. Formes différentielles rationnelles.

Dans cet exercice, on utilise quelques notions relatives à la théorie des polynômes à deux indéterminées.

1. Soit R un élément de $K(X)$, où K est un corps de caractéristique nulle. Prouver qu'il existe un élément S de $K(X)$ et un seul tel que $R(X + Y)$ puisse s'écrire sous la forme

$$R(X + Y) = R(X) + S(X)Y + R_1(X, Y)Y^2,$$

où S appartient à $K(X)$, où R_1 appartient à $K(X, Y)$ et où $(X, 0)$ est substituable dans R_1 , et montrer que $S = R'$. La fraction rationnelle à deux indéterminées $R'(X)Y$ s'appelle *différentielle* de R , et se note dR , ou encore $dR(X, Y)$.

Montrer que l'application $R \mapsto dR$ est une application linéaire de $K(X)$ dans $K(X, Y)$, et que, pour tout couple (R_1, R_2) d'éléments de $K(X)$,

$$d(R_1 R_2) = (dR_1)R_2 + R_1(dR_2).$$

Soit F un élément non constant de $K(X)$. Montrer que, pour tout élément R de $K(X)$,

$$d(R \circ F) = dR(F, dF) = (R' \circ F)dF.$$

2. On appelle *forme différentielle rationnelle* à une indéterminée tout élément ω de $K(X, Y)$ de la forme $\omega = S(X)Y$. L'ensemble $\Omega(X)$ des formes différentielles rationnelles à une indéterminée est un sous-espace vectoriel de $K(X, Y)$, et le produit d'un élément ω de $\Omega(X)$ par un élément T de $K(X)$ est encore un élément de $\Omega(X)$. La différentielle dR d'un élément R de $K(X)$ est un élément de $\Omega(X)$. Ainsi, tout élément ω de $\Omega(X)$ peut s'écrire d'une manière et d'une seule sous la forme $\omega = S(X)dX$, où $S \in K(X)$.

Soit maintenant F un élément non constant de $K(X)$. On appelle image réciproque par F d'un élément ω de $\Omega(X)$ l'élément, noté $F^*(\omega)$, de $\Omega(X)$, défini par la relation

$$F^*(\omega)(X, Y) = \omega(F, dF).$$

Prouver que si $\omega = S(X)dX$, alors $F^*(\omega) = (S \circ F)dF$. Prouver que l'application $\omega \mapsto F^*(\omega)$ est linéaire, et que, pour tout élément T de $K(X)$ et pour tout élément ω de $\Omega(X)$,

$$F^*(T\omega) = (T \circ F)F^*(\omega).$$

Prouver que, pour tout élément R de $K(X)$,

$$F^*(dR) = d(R \circ F).$$

Soit enfin G un élément non constant de $K(X)$. Montrer que, pour tout élément ω de $\Omega(X)$,

$$(F \circ G)^*(\omega) = G^*[F^*(\omega)].$$

3. On dit qu'une forme différentielle ω est paire (resp. impaire) si

$$F^*(\omega) = \omega \quad (\text{resp. } F^*(\omega) = -\omega), \quad \text{où } F(X) = -X.$$

Montrer que ω est paire (resp. impaire) si et seulement s'il existe un élément R de $K(X)$ tel que $\omega = R(X^2)XdX$ (resp. $\omega = R(X^2)dX$). (On pourra d'abord démontrer que toute fraction rationnelle S peut s'écrire sous la forme

$$S = U(X^2) + XV(X^2), \quad \text{où } U, V \in K(X).)$$

4. On dit qu'une forme différentielle ω est réciproque de première espèce (resp. de deuxième espèce) si $F^*(\omega) = \omega$, où $F(X) = \frac{1}{X}$ (resp. $F(X) = -\frac{1}{X}$). Prouver que ω est réciproque de première espèce (resp. de deuxième espèce) si et seulement s'il existe un élément R de $K(X)$ tel que

$$\omega = \left(X - \frac{1}{X}\right)R\left(X + \frac{1}{X}\right)\frac{dX}{X} \quad \left(\text{resp. } \omega = \left(X + \frac{1}{X}\right)R\left(X - \frac{1}{X}\right)\frac{dX}{X}\right).$$

(Pour étudier le premier cas, on pourra écrire ω sous la forme $S\frac{dX}{X}$, et démontrer que S peut s'écrire sous la forme $S = U\left(X + \frac{1}{X}\right) + XV\left(X + \frac{1}{X}\right)$. On en déduira que ω peut s'écrire sous la forme

$$\omega = \left[U_1\left(X + \frac{1}{X}\right) + \left(X - \frac{1}{X}\right)U_2\left(X + \frac{1}{X}\right)\right]\frac{dX}{X}.$$

Le deuxième cas se traite de manière analogue.)

73 B. Résidus d'une forme différentielle rationnelle.

On conserve les notations de l'exercice précédent.

Soit K un corps de caractéristique nulle. On appelle zéros, pôles et résidus d'une forme différentielle rationnelle $\omega = S(X)dX$ les zéros, pôles et résidus de S .

1. Soient F un élément non constant de $K(X)$, S un élément de $K(X)$ et β un élément de K substituable dans S . Prouver que β est un zéro (resp. un pôle) de $S \circ F$ si et seulement si $\alpha = F(\beta)$ est un zéro (resp. un pôle) de S . On désigne par m_β l'ordre de multiplicité de la racine β de la fraction rationnelle $F(X) - F(\beta)$. Prouver que

$$v_\beta(S \circ F) = m_\beta v_\alpha(S).$$

En déduire que si α n'est pas un pôle de S , $\text{Res}_\beta F^*(\omega) = 0$. Prouver que si $S = \frac{1}{(X - \alpha)^p}$,

où $p > 1$, $\text{Res}_\beta F^*(\omega) = 0$ (cf. exercice 67), et que si $S = \frac{1}{X - \alpha}$, $\text{Res}_\beta F^*(\omega) = m_\beta$.

Déduire de ce qui précède que, pour tout élément ω de $\Omega(X)$,

$$\text{Res}_\beta F^*(\omega) = m_\beta \text{Res}_{F(\beta)} \omega.$$

2. On suppose maintenant que F est de la forme $\frac{\gamma X + \delta}{\gamma' X + \delta'}$, où $\gamma\delta' - \gamma'\delta \neq 0$. Montrer que si β est un élément de K tel que $\gamma'\beta + \delta' \neq 0$, alors, pour tout élément ω de $\Omega(X)$,

$$(1) \quad \text{Res}_\beta F^*(\omega) = \text{Res}_{F(\beta)} \omega.$$

Soit en particulier $F(X) = \frac{1}{X}$. Prouver que, pour tout élément ω de $\Omega(X)$,

$$(2) \quad \text{Res}_0 F^*(\omega) = \text{Res}_\infty \omega.$$

En conclure que la formule (1) reste valable lorsque β n'est pas substituable dans F , en convenant alors que $F(\beta) = \infty$. (On pourra introduire une fraction rationnelle homographique G telle que $G(0) = \beta$, et appliquer la formule (2) à $(F \circ G)^*(\omega)$.)

Prouver de même que la formule (1) reste valable lorsque $\beta = \infty$.

SÉRIES ENTIÈRES FORMELLES

74 A. Caractérisation des fractions rationnelles.

Dans cet exercice, on utilise la théorie des déterminants.

Soit $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ un élément non nul de $K[[X]]$.

1. On suppose qu'il existe deux éléments P et Q de $K[X]$, $Q \neq 0$, tels que $A = \frac{P}{Q}$.

Soient p et q les degrés respectifs de P et Q . Montrer que si $Q = \sum_{j=0}^q \lambda_j X^j$, alors, pour tout entier naturel $n \geq p - q$,

$$(1) \quad \lambda_0 \alpha_n + \lambda_1 \alpha_{n+1} + \dots + \lambda_q \alpha_{n+q} = 0.$$

Réciproquement, prouver que s'il existe une suite $(\lambda_0, \lambda_1, \dots, \lambda_q)$ de scalaires, où $\lambda_q \neq 0$, satisfaisant à la condition (1), A peut se mettre sous la forme $\frac{P}{Q}$, où $\text{d}^\circ(Q) = q$ et $\text{d}^\circ(P) \leq n + q$.

2. Soient n et k deux entiers naturels, et (α_n) une suite d'éléments de K . On appelle *déterminant de Hankel* de type (n, k) le déterminant de la matrice $H_{n,k} = (\beta_{ij})$ définie par la relation

$$H_{n,k} = \begin{pmatrix} \alpha_n & \alpha_{n+1} & \dots & \alpha_{n+k} \\ \alpha_{n+1} & \alpha_{n+2} & \dots & \alpha_{n+k+1} \\ \dots & \dots & \dots & \dots \\ \alpha_{n+k} & \alpha_{n+k+1} & \dots & \alpha_{n+2k} \end{pmatrix}.$$

Prouver que, sous les hypothèses de la question 1, $\text{Det } H_{n,k} = 0$ pour tout couple (n, k) d'entiers naturels tel que $n \geq p - q$ et $k \geq q$.

3. Soient n et k deux entiers naturels, $k > 0$, tels que le cofacteur de $\beta_{1,q+1}$ ne soit pas nul et que le cofacteur de β_{11} soit nul. Prouver que $\text{Det } H_{n,k} \neq 0$. (On pourra démontrer que, dans ces conditions, les k derniers vecteurs colonnes a_2, a_3, \dots, a_{k+1} de $H_{n,k}$ sont linéairement indépendants, en considérant le cofacteur de $\beta_{q+1,1}$. On montrera d'autre part qu'il existe une suite $(\mu_2, \mu_3, \dots, \mu_k)$ d'éléments de K telle que toutes les composantes du vecteur $b = a_{k+1} - \sum_{j=2}^k \mu_j a_j$ d'indice supérieur ou égal à 2 soient nulles. On prouvera que b n'est pas nul, et on en déduira que $\text{Det } H_{n,k} \neq 0$.)

4. On suppose qu'il existe deux entiers naturels n et k , $k \neq 0$, tels que, pour tout entier naturel j , $\text{Det } H_{n+j,k} = 0$.

A l'aide de la question précédente, montrer que s'il existe un entier $i \geq 1$ tel que $\text{Det } H_{n+i,k-1} \neq 0$, alors, pour tout entier $j \geq 1$, $\text{Det } H_{n+j,k-1} \neq 0$.

En déduire que si la suite (α_n) n'est pas à support fini, il existe un entier naturel m et un entier naturel non nul k tels que, pour tout entier naturel j , $\text{Det } H_{m+j,k} = 0$ et que, pour tout entier $j \geq 1$, $\text{Det } H_{m+j,k-1} \neq 0$.

Soit alors $(\lambda_0, \lambda_1, \dots, \lambda_q)$ une relation linéaire non triviale entre les vecteurs colonnes de la matrice $H_{m,k}$. Prouver que, pour tout entier naturel j , $(\lambda_0, \lambda_1, \dots, \lambda_q)$ est une relation linéaire entre les vecteurs colonnes de la matrice $H_{m+j,k}$.

Prouver finalement que A est une fraction rationnelle. On obtient ainsi le résultat suivant :

Pour qu'une série entière formelle $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ soit une fraction rationnelle, il faut et il suffit qu'il existe deux entiers naturels n et k tels que, pour tout entier naturel j ,

$$\text{Det } H_{n+j,k} = 0.$$

En particulier, prouver que, pour tout élément P de $K[X]$, $\sum_{n=0}^{+\infty} P(n) X^n$ est une fraction rationnelle.

5. *Application.* — Soient p un entier naturel non nul et $(\alpha_0, \alpha_1, \dots, \alpha_{2p-1})$ une suite de nombres complexes.

On suppose d'abord qu'il existe deux suites $(\beta_1, \beta_2, \dots, \beta_p)$ et $(\lambda_1, \lambda_2, \dots, \lambda_p)$ de nombres complexes non nuls, les nombres $\lambda_1, \lambda_2, \dots, \lambda_p$ étant distincts deux à deux, telles que, pour tout entier $j \in [0, 2p - 1]$,

$$(1) \quad \sum_{k=1}^p \beta_k \lambda_k^j = \alpha_j.$$

Pour tout entier naturel $j \geq 2p$, on définit α_j par la formule (1). Calculer la série entière formelle $\sum_{n=0}^{+\infty} \alpha_n X^n$; prouver que c'est une fraction rationnelle de la forme $\frac{P}{Q}$, où Q a p pôles simples différents de 0, et $d^\circ(P) < d^\circ(Q)$.

Réciproquement, soit (α_n) une suite de nombres complexes telle que $\sum_{n=0}^{+\infty} \alpha_n X^n$ soit une fraction rationnelle satisfaisant aux conditions précédentes. Montrer qu'il existe un couple $((\beta_1, \beta_2, \dots, \beta_p), (\lambda_1, \lambda_2, \dots, \lambda_p))$ et un seul de suites de nombres complexes satisfaisant aux conditions (1) pour tout élément j de $[0, 2p - 1]$.

La résolution du système (1) se ramène ainsi à la détermination d'une suite $(\alpha_n)_{n \geq 2p}$ de nombres complexes telle que $\sum_{n=0}^{+\infty} \alpha_n X^n$ soit une fraction rationnelle satisfaisant aux conditions précitées. A cet effet, on peut utiliser les déterminants de Hankel.

Exemple. — Étudier le cas où $p = 2$ et où $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = 3$, $\alpha_3 = 7$. Étudier aussi le cas où $p = 2$ et où $\alpha_0 = \alpha_1 = \alpha_2 = 1$, $\alpha_3 = 2$.

75 A. Dérivations de $K[[X]]$ et de $K((X))$.

1. Soient A un élément de $K[[X]]$ et D la dérivation canonique de $K[[X]]$. Montrer qu'il existe une dérivation D_1 de $K[[X]]$ et une seule telle que $D_1(X) = A$. Prouver que $D_1 = AD$. (On prouvera d'abord que, pour tout élément B de $K[[X]]$, $v_0(D(B)) \geq v_0(B) - 1$.)

2. Déterminer de même toutes les dérivations D_1 de $K((X))$ satisfaisant à la condition suivante : Pour toute suite (A_n) de séries entières formelles généralisées telle que $v_0(A_n)$ tende vers $+\infty$ lorsque n tend vers $+\infty$, $v_0(D_1(A_n))$ tend vers $+\infty$.

76. Pour tout nombre complexe γ et pour tout entier naturel non nul n , on pose

$$C_n^\gamma = \frac{\gamma(\gamma-1)\dots(\gamma-n+1)}{n!}.$$

De plus, on convient que $C_0^\gamma = 1$.

1. Soient α et β deux nombres complexes. En utilisant la relation

$$(1) \quad (1+X)^\alpha(1+X)^\beta = (1+X)^{\alpha+\beta}.$$

montrer que, pour tout entier naturel n ,

$$(2) \quad C_n^{\alpha+\beta} = \sum_{p+q=n} C_p^\alpha C_q^\beta.$$

2. On se propose de donner une démonstration directe de la formule (2) et, par suite, de la formule (1). La formule (1) étant valable lorsque α et β sont des entiers naturels, il en est de même de la formule (2). En déduire que la formule (2) est valable lorsque α et β sont des nombres complexes.

77. Partitions d'un entier.

Soient p un entier strictement supérieur à 1 et $s = (s_1, s_2, \dots, s_p)$ une suite strictement croissante d'entiers naturels non nuls. Pour tout entier naturel n , on note $P_s(n)$ le

nombre des suites (n_1, n_2, \dots, n_p) d'entiers naturels telles que $\sum_{j=1}^p s_j n_j = n$. Prouver que

$$\sum_{n=0}^{+\infty} P_s(n) X^n = \prod_{j=1}^p \frac{1}{1 - X^{s_j}}.$$

En déduire une méthode de calcul de $P_s(n)$.

Expliciter les calculs dans les cas particuliers suivants : $p = 2$; $p = 3$ et $s = (1, 2, 4)$; $p = 3$ et $s = (1, 2, 5)$.

78. Problème des rencontres.

Soient n un entier naturel non nul et, pour tout élément k de $[0, n]$, $A_{n,k}$ le nombre des permutations de $[1, n]$ laissant fixes k éléments de $[1, n]$. On convient de poser $A_{0,0} = 1$.

1. Prouver que, pour tout entier naturel n , $\sum_{k=0}^n A_{n,k} = n!$ et que, pour tout élément k de $[1, n]$, $A_{n,k} = C_n^k A_{n-k,0}$.

2. On considère la série entière formelle $A = \sum_{n=0}^{+\infty} A_{n,0} \frac{X^n}{n!}$. Prouver que

$$A \exp X = \frac{1}{1-X}.$$

En déduire la valeur de $A_{n,0}$ et, plus généralement, de $A_{n,k}$.

79. Partitions généralisées.

Soient p un entier naturel non nul, $s = (s_1, s_2, \dots, s_p)$ une suite strictement croissante d'entiers naturels non nuls, et I l'ensemble $\{0, s_1, s_2, \dots, s_p\}$. Pour tout entier naturel non nul n , on note Q_n le nombre d'applications φ de $[1, n]$ dans I telles

que $\sum_{j=1}^n \varphi(j) = n$. Prouver que

$$\sum_{n=0}^{+\infty} Q_n X^n = \frac{1}{1 - X^{s_1} - X^{s_2} - \dots - X^{s_p}}.$$

80. Racines $n^{\text{ièmes}}$ d'une série entière formelle.

Soient K un corps de caractéristique 0 et n un entier strictement supérieur à 1.

1. Soit E_n l'ensemble des éléments A de $K[[X]]$ satisfaisant à la condition suivante : il existe un élément B de $K[[X]]$ tel que $B^n = A$. Montrer que E_n est stable par multiplication et que, pour tout élément A de E_n inversible dans $K[[X]]$, A^{-1} appartient à E_n . Prouver que \mathbb{I} est contenu dans E_n .

2. En déduire qu'un élément non nul $A = \sum_{q=0}^{+\infty} \alpha_q X^q$ de $K[[X]]$ appartient à E_n si et seulement s'il satisfait à la condition suivante : la valuation p de A est un multiple de n , et il existe un scalaire β tel que $\beta^n = \alpha_p$.

Déterminer alors tous les éléments B de $K[[X]]$ tels que $B^n = A$, à l'aide des racines $n^{\text{ièmes}}$ de l'unité dans K .

3. Soit $B = \sum_{q=1}^{+\infty} \beta_q X^q$ une série entière formelle de valuation 1, où β_1 est de la forme β^n , $\beta \in K$. Montrer que l'application $A \mapsto B \circ A$ est une bijection de E_n sur lui-même.

4. Étudier les cas particuliers où $K = \mathbf{R}$ et $K = \mathbf{C}$.

81. Étude du cosinus hyperbolique formel.

On conserve les notations de l'exercice précédent.

1. Soit F_2 l'ensemble des éléments U de $\mathbf{C}[[X]]$ de la forme $U = 1 + N^2$, où $N \in \mathfrak{M}$. Prouver que l'application $A \mapsto \operatorname{ch} A$ est une surjection de \mathfrak{M} sur F_2 .

2. On suppose que $K = \mathbf{R}$; on note \mathfrak{M}_+ l'ensemble des éléments A de \mathfrak{M} dont le premier coefficient non nul est strictement positif. Prouver que l'application $A \mapsto \operatorname{ch} A$ est une bijection de \mathfrak{M}_+ sur F_2 .

82. Séries entières formelles trigonométriques réciproques.

1. Prouver que

$$\operatorname{Arg} \operatorname{sh} X = \operatorname{Log} [X + (1 + X^2)^{\frac{1}{2}}]$$

et que

$$\operatorname{Arg} \operatorname{th} X = \frac{1}{2} \operatorname{Log} \frac{1+X}{1-X}.$$

(Dans chaque cas, on pourra calculer les dérivées des deux membres.)

2. En déduire que

$$\operatorname{Arc} \sin X = -i \operatorname{Log} [iX + (1 - X^2)^{\frac{1}{2}}]$$

et que

$$\operatorname{Arc} \operatorname{tg} X = -\frac{i}{2} \operatorname{Log} \frac{1 + iX}{1 - iX}.$$

83 A. Équations récurrentes.

Soient K un corps algébriquement clos, $(\alpha_0, \alpha_1, \dots, \alpha_p)$ une suite non nulle d'éléments de K , $\alpha_p \neq 0$, et $\beta = (\beta_0, \beta_1, \dots, \beta_{p-1})$ une suite d'éléments de K . Soit $A(\mathbb{N})$ l'algèbre de convolution du monoïde \mathbb{N} .

1. Prouver qu'il existe une application f_β et une seule de \mathbb{N} dans K telle que, pour tout entier naturel n ,

$$(1) \quad \sum_{j=0}^p \alpha_j f_\beta(n+j) = 0$$

et que, pour tout entier $n \in [0, p-1]$, $f_\beta(n) = \beta_n$. Montrer que l'application $\beta \mapsto f_\beta$ est un isomorphisme de l'espace vectoriel K^p sur le sous-espace vectoriel de $A(\mathbb{N})$ constitué des applications f satisfaisant pour tout entier naturel n à la relation (1).

2. Soient g l'application de \mathbb{N} dans K définie par les formules

$$\begin{aligned} g(n) &= \alpha_{p-n} & \text{si } n \in [0, p] \\ g(n) &= 0 & \text{si } n > p, \end{aligned}$$

et h l'application de \mathbb{N} dans K définie par les formules

$$\begin{aligned} h(n) &= \sum_{k=0}^n \alpha_{p-k} \beta_{n-k} & \text{si } n \in [0, p-1] \\ h(n) &= 0 & \text{si } n \geq p. \end{aligned}$$

Montrer que f_β est la seule fonction satisfaisant à la relation $g * f_\beta = h$. En déduire que

$$(2) \quad \sum_{n=0}^{+\infty} f_\beta(n) X^n = \frac{\sum_{n=0}^{p-1} \left(\sum_{k=0}^n \alpha_{p-k} \beta_{n-k} \right) X^n}{\sum_{n=0}^p \alpha_{p-n} X^n}.$$

Lorsque $\beta_1, \beta_2, \dots, \beta_{p-1}$ sont fixés, on obtient f_β en décomposant en éléments simples la fraction rationnelle (2).

3. Applications. — Résoudre les équations récurrentes suivantes :

$$\begin{aligned} u_{n+2} &= 3u_{n+1} - 2u_n & u_0 &= 0 & u_1 &= 1 \\ u_{n+2} &= 4u_{n+1} - 4u_n & u_0 &= 1 & u_1 &= 1 \\ u_{n+5} &= u_{n+4} + 2u_{n+3} - 2u_{n+2} - u_{n+1} + u_n & u_0 &= u_1 = u_2 = u_3 = 0, & u_4 &= 1. \end{aligned}$$

4. Montrer qu'il existe un élément ε de K^p et un seul tel que $g * f_\varepsilon = \delta$, où δ désigne l'élément neutre de l'algèbre de convolution $A(\mathbb{N})$.

En déduire que, pour tout élément b de $A(\mathbb{N})$, il existe un élément f_b de $A(\mathbb{N})$ et un seul tel que $f_b * g = b$, et que $f_b = f_\varepsilon * b$.

Prouver finalement que, pour tout élément b de $A(\mathbb{N})$ et pour tout élément β de K^p , il existe un élément $f_{b,\beta}$ de $A(\mathbb{N})$ et un seul satisfaisant à la relation

$$(3) \quad \sum_{j=0}^p \alpha_j f_b(n+j) = b(n)$$

et tel que, pour tout élément j de $[0, p-1]$, $f_{b,\beta}(j) = \beta_j$.

5. *Application.* — Résoudre les équations récurrentes suivantes :

$$\begin{aligned} u_{n+2} - 3u_{n+1} + 2u_n &= n & u_0 &= 1 & u_1 &= 0 \\ u_{n+2} - 4u_{n+1} + 4u_n &= \frac{n}{2^n} & u_0 &= 1 & u_1 &= 1. \end{aligned}$$

Nous verrons au § 5.8 une autre méthode de résolution des équations récurrentes, utilisant l'opérateur de Hilbert.

84 B. Séries de Dirichlet formelles.

1. Soit E l'espace vectoriel des applications de \mathbb{N}^* dans \mathbb{C} . On considère l'application qui à tout couple (f, g) d'éléments de E associe l'élément $h = f * g$ défini par la relation

$$h(n) = \sum_{pq=n} f(p)g(q) = \sum_{p|n} f(p)g\left(\frac{n}{p}\right).$$

Montrer que cette application est bilinéaire, et qu'elle définit sur E une structure de \mathbb{C} -algèbre commutative unitaire, l'élément neutre étant $\delta = \delta_{1n}$.

2. Pour tout entier naturel non nul p , on note e_p l'élément de E défini par la relation $e_p(n) = \delta_{np}$. Montrer que, pour tout couple (m, n) d'entiers naturels non nuls,

$$e_m * e_n = e_{mn}.$$

Prouver que le sous-espace vectoriel E_0 de E engendré par les éléments e_p , où p parcourt \mathbb{N}^* , est une sous-algèbre associative unitaire de E dont $(e_p)_{p \in \mathbb{N}^*}$ est une base, dite canonique.

3. Pour tout entier naturel $n \geq 1$, on note n^X l'élément e_n , l'élément unité de E étant alors noté 1. Tout élément f de E_0 s'écrit d'une manière et d'une seule sous la forme

$$f = \sum_{n=1}^{+\infty} \alpha_n n^X,$$

où $(\alpha_n)_{n \in \mathbb{N}^*}$ est une suite de nombres complexes à support fini. De plus, pour tout entier naturel non nul n , $\alpha_n = f(n)$. Les éléments de E_0 s'appellent polynômes de Dirichlet, et E_0 se note $\text{Dir}[X]$.

Montrer que, pour tout nombre complexe s , il existe un morphisme χ_s et un seul de l'algèbre unitaire $\text{Dir}[X]$ dans \mathbb{C} tel que, pour tout entier naturel non nul n , $\chi_s(n^X) = n^{-s}$,

et que, pour tout élément $f = \sum_{n=1}^{+\infty} \alpha_n X^n$ de $\text{Dir}[X]$,

$$\chi_s(f) = \sum_{n=1}^{+\infty} \alpha_n n^{-s}.$$

Pour tout élément f de $\text{Dir}[X]$, la fonction \hat{f} définie sur \mathbb{C} par la formule $\hat{f}(s) = \sum_{n=1}^{+\infty} \alpha_n n^{-s}$

s'appelle transformée de Dirichlet-Laplace de f . Montrer que l'application $f \mapsto \hat{f}$ est un morphisme de l'algèbre $\text{Dir}[X]$ sur une sous-algèbre unitaire de l'algèbre unitaire $\mathcal{F}(\mathbb{C}, \mathbb{C})$. Prouver que ce morphisme est injectif. (On pourra montrer que les fonctions $s \mapsto a^s$, où a parcourt \mathbb{R}_+^* , sont linéairement indépendantes dans $\mathcal{F}(\mathbb{C}, \mathbb{C})$.)

4. On appelle valuation d'un élément f de E , et on note $v_0(f)$, le plus petit des entiers naturels non nuls n tels que $f(n) \neq 0$ si $f \neq 0$; on convient que $v_0(0) = +\infty$. Détailler les propriétés des valuations, et prouver que, pour tout entier naturel non nul r , l'ensemble E_r des éléments de E de valuation supérieure ou égale à r est un idéal de E , et

que $\bigcap_{r=1}^{+\infty} E_r = \{0\}$. En déduire que l'algèbre E est associative et intègre.

5. On dit qu'une famille $(f_i)_{i \in I}$ d'éléments de E est sommable si, pour tout entier naturel non nul n , l'ensemble des éléments i de I tels que $v_0(f_i) \leq n$ est fini. L'élément f défini par la formule

$$f(n) = \sum_{i \in I} f_i(n)$$

s'appelle alors somme de la famille $(f_i)_{i \in I}$ et se note $\sum_{i \in I} f_i$.

Prouver que, pour tout élément f de E , la famille $(f(n)n^X)_{n \in \mathbb{N}^*}$ est sommable, et que $f = \sum_{n=1}^{+\infty} f(n)n^X$. C'est pourquoi E s'appelle algèbre des séries de Dirichlet formelles, et se note $\text{Dir}[[X]]$.

Étudier les propriétés des familles sommables (somme par paquets, distributivité, etc.).

6. Prouver enfin qu'un élément $f = \sum_{n=1}^{+\infty} \alpha_n n^X$ de $\text{Dir}[[X]]$ est inversible dans $\text{Dir}[[X]]$ si et seulement si $\alpha_1 \neq 0$; en déduire la structure des idéaux de $\text{Dir}[[X]]$.

*7. Prouver que l'ensemble, noté $\text{Dir}_c[[X]]$, des éléments $f = \sum_{n=1}^{+\infty} \alpha_n n^X$ de $\text{Dir}[[X]]$ tels que la suite (α_n) soit à croissance lente est une sous-algèbre pleine de $\text{Dir}[[X]]$. (On dit qu'une suite (α_n) de nombres complexes est à croissance lente s'il existe un nombre réel positif β tel que (α_n) soit dominée à l'ordre β .)

Prouver que si (α_n) est dominée à l'ordre β , la série de terme général $\left(\frac{\alpha_n}{n^s}\right)$ où $s \in \mathbb{C}$, est absolument convergente lorsque $\text{Re}(s) > \beta + 1$.

On appelle *abscisse de convergence absolue* d'un élément $f = \sum_{n=1}^{+\infty} \alpha_n n^X$ de $\text{Dir}_c[[X]]$, et on note σ_f , le plus petit des éléments γ de $\overline{\mathbb{R}}$ tels que la série de terme général $\left(\frac{|\alpha_n|}{n^\gamma}\right)$ soit convergente. Montrer que la série de terme général $\left(\frac{\alpha_n}{n^s}\right)$ est absolument convergente pour tout nombre complexe s tel que $\text{Re}(s) > \sigma_f$.

Réciproquement, prouver que si l'ensemble des nombres complexes s tels que la série de terme général $\left(\frac{\alpha_n}{n^s}\right)$ converge est non vide, la suite (α_n) est à croissance lente.

8. Pour tout élément $f = \sum_{n=1}^{+\infty} \alpha_n n^X$ de $\text{Dir}_c [[X]]$, la fonction \widehat{f} qui à tout nombre complexe s tel que $\text{Re}(s) > \sigma_f$ associe le nombre complexe

$$\widehat{f}(s) = \sum_{n=1}^{+\infty} \frac{\alpha_n}{n^s}$$

s'appelle transformée de Dirichlet-Laplace de f , et se note encore $\mathfrak{L}(f)$.

Prouver que, pour tout couple (f, g) d'éléments de $\text{Dir}_c [[X]]$ et pour tout couple (α, β) de nombres complexes,

$$\begin{aligned}\sigma_{\alpha f + \beta g} &\leq \sup(\sigma_f, \sigma_g) \\ \sigma_{f * g} &\leq \sup(\sigma_f, \sigma_g),\end{aligned}$$

et que, pour tout nombre complexe s tel que $\text{Re}(s) > \sup(\sigma_f, \sigma_g)$,

$$\begin{aligned}\mathfrak{L}(\alpha f + \beta g)(s) &= \alpha \mathfrak{L}(f)(s) + \beta \mathfrak{L}(g)(s) \\ \mathfrak{L}(f * g)(s) &= \mathfrak{L}(f)(s) \cdot \mathfrak{L}(g)(s)\end{aligned}$$

(propriétés de la transformation de Dirichlet-Laplace).*

85 B. Fonctions arithmétiques multiplicatives.

On utilise les notations et les résultats de l'exercice précédent.

On note \mathfrak{E} l'ensemble des nombres premiers. On dit qu'une application f de \mathbb{N}^* dans \mathbb{C} est *faiblement multiplicative* si, pour tout couple (p, q) d'éléments de \mathbb{N}^* premiers entre eux, $f(pq) = f(p)f(q)$. On note \mathcal{M} la partie de $\text{Dir} [[X]]$ constituée des applications de \mathbb{N}^* dans \mathbb{C} faiblement multiplicatives.

1. Prouver que δ appartient à \mathcal{M} , et que le produit de deux éléments de \mathcal{M} appartient encore à \mathcal{M} . Prouver qu'un élément f de \mathcal{M} est inversible dans $\text{Dir} [[X]]$ si et seulement si $f(1) = 1$, et que l'inverse g de f appartient encore à \mathcal{M} . (On établira la relation $g(pq) = g(p)g(q)$ par récurrence sur $p + q$, où (p, q) parcourt l'ensemble des couples d'éléments de \mathbb{N}^* premiers entre eux.)

2. Soit g un élément de $\text{Dir} [[X]]$ tel que $g(1) = 1$ et satisfaisant à la condition suivante : il existe un nombre premier p tel que $g(n) = 0$ lorsque n n'est pas de la forme p^r , où $r \in \mathbb{N}$. Prouver que g appartient à \mathcal{M} .

Soit maintenant $(g_p)_{p \in \mathfrak{E}}$ une suite d'éléments de $\text{Dir} [[X]]$ telle que, pour tout nombre premier p , $g_p(1) = 1$ et que $g_p(n) = 0$ lorsque n n'est pas de la forme p^r , où $r \in \mathbb{N}$. On considère l'élément de $\text{Dir} [[X]]$, noté $\star_{p \in \mathfrak{E}} g_p$, défini par les relations

$$\begin{aligned}\left(\star_{p \in \mathfrak{E}} g_p\right)(n) &= \left(\star_{\substack{p \in \mathfrak{E} \\ p|n}} g_p\right)(n) \quad \text{si} \quad n > 1 \\ \left(\star_{p \in \mathfrak{E}} g_p\right)(1) &= 1.\end{aligned}$$

Prouver que cette fonction est faiblement multiplicative.

3. Réciproquement, soit f un élément de \mathcal{M} tel que $f(1) = 1$. Pour tout nombre premier p , on considère la fonction f_p définie par les relations

$$\begin{aligned}f_p(n) &= f(n) \quad \text{si } n \text{ est de la forme } p^r, r \in \mathbb{N} \\ &= 0 \quad \text{dans le cas contraire.}\end{aligned}$$

Prouver que $f = \star_{p \in \mathcal{E}} f_p$. Autrement dit,

$$\sum_{n=1}^{+\infty} f(n)n^X = \prod_{p \in \mathcal{E}} \sum_{r=0}^{+\infty} f(p^r)(p^r)^X$$

(formule de localisation des fonctions faiblement multiplicatives).

86 B. Caractères de \mathbf{N}^* .

On utilise les notations et les résultats des deux exercices précédents.

I. — Soit ε la fonction constante et égale à 1. Ainsi, $\varepsilon = \sum_{n=1}^{+\infty} n^X$.

1. Prouver que, pour tout élément f de $\text{Dir}[[X]]$ et pour tout élément n de \mathbf{N}^* ,

$$(f * \varepsilon)(n) = \sum_{p|n} f(p).$$

En déduire que si f est faiblement multiplicative, il en est de même de la fonction g définie par la relation

$$g(n) = \sum_{p|n} f(p).$$

2. Soit $d(n)$ le nombre de diviseurs d'un élément n de \mathbf{N}^* . Prouver que la fonction d est faiblement multiplicative et que, pour tout élément n de \mathbf{N}^* ,

$$d(n) = \prod_{p \in \mathcal{E}} [v_p(n) + 1].$$

3. Prouver que pour tout élément g de $\text{Dir}[[X]]$, il existe un élément f et un seul de $\text{Dir}[[X]]$ tel que $f * \varepsilon = g$, et que $f = g * \mu$, où μ désigne l'inverse de ε dans l'algèbre $\text{Dir}[[X]]$. La fonction μ est faiblement multiplicative; on l'appelle *fonction de Möbius*.

Prouver que $\mu(1) = 1$ et que, pour tout élément p de \mathcal{E} ,

$$\begin{aligned} \mu(p) &= -1 \\ \mu(p^r) &= 0 \quad \text{si } r > 1. \end{aligned}$$

En déduire le résultat suivant : soit n un élément de \mathbf{N}^* . S'il existe un élément p de \mathcal{E} tel que $v_p(n) > 1$, $\mu(n) = 0$. Dans le cas contraire, $\mu(n) = (-1)^q$, où $q = \sum_{p \in \mathcal{E}} v_p(n)$.

*4. Prouver que l'abscisse de convergence absolue de la série de Dirichlet formelle ε est égale à 1. La transformée de Dirichlet-Laplace de ε s'appelle fonction ζ de Riemann. Ainsi, pour tout nombre complexe s tel que $\text{Re}(s) > 1$,

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}.$$

Montrer que

$$\zeta(s) = \prod_{p \in \mathcal{E}} \frac{1}{1 - p^{-s}}.$$

(On pourra utiliser la formule de localisation des fonctions faiblement multiplicatives).

Montrer que l'abscisse de convergence absolue de d est égale à 1 et que

$$\sum_{n=1}^{+\infty} \frac{d(n)}{n^s} = [\zeta(s)]^2.$$

Montrer enfin que l'abscisse de convergence absolue de μ est supérieure ou égale à 1, et que, pour tout nombre complexe s tel que $\operatorname{Re}(s) > 1$,

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)} \cdot *$$

II. — Pour tout nombre complexe s , on note χ_s l'élément de $\operatorname{Dir}[[X]]$ défini par la relation $\chi_s(n) = n^s$.

1. Prouver que, pour tout couple (s, t) de nombres complexes distincts,

$$(\chi_s * \chi_t)(p^r) = \frac{p^{(r+1)s} - p^{(r+1)t}}{p^s - p^t}.$$

En déduire la valeur de $(\chi_s * \chi_t)(n)$ pour tout élément n de \mathbf{N}^* .

Prouver que, pour tout nombre complexe s ,

$$(\chi_s * \chi_s)(p^r) = (r+1)p^{rs}.$$

2. Pour tout nombre complexe s , on pose $\sigma_s = \chi_s * \varepsilon$. Prouver que, pour tout élément n de \mathbf{N}^* , $\sigma_s(n)$ n'est autre que la somme des puissances $s^{\text{ièmes}}$ des diviseurs de n . Ainsi, $\sigma_0 = d$.

En utilisant la question précédente, prouver que pour tout nombre complexe non nul s et pour tout élément n de \mathbf{N}^* ,

$$\sigma_s(n) = \prod_{p \in \mathfrak{P}} \frac{p^{s[v_p(n)+1]} - 1}{p^s - 1}.$$

En outre, la fonction σ_s est faiblement multiplicative.

3. Prouver que, pour tout nombre complexe s , il existe un élément μ_s et un seul de $\operatorname{Dir}[[X]]$ tel que $\chi_s * \mu_s = \delta$, et que μ_s est faiblement multiplicative (en particulier, $\mu_0 = \mu$). Expliciter μ_s .

4. Prouver que, pour tout couple (s, t) de nombres complexes, il existe un élément $\varphi_{s,t}$ et un seul de $\operatorname{Dir}[[X]]$ tel que $\chi_s * \varphi_{s,t} = \chi_t$, et que $\varphi_{s,t}$ est faiblement multiplicative. Expliciter $\varphi_{s,t}$ en utilisant la formule $\varphi_{s,t} = \chi_t * \mu_s$.

*5. Soit t un nombre complexe. Prouver que l'abscisse de convergence absolue de χ_t est égale à $1 + \operatorname{Re}(t)$, et que $\widehat{\chi_t}(s) = \zeta(s - t)$. Montrer que l'abscisse de convergence absolue de σ_t est égale à $1 + \operatorname{Re}(t)$, et que

$$\sum_{n=1}^{+\infty} \frac{\sigma_t(n)}{n^s} = \zeta(s)\zeta(s - t).$$

Montrer de même que l'abscisse de convergence absolue de μ_t est supérieure ou égale à $1 + \operatorname{Re}(t)$, et que

$$\sum_{n=1}^{+\infty} \frac{\mu_t(n)}{n^s} = \frac{1}{\zeta(s - t)} \cdot *$$

87 B. Sommes de Ramanujan.

On utilise les notations et les résultats des trois exercices précédents.

I. — *Indicateur d'Euler*. — On appelle indicateur d'Euler d'un élément n de \mathbf{N}^* , et on note $\varphi(n)$, le cardinal de l'ensemble des éléments de \mathbf{N}^* inférieurs ou égaux à n et premiers avec n .

1. Prouver que, pour tout diviseur p de n , le cardinal de l'ensemble des éléments m de \mathbf{N}^* inférieurs ou égaux à n et tels que P. G. C. D. $(m, n) = p$ est égal à $\varphi\left(\frac{n}{p}\right)$. En déduire que $\varphi * \varepsilon = \chi_1$. Autrement dit,

$$\sum_{p|n} \varphi(p) = n.$$

En déduire que φ est faiblement multiplicative, et que, pour tout entier n strictement supérieur à 1,

$$\varphi(n) = n \prod_{\substack{p \in \mathcal{E} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

2. Soit t un nombre complexe. Montrer qu'il existe un élément φ_t et un seul de Dir $[[X]]$ tel que $\varphi_t * \varepsilon = \chi_t$, et que φ_t est faiblement multiplicative (en particulier, $\varphi_1 = \varepsilon$). Expliciter φ_t .

*3. Prouver que l'abscisse de convergence absolue de φ_t est supérieure ou égale à $1 + \operatorname{Re}(t)$, et que

$$\sum_{n=1}^{+\infty} \frac{\varphi_t(n)}{n^s} = \frac{\zeta(s-t)}{\zeta(s)}.$$

En particulier, l'abscisse de convergence absolue de φ est supérieure ou égale à 2, et

$$\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \cdot *$$

II. — Sommes de Ramanujan.

1. Soit f une application de \mathbf{Q} dans \mathbf{C} telle que $f(1) = 1$ et que, pour tout couple (a, b) d'éléments de \mathbf{Q} ,

$$f(a+b) = f(a)f(b).$$

On appelle somme de Ramanujan associée à f l'élément ρ_f de Dir $[[X]]$ défini par la relation

$$\rho_f(n) = \sum_{m \in \mathcal{E}_n} f\left(\frac{m}{n}\right),$$

où \mathcal{E}_n désigne l'ensemble des éléments de \mathbf{N}^* inférieurs ou égaux à n et premiers avec n . Prouver que

$$(\rho_f * \varepsilon)(n) = \sum_{p=1}^n f\left(\frac{p}{n}\right).$$

En déduire que

$$\begin{aligned} (\rho_f * \varepsilon)(n) &= 0 & \text{si} & \quad f\left(\frac{1}{n}\right) \neq 1 \\ &= n & \text{si} & \quad f\left(\frac{1}{n}\right) = 1. \end{aligned}$$

2. Montrer que les fonctions $x \mapsto e^{2i\pi r x}$, où $r \in \mathbf{Z}$, sont les seules applications continues f de \mathbf{R} dans \mathbf{C} telles que $f(1) = 1$ et que, pour tout couple (x, y) d'éléments de \mathbf{R} ,

$$f(x+y) = f(x)f(y).$$

On suppose désormais que $f(x) = e^{2i\pi r x}$, où $r \in \mathbb{Z}$. Alors ρ_f se note ρ_r , et $\rho_r(n)$ n'est autre que la somme des puissances $r^{\text{ièmes}}$ des racines primitives $n^{\text{ièmes}}$ de l'unité :

$$\rho_r(n) = \sum_{m \in \delta_n} e^{2i\pi r \frac{m}{n}}.$$

En particulier, ρ_0 n'est autre que l'indicateur d'Euler.

Prouver que, pour tout élément r de \mathbb{Z} ,

$$\begin{aligned} (\rho_r * \varepsilon)(n) &= n && \text{si } n \text{ divise } r \\ &= 0 && \text{dans le cas contraire.} \end{aligned}$$

En déduire que $\rho_1 = \mu$ et que $\rho_{-r} = \rho_r$.

3. Pour tout élément r de \mathbb{Z} , on considère l'élément δ_r de $\text{Dir}[[X]]$ défini par les relations

$$\begin{aligned} \delta_r(n) &= n && \text{si } n \text{ divise } r \\ &= 0 && \text{dans le cas contraire.} \end{aligned}$$

(En particulier, $\delta_1 = \delta$). Prouver que δ_r est faiblement multiplicative. En déduire que les sommes de Ramanujan ρ_r sont faiblement multiplicatives. Calculer $\rho_r(n)$ lorsque n est une puissance d'un nombre premier.

4. Prouver que

$$\rho_r(n) = \sum_{\substack{p|r \\ p|n}} p^{\mu\left(\frac{n}{p}\right)}.$$

En déduire que

$$\rho_r(n) = \mu(n) \quad \text{si P. G. C. D.}(r, n) = 1.$$

Plus généralement, on pose $d = \text{P. G. C. D.}(r, n)$ et $n_1 = \frac{n}{d}$. On note d' le plus grand diviseur de d premier avec n_1 . Prouver que

$$\rho_r(n) = \frac{d}{d'} \mu(n_1) \varphi(d').$$

*5. Prouver que l'abscisse de convergence absolue de ρ_r est supérieure ou égale à 1, et que

$$\sum_{n=1}^{+\infty} \frac{\rho_r(n)}{n^s} = \frac{\sigma_{s-1}(r)}{r^{s-1} \zeta(s)} \cdot *$$

CHAPITRE 2

POLYNÔMES A PLUSIEURS INDÉTERMINÉES

INTRODUCTION

Dans les cinq premiers paragraphes de ce chapitre, nous exposons la théorie des polynômes à plusieurs indéterminées à coefficients dans un anneau commutatif unitaire.

La démonstration des théorèmes les plus importants procède par récurrence sur le nombre des indéterminées; c'est pourquoi l'étude des polynômes à plusieurs indéterminées, même à coefficients dans un corps commutatif, nécessite celle des polynômes à une indéterminée à coefficients dans un anneau commutatif unitaire, effectuée au § 1. Aux §§ 2 et 3, nous appliquons les résultats obtenus à la théorie des polynômes et des fractions rationnelles à plusieurs indéterminées, et aux fonctions polynomiales et rationnelles. Les propriétés de l'ensemble des zéros d'un polynôme à plusieurs indéterminées seront approfondies au chapitre III.4; nous nous sommes borné ici au principe de prolongement des identités algébriques, qu'il est utile de comparer au principe de prolongement des égalités (cf. prop. I.5.32) et au principe de prolongement analytique (cf. *Analyse* III).

Le § 4 est consacré à la dérivation des polynômes et des fractions rationnelles. La présentation adoptée utilise les notions de développement taylorien et de différentielle, afin de mettre en évidence le lien avec les théories correspondantes en analyse (cf. *Analyse* III).

Dans le § 5, nous étudions les polynômes et fractions rationnelles symétriques. La notion fondamentale est ici celle d'opération du groupe symétrique sur l'algèbre des polynômes. L'application de cette théorie à l'élimination est reportée au chapitre III.4.

Enfin, le dernier paragraphe, nous exposons la théorie des séries entières formelles à plusieurs indéterminées à coefficients dans un anneau commutatif unitaire, dont l'utilité apparaît en géométries algébrique et analytique (théorème des fonctions implicites et étude locale des ensembles algébriques et analytiques) et dans la résolution des équations aux dérivées partielles. Nous appliquons cette théorie à celle des opérateurs de composition, qui interviennent dans l'étude des développements tayloriens généralisés (cf. *Analyse* III). En particulier, nous montrons comment les nombres de Bernoulli interviennent dans les développements en série des fonctions hyperboliques et trigonométriques.

Dans tout ce chapitre, A désigne un anneau commutatif unitaire, et K désigne un corps commutatif.

§. 1. POLYNÔMES À UNE INDÉTERMINÉE À COEFFICIENTS DANS UN ANNEAU

1. POLYNÔMES. FONCTIONS POLYNOMIALES

DÉFINITION 2.1. — **Algèbre des polynômes à une indéterminée à coefficients dans un anneau.** — Soient A un anneau commutatif unitaire, $A^{(\mathbb{N})}$ le A -module libre des suites d'éléments de A nuls à partir d'un certain rang, et $(e_n)_{n \in \mathbb{N}}$ la base canonique de $A^{(\mathbb{N})}$. On considère la structure de A -algèbre définie sur $A^{(\mathbb{N})}$ par la table de multiplication

$$e_i \cdot e_j = e_{i+j},$$

pour tout couple (i, j) d'entiers naturels. Cette algèbre est associative, commutative et unitaire; elle se note $\mathbf{P}(A)$, et s'appelle algèbre des polynômes à coefficients dans A . Le monôme e_0 se note 1, le monôme e_1 s'appelle indéterminée, et se note souvent X . L'algèbre $\mathbf{P}(A)$ se note alors $A[X]$.

La proposition 1.1 se généralise aussitôt.

Comme au § 1.1, on définit le degré du polynôme $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ comme étant le plus grand des entiers n tels que α_n soit non nul, si P est non nul, et $-\infty$ si P est nul.

La proposition 1.2 s'étend en la suivante :

PROPOSITION 2.1. — **Degré d'une somme, degré d'un produit.** — Soient P et Q deux éléments de $A[X]$. Alors

$$d^0(P + Q) \leq \sup [d^0(P), d^0(Q)],$$

avec égalité si $d^0(P) \neq d^0(Q)$;

$$d^0(PQ) \leq d^0(P) + d^0(Q),$$

avec égalité si le coefficient dominant de P , ou celui de Q , n'est pas diviseur de zéro dans l'anneau A . Cette circonstance se produit si l'un des deux polynômes P et Q est unitaire, ou encore si l'anneau A est intègre.

COROLLAIRE 1. — Permanence de l'intégrité. — *Si l'anneau A est intègre, l'anneau $A[X]$ est intègre, et les constantes inversibles sont les seuls éléments inversibles de cet anneau.*

La démonstration est calquée sur celle de la proposition 1.5, qui s'applique mot pour mot puisque, A étant intègre,

$$d^0(PQ) = d^0(P) + d^0(Q).$$

COROLLAIRE 2. — Permanence de la divisibilité et de l'irréductibilité. — *On suppose que l'anneau A est intègre. Soit a un élément non nul de A . Pour qu'un élément P de $A[X]$ divise a dans $A[X]$, il faut et il suffit que P soit un élément b de A et que b divise a dans A . Par suite, a est irréductible dans A si et seulement si a est irréductible dans $A[X]$.*

Si P divise a dans $A[X]$, il existe un élément non nul Q de $A[X]$ tel que $PQ = a$. Il en découle que $d^0(P) = d^0(Q) = 0$, ce qu'il fallait démontrer.

EXEMPLE. — On suppose que l'anneau A est intègre. Soient a et b deux éléments non nuls de A et $P = aX + b$. Pour que P soit irréductible dans $A[X]$, il faut et il suffit que a et b soient premiers entre eux dans A .

Il est évident que si a et b ne sont pas premiers entre eux, P n'est pas irréductible. Réciproquement, supposons que P n'est pas irréductible. Il existe alors un élément c de A non inversible dans A et deux éléments a' et b' de A , $a' \neq 0$, tels que $aX + b = c(a'X + b')$. Il en découle que c est un diviseur commun à a et b , non inversible, ce qui montre que a et b ne sont pas premiers entre eux.

Soit maintenant E une A -algèbre associative unitaire. Pour tout élément $P = \sum_{n=0}^{+\infty} \alpha_n X^n$ de $A[X]$, on note \tilde{P} l'application de E dans E qui à tout élément a de E associe l'élément $\sum_{n=0}^{+\infty} \alpha_n a^n$ obtenu en substituant a à l'indéterminée X dans le polynôme P . Une application f de E dans E de la forme \tilde{P} est dite fonction polynomiale à une variable sur E . L'élément $\tilde{P}(a)$ s'appelle encore valeur de P au point a .

On dit qu'un élément α de l'anneau A est une *racine* d'un élément P de $A[X]$ si $\tilde{P}(\alpha) = 0$. La proposition 1.10, ainsi que sa démonstration, s'étendent sans changement : *pour qu'un élément α de A soit racine d'un élément P de $A[X]$, il faut et il suffit que P soit divisible par $X - \alpha$.*

Soient P un élément non nul de $A[X]$, et α un élément de A . D'après la proposition 2.1, l'ensemble des entiers naturels m tels que $(X - \alpha)^m$ divise P est majoré par le degré de P . On peut donc étendre la définition des valuations (cf. déf. 1.8) en la suivante :

DÉFINITION 2.2. — Valuation d'un polynôme en un point. — *Soient P un élément de $A[X]$, et α un élément de A . On appelle valuation de P au point α , et on note $v_\alpha(P)$, le plus grand des entiers m tels que $(X - \alpha)^m$ divise P , si P est non nul, et $+\infty$ si P est nul.*

Lorsque α est racine de P , $v_\alpha(P)$ s'appelle ordre de multiplicité de la racine α .

La proposition 1.11 se généralise en la

PROPOSITION 2.2. — Propriétés de la valuation en un point.

1. Soit P un élément non nul de $A[X]$; pour que $v_\alpha(P)$ soit égal à un entier naturel m , il faut et il suffit qu'il existe un élément Q de $A[X]$ tel que

$$P = (X - \alpha)^m Q, \quad \text{et} \quad \tilde{Q}(\alpha) \neq 0.$$

2. Soient P et Q deux éléments de $A[X]$; alors, pour tout élément α de A ,

$$v_\alpha(P + Q) \geq \inf [v_\alpha(P), v_\alpha(Q)],$$

avec égalité si $v_\alpha(P) \neq v_\alpha(Q)$;

$$v_\alpha(PQ) \geq v_\alpha(P) + v_\alpha(Q),$$

avec égalité si l'anneau A est intègre.

Les théorèmes 1.2 et 1.3 s'étendent de la manière suivante :

THÉORÈME 2.1. — Divisibilité par un produit de facteurs du premier degré. — Soient A un anneau intègre, P un élément non nul de $A[X]$, et $(\alpha_1, \alpha_2, \dots, \alpha_r)$ une suite de r éléments de A distincts deux à deux. Si, pour tout $i \in [1, r]$, le scalaire α_i est racine d'ordre n_i de P , il existe un élément R de $A[X]$ et un seul tel que $P = R \prod_{i=1}^r (X - \alpha_i)^{n_i}$. De plus, pour tout $i \in [1, r]$, $\tilde{R}(\alpha_i) \neq 0$.

En particulier, soit P un élément de $A[X]$. S'il existe r éléments $\alpha_1, \alpha_2, \dots, \alpha_r$ de A distincts deux à deux tels que $\sum_{i=1}^r v_{\alpha_i}(P) > d^0(P)$, alors P est nul.

La démonstration du théorème 1.2 s'applique mot pour mot, puisque A est intègre.

Il en découle, en supposant toujours A intègre, qu'un polynôme non nul de degré n a au plus n racines. Lorsque A est un anneau intègre infini, deux fonctions polynomiales sur A prenant même valeur sur une partie infinie de A sont égales; en particulier, l'application qui à tout élément P de $A[X]$ associe la fonction polynomiale \tilde{P} est injective.

REMARQUE. — Le théorème précédent peut tomber en défaut lorsque l'anneau A n'est pas intègre. Plus précisément, si α est un diviseur de zéro dans A , le polynôme αX admet pour racines tous les éléments β de A tels que $\alpha\beta = 0$. En prenant par exemple pour A l'algèbre des nombres duaux (cf. exercice I.3.68), et pour α l'élément $(0,1)$, on voit qu'un polynôme de degré 1 peut fort bien avoir une infinité de racines.

2. IDÉAUX DE POLYNÔMES

Le théorème de division euclidienne (cf. th. 1.4) s'étend aussitôt en le suivant, la démonstration étant inchangée :

THÉORÈME 2.2. — Division euclidienne d'un polynôme par un polynôme unitaire. — Soient B et C deux éléments de $A[X]$, le polynôme C étant supposé unitaire. Il existe un couple (Q, R) et un seul d'éléments de $A[X]$ tel que

$$B = CQ + R \quad \text{et} \quad d^0(R) < d^0(C).$$

REMARQUE. — Le résultat précédent est encore valable si le coefficient dominant du polynôme C est inversible dans l'anneau A ; dans le cas contraire, l'existence du couple (Q, R) n'est plus assurée, ce qui introduit une différence *essentielle* entre le cas où A est un anneau et le cas où A est un corps. C'est pourquoi le théorème de structure des idéaux de l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans un corps ne s'étend pas, même lorsque l'anneau A est principal.

Par exemple, l'idéal de l'anneau $\mathbb{Z}[X]$ engendré par les polynômes 2 et X n'est évidemment pas principal.

De même, soit A l'anneau $K[Y]$ des polynômes à une indéterminée à coefficients dans un corps K ; alors, dans l'anneau $A[X]$, c'est-à-dire dans l'anneau $K[X, Y]$ des polynômes à deux indéterminées à coefficients dans K , l'idéal engendré par les polynômes X et Y n'est pas principal.

Il existe cependant une généralisation très intéressante du théorème 1.5, qui repose sur la notion d'anneau noethérien. Rappelons qu'un anneau commutatif unitaire A est dit *noethérien* si tout idéal de A admet une famille génératrice finie, ou, ce qui revient au même, si toute suite croissante d'idéaux de A est stationnaire (cf. exercice I.3.95). Rappelons encore qu'un corps commutatif, qu'un anneau principal, sont des anneaux noethériens.

Nous pouvons alors énoncer le

THÉORÈME 2.3. — Théorème de permanence de Hilbert. — Soit A un anneau commutatif unitaire. Si A est noethérien, l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est encore noethérien.

Soit en effet \mathfrak{J} un idéal de $A[X]$. Pour tout entier naturel n , désignons par E_n l'ensemble des éléments P de \mathfrak{J} de degré n et par \mathfrak{U}_n la réunion de $\{0\}$ et de l'ensemble des coefficients dominants des éléments P de E_n . Il est immédiat que \mathfrak{U}_n est un idéal de A .

Notons que \mathfrak{U}_n est encore l'ensemble des coefficients dominants des éléments P de \mathfrak{J} de degré inférieur ou égal à n : en effet, si P est un élément non nul de \mathfrak{J} de degré m inférieur ou égal à n , alors le polynôme $X^{n-m}P$ est un élément de \mathfrak{J} de degré n , et les coefficients dominants de P et de $X^{n-m}P$ sont égaux.

Il en découle aussitôt que la suite (\mathfrak{U}_n) est croissante. Comme l'anneau A est noethérien, cette suite est stationnaire, c'est-à-dire qu'il existe un entier naturel r tel que, pour tout $n \geq r$, $\mathfrak{U}_n = \mathfrak{U}_r$.

D'autre part, puisque A est noethérien, pour tout entier $j \in [0, r]$, l'idéal \mathfrak{U}_j de A admet une famille génératrice $(\alpha_{ij})_{i \in I_j}$, où I_j est un ensemble fini. Pour tout $j \in [0, r]$, et pour tout $i \in I_j$, désignons par P_{ij} un élément de E_j admettant α_{ij} comme coefficient dominant.

Nous allons prouver que l'idéal \mathfrak{I} n'est autre que l'idéal \mathfrak{I}' de $A[X]$ engendré par les polynômes P_{ij} . Il est évident que \mathfrak{I}' est contenu dans \mathfrak{I} ; il suffit donc de montrer que, pour tout entier naturel n , E_n est contenu dans \mathfrak{I}' . Nous procéderons par récurrence sur n . Il est immédiat que $\mathfrak{U}_0 = E_0 \cup \{0\}$; donc E_0 est contenu dans \mathfrak{I}' . Supposons donc que, pour tout entier p strictement inférieur à n , $n \geq 1$, E_p soit contenu dans \mathfrak{I}' , considérons un élément P de E_n , et désignons par α le coefficient dominant de P .

Ou bien n est inférieur ou égal à r ; puisque α appartient à \mathfrak{U}_n , il existe une famille $(\beta_i)_{i \in I_n}$ d'éléments de A telle que

$$\alpha = \sum_{i \in I_n} \beta_i \alpha_{in}.$$

Il en découle aussitôt que le polynôme

$$Q = P - \sum_{i \in I_n} \beta_i P_{in}$$

est de degré strictement inférieur à n . Comme d'autre part Q appartient à \mathfrak{I} , l'hypothèse de récurrence s'applique, et montre que Q appartient à \mathfrak{I}' . Finalement, le polynôme P appartient à \mathfrak{I}' , ce qu'il fallait prouver.

Ou bien n est strictement supérieur à r ; puisque $\mathfrak{U}_n = \mathfrak{U}_r$, les coefficients dominants des polynômes $X^{n-r} P_{ir}$, où i parcourt I_r , engendrent l'idéal \mathfrak{U}_n . Il en découle comme ci-dessus qu'il existe une famille $(\beta_i)_{i \in I_r}$ d'éléments de A telle que le polynôme

$$Q = P - X^{n-r} \sum_{i \in I_r} \beta_i P_{ir}$$

soit de degré strictement inférieur à n , et que, par suite, le polynôme P appartient à \mathfrak{I}' , ce qui achève la démonstration.

3. DÉCOMPOSITION EN FACTEURS IRRÉDUCTIBLES

Les résultats concernant la décomposition d'un polynôme en facteurs irréductibles (cf. § 1.5) s'étendent, grâce à la notion d'anneau factoriel, que nous allons introduire maintenant.

Notons d'abord que dans l'ensemble des éléments irréductibles d'un anneau intègre unitaire A , la relation de divisibilité est une relation d'équivalence, et que la classe d'un élément irréductible a est formée des éléments ua , où u parcourt l'ensemble des éléments inversibles de A . Dans la suite, nous choisirons fréquemment un ensemble E de représentants de ces classes.

DÉFINITION 2.3. — Anneaux factoriels. — *On dit qu'un anneau commutatif unitaire A est factoriel s'il est intègre, et s'il satisfait aux deux conditions suivantes :*

a) *Tout élément non inversible de A peut être décomposé en un produit fini d'éléments irréductibles.*

b) *Propriété de Gauss.* — Pour tout triplet (a, b, c) d'éléments non nuls de A tel que a divise bc et que a et b soient premiers entre eux, alors a divise c .

REMARQUE 1. — Si A est noethérien, la condition a) est automatiquement satisfaite (cf. exercice 8).

REMARQUE 2. — On peut prouver (cf. exercice I.2.45) que les anneaux principaux sont factoriels.

La proposition 1.15 s'étend en la

PROPOSITION 2.3. — Soient A un anneau factoriel, a, b et c trois éléments non nuls de A . Si a est premier avec b et c , alors a est premier avec bc .

La démonstration est calquée sur celle de la proposition 1.15.

COROLLAIRE. — Soit A un anneau factoriel. Si un élément a de A est premier avec les éléments a_1, a_2, \dots, a_n , alors a est premier avec $a_1 a_2 \dots a_n$.

La terminologie d'anneau factoriel provient du théorème suivant, qui généralise le théorème 1.6.

THÉORÈME 2.4. — **Décomposition en facteurs irréductibles.** — Soit A un anneau factoriel.

1. Soit p un élément irréductible de A . Pour tout élément a non nul de A , il existe un couple (n, b) , où n est un entier naturel et où b est un élément non nul de A premier avec p , tel que $a = p^n b$. Un tel couple est unique.

L'entier n s'appelle *valuation de a relative à p* , et se note $v_p(a)$. Cet entier ne dépend que de la classe d'équivalence de p , c'est-à-dire de l'idéal principal \mathfrak{P} engendré par p ; c'est pourquoi n s'appelle aussi *valuation de a relative à \mathfrak{P}* .

2. Soit E un ensemble de représentants des classes d'éléments irréductibles de A . Alors, pour tout élément non nul a de A , l'ensemble des éléments p de E tels que $v_p(a)$ soit non nul est fini, et

$$(1) \quad a = u \prod_{p \in E} p^{v_p(a)},$$

où u est un élément inversible de l'anneau A .

Une telle décomposition est unique, c'est-à-dire que si a peut être écrit sous la forme

$$(2) \quad a = v \prod_{p \in E} p^{m_p},$$

où v est un élément inversible de A , et où m_p est un entier naturel nul sauf pour une famille finie d'éléments de E , alors, pour tout élément p de E , $m_p = v_p(a)$ et $v = u$.

Assertion 1. — **Existence.** — Écartons le cas trivial où a est inversible. Alors, A étant factoriel, a peut s'écrire sous la forme

$$a = p^n p_1 p_2 \dots p_r,$$

où n est un entier naturel, et où p_1, p_2, \dots, p_r sont irréductibles et premiers avec p . Il s'ensuit que $b = p_1 p_2 \dots p_r$ est premier avec p (cf. cor. de la prop. 2.3), et donc avec p^n (d'après ce même corollaire).

Unicité. — Considérons deux couples (n, b) et (n', b') satisfaisant aux conditions de l'énoncé; alors $p^n b = p^{n'} b'$. L'élément p^n divise $p^{n'} b'$, et est premier avec b' (cf. cor. de la prop. 2.3); il divise donc $p^{n'}$ (d'après la propriété de Gauss). Comme A est intègre, il en découle que $n \leq n'$. De même, $n' \leq n$; finalement, $n' = n$, et donc $b' = b$, puisque A est intègre.

Assertion 2. — Comme A est factoriel, on voit aussitôt que a peut être écrit sous la forme (2).

Considérons maintenant un élément p de E , et écrivons a sous la forme

$$a = p^{m_p} \cdot b, \quad \text{où} \quad b = v \prod_{\substack{p' \in E \\ p' \neq p}} p'^{m_{p'}}$$

Il résulte du corollaire de la proposition 2.3 que b est premier avec p . L'assertion 1 montre alors que $m_p = v_p(a)$. Comme cette relation est vraie pour tout élément p de E , et que A est intègre, il en découle que $v = u$, ce qui achève la démonstration.

REMARQUE. — Inversement, il est immédiat que si A est intègre, l'existence et l'unicité d'une décomposition en facteurs irréductibles pour tout élément de A impliquent que A est factoriel.

Dans les corollaires qui suivent, on conserve les mêmes notations, et on désigne par K le corps des quotients de l'anneau factoriel A .

COROLLAIRE 1. — **Décomposition en facteurs irréductibles d'un élément du corps des quotients.**

1. Soit p un élément irréductible de A . Pour tout élément k non nul de K , il existe un triplet (n, a, b) , où n est un entier rationnel et où a et b sont deux éléments non nuls de A premiers avec p , tel que $k = p^n \frac{a}{b}$. Pour tout autre triplet (n', a', b') satisfaisant à ces conditions, $n' = n$.

L'entier n s'appelle valuation de k relative à p , et se note $v_p(k)$. On convient de poser $v_p(0) = +\infty$.

2. Pour tout élément k non nul de K , l'ensemble des éléments p de E tels que $v_p(k)$ soit non nul est fini, et

$$k = u \prod_{p \in E} p^{v_p(k)},$$

où u est un élément inversible de l'anneau A .

Une telle décomposition est unique.

Assertion 1. — Pour montrer l'existence d'un tel triplet, il suffit d'écrire k sous la forme $k = \frac{a_1}{b_1}$, où a_1 et b_1 sont deux éléments non nuls de A , et d'appliquer l'assertion 1 du théorème aux éléments a_1 et b_1 .

Soient (n, a, b) et (n', a', b') deux triplets satisfaisant aux conditions de l'énoncé. Supposons par exemple $n' \geq n$, et posons $m = n' - n$. La relation $p^n \frac{a}{b} = p^{n'} \frac{a'}{b'}$ équivaut à la suivante : $b'a = p^m ba'$. Comme a, b, a' et b' sont premiers avec p , il en est de même de $b'a$ et de ba' . Par suite, $m = 0$, c'est-à-dire $n' = n$.

L'assertion 2 se ramène facilement à l'assertion 2 du théorème : on écrit tout élément k non nul de K sous la forme $k = \frac{a}{b}$, où a et b sont deux éléments non nuls de A .

COROLLAIRE 2. — Forme réduite d'un élément du corps des quotients. — Pour tout élément k de K , il existe un couple (a, b) d'éléments non nuls de A premiers entre eux et tels que $k = \frac{a}{b}$. Pour tout autre couple satisfaisant à ces conditions, il existe un élément inversible u de A tel que $a' = au$ et $b' = bu$.

Un tel couple s'appelle *forme réduite* de k .

L'existence se déduit aussitôt du corollaire 1.

La démonstration de l'unicité est calquée sur le cas des polynômes à une indéterminée (cf. prop. 1.19).

Les corollaires 1 et 2 du théorème 1.6 se généralisent aussitôt en les suivants :

COROLLAIRE 3. — Propriétés des valuations.

1. Pour tout couple (h, k) d'éléments du corps K des quotients de l'anneau A et pour tout élément irréductible p de A ,

$$(1) \quad v_p(hk) = v_p(h) + v_p(k)$$

$$(2) \quad v_p(h + k) \geq \inf(v_p(h), v_p(k)),$$

avec égalité si $v_p(h) \neq v_p(k)$.

Il en découle que l'ensemble $\mathfrak{I}_n(p)$ des éléments k de K tels que $v_p(k)$ soit strictement supérieur à un entier rationnel donné n est un sous-groupe additif de K , et que, pour tout couple (n, n') d'entiers rationnels, $\mathfrak{I}_n(p)\mathfrak{I}_{n'}(p)$ est contenu dans $\mathfrak{I}_{n+n'}(p)$.

2. Pour qu'un élément non nul a de A divise un élément non nul b de A , il faut et il suffit que, pour tout élément irréductible p de A , $v_p(a) \leq v_p(b)$.

COROLLAIRE 4. — Soit a un élément non nul de A , divisible par des éléments non nuls a_1, a_2, \dots, a_n de A premiers entre eux deux à deux. Alors a est divisible par le produit $a_1 a_2 \dots a_n$.

De même, les corollaires 3 et 4 du théorème 1.6 se généralisent de la manière suivante :

On choisit un ensemble E de représentants des classes d'éléments irréductibles de A .

1. *On considère une partie non vide \mathcal{A} de A constituée d'éléments non tous nuls. Pour tout élément p de E , on pose*

$$n_p = \inf_{a \in \mathcal{A}} v_p(a).$$

Alors l'élément

$$d = \prod_{p \in E} p^{n_p}$$

est un plus grand commun diviseur des éléments de \mathcal{A} .

Tout P. G. C. D. des éléments de \mathcal{A} est évidemment de la forme ud , où u est un élément inversible de A .

2. *On considère une partie finie non vide \mathcal{A} de A constituée d'éléments non nuls. Pour tout élément p de E , on pose*

$$n'_p = \sup_{a \in \mathcal{A}} v_p(a).$$

Alors l'élément

$$m = \prod_{p \in E} p^{n'_p}$$

est un plus petit commun multiple des éléments de \mathcal{A} .

Tout P. P. C. M. des éléments de \mathcal{A} est évidemment de la forme um , où u est un élément inversible de A .

La proposition 1.16 se généralise alors en l'énoncé suivant :

Soient a_1, a_2, \dots, a_n des éléments non nuls d'un anneau factoriel A , d un P. G. C. D. (resp. m un P. P. C. M.) de ces éléments, et b un élément non nul de A . Alors bd est un P. G. C. D. (resp. bm est un P. P. C. M.) de ba_1, ba_2, \dots, ba_n . En particulier, les éléments $\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}$ sont premiers entre eux dans leur ensemble.

THÉOREME 2.5. — Permanence de la factorialité. — *Soit A un anneau commutatif unitaire. Si A est factoriel, l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est encore factoriel.*

La démonstration, due à Gauss, repose sur la notion suivante :

DÉFINITION 2.4. — Polynômes primitifs. — *Soit A un anneau factoriel. On dit qu'un élément non nul P de $A[X]$ est primitif si les éléments inversibles de A sont les seuls diviseurs communs à ses coefficients non nuls.*

LEMME 1. — (**Lemme de Gauss.**) — Soient A un anneau factoriel, P et Q deux éléments de $A[X]$. Si P et Q sont primitifs, il en est de même de PQ .

Écrivons P et Q sous la forme

$$P = \sum_{m=0}^{+\infty} a_m X^m, \quad Q = \sum_{n=0}^{+\infty} b_n X^n.$$

Supposons que PQ ne soit pas primitif, et considérons un élément non inversible p de A divisant tous les coefficients non nuls de PQ . Puisque P (resp. Q) est primitif, il existe un plus petit entier m_0 (resp. n_0) tel que p ne divise pas a_{m_0} (resp. b_{n_0}). Or, le coefficient de $X^{m_0+n_0}$ dans le polynôme PQ n'est autre que

$$c = \sum_{m+n=m_0+n_0} a_m b_n.$$

Puisque p est premier avec a_{m_0} et b_{n_0} , p est premier avec $a_{m_0}b_{n_0}$. Comme p divise tous les autres termes de la somme précédente, c n'est pas nul, et p ne divise pas c , ce qui contredit l'hypothèse.

LEMME 2. — Soient A un anneau factoriel, et K son corps des quotients.

1. Tout élément non nul P de $A[X]$ peut s'écrire sous la forme $P = aP'$, où a est un élément non nul de A , et où P' est un élément primitif de $A[X]$.

De même, tout élément Q non nul de $K[X]$ peut s'écrire sous la forme $Q = kQ'$, où k est un élément non nul de K , et où Q' est un élément primitif de $A[X]$.

2. Soient P'_1 et P'_2 deux éléments primitifs de $A[X]$.

Soient a_1 et a_2 deux éléments non nuls de A ; si $a_1P'_1$ divise $a_2P'_2$ dans $A[X]$, alors P'_1 divise P'_2 dans $A[X]$, et a_1 divise a_2 dans A .

Si P'_1 divise P'_2 dans $K[X]$, alors P'_1 divise P'_2 dans $A[X]$; si P'_1 et P'_2 sont premiers entre eux dans $A[X]$, alors P'_1 et P'_2 sont premiers entre eux dans $K[X]$.

3. Pour qu'un élément non nul P de $A[X]$ soit irréductible dans $A[X]$, il faut et il suffit que P soit irréductible dans $K[X]$.

Assertion 1. — Puisque A est un anneau factoriel, il existe un plus grand commun diviseur a des coefficients non nuls de P . Il suffit alors de poser $P' = a^{-1}P$.

Soit maintenant Q un élément non nul de $K[X]$. Écrivons Q sous la forme

$$Q = \sum_{n=0}^m \frac{a_n}{b_n} X^n,$$

où, pour tout $n \in \mathbb{N}$, a_n et b_n appartiennent à A , et posons $b = \prod_{n=0}^m b_n$. Il est

clair que bQ est un élément non nul de $A[X]$; il existe donc un élément a non nul de A et un élément primitif P' de $A[X]$ tels que $bQ = aQ'$. Alors $Q = kQ'$,

où $k = \frac{a}{b}$.

Assertion 2. — Il existe par hypothèse un élément R de $A[X]$ tel que $a_2P'_2 = a_1P'_1R$. Écrivons R sous la forme $R = bR'$, où b appartient à A et où R' est primitif. Considérons alors le polynôme $P = a_2P'_2 = a_1bP'_1R'$. D'après le lemme 1, P'_1R' est primitif; les scalaires a_2 et a_1b sont donc des P. G. C. D. des coefficients non nuls de P . Il en découle qu'il existe un élément inversible u de A tel que $a_2 = a_1bu$; par suite, a_1 divise a_2 dans A , et P'_1 divise P'_2 dans $A[X]$.

Supposons maintenant que P'_1 divise P'_2 dans $K[X]$, c'est-à-dire qu'il existe un élément Q non nul de $K[X]$ tel que $P'_2 = QP'_1$. D'après l'assertion 1, Q peut s'écrire sous la forme $Q = \frac{a}{b}Q'$, où a et b sont des éléments non nuls de A , et où Q' est un élément primitif de $A[X]$. La relation $bP'_2 = aP'_1Q'$ montre que aP'_1 divise bP'_2 dans $A[X]$; il s'ensuit que P'_1 divise P'_2 dans $A[X]$, ce qu'il fallait prouver.

Supposons maintenant que P'_1 et P'_2 sont premiers entre eux dans $A[X]$, et considérons un élément Q de $K[X]$ diviseur commun à P'_1 et P'_2 dans $K[X]$. Écrivons encore Q sous la forme $Q = \frac{a}{b}Q'$. Il est clair que Q' divise P'_1 et P'_2 dans $K[X]$; comme ces trois polynômes sont primitifs, Q' divise P'_1 et P'_2 dans $A[X]$, ce qui montre que Q' est constant.

Assertion 3. — Il est évident que si P est irréductible dans $K[X]$, P est irréductible dans $A[X]$. Réciproquement, supposons que P soit irréductible dans $A[X]$, et considérons un diviseur Q de P dans $K[X]$ tel que $d^\circ(Q) < d^\circ(P)$. Notons d'abord que P est primitif, car tout P. G. C. D. des coefficients non nuls de P , étant un diviseur de P , est inversible. Écrivons encore Q sous la forme $Q = \frac{a}{b}Q'$. Le polynôme primitif Q' divise le polynôme primitif P dans $K[X]$. Par suite, Q' divise P dans $A[X]$, et, puisque P est irréductible dans $A[X]$, Q' est constant, ce qui achève la démonstration.

Ces lemmes étant prouvés, démontrons le théorème de permanence.

1. Tout élément non inversible P de $A[X]$ peut être décomposé en un produit de facteurs irréductibles. — Raisonnons par récurrence sur le degré de P . Lorsque $d^\circ(P) = 0$, cela résulte du fait que A est un anneau factoriel, puisque tout élément irréductible de A est évidemment un élément irréductible de $A[X]$.

Supposons donc l'assertion prouvée pour tous les polynômes de degré strictement inférieur à n , $n \geq 1$, et considérons un polynôme P de degré n . D'après le lemme 2, P peut s'écrire sous la forme $P = cP'$, où $c \in A$, et où P' est primitif. Si P' est irréductible, l'assertion est claire; dans le cas contraire, P' peut s'écrire sous la forme $P' = QR$, où Q et R sont des éléments non inversibles de $A[X]$. Comme P' est primitif, Q et R ne sont pas des polynômes constants. Par suite, Q et R sont de degré strictement inférieur à n , et l'hypothèse de récurrence s'applique à Q et R , ce qui achève la démonstration.

2. **L'anneau $A[X]$ satisfait à la propriété de Gauss.** — Soient en effet P , Q et R trois éléments non nuls de $A[X]$ tels que P divise QR et que P et Q soient premiers entre eux. D'après le lemme 2, P , Q et R peuvent s'écrire sous la forme $P = aP'$, $Q = bQ'$ et $R = cR'$, où a , b et c sont trois éléments non nuls de A , et où P' , Q' et R' sont primitifs. Comme P et Q sont premiers entre eux, il est clair que P' et Q' le sont, ainsi que a et b .

De plus, $P = aP'$ divise $QR = bcQ'R'$, et, d'après le lemme 1, $Q'R'$ est primitif. Le lemme 2 montre alors que a divise bc dans A , et que P' divise $Q'R'$ dans $A[X]$.

Puisque a divise bc dans A , et que a et b sont premiers entre eux, a divise c dans A , car A est factoriel.

D'autre part, P' et Q' , étant premiers entre eux dans $A[X]$, le sont dans $K[X]$, d'après le lemme 2. La propriété de Gauss étant valable dans l'anneau $K[X]$ (cf. cor. 3 du th. 1.5), P' divise R' dans $K[X]$. Le lemme 2 montre alors que P' divise R' dans $A[X]$.

Finalement, le polynôme $P = aP'$ divise le polynôme $R = cR'$ dans $A[X]$, ce qui achève la démonstration du théorème.

PROPOSITION 2.4. — Règle d'irréductibilité d'Eisenstein. — Soient A un anneau factoriel, et

$$P = a_0 + a_1X + \dots + a_nX^n$$

un élément non constant de $A[X]$. On suppose qu'il existe un élément irréductible p de A divisant a_0, a_1, \dots, a_{n-1} , ne divisant pas a_n , et tel que p^2 ne divise pas a_0 . Alors P est un élément irréductible de l'anneau $A[X]$.

Supposons par l'absurde qu'il existe deux éléments non constants

$$Q = b_0 + b_1X + \dots + b_qX^q$$

et

$$R = c_0 + c_1X + \dots + c_rX^r$$

de $A[X]$ tels que $P = QR$. Puisque $a_0 = b_0c_0$, et que p est irréductible, p divise l'un des deux éléments b_0 et c_0 . Supposons par exemple que p divise b_0 . Puisque p^2 ne divise pas a_0 , p ne divise pas c_0 . Ainsi, p est premier avec c_0 . Or, pour tout entier $s \in [1, q]$,

$$a_s = b_0c_s + b_1c_{s-1} + \dots + b_{s-1}c_1 + b_sc_0.$$

Puisque p divise b_0 et que p est premier avec c_0 , on montre par récurrence sur s que p divise b_s . Finalement, p divise b_q , donc p divise $a_n = b_qc_r$, ce qui contredit l'hypothèse.

EXEMPLES.

1. Soient p_1, p_2, \dots, p_r des nombres premiers distincts deux à deux, et $a = p_1p_2 \dots p_r$. Alors, pour tout entier strictement positif n , le polynôme $X^n - a$ est irréductible sur \mathbb{Q} .

2. Soit p un nombre premier. Alors le polynôme cyclotomique

$$F_p = 1 + X + \dots + X^{p-1}$$

est irréductible sur \mathbb{Q} .

Ici, la règle d'Eisenstein ne s'applique pas directement; mais l'irréductibilité de F_p équivaut à celle du polynôme $G_p = F_p(X + 1)$.

Or, puisque $F_p = \frac{X^p - 1}{X - 1}$,

$$G_p = \frac{(X + 1)^p - 1}{(X + 1) - 1} = C_p^{p-1} + C_p^{p-2}X + \dots + C_p^1 X^{p-2} + X^{p-1}.$$

Comme p divise C_p^q pour tout entier $q \in [1, p - 1]$, la règle d'Eisenstein s'applique.

Exercices conseillés : 1 à 8.

§ 2. POLYNÔMES ET FRACTIONS RATIONNELLES À PLUSIEURS INDÉTERMINÉES

PROPOSITION 2.5. — Sous-algèbre unitaire engendrée par une famille d'éléments commutant deux à deux. — Soient E une A -algèbre associative unitaire, et $a = (a_i)_{i \in I}$ une famille finie d'éléments de E commutant deux à deux. On désigne par S l'ensemble \mathbf{N}^I des applications de I dans \mathbf{N} , et, pour tout élément s de S , on pose

$$a^s = \prod_{i \in I} a_i^{s(i)}.$$

(Lorsque $s = 0$, on convient que le second membre désigne l'élément neutre de E .)

1. Pour tout couple (s, t) d'éléments de S ,

$$(1) \quad a^s a^t = a^t a^s = a^{s+t}.$$

2. La sous-algèbre unitaire E' de E engendrée par la famille $a = (a_i)_{i \in I}$ n'est autre que l'ensemble des combinaisons linéaires des éléments a^s , où s parcourt S . De plus, E' est une algèbre commutative.

Assertion 1. — Pour tout élément s de S , posons

$$|s| = \sum_{i \in I} s(i).$$

La formule (1) s'établit facilement par récurrence sur $|s|$.

Assertion 2. — Désignons par E'_1 l'ensemble des combinaisons linéaires des éléments a^s . Il est clair que E'_1 est contenu dans E' , et il découle aussitôt de la formule (1) que E' est contenu dans E'_1 . La même formule montre alors que E' est commutative.

Nous sommes donc amené à effectuer la construction suivante :

Soient A un anneau commutatif unitaire, I un ensemble fini non vide, et S l'ensemble N^I des applications de I dans N . On considère le A -module libre $A^{(S)}$ muni de sa base canonique $(e_s)_{s \in S}$, et la structure de A -algèbre définie sur $A^{(S)}$ par la table de multiplication

$$(1) \quad e_s \cdot e_t = e_{s+t},$$

pour tout couple (s, t) d'éléments de S .

Il résulte immédiatement de la formule (1) et de la proposition I.3.38 que cette algèbre est associative et commutative, et qu'elle admet e_0 pour élément unité. Cette algèbre unitaire se note $P_I(A)$.

Ainsi, tout élément P de $P_I(A)$ s'écrit d'une manière et d'une seule sous la forme

$$P = \sum_{s \in S} \alpha_s e_s,$$

où, pour tout élément s de S , α_s est un scalaire. Les scalaires α_s s'appellent coefficients de P .

DÉFINITION 2.5. — Algèbre des polynômes construits sur un ensemble fini. — Les éléments de $P_I(A)$ s'appellent polynômes à coefficients dans A construits sur I , et l'algèbre unitaire $P_I(A)$ s'appelle algèbre des polynômes à coefficients dans A construits sur I .

Un polynôme dont tous les coefficients sauf au plus un sont nuls est appelé monôme.

L'application de A dans $P_I(A)$ qui à tout scalaire α associe le monôme αe_0 définit un isomorphisme de l'anneau unitaire A sur la sous-algèbre unitaire Ae_0 de $P_I(A)$. On identifiera désormais A et Ae_0 . En particulier, e_0 sera noté 1, où 1 désigne l'élément unité de l'anneau A .

Soit, pour tout élément i de I , s_i l'application de I dans N définie par les relations $s_i(i) = 1$ et $s_i(i') = 0$ si $i \neq i'$. Pour tout élément s de S ,

$$(2) \quad e_s = \prod_{i \in I} e_i^{s(i)} = e^s,$$

où e désigne la famille $(e_i)_{i \in I}$.

Les éléments e_i s'appellent indéterminées construites sur I et se notent souvent X_i .

L'algèbre unitaire $P_I(A)$ se note alors $A[X_i]_{i \in I}$. En particulier, lorsque $I = [1, n]$, l'algèbre unitaire $P_I(A)$ s'appelle algèbre des polynômes à n indéterminées à coefficients dans A , et se note $A[X_1, X_2, \dots, X_n]$.

Plus particulièrement encore, lorsque $n = 1$, $P_I(A)$ n'est autre que l'algèbre $P(A)$ des polynômes à une indéterminée à coefficients dans A .

PROPOSITION 2.6. — Propriétés de l'algèbre des polynômes. — Soient A un anneau commutatif unitaire, I un ensemble fini non vide, et $A[X_i]_{i \in I}$ l'algèbre des polynômes à coefficients dans A construits sur I .

1. L'application $j : i \mapsto X_i$ est une injection, dite canonique, de I dans $A[X_i]_{i \in I}$. La sous-algèbre unitaire de $A[X_i]_{i \in I}$ engendrée par les éléments X_i , où i parcourt I , n'est autre que $A[X_i]_{i \in I}$.

2. L'algèbre $A[X_i]_{i \in I}$ possède la propriété universelle suivante :

Pour toute A -algèbre associative unitaire E , et pour toute famille finie $a = (a_i)_{i \in I}$ d'éléments de E commutant deux à deux, il existe un morphisme f et un seul de l'algèbre unitaire $A[X_i]_{i \in I}$ dans l'algèbre unitaire E tel que, pour tout élément i de I ,

$$(3) \quad f(X_i) = a_i.$$

Alors, pour tout élément s de S ,

$$(4) \quad f(X^s) = \prod_{i \in I} a_i^{s(i)} = a^s.$$

L'image de f n'est autre que la sous-algèbre unitaire de E engendrée par les éléments $(a_i)_{i \in I}$.

Le noyau du morphisme f est un idéal de l'algèbre $A[X_i]_{i \in I}$, dont les éléments sont appelés relations algébriques entre les éléments a_i .

Lorsque ce noyau est réduit à $\{0\}$, on dit que la famille $(a_i)_{i \in I}$ est algébriquement libre (sur A), ou encore que les éléments a_i sont algébriquement indépendants (sur A). Dans le cas contraire, on dit que les éléments a_i sont algébriquement dépendants.

Assertion 1. — D'après la formule (2), la sous-algèbre unitaire de $A[X_i]_{i \in I}$ engendrée par les éléments X_i contient tous les éléments X^s , où s parcourt S . Elle est donc égale à $A[X_i]_{i \in I}$, puisque tout polynôme est une combinaison linéaire des éléments X^s .

Assertion 2. — Unicité de f . — Puisque f est un morphisme d'algèbres unitaires, les relations (2) et (3) montrent que, pour tout élément s de S , $f(X^s)$ est nécessairement donné par la formule (4). L'unicité de f en découle, puisque f est linéaire.

Existence de f . — Puisque $(X^s)_{s \in S}$ est une base de $A[X_i]_{i \in I}$, il existe une application linéaire f et une seule de $A[X_i]_{i \in I}$ dans E telle que, pour tout élément s de S ,

$$(5) \quad f(X^s) = \prod_{i \in I} a_i^{s(i)}.$$

Il reste à prouver que f est un morphisme d'algèbres. Puisque f est linéaire, il suffit de montrer que, pour tout couple (s, t) d'éléments de S ,

$$f(X^s \cdot X^t) = f(X^s) \cdot f(X^t),$$

ce qui résulte aussitôt de la formule

$$X^s \cdot X^t = X^{s+t},$$

de la relation (4), de l'associativité de l'algèbre E , et du fait que les éléments a_i commutent deux à deux (cf. formule (1) de la prop. 2.5).

COROLLAIRE 1. — Isomorphismes d'équipotence. — Soient A un anneau commutatif unitaire, I et J deux ensembles finis non vides ayant même cardinal. Alors les algèbres unitaires $\mathbf{P}_I(A)$ et $\mathbf{P}_J(A)$ sont isomorphes. Plus précisément, soit φ une bijection de I sur J ; il existe un morphisme f et un seul de $\mathbf{P}_I(A)$ dans $\mathbf{P}_J(A)$ tel que, pour tout élément i de I , $f(X_i) = Y_{\varphi(i)}$, où $(X_i)_{i \in I}$ et $(Y_j)_{j \in J}$ désignent les familles d'indéterminées construites respectivement sur I et sur J . De plus, f est un isomorphisme de $\mathbf{P}_I(A)$ sur $\mathbf{P}_J(A)$.

L'existence et l'unicité de f résultent de l'assertion 2. Soit ψ la bijection réciproque de φ ; il existe de même un morphisme g et un seul de $\mathbf{P}_J(A)$ dans $\mathbf{P}_I(A)$ tel que, pour tout élément j de J , $g(Y_j) = X_{\psi(j)}$. Il est clair que f et g sont deux isomorphismes réciproques.

COROLLAIRE 2. — Isomorphismes d'associativité. — Soient A un anneau commutatif unitaire, H un ensemble fini non vide, et (I, J) une partition de H . On désigne par $(X_h)_{h \in H}$, $(Y_i)_{i \in I}$ et $(Z_j)_{j \in J}$ les familles d'indéterminées construites respectivement sur H , I et J . Il existe alors un morphisme f et un seul de la A -algèbre unitaire $\mathbf{P}_H(A)$ sur la A -algèbre unitaire sous-jacente à la $\mathbf{P}_J(A)$ -algèbre unitaire $\mathbf{P}_I(\mathbf{P}_J(A))$ tel que, pour tout élément i de I , $f(X_i) = Y_i$, et que, pour tout élément j de J , $f(X_j) = Z_j$. De plus, f est un isomorphisme de A -algèbres unitaires, dit canonique.

On construirait de même un isomorphisme canonique de $\mathbf{P}_H(A)$ sur $\mathbf{P}_J(\mathbf{P}_I(A))$. Grâce à ces isomorphismes, on identifie les A -algèbres unitaires $\mathbf{P}_H(A)$, $\mathbf{P}_I(\mathbf{P}_J(A))$ et $\mathbf{P}_J(\mathbf{P}_I(A))$.

En particulier, pour tout couple (n, p) d'entiers strictement positifs, on peut identifier les A -algèbres unitaires $A[X_1, X_2, \dots, X_n, X_{n+1}, \dots, X_{n+p}]$ et $A[X_1, X_2, \dots, X_n][X_{n+1}, \dots, X_{n+p}]$.

Plus particulièrement encore, l'algèbre unitaire $A[X_1, X_2, \dots, X_n, X_{n+1}]$ s'identifie à l'algèbre unitaire $B[X_{n+1}]$, où B désigne l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$.

L'existence et l'unicité de f résultent aussitôt de l'assertion 2.

Désignons par S , T et U les ensembles \mathbf{N}^H , \mathbf{N}^I et \mathbf{N}^J . Puisque (I, J) est une partition de H , il est clair que S s'identifie à $T \times U$. Tout élément P de $\mathbf{P}_H(A)$ s'écrit donc d'une manière et d'une seule sous la forme

$$(1) \quad P = \sum_{(t,u) \in T \times U} \alpha_{t,u} X^t X^u,$$

où, pour tout élément t de T ,

$$(2) \quad X^t = \prod_{i \in I} X_i^{t(i)},$$

et où, pour tout élément u de U ,

$$(3) \quad X^u = \prod_{j \in J} X_j^{u(j)}.$$

Puisque f est un morphisme, il découle des relations (1), (2) et (3) que

$$(1') \quad f(P) = \sum_{t \in T} \left(\sum_{u \in U} \alpha_{t,u} Z^u \right) Y^t,$$

où, pour tout élément t de T ,

$$(2') \quad Y^t = \prod_{i \in I} Y_i^{t(i)},$$

et où, pour tout élément u de U ,

$$(3') \quad Z^u = \prod_{j \in J} Z_j^{u(j)}.$$

De la formule (1'), nous déduisons aussitôt que le noyau du morphisme f est réduit à $\{0\}$, et que f est surjectif.

REMARQUE 1. — Changement d'anneau de base. — Soient B et B' deux A -algèbres commutatives unitaires, et j un morphisme de B dans B' . Il existe un morphisme \tilde{j} et un seul de la A -algèbre unitaire $B[X_i]_{i \in I}$ dans la A -algèbre unitaire $B'[X_i]_{i \in I}$ prolongeant j et tel que, pour tout élément i de I , $\tilde{j}(X_i) = X_i$. La valeur de \tilde{j} sur un polynôme $P = \sum_{s \in S} \beta_s X^s$ est donnée par la formule

$$(1) \quad \tilde{j} \left(\sum_{s \in S} \beta_s X^s \right) = \sum_{s \in S} j(\beta_s) X^s.$$

D'une part, il est évident que \tilde{j} est nécessairement défini par la formule (1). Réciproquement, l'application \tilde{j} ainsi définie est linéaire. Enfin, pour tout couple (P, Q) d'éléments de $B[X_i]_{i \in I}$,

$$\tilde{j}(PQ) = \tilde{j}(P)\tilde{j}(Q).$$

En effet, les applications $(P, Q) \mapsto \tilde{j}(PQ)$ et $(P, Q) \mapsto \tilde{j}(P)\tilde{j}(Q)$ sont A -bilinéaires, et elles coïncident lorsque $P = \beta X^s$ et $Q = \gamma X^t$, où β et γ appartiennent à B , et où s et t appartiennent à S .

REMARQUE 2. — L'isomorphisme entre l'anneau unitaire $A[X_1, X_2, \dots, X_{n+1}]$ et l'anneau unitaire $B[X_{n+1}]$, où $B = A[X_1, X_2, \dots, X_n]$, est d'une grande importance pour la théorie des polynômes à plusieurs indéterminées, car il permet souvent d'effectuer des raisonnements par récurrence sur le nombre d'indéterminées. On notera qu'il est nécessaire pour cela de se placer dans le cadre de la théorie des polynômes à coefficients dans un anneau commutatif unitaire, puisque, même si A est un corps, $A[X_1, X_2, \dots, X_n]$ n'en est pas un.

Nous allons illustrer cette méthode :

THÉORÈME 2.6. — Permanence de l'intégrité. — Soient A un anneau commutatif unitaire, et I un ensemble fini non vide. Si l'anneau A est intègre, il en est de même de l'anneau $A[X_i]_{i \in I}$ des polynômes à coefficients dans A construits sur I .

En particulier, l'anneau $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans un corps commutatif K est intègre.

Lorsque $\text{card}(I) = 1$, le théorème n'est autre que le corollaire de la proposition 2.1. Le cas général s'en déduit aussitôt par récurrence sur $\text{card}(I)$, en utilisant ce même corollaire.

COROLLAIRE 1. — Permanence de la divisibilité et de l'irréductibilité. — *On suppose que l'anneau A est intègre.*

1. Soient n un entier naturel non nul et α un élément non nul de A . Pour qu'un élément P de $A[X_1, X_2, \dots, X_n]$ divise α dans $A[X_1, X_2, \dots, X_n]$, il faut et il suffit que P soit un élément β de A et que β divise α dans A . Par suite, α est irréductible dans A si et seulement si α est irréductible dans $A[X_1, X_2, \dots, X_n]$.

2. Soient n et p deux entiers naturels non nuls tels que $p < n$, et Q un élément non nul de $A[X_1, X_2, \dots, X_p]$. Pour qu'un élément P de $A[X_1, X_2, \dots, X_n]$ divise Q dans $A[X_1, X_2, \dots, X_n]$, il faut et il suffit que P divise Q dans $A[X_1, X_2, \dots, X_p]$. Par suite, Q est irréductible dans $A[X_1, X_2, \dots, X_p]$ si et seulement si Q est irréductible dans $A[X_1, X_2, \dots, X_n]$.

L'assertion 1 se démontre par récurrence sur l'entier n , à l'aide du corollaire 2 de la proposition 2.1.

L'assertion 2 s'obtient en remplaçant dans l'assertion 1 l'anneau A par l'anneau $B = A[X_1, X_2, \dots, X_p]$.

COROLLAIRE 2. — *On suppose que l'anneau A est intègre. Soient P un élément non nul de $A[X_1, X_2, \dots, X_n]$ et Q un élément non nul de*

$$B = A[X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n].$$

Si le coefficient dominant de P , considéré comme élément de $B[X_j]$, est un élément inversible α de A , alors P et Q sont premiers entre eux dans l'anneau $A[X_1, X_2, \dots, X_n]$.

En effet, l'anneau B est intègre; par suite, tout diviseur commun à P et Q dans $A[X_1, X_2, \dots, X_n]$ est un élément non nul c de B (cf. cor. 1). Il est immédiat que c divise dans B le coefficient dominant α de P . Puisque α est un élément de A , c appartient à A (cf. cor. 1), et divise α dans A . Puisque α est inversible, il en est de même de c , ce qui prouve que P et Q sont premiers entre eux dans $A[X_1, X_2, \dots, X_n]$.

EXEMPLES.

1. Soient K un corps commutatif, P un élément non nul de $K[X_j]$ et Q un élément non nul de $K[X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$. Alors P et Q sont premiers entre eux dans $K[X_1, X_2, \dots, X_n]$.

2. Si l'anneau A est intègre, les polynômes $P_{ij} = X_i - X_j$, où $i, j \in [1, n]$ et $i < j$, sont premiers entre eux deux à deux dans $A[X_1, X_2, \dots, X_n]$.

3. Soient K un corps commutatif, P et Q deux éléments premiers entre eux de $B = K[X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$. Alors le polynôme $PX_j + Q$ est irréductible dans $K[X_1, X_2, \dots, X_n]$.

En effet, l'anneau B étant intègre, on peut appliquer le corollaire 2 de la proposition 2.1.

DÉFINITION 2.6. — Polynômes homogènes. — Soient A un anneau commutatif unitaire, I un ensemble fini non vide, et $A[X_i]_{i \in I}$ l'algèbre des polynômes à coefficients dans A construits sur I . Pour tout élément s de $S = \mathbb{N}^I$, on appelle longueur de s le nombre entier naturel $|s| = \sum_{i \in I} s(i)$, et, pour tout entier naturel p , on note S_p l'ensemble des éléments s de S tels que $|s| = p$. Les ensembles S_p , où p parcourt \mathbb{N} , constituent une partition de S . Pour tout $p \in \mathbb{N}$, on désigne par H_p le sous-module de $A[X_i]_{i \in I}$ engendré par les monômes X^s , où s parcourt S_p . Les éléments de H_p sont appelés polynômes p -homogènes. On dit enfin qu'un polynôme est homogène s'il appartient à l'un des sous-modules H_p .

PROPOSITION 2.7. — Composantes homogènes d'un polynôme.

1. Le A -module $A[X_i]_{i \in I}$ est somme directe des sous-modules H_p , où p parcourt \mathbb{N} . Ainsi, tout élément P de $A[X_i]_{i \in I}$ peut s'écrire d'une manière et d'une seule sous la forme

$$P = \sum_{p=0}^{+\infty} U_p,$$

où, pour tout entier naturel p , U_p est un polynôme p -homogène. Le polynôme U_p s'appelle composante p -homogène du polynôme P .

2. Soient U un polynôme r -homogène et V un polynôme s -homogène. Alors le polynôme UV est $(r + s)$ -homogène.

3. Soient P et Q deux éléments de $A[X_i]_{i \in I}$,

$$P = \sum_{r=0}^{+\infty} U_r \quad \text{et} \quad Q = \sum_{s=0}^{+\infty} V_s$$

leurs décompositions en composantes homogènes. Alors, pour tout entier naturel p , la composante p -homogène W_p du produit PQ est donnée par la formule

$$W_p = \sum_{r+s=p} U_r V_s.$$

4. Soient j un élément de $[1, n]$ et P un élément de $A[X_1, X_2, \dots, X_n]$, écrit sous la forme

$$P = \sum_{r=0}^{+\infty} Q_r X_j^r,$$

où (Q_r) est une suite à support fini d'éléments de

$$B = A[X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n].$$

Alors, pour tout entier naturel p , pour que P soit p -homogène, il faut et il suffit que, pour tout entier r strictement supérieur à p , $Q_r = 0$, et que, pour tout entier $r \in [0, p]$, Q_r soit $(p - r)$ -homogène dans B .

L'assertion 1 découle de la proposition I.3.23, qui s'étend aussitôt au cas des modules.

L'assertion 2 est immédiate, puisque, pour tout couple (s, t) d'éléments de S ,

$$X^s \cdot X^t = X^{s+t},$$

et que

$$|s + t| = |s| + |t|.$$

L'assertion 3 résulte aussitôt de l'assertion 2.

L'assertion 4 s'obtient en décomposant, pour tout entier naturel r , Q_r en ses composantes homogènes dans B , et en écrivant que P est p -homogène.

REMARQUE. — Lorsque A est un corps commutatif, on notera que le sous-espace vectoriel H_p est de dimension finie, et que sa dimension est égale à $\text{card}(S_p)$, c'est-à-dire au nombre de combinaisons avec répétitions de n éléments p à p , où n désigne le cardinal de I . Ce nombre est égal à C_{p+n-1}^p . (cf. sous-paragraphe 3 du § 1.10).

DÉFINITION 2.7. — **Degré d'un polynôme.** — Soit $P = \sum_{p=0}^{+\infty} U_p$ un élément de $A[X_i]_{i \in I}$, où, pour tout entier naturel p , U_p est p -homogène.

Si P est non nul, on appelle degré total de P , ou, plus simplement, degré, de P le plus grand des entiers p tels que U_p soit non nul.

Si P est nul, on appelle degré de P l'élément $-\infty$.

Le degré d'un polynôme P se note $d^0(P)$.

On remarquera que si P est un polynôme p -homogène non nul, alors P est de degré p ; c'est pourquoi, par abus de langage, les polynômes p -homogènes sont encore appelés polynômes homogènes de degré p .

PROPOSITION 2.8. — **Degré d'une somme, degré d'un produit.** — Soient P et Q deux éléments de $A[X_i]_{i \in I}$. Alors

$$(1) \quad d^0(P + Q) \leq \sup [d^0(P), d^0(Q)],$$

avec égalité si $d^0(P) \neq d^0(Q)$;

$$(2) \quad d^0(PQ) \leq d^0(P) + d^0(Q),$$

avec égalité si l'anneau A est intègre.

Le cas de la somme est immédiat, ainsi que l'inégalité (2). Supposons donc que A est intègre; considérons un polynôme P de degré p et un polynôme Q de degré q . Écartons le cas trivial où l'un de ces polynômes est nul. D'après la proposition 2.7, la composante $(p + q)$ -homogène W_{p+q} de PQ n'est autre que $U_p V_q$, où U_p désigne la composante p -homogène de P , et V_q la composante q -homogène de Q . Puisque A est intègre, il en est de même de $A[X_i]_{i \in I}$ (cf. th. 2.6). Or, par hypothèse, U_p et V_q sont non nuls; il en est donc de même de W_{p+q} .

DÉFINITION 2.8. — Degrés partiels. — Soient A un anneau commutatif unitaire, H un ensemble fini non vide, et (I, J) une partition de H . On désigne par B l'anneau unitaire $\mathbf{P}_J(A)$. On sait que l'anneau $\mathbf{P}_H(A)$ s'identifie à l'anneau $\mathbf{P}_I(B)$. On appelle degré partiel relativement à I d'un élément P de $\mathbf{P}_H(A)$, et on note $d_I^\circ(P)$, le degré total de P considéré comme élément de l'anneau $\mathbf{P}_I(B)$ des polynômes à coefficients dans B construits sur I .

Lorsque I est réduit au seul élément i , $d_I^\circ(P)$ se note plus simplement $d_i^\circ(P)$, et s'appelle degré de P par rapport à l'indéterminée X_i .

L'application $P \mapsto d_I^\circ(P)$ possède bien évidemment les propriétés énoncées dans la proposition 2.1.

Considérons maintenant un corps commutatif K , et l'algèbre $K[X_i]_{i \in I}$ des polynômes à coefficients dans K construits sur un ensemble fini non vide I . D'après le théorème 2.6, l'anneau $K[X_i]_{i \in I}$ est intègre. D'autre part, il résulte aussitôt de la formule $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$ que les seuls éléments inversibles de cet anneau sont les polynômes de degré 0. Nous pouvons donc appliquer à cet anneau le théorème d'existence du corps des quotients (cf. th. I.2.7). Nous obtenons ainsi le

THÉORÈME 2.7. — Corps des fractions rationnelles à plusieurs indéterminées. Il existe un corps commutatif, appelé corps des fractions rationnelles à coefficients dans K construites sur I et noté $K(X_i)_{i \in I}$, possédant les propriétés suivantes :

- a) L'anneau $K[X_i]_{i \in I}$ est un sous-anneau unitaire du corps $K(X_i)_{i \in I}$.
- b) Le corps $K(X_i)_{i \in I}$ est engendré par l'anneau $K[X_i]_{i \in I}$, c'est-à-dire que tout élément R de $K(X_i)_{i \in I}$ peut s'écrire sous la forme $R = PQ^{-1}$, où P et Q sont des polynômes, Q étant non nul.

Deux tels corps sont isomorphes.

Lorsque $I = [1, n]$, $K(X_i)_{i \in I}$ se note $K(X_1, X_2, \dots, X_n)$, et s'appelle corps des fractions rationnelles à n indéterminées à coefficients dans K .

Comme dans le cas des fractions rationnelles à une indéterminée, $K(X_i)_{i \in I}$ est aussi une K -algèbre.

Soient maintenant H un ensemble fini non vide, et (I, J) une partition de H . Le sous-corps de $K(X_h)_{h \in H}$ engendré par les indéterminées X_h n'est autre que $K(X_h)_{h \in H}$. Il en résulte que si K' désigne le corps $K(X_i)_{i \in I}$, le corps $K'(X_j)_{j \in J}$ n'est autre que $K(X_h)_{h \in H}$. En particulier, le corps $K(X_1, X_2, \dots, X_n, X_{n+1})$ s'identifie au corps $K'(X_{n+1})$, où K' désigne le corps $K(X_1, X_2, \dots, X_n)$.

La définition et les propriétés du degré d'une fraction rationnelle (cf. prop. 1.7) s'étendent aussitôt.

DÉFINITION 2.9. — Fractions rationnelles homogènes. — Soient K un corps commutatif, et I un ensemble fini non vide. On dit qu'un élément R de $K(X_i)_{i \in I}$ est homogène s'il existe un couple (P, Q) d'éléments homogènes de $K[X_i]_{i \in I}$, $Q \neq 0$, tel que $R = \frac{P}{Q}$.

Soit p un entier rationnel. On dit que R est p -homogène si R est homogène, et si $d^0(R) = p$. Pour toute décomposition $R = \frac{P}{Q}$ de la forme précédente, l'entier rationnel p est donc égal à $d^0(P) - d^0(Q)$.

Il découle de la proposition 2.7 que les fractions rationnelles p -homogènes constituent un sous-espace vectoriel, noté H'_p , de l'espace vectoriel $K(X_i)_{i \in I}$, et que le produit d'une fraction rationnelle p -homogène par une fraction rationnelle q -homogène est $(p + q)$ -homogène.

Passons maintenant à l'étude des idéaux de $K[X_1, X_2, \dots, X_n]$. Comme nous l'avons déjà vu (cf. remarque suivant le th. 2.2), ces idéaux ne sont pas nécessairement principaux lorsque n est strictement supérieur à 1. Cependant, nous pouvons énoncer le

THÉORÈME 2.8. — Théorème de permanence de Hilbert. — Soient A un anneau commutatif unitaire, et I un ensemble fini non vide. Si A est noethérien, l'anneau $A[X_i]_{i \in I}$ des polynômes à coefficients dans A construits sur I est encore noethérien.

En particulier, l'anneau $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans un corps commutatif K est noethérien.

Cela découle du théorème 2.3, par récurrence sur $\text{card}(I)$. De même, on déduit aussitôt des théorèmes 2.4 et 2.5 le résultat suivant :

THÉORÈME 2.9. — Permanence de la factorialité. — Soient A un anneau commutatif unitaire, et I un ensemble fini non vide. Si A est factoriel, l'anneau $A[X_i]_{i \in I}$ des polynômes à coefficients dans A construits sur I est encore factoriel.

En particulier, l'anneau $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans un corps commutatif K est factoriel. Les éléments de $K[X_1, X_2, \dots, X_n]$, et, plus généralement, les éléments de $K(X_1, X_2, \dots, X_n)$, peuvent être décomposés en produits de facteurs irréductibles.

On peut donc appliquer les corollaires du théorème 2.4 :

— Tout élément non nul R de $K(X_1, X_2, \dots, X_n)$ peut s'écrire sous la forme $R = \frac{P}{Q}$, où P et Q sont deux éléments de $K[X_1, X_2, \dots, X_n]$ non nuls et premiers entre eux.

— Si un élément non nul P de $K[X_1, X_2, \dots, X_n]$ est divisible par des éléments non nuls P_1, P_2, \dots, P_r de $K[X_1, X_2, \dots, X_n]$, premiers entre eux deux à deux, alors P est divisible par le produit $P_1 P_2 \dots P_r$.

— Tout ensemble de polynômes à n indéterminées non tous nuls admet un P. G. C. D.

— Tout ensemble fini de polynômes à n indéterminées non tous nuls admet un P. P. C. M.

§ 3. FONCTIONS POLYNOMIALES ET RATIONNELLES DE PLUSIEURS VARIABLES

DÉFINITION 2.10. — Substitutions dans un polynôme. — Soient $A[X_i]_{i \in I}$ l'algèbre des polynômes à coefficients dans A construits sur un ensemble fini non vide I , E une A -algèbre associative unitaire, et $a = (a_i)_{i \in I}$ une famille d'éléments de E commutant deux à deux. On sait (cf. prop. 2.6) qu'il existe un morphisme δ_a et un seul de l'algèbre unitaire $A[X_i]_{i \in I}$ dans l'algèbre unitaire E tel que, pour tout $i \in I$, $\delta_a(X_i) = a_i$. Soit P un élément de $A[X_i]_{i \in I}$, écrit sous la forme

$$P = \sum_{s \in S} \alpha_s X^s ;$$

alors

$$\delta_a(P) = \sum_{s \in S} \alpha_s a^s.$$

C'est pourquoi on dit que l'élément $\delta_a(P)$ est obtenu en substituant les éléments a_i de E aux indéterminées X_i dans le polynôme P .

DÉFINITION 2.11. — Fonctions polynomiales. — Soit E une A -algèbre associative, COMMUTATIVE et unitaire. Étant donné un élément P de $A[X_i]_{i \in I}$, on note \tilde{P} l'application de E^I dans E qui à toute famille $a = (a_i)_{i \in I}$ associe l'élément $\delta_a(P)$.

Soit maintenant B une partie de E^I . On dit qu'une application f de B dans E est une fonction polynomiale s'il existe un élément P de $A[X_i]_{i \in I}$ tel que, pour tout élément a de B , $f(a) = \tilde{P}(a)$.

C'est pourquoi, étant donné un élément P de $A[X_i]_{i \in I}$, la fonction \tilde{P} s'appelle fonction polynomiale sur E^I associé à P : pour tout élément a de E^I , l'élément $\tilde{P}(a)$, valeur au point a de la fonction polynomiale P , s'appelle encore valeur de P en a .

REMARQUE. — On suppose que $E = A$. Lorsque $P = \alpha$, où $\alpha \in A$, \tilde{P} n'est autre que la fonction constante α . C'est pourquoi la composante 0-homogène d'un polynôme P s'appelle aussi terme constant de P . De plus, $U_0 = \tilde{P}(0, 0, \dots, 0)$.

DÉFINITION 2.12. — Applications polynomiales. — Soient E une A -algèbre associative commutative unitaire, I et J deux ensembles finis non vides, et B une partie de E^I . On dit qu'une application f de B dans E^J est une application polynomiale si, pour tout élément j de J , la fonction $\text{pr}_j \circ f$ est une fonction polynomiale sur B .

Cela revient à dire qu'il existe une famille $(P_j)_{j \in J}$ d'éléments de $A[X_i]_{i \in I}$ telle que, pour tout élément a de B ,

$$f(a) = (\tilde{P}_j(a))_{j \in J}.$$

PROPOSITION 2.9. — Propriétés des substitutions dans les polynômes. — Soit A une algèbre associative, commutative et unitaire. Alors l'application de $A[X_i]_{i \in I}$ dans l'algèbre $\mathcal{F}(E^I, E)$ des applications de E^I dans E qui à tout polynôme P associe la fonction polynomiale \tilde{P} est un morphisme d'algèbres unitaires.

EXEMPLES.

1. On prend pour E un corps commutatif K . Lorsque $K = \mathbf{R}$, ou que $K = \mathbf{C}$, la notion de fonction polynomiale sur K^n définie dans ce paragraphe coïncide avec celle qui a été introduite au § I.5.5.

2. **Substitutions de polynômes dans un polynôme.** — On considère un anneau commutatif unitaire A , et deux entiers strictement positifs n et p . En prenant pour E l'algèbre $A[Y_1, Y_2, \dots, Y_p]$, nous voyons que, pour toute famille (Q_1, Q_2, \dots, Q_n) d'éléments de $A[Y_1, Y_2, \dots, Y_p]$, il existe un morphisme f et un seul de $A[X_1, X_2, \dots, X_n]$ dans $A[Y_1, Y_2, \dots, Y_p]$ tel que, pour tout $i \in [1, n]$, $f(X_i) = Q_i$. Pour tout élément P de $A[X_1, X_2, \dots, X_n]$, $f(P)$ est l'élément de $A[Y_1, Y_2, \dots, Y_p]$ obtenu en substituant les polynômes Q_i aux indéterminées X_i dans le polynôme P ; on le note $P(Q_1, Q_2, \dots, Q_n)$. Ainsi, l'application $P \mapsto P(Q_1, Q_2, \dots, Q_n)$ est un morphisme de l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$ dans l'algèbre unitaire $A[Y_1, Y_2, \dots, Y_p]$.

En particulier, lorsque $E = A[X_1, X_2, \dots, X_n]$ et que, pour tout élément i de $[1, n]$, $Q_i = X_i$, $P(Q_1, Q_2, \dots, Q_n) = P$; c'est pourquoi le polynôme P se note encore $P(X_1, X_2, \dots, X_n)$.

La notation $P(Q_1, Q_2, \dots, Q_n)$ est suggérée par la

PROPOSITION 2.10. — Propriétés de la composition des polynômes. — Pour toute A -algèbre associative commutative unitaire E , la fonction polynomiale sur E^p associée au polynôme $R = P(Q_1, Q_2, \dots, Q_n)$ n'est autre que l'application qui à tout élément a de E^p associe l'élément $\tilde{P}(\tilde{Q}_1(a), \tilde{Q}_2(a), \dots, \tilde{Q}_n(a))$ de E . Autrement dit,

$$\tilde{R}(a) = \tilde{P}(\tilde{Q}_1(a), \tilde{Q}_2(a), \dots, \tilde{Q}_n(a)).$$

Le raisonnement est calqué sur celui de la proposition 2.9. Nous nous ramenons cette fois à prouver la formule (1) lorsque $P = X_i$, où $i \in [1, n]$, ce qui est trivial.

COROLLAIRE 1. — Associativité de la substitution. — Soient P un élément de $A[X_1, X_2, \dots, X_n]$, Q_1, Q_2, \dots, Q_n des éléments de $A[Y_1, Y_2, \dots, Y_p]$ et R_1, R_2, \dots, R_p des éléments de $A[Z_1, Z_2, \dots, Z_q]$. Alors

$$\begin{aligned} & [P(Q_1, Q_2, \dots, Q_n)](R_1, R_2, \dots, R_p) \\ &= P[Q_1(R_1, R_2, \dots, R_p), Q_2(R_1, R_2, \dots, R_p), \dots, Q_n(R_1, R_2, \dots, R_p)]. \end{aligned}$$

Il suffit d'appliquer la proposition au cas où

$$E = A[Z_1, Z_2, \dots, Z_q] \quad \text{et où} \quad a = (R_1, R_2, \dots, R_p).$$

COROLLAIRE 2. — Caractérisation des polynômes homogènes.

1. Soient P un élément de $A[X_1, X_2, \dots, X_n]$, $(U_m)_{m \in \mathbb{N}}$ la famille de ses composantes homogènes, et $P(TX_1, TX_2, \dots, TX_n)$ l'élément de $A[X_1, X_2, \dots, X_n, T]$ obtenu en substituant les polynômes TX_i aux indéterminées X_i dans le polynôme P . Alors

$$(1) \quad P(TX_1, TX_2, \dots, TX_n) = \sum_{m=0}^{+\infty} U_m(X_1, X_2, \dots, X_n) T^m.$$

2. Pour qu'un élément P de $A[X_1, X_2, \dots, X_n]$ soit p -homogène, il faut et il suffit que

$$(2) \quad P(TX_1, TX_2, \dots, TX_n) = P(X_1, X_2, \dots, X_n) T^p.$$

Assertion 1. — Les deux membres de la formule (1) dépendent linéairement de P . Il suffit donc de prouver la formule (1) lorsque P est un monôme, ce qui est immédiat.

Assertion 2. — Si P est p -homogène, $P = U_p$, et la formule (2) résulte de la formule (1).

Réciproquement, posons $A' = A[X_1, X_2, \dots, X_n]$, et supposons que P satisfait à la relation (2). Alors les deux éléments

$$\sum_{m=0}^{+\infty} U_m(X_1, X_2, \dots, X_n) T^m \quad \text{et} \quad P(X_1, X_2, \dots, X_n) T^p$$

de $A'[T]$ sont égaux. Par suite, $U_m(X_1, X_2, \dots, X_n) = 0$ si $m \neq p$, et $U_p(X_1, X_2, \dots, X_n) = P$.

COROLLAIRE 3. — Autre caractérisation des polynômes homogènes. — On suppose que l'anneau A est intègre et infini. Soient B une partie infinie de A , et P un élément de $A[X_1, X_2, \dots, X_n]$. Pour que le polynôme P soit p -homogène, il faut et il suffit que, pour tout élément α de B ,

$$(1) \quad P(\alpha X_1, \alpha X_2, \dots, \alpha X_n) = \alpha^p P(X_1, X_2, \dots, X_n).$$

Posons encore $A' = A[X_1, X_2, \dots, X_n]$. D'après la proposition 2.10, la condition (1) est réalisée si et seulement si les deux éléments $P(TX_1, TX_2, \dots, TX_n)$ et $P(X_1, X_2, \dots, X_n) T^p$ de $A'[T]$ prennent même valeur sur B . Ceci revient à dire que ces deux polynômes sont égaux, puisque A' est intègre (cf. th. 2.1), et que B est une partie infinie de A . Le corollaire 3 résulte alors de l'assertion 2 du corollaire 2.

COROLLAIRE 4. — Divisibilité par des produits de facteurs de degré 1. — On suppose que l'anneau A est intègre. Soit P un élément de $A[X_1, X_2, \dots, X_n]$.

1. Soit Q un élément de $B = A[X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$. Pour que P soit divisible par $X_j - Q$, il faut et il suffit que le polynôme R obtenu en substituant Q à X_j soit nul.

2. Si, pour tout couple (i, j) d'éléments de $[1, n]$ tel que $i < j$, P est divisible par $(X_j - X_i)^{r_{ij}}$, où $r_{ij} \in \mathbb{N}^*$, alors P est divisible par $\prod_{i < j} (X_j - X_i)^{r_{ij}}$.

3. Soit, pour tout élément j de $[1, n]$, Q_j un élément de $A[X_1, X_2, \dots, X_{j-1}]$. Pour que P soit divisible par $\prod_{j=1}^n (X_j - Q_j)$, il faut et il suffit que, pour tout $j \in [1, n]$, le polynôme obtenu en substituant Q_j à X_j soit nul.

Assertion 1. — Il est évident que si P est divisible par $X_j - Q$, $R = 0$. Réciproquement, supposons que $R = 0$. Soit \tilde{P} la fonction polynomiale de B dans B associée à P , considéré comme élément de $B[X_j]$. La relation $R = 0$ signifie que \tilde{P} s'annule au point Q . Par suite, P est divisible par $X_j - Q$ dans $B[X_j]$ (cf. § 1), ce qui signifie encore que P est divisible par $X_j - Q$ dans $A[X_1, X_2, \dots, X_n]$.

Assertion 2. — Pour tout élément i de $[1, n]$, introduisons l'anneau $B_i = A[X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$. Considérons d'abord P comme élément de $B_n[X_n]$. Alors, pour tout élément i de $[1, n-1]$, $v_{X_i}(P) \geq r_{in}$. Puisque l'anneau B_n est intègre, on peut appliquer le théorème 2.1 : le polynôme P est divisible par $\prod_{i < n} (X_n - X_i)^{r_{in}}$ dans $B_n[X_n]$. Autrement dit, il existe un élément P_1 de $A[X_1, X_2, \dots, X_n]$ tel que

$$P = \prod_{i < n} (X_n - X_i)^{r_{in}} P_1.$$

Considérons maintenant tous ces polynômes comme éléments de $B_{n-1}[X_{n-1}]$. Puisque B_{n-1} est intègre, pour tout élément i de $[1, n-2]$,

$$v_{X_i}(P) = v_{X_i}(P_1) \geq r_{i,n-1}.$$

En raisonnant comme ci-dessus, nous voyons qu'il existe un élément P_2 de $A[X_1, X_2, \dots, X_n]$ tel que

$$P_1 = \prod_{i < n-1} (X_{n-1} - X_i)^{r_{i,n-1}} P_2.$$

En raisonnant par récurrence, nous voyons qu'il existe un élément P_{n-1} de $A[X_1, X_2, \dots, X_n]$ tel que

$$P = \prod_{i < j} (X_j - X_i)^{r_{ij}} P_{n-1},$$

ce qu'il fallait démontrer.

L'assertion 3 se démontre par récurrence à partir de l'assertion 1 : on applique encore le théorème 2.1, en raisonnant comme dans l'assertion 2.

THÉORÈME 2.10. — **Ensemble des zéros d'un polynôme à plusieurs indéterminées.** — Soient A un anneau unitaire intègre et infini, et I un ensemble

fini non vide. Pour tout élément P de $A[X_i]_{i \in I}$, on désigne par $V(P)$ l'ensemble des points a de A^I tels que $P(a) = 0$.

1. Si P est non nul, l'ensemble $V(P)$ n'est pas égal à A^I ; autrement dit, il existe un point a de A^I tel que $P(a)$ soit non nul. Cela revient encore à dire que le morphisme $P \mapsto \tilde{P}$ de $A[X_i]_{i \in I}$ dans $\mathcal{F}(A^I, A)$ est injectif.

2. Soient a un point de A^I n'appartenant pas à $V(P)$, b un point quelconque de A^I , et D l'ensemble des points de A^I de la forme $a + \lambda b$, où λ parcourt A . Alors l'intersection de D et de $V(P)$ est finie.

* Autrement dit, pour toute droite affine D de A^I non contenue dans $V(P)$, l'intersection de D et de $V(P)$ est finie. *

Vu le corollaire 1 de la proposition 2.6, on se ramène aussitôt au cas où $I = [1, n]$.

Assertion 1. — La démonstration s'effectue par récurrence sur l'entier n . Lorsque $n = 1$, l'assertion résulte du théorème 2.1. Supposons donc l'assertion établie pour tous les éléments non nuls de $A[X_1, X_2, \dots, X_{n-1}]$, et considérons un élément non nul P de $A[X_1, X_2, \dots, X_n]$. Ce polynôme peut s'écrire d'une manière et d'une seule sous la forme

$$P = \sum_{p=0}^{+\infty} Q_p X_n^p,$$

où, pour tout $p \in \mathbb{N}$, Q_p appartient à $A[X_1, X_2, \dots, X_{n-1}]$. Puisque $P \neq 0$, il existe un entier naturel p_0 tel que Q_{p_0} soit non nul. D'après l'hypothèse de récurrence, il existe un point $(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ de A^{n-1} tel que

$$\tilde{Q}_{p_0}(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) \neq 0.$$

Il en résulte que l'élément

$$R = \sum_{p=0}^{+\infty} \tilde{Q}_p(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) X_n^p$$

de $A[X_n]$ est non nul. D'après le théorème 2.1, il existe un élément α_n de A tel que $\tilde{R}(\alpha_n) \neq 0$. Enfin, d'après la proposition 2.10, $\tilde{R}(\alpha_n) = \tilde{P}(\alpha_1, \alpha_2, \dots, \alpha_n)$, ce qui achève la démonstration.

Assertion 2. — Posons $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ et $b = (\beta_1, \beta_2, \dots, \beta_n)$. Considérons l'élément $Q = P(\alpha_1 + \beta_1 T, \alpha_2 + \beta_2 T, \dots, \alpha_n + \beta_n T)$ de $A[T]$. D'après la proposition 2.10, $\tilde{Q}(0) = \tilde{P}(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$. Le polynôme Q n'est donc pas nul. Il résulte alors du théorème 2.1 que l'ensemble des éléments λ de A tels que $\tilde{Q}(\lambda) = 0$ est fini, ce qu'il fallait prouver.

Vu l'injectivité de l'application $P \mapsto \tilde{P}$, nous noterons désormais $P(a)$ le scalaire $\tilde{P}(a)$.

COROLLAIRE 1. — Prolongement des identités algébriques. — Soient A un anneau unitaire intègre et infini, I un ensemble fini non vide, (P_1, P_2, \dots, P_r) une suite de r éléments non nuls de $A[X_i]_{i \in I}$, et, pour tout $q \in [1, r]$, $V(P_q)$ l'ensemble des points a de A^I tels que $P_q(a) = 0$. Soient enfin Q et Q' deux éléments de $A[X_i]_{i \in I}$. Si, pour tout élément a de A^I n'appartenant pas à $\bigcup_{q=1}^r V(P_q)$, $Q(a) = Q'(a)$, alors $Q = Q'$.

Supposons par l'absurde que $Q \neq Q'$, et considérons le polynôme $R = (Q - Q') \prod_{q=1}^r P_q$. Puisque l'anneau $A[X_i]_{i \in I}$ est intègre (cf. th. 2.6), le polynôme R n'est pas nul. Il résulte alors du théorème précédent qu'il existe un point a de A^I tel que $R(a) \neq 0$. Puisque A est intègre, cette dernière relation est équivalente aux suivantes :

$$Q(a) \neq Q'(a), \quad \text{et, pour tout } q \in [1, r], P_q(a) \neq 0,$$

lesquelles contredisent l'hypothèse.

REMARQUE. — Ce corollaire montre en particulier que la réunion des parties $V(P_q)$, où q parcourt $[1, r]$, n'est pas égale à A^I tout entier.

COROLLAIRE 2. — Soit P un élément non nul de $K[X_1, X_2, \dots, X_n]$. Lorsque $K = \mathbb{R}$ ou que $K = \mathbb{C}$, l'ensemble U des points a de K^n tels que $P(a) \neq 0$ est un ouvert dense dans K^n .

En effet, d'après le théorème I.5.6, U est ouvert. D'après l'assertion 1 du théorème précédent, U est non vide. Soit donc a un point de U . Alors, pour tout point b de K^n , l'intersection de l'ensemble D des points de K^n de la forme $a + \lambda(b - a)$, où λ parcourt K , et du complémentaire de U dans K^n est finie. Il en découle que $U \cap D$ est dense dans D , et que b est adhérent à $U \cap D$, ce qui achève la démonstration.

L'étude des fonctions rationnelles d'une variable s'étend de la manière suivante :

DÉFINITION 2.13. — Éléments substituables dans une fraction rationnelle. — Soient I un ensemble fini non vide, $B = K[X_i]_{i \in I}$ l'algèbre des polynômes à coefficients dans A construits sur I , et E une K -algèbre associative unitaire. On dit qu'une famille $a = (a_i)_{i \in I}$ d'éléments de E commutant deux à deux est substituable dans un élément R de $K(X_i)_{i \in I}$ s'il existe un élément (P, Q) de $B \times B^*$ tel que $R = \frac{P}{Q}$ et que $Q(a)$ soit un élément inversible dans E .

Exactement comme au § 1.3, on vérifie que l'élément $P(a) \cdot [Q(a)]^{-1}$ ne dépend que de R ; on l'appelle valeur de R au point a .

DÉFINITION 2.14. — Fonctions rationnelles. — Soit E une K -algèbre associative, COMMUTATIVE et unitaire. Étant donné un élément R de $K(X_i)_{i \in I}$, on note \tilde{R}

l'application qui à tout élément a de E^I substituable dans R associe la valeur de R au point a .

Soit maintenant B une partie de E^I . On dit qu'une application f de B dans E est une fonction rationnelle s'il existe un élément R de $K(X_i)_{i \in I}$ satisfaisant aux conditions suivantes :

a) *tout élément de B est substituable dans R ;*

b) *pour tout élément a de B , $f(a) = \tilde{R}(a)$.*

C'est pourquoi, étant donné un élément R de $K(X_i)_{i \in I}$, l'application \tilde{R} s'appelle fonction rationnelle sur E^I associée à R .

DÉFINITION 2.15. — Applications rationnelles. — *Soient E une A -algèbre associative commutative unitaire, I et J deux ensembles finis non vides, et B une partie de E^I . On dit qu'une application f de B dans E^J est une application rationnelle si, pour tout élément j de J , la fonction $\text{pr}_j \circ f$ est une fonction rationnelle sur B .*

Cela revient à dire qu'il existe une famille $(R_j)_{j \in J}$ d'éléments de $A(X_i)_{i \in I}$ telle que tout élément a de B soit substituable dans chaque fraction rationnelle R_j et que

$$f(a) = (\tilde{R}_j(a))_{j \in J}.$$

EXEMPLES.

1. Lorsque $E = K$, pour qu'un élément a de K^n soit substituable dans un élément R de $K(X_1, X_2, \dots, X_n)$, il faut et il suffit qu'il existe un élément (P, Q) de $K[X_1, X_2, \dots, X_n] \times K[X_1, X_2, \dots, X_n]^*$ tel que $R = \frac{P}{Q}$ et que $Q(a)$ soit non nul. Lorsque $K = \mathbf{R}$ ou que $K = \mathbf{C}$, il découle du corollaire 2 du théorème 2.10 que l'ensemble des éléments de K^n substituables dans R est un ouvert dense dans K^n .

2. Lorsque $K = \mathbf{R}$ ou que $K = \mathbf{C}$, la notion de fonction rationnelle sur K^n définie dans ce paragraphe coïncide avec celle qui a été introduite au § I.5.5.

3. **Substitutions de fractions rationnelles dans une fraction rationnelle.** — On prend pour E le corps $K(Y_1, Y_2, \dots, Y_p)$, et on considère une famille (S_1, S_2, \dots, S_n) d'éléments de $K(Y_1, Y_2, \dots, Y_p)$ substituables dans un élément R de $K(X_1, X_2, \dots, X_n)$. L'élément de $K(Y_1, Y_2, \dots, Y_p)$ obtenu en substituant dans R les fractions rationnelles S_1, S_2, \dots, S_n aux indéterminées X_1, X_2, \dots, X_n se note $R(S_1, S_2, \dots, S_n)$. On laisse au lecteur le soin de prouver, en s'inspirant du cas des fractions rationnelles à une indéterminée, que, pour toute suite (a_1, a_2, \dots, a_n) d'éléments de E^p telle que, pour tout $i \in [1, n]$, a_i soit substituable dans S_i , et que $(\tilde{S}_1(a_1), \tilde{S}_2(a_2), \dots, \tilde{S}_n(a_n))$ soit substituable dans R , alors (S_1, S_2, \dots, S_n) est substituable dans R , (a_1, a_2, \dots, a_n) est substituable dans $T = R(S_1, S_2, \dots, S_n)$, et

$$\tilde{T}(a_1, a_2, \dots, a_n) = \tilde{R}(\tilde{S}_1(a_1), \tilde{S}_2(a_2), \dots, \tilde{S}_n(a_n)).$$

On laisse encore au lecteur le soin de démontrer l'associativité de la substitution dans les fractions rationnelles.

Les caractérisations des polynômes homogènes (cf. cor. 2 et 3 de la prop. 2.10) s'étendent en la proposition suivante :

PROPOSITION 2.11. — Caractérisations des fractions rationnelles homogènes.
Soit R un élément de $K(X_1, X_2, \dots, X_n)$.

1. La suite $(TX_1, TX_2, \dots, TX_n)$ d'éléments de $K[X_1, X_2, \dots, X_n, T]$ est substituable dans R , et, pour que R soit p -homogène, où $p \in \mathbb{Z}$, il faut et il suffit que

$$(1) \quad R(TX_1, TX_2, \dots, TX_n) = R(X_1, X_2, \dots, X_n)T^p.$$

2. On suppose que le corps K est infini. Alors l'ensemble E des éléments α de K tels que $(\alpha X_1, \alpha X_2, \dots, \alpha X_n)$ soit substituable dans R est infini, et, pour que R soit p -homogène, il faut et il suffit que, pour tout élément α d'une partie infinie de E ,

$$(2) \quad R(\alpha X_1, \alpha X_2, \dots, \alpha X_n) = \alpha^p R(X_1, X_2, \dots, X_n).$$

Assertion 1. — Il est immédiat que si Q est un élément non nul de $A = K[X_1, X_2, \dots, X_n]$, $Q(TX_1, TX_2, \dots, TX_n)$ est un élément non nul de $K[X_1, X_2, \dots, X_n, T]$. (Il suffit de considérer ces polynômes comme des éléments de $A[T]$.) Par suite $(TX_1, TX_2, \dots, TX_n)$ est substituable dans tout élément R de $K(X_1, X_2, \dots, X_n)$. Il est évident que si R est p -homogène, R satisfait à (1). Pour démontrer que la condition est suffisante, écartons le cas trivial où $R = 0$. En changeant éventuellement R en $\frac{1}{R}$, nous nous ramenons au cas où p est un entier naturel. Écrivons R sous forme réduite $R = \frac{P}{Q}$, où P et Q sont deux éléments non nuls de $K[X_1, X_2, \dots, X_n]$ premiers entre eux. La relation (1) équivaut à la suivante :

$$(3) \quad P(TX_1, TX_2, \dots, TX_n)Q(X_1, X_2, \dots, X_n) = Q(TX_1, TX_2, \dots, TX_n)P(X_1, X_2, \dots, X_n)T^p.$$

Il en découle que P divise $P(TX_1, TX_2, \dots, TX_n)$ dans l'anneau $A[T]$, c'est-à-dire qu'il existe un élément non nul U de $A[T]$ tel que

$$(4) \quad P(TX_1, TX_2, \dots, TX_n) = U(X_1, X_2, \dots, X_n, T)P(X_1, X_2, \dots, X_n).$$

Il en résulte que, pour tout $i \in [1, n]$, $d_i^0(U) = 0$. Par suite, U appartient à $K[T]$. La relation (4) s'écrit donc

$$(5) \quad P(TX_1, TX_2, \dots, TX_n) = U(T)P(X_1, X_2, \dots, X_n).$$

Il s'ensuit que

$$U(TT') = U(T)U(T').$$

Soit $q = v_0(U)$; alors $U(T) = T^q V(T)$, où $V(0) \neq 0$, et

$$V(TT') = V(T)V(T').$$

En substituant 0 à T' nous en déduisons que $V = 1$, c'est-à-dire que $U(T) = T^q$. La relation (5) montre alors que P est q -homogène (cf. cor. 2 de la prop. 2.10). De même, il existe un entier r tel que Q soit r -homogène. Par suite, $R = \frac{P}{Q}$ est $(q - r)$ -homogène, et, enfin, $p = q - r$.

Assertion 2. — Soit Q un élément non nul de $A = K[X_1, X_2, \dots, X_n]$. Puisque $Q(TX_1, TX_2, \dots, TX_n)$ est un élément non nul de $A[T]$ et que le corps K est infini, l'ensemble E des éléments α de K tels que $Q(\alpha X_1, \alpha X_2, \dots, \alpha X_n) \neq 0$ est infini. Enfin, pour la même raison, la relation (2) implique la relation (1), ce qui prouve que R est p -homogène.

PROPOSITION 2.12. — Prolongement des identités algébriques pour les fonctions rationnelles. — Soient K un corps infini, (P_1, P_2, \dots, P_r) une suite de r éléments non nuls de $K[X_i]_{i \in I}$, et, pour tout $q \in [1, r]$, $V(P_q)$ l'ensemble des points a de K^I tels que $P_q(a) = 0$. Soient enfin R et R' deux éléments de $K(X_i)_{i \in I}$. Si, pour tout élément a de K^I substituable à la fois dans R et dans R' et n'appartenant pas à $\bigcup_{q=1}^r V(P_q)$, $\tilde{R}(a) = \tilde{R}'(a)$, alors $R = R'$.

Écrivons R et R' sous la forme $R = \frac{P}{Q}$, $R' = \frac{P'}{Q'}$, où P et P' sont des éléments de $K[X_i]_{i \in I}$, et où Q et Q' sont des éléments non nuls de $K[X_i]_{i \in I}$. Désignons par $V(Q)$ (resp. par $V(Q')$) l'ensemble des points a de K^I tels que $Q(a) = 0$ (resp. $Q'(a) = 0$). Tout élément a de K^I n'appartenant pas à $V(Q) \cup V(Q')$ est substituable à la fois dans R et dans R' . Par suite, pour tout élément a de K^I n'appartenant pas à $W = V(Q) \cup V(Q') \cup \bigcup_{q=1}^r V(P_q)$,

$$\tilde{R}(a) = \tilde{R}'(a),$$

ce qui revient à dire que

$$P(a) \cdot Q'(a) = P'(a) \cdot Q(a).$$

Ainsi, le polynôme $PQ' - P'Q$ s'annule en tous les points a de K^I n'appartenant pas à W . D'après le principe de prolongement des identités algébriques pour les polynômes (cf. cor. 1 du th. 2.10), $PQ' - P'Q = 0$; donc $R = R'$.

COROLLAIRE. — Soit K un corps infini. Si les fonctions rationnelles sur K^I associées à deux éléments R et R' de $K(X_i)_{i \in I}$ prennent même valeur en tout point de K^I où elles sont toutes deux définies, alors $R = R'$.

Nous noterons désormais $R(a)$ le scalaire $\tilde{R}(a)$.

DÉFINITION 2.16. — Pôles, zéros, points d'indétermination. — Soient R un élément non nul de $K(X_i)_{i \in I}$, et a un élément de K^I .

On dit que a est un zéro de R si a est substituable dans R , et si $R(a) = 0$.

On dit que a est un pôle de R si a est substituable dans R^{-1} , et si $R^{-1}(a) = 0$.

On dit enfin que a est un point d'indétermination de R si a n'est substituable ni dans R , ni dans R^{-1} .

Pour que a soit un zéro de R , il faut et il suffit que R puisse s'écrire sous la forme $R = \frac{P}{Q}$, où P et Q appartiennent à $K[X_i]_{i \in I}$, $P(a) = 0$ et $Q(a) \neq 0$.

Pour que a soit un pôle de R il faut et il suffit que R puisse s'écrire sous la forme $R = \frac{P}{Q}$, où P et Q appartiennent à $K[X_i]_{i \in I}$, $P(a) \neq 0$ et $Q(a) = 0$.

Pour que a soit un point d'indétermination de R , il faut et il suffit que, pour tout couple (P, Q) d'éléments non nuls de $K[X_i]_{i \in I}$ tel que $R = \frac{P}{Q}$, $P(a) = 0$ et $Q(a) = 0$.

EXEMPLES. — Le point $(0, 0)$ est un zéro de la fraction rationnelle $\frac{X + Y}{1 + X^2 + Y^2}$; c'est un pôle de la fraction rationnelle $\frac{1}{X^3 + Y^3}$; c'est un point d'indétermination de la fraction rationnelle $\frac{X - Y}{X^2 + Y^2}$.

De façon générale, soit $\frac{P}{Q}$ la forme réduite de R . Pour que a soit un zéro de R , il faut et il suffit que $P(a) = 0$ et $Q(a) \neq 0$; pour que a soit un pôle de R , il faut et il suffit que $P(a) \neq 0$ et $Q(a) = 0$; pour que a soit un point d'indétermination, il faut et il suffit que $P(a) = 0$ et $Q(a) = 0$.

REMARQUE 1. — Il n'existe pas de point d'indétermination pour les fractions rationnelles à une indéterminée.

REMARQUE 2. — La théorie des valuations permet de définir la multiplicité d'un pôle ou d'un zéro (cf. exercice 24).

Exercices conseillés : 9 à 17.

§ 4. DÉRIVATION DES POLYNÔMES ET DES FRACTIONS RATIONNELLES

Commençons par étudier le cas des polynômes à une indéterminée à coefficients dans un anneau. La proposition 1.23 se généralise aussitôt en la suivante :

PROPOSITION 2.13. — **Dérivation des polynômes.** — *Il existe une dérivation D de la A -algèbre $A[X]$ et une seule telle que $D(X) = 1$. On l'appelle dérivation canonique de $A[X]$.*

Le corollaire de la proposition 1.24 et la proposition 1.25 subsistent sans aucun changement. En revanche, la théorie des primitives ne se généralise pas.

Passons maintenant au cas des polynômes à plusieurs indéterminées.

DÉFINITION 2.17. — **Développement taylorien d'un polynôme.** Soient $A[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]$ l'algèbre des polynômes à $2n$ indéterminées à coefficients dans un anneau commutatif unitaire A , et $B = A[X_1, X_2, \dots, X_n]$ la sous-algèbre unitaire engendrée par X_1, X_2, \dots, X_n . Pour tout élément P de $A[X_1, X_2, \dots, X_n]$, soit $P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n)$ l'élément de $A[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]$ obtenu en substituant les polynômes

$X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n$ aux indéterminées X_1, X_2, \dots, X_n dans le polynôme P . Pour tout entier naturel p , on désigne par $T_p(P)$ la composante p -homogène du polynôme $P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n)$, considéré comme élément de $B[Y_1, Y_2, \dots, Y_n]$. Ainsi, $T_p(P)$ est un polynôme p -homogène, et

$$(1) \quad P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} T_p(P).$$

La famille des polynômes $T_p(P)$, où p parcourt \mathbf{N} , s'appelle *développement taylorien du polynôme P* .

EXEMPLE. — Développement taylorien d'un polynôme à une indéterminée. — Dans le cas particulier des polynômes à une indéterminée, B n'est autre que la sous-algèbre unitaire $A[X]$ de la A -algèbre unitaire $A[X, Y]$, et, pour tout élément P de $A[X]$ et pour tout entier naturel p , $T_p(P)$ est la partie p -homogène du polynôme $P(X + Y)$, considéré comme élément de $B[Y]$:

$$P(X + Y) = \sum_{p=0}^{+\infty} T_p(P).$$

PROPOSITION 2.14. — Propriétés des développements tayloriens. — On conserve les notations précédentes.

1. L'application $P \mapsto T_p(P)$ est une application A -linéaire de $A[X_1, X_2, \dots, X_n]$ dans $B[Y_1, Y_2, \dots, Y_n]$.

2. Pour tout couple (P, Q) d'éléments de $A[X_1, X_2, \dots, X_n]$, et pour tout entier naturel p ,

$$(2) \quad T_p(PQ) = \sum_{r+s=p} T_r(P) \cdot T_s(Q).$$

En particulier,

$$(3) \quad T_0(PQ) = T_0(P) \cdot T_0(Q),$$

et

$$(4) \quad T_1(PQ) = T_1(P)T_0(Q) + T_0(P)T_1(Q).$$

C'est une conséquence immédiate de la proposition 2.7, appliquée à l'algèbre $B[Y_1, Y_2, \dots, Y_n]$.

Dans la suite de ce paragraphe, nous allons expliciter les polynômes $T_p(P)$.

Il résulte aussitôt de la proposition 2.10 qu'en substituant 0 à chacune des indéterminées Y_1, Y_2, \dots, Y_n dans la relation (1), on obtient la formule suivante :

$$(5) \quad T_0(P) = P(X_1, X_2, \dots, X_n).$$

DÉFINITION 2.18. — Différentielle d'un polynôme. — Soit M le sous-module constitué des éléments 1-homogènes du A -module $B[Y_1, Y_2, \dots, Y_n]$. Pour tout élément P de $A[X_1, X_2, \dots, X_n]$, $T_1(P)$ est un élément de M , appelé *différentielle du polynôme P* , et noté plus simplement dP .

REMARQUE. — Nous verrons (cf. *Analyse* III) que si l'on identifie les polynômes à coefficients réels aux fonctions polynomiales qu'ils définissent, la notion de différentielle introduite ici coïncide avec la notion de différentielle introduite en *Analyse*, lorsque $K = \mathbf{R}$ ou $K = \mathbf{C}$.

PROPOSITION 2.15. — **Propriétés de la différentiation des polynômes.** — *On conserve les mêmes notations.*

1. L'application d de $A[X_1, X_2, \dots, X_n]$ dans M qui à tout polynôme P associe sa différentielle dP est la seule application A -linéaire de $A[X_1, X_2, \dots, X_n]$ dans M satisfaisant aux deux conditions suivantes :

a) pour tout couple (P, Q) d'éléments de $A[X_1, X_2, \dots, X_n]$,

$$(6) \quad d(PQ) = dP \cdot Q + P \cdot dQ;$$

b) pour tout élément i de $[1, n]$,

$$(7) \quad dX_i = Y_i.$$

2. Pour tout entier strictement positif m , et pour tout polynôme P ,

$$(8) \quad d(P^m) = mP^{m-1}dP.$$

Assertion 1. — D'après la proposition 2.14, l'application $P \mapsto dP$ est A -linéaire, et elle satisfait à la condition a); elle satisfait évidemment à la condition b).

Réciproquement, soit d' une application A -linéaire de $A[X_1, X_2, \dots, X_n]$ dans M satisfaisant aux conditions a) et b). D'après la relation (6), $d'(1) = 0 = d(1)$, et d'après la relation (7), $d'(X_i) = d(X_i)$. En utilisant la formule (6), on vérifie alors par récurrence sur l'entier $|s|$ que, pour tout élément s de $S = \mathbf{N}^n$, $d'(X^s) = d(X^s)$. Comme d et d' sont A -linéaires, il en découle que $d' = d$.

L'assertion 2 se déduit de même de la formule (6) par récurrence sur l'entier m .

PROPOSITION 2.16. — **Différentielle d'un polynôme composé.** — Soient P un élément de $A[X_1, X_2, \dots, X_n]$, (Q_1, Q_2, \dots, Q_n) une famille d'éléments de $A[X'_1, X'_2, \dots, X'_p]$, et $R = P(Q_1, Q_2, \dots, Q_n)$ l'élément de $A[X'_1, X'_2, \dots, X'_p]$ obtenu en substituant Q_1, Q_2, \dots, Q_n aux indéterminées X_1, X_2, \dots, X_n dans P . On sait que dP est un élément de $A[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]$ homogène de degré 1 relativement aux indéterminées Y_1, Y_2, \dots, Y_n , et que, pour tout $i \in [1, n]$, dQ_i est un élément de $A[X'_1, X'_2, \dots, X'_p, Y'_1, Y'_2, \dots, Y'_p]$ homogène de degré 1 relativement aux indéterminées Y'_1, Y'_2, \dots, Y'_p . Alors la différentielle dR du polynôme composé $R = P(Q_1, Q_2, \dots, Q_n)$ est l'élément de $A[X'_1, X'_2, \dots, X'_p, Y'_1, Y'_2, \dots, Y'_p]$ obtenu en substituant dans dP les polynômes Q_1, Q_2, \dots, Q_n aux indéterminées X_1, X_2, \dots, X_n et les polynômes dQ_1, dQ_2, \dots, dQ_n aux indéterminées Y_1, Y_2, \dots, Y_n :

$$(9) \quad dR = dP(Q_1, Q_2, \dots, Q_n, dQ_1, dQ_2, \dots, dQ_n).$$

L'application $P \mapsto P(Q_1, Q_2, \dots, Q_n)$ est un morphisme d'algèbres unitaires; grâce à la proposition 2.15, il en découle que les polynômes P tels que la formule (9) soit vraie constituent une sous-algèbre unitaire de $A[X_1, X_2, \dots, X_n]$. Puisque les monômes X_i , où i parcourt $[1, n]$, engendrent l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$, il suffit de prouver la formule (9) lorsque $P = X_i$, ce qui est immédiat.

EXEMPLE 1. — Différentielle d'un polynôme à une indéterminée. — Dans le cas particulier des polynômes à une indéterminée, B est égal à $A[X]$, et M est le sous-module du A -module $B[Y]$ constitué des éléments $P(X)Y$, où $P(X) \in A[X]$. Ainsi pour tout polynôme P , $T_1(P)$ s'écrit d'une manière et d'une seule sous la forme

$$T_1(P) = D_1(P)Y, \quad \text{où} \quad D_1(P) \in A[X].$$

Puisque d est A -linéaire et que d satisfait aux relations (6) et (7), D_1 est un endomorphisme du A -module $A[X]$, et

$$(6') \quad D_1(PQ) = D_1(P)Q + PD_1(Q)$$

$$(7') \quad D_1(X) = 1.$$

D'après la proposition 2.13, D_1 n'est autre que la dérivation canonique de $A[X]$. Nous obtenons ainsi le résultat suivant : pour tout élément P de $A[X]$,

$$(10) \quad dP = D(P)Y.$$

REMARQUE. — On trouvera dans l'exercice 29 la théorie des différentielles des polynômes à coefficients vectoriels.

PROPOSITION 2.17. — Dérivées partielles. — Soit $A[X_1, X_2, \dots, X_n]$ l'algèbre des polynômes à n indéterminées à coefficients dans A .

1. Pour tout élément i de $[1, n]$, il existe une dérivation D_i de la A -algèbre $A[X_1, X_2, \dots, X_n]$ et une seule telle que, pour tout élément j de $[1, n]$,

$$D_i(X_j) = \delta_{ij}.$$

2. Pour tout entier naturel non nul m , et pour tout polynôme P ,

$$D_i(P^m) = mP^{m-1}D_i(P).$$

3. Pour tout polynôme

$$P = \sum_{p=0}^{+\infty} a_p X_i^p, \quad \text{où} \quad a_p \in B = A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n],$$

le polynôme $D_i(P)$ est donné par la formule

$$(1) \quad D_i(P) = \sum_{p=1}^{+\infty} p a_p X_i^{p-1}.$$

C'est pourquoi le polynôme $D_i(P)$ s'appelle $i^{\text{ième}}$ dérivée partielle de P ; il se note encore $\frac{\partial P}{\partial X_i}$.

4. L'application $P \mapsto D_i(P)$ est un endomorphisme du B -module $B[X_i]$; elle n'est autre que la dérivation canonique de la B -algèbre $B[X_i]$.

5. Si la caractéristique de A est nulle, pour que la dérivée partielle $D_i(P)$ d'un polynôme P soit nulle, il faut et il suffit que le polynôme P appartienne à $A[X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$.

Il est immédiat que la dérivation canonique D_i de la B -algèbre $B[X_i]$ est une dérivation de la A -algèbre $A[X_1, X_2, \dots, X_n]$ satisfaisant aux conditions de l'assertion 1.

Réciproquement, toute dérivation D_i de la A -algèbre $A[X_1, X_2, \dots, X_n]$ satisfaisant à ces conditions s'annule sur B . Il en découle que, pour tout élément a de B , et pour tout entier naturel p , $D_i(aX_i^p) = aD_i(X_i^p) = apX_i^{p-1}$. La dérivation D_i est donc nécessairement donnée par la formule (1).

PROPOSITION 2.18. — Calcul de la différentielle à l'aide des dérivées partielles. — Pour tout élément P de $B = A[X_1, X_2, \dots, X_n]$, la différentielle de P est liée aux dérivées partielles de P par la relation

$$(2) \quad dP = \sum_{i=1}^n D_i(P) \cdot Y_i.$$

Autrement dit, $D_i(P)$ n'est autre que le coefficient de dP relatif à Y_i .

En particulier, on retrouve le fait que, pour tout élément P de $A[X]$, la dérivée $D(P)$ et la différentielle dP du polynôme P sont liées par la relation

$$dP = D(P)Y.$$

Désignons en effet par $D'_i(P)$ le coefficient de dP relatif à Y_i . Il découle de la proposition 2.15 que l'application $P \mapsto D'_i(P)$ est une dérivation du A -module B satisfaisant aux relations $D'_i(X_j) = \delta_{ij}$. D'après la proposition 2.17, $D'_i(P) = D_i(P)$, ce qu'il fallait prouver.

COROLLAIRE 1. — Soit K un corps de caractéristique nulle. Les polynômes constants sont les seuls éléments P de $A[X_1, X_2, \dots, X_n]$ tels que $dP = 0$.

En effet, si $dP = 0$, alors, pour tout $i \in [1, n]$, $D_i(P) = 0$, donc $d_i^0(P) \leq 0$; finalement, $d^0(P) \leq 0$.

COROLLAIRE 2. — Dérivées partielles d'un polynôme composé. — Soient P un élément de $A[X_1, X_2, \dots, X_n]$, (Q_1, Q_2, \dots, Q_n) une suite d'éléments de $A[X'_1, X'_2, \dots, X'_n]$, et $R = P(Q_1, Q_2, \dots, Q_n)$. Alors, pour tout élément j de $[1, n]$,

$$\frac{\partial R}{\partial X'_j} = \sum_{i=1}^n \frac{\partial P}{\partial X_i}(Q_1, Q_2, \dots, Q_n) \frac{\partial Q_i}{\partial X'_j}.$$

Cela résulte aussitôt de la proposition 2.16, et de la formule (2).

EXEMPLE. — Soient P un élément de $A[X_1, X_2, \dots, X_n]$, (Q_1, Q_2, \dots, Q_n) une suite d'éléments de $A[X]$, et $R = P(Q_1, Q_2, \dots, Q_n)$. Alors

$$D(R) = \sum_{i=1}^n \frac{\partial P}{\partial X_i}(Q_1, Q_2, \dots, Q_n) D(Q_i).$$

THÉORÈME 2.11. — **Dérivation des polynômes homogènes.** — Soient P un élément de $A[X_1, X_2, \dots, X_n]$, et p un entier strictement positif.

1. Si P est p -homogène, alors, pour tout élément i de $[1, n]$, $\frac{\partial P}{\partial X_i}$ est $(p-1)$ -homogène.

2. Lorsque A est de caractéristique nulle, pour que P soit p -homogène, il faut et il suffit que

$$(1) \quad \sum_{i=1}^n X_i \cdot \frac{\partial P}{\partial X_i} = pP.$$

La relation (1) s'appelle identité d'Euler.

Introduisons l'élément $P(XX_1, XX_2, \dots, XX_n)$ de $A[X_1, X_2, \dots, X_n, X]$ obtenu en substituant les polynômes XX_1, XX_2, \dots, XX_n aux indéterminées X_1, X_2, \dots, X_n dans P . Nous savons (cf. cor. de la prop. 2.10) que P est p -homogène si et seulement si

$$(2) \quad P(XX_1, XX_2, \dots, XX_n) = X^p P(X_1, X_2, \dots, X_n).$$

Assertion 1. — La formule de dérivation des polynômes composés fournit la relation

$$(3) \quad D_i[P(XX_1, XX_2, \dots, XX_n)] = X \frac{\partial P}{\partial X_i}(XX_1, XX_2, \dots, XX_n).$$

Si P est p -homogène, il découle aussitôt des relations (2) et (3) que

$$(4) \quad \frac{\partial P}{\partial X_i}(XX_1, XX_2, \dots, XX_n) = X^{p-1} \frac{\partial P}{\partial X_i}(X_1, X_2, \dots, X_n).$$

Le polynôme $\frac{\partial P}{\partial X_i}$ est donc $(p-1)$ -homogène.

Assertion 2. — Notons D la dérivation partielle par rapport à X dans $A[X_1, X_2, \dots, X_n, X]$. La formule de dérivation des polynômes composés fournit la relation

$$(5) \quad D[P(XX_1, XX_2, \dots, XX_n)] = \sum_{i=1}^n X_i \cdot \frac{\partial P}{\partial X_i}(XX_1, XX_2, \dots, XX_n).$$

Si P est p -homogène, la relation (1) résulte des relations (2), (4) et (5).

Réciproquement, si P satisfait à la relation (1), la relation (5) peut encore s'écrire sous la forme

$$(6) \quad X \cdot Q'(X) = pQ(X),$$

où Q désigne le polynôme à une indéterminée X à coefficients dans $B = A[X_1, X_2, \dots, X_n]$ défini par la formule

$$Q(X) = P(XX_1, XX_2, \dots, XX_n).$$

Or, les seuls éléments Q de $B[X]$ satisfaisant à la relation (6) sont évidemment les monômes de la forme αX^p , où $\alpha \in B$. En substituant à X le scalaire 1 dans Q , nous voyons que

$$\alpha = Q(1) = P(X_1, X_2, \dots, X_n).$$

Donc

$$P(XX_1, XX_2, \dots, XX_n) = Q(X) = \alpha X^p = X^p P(X_1, X_2, \dots, X_n).$$

THÉORÈME 2.12. — Théorème de Schwarz. — Soit $\mathfrak{L}(B)$ l'algèbre des endomorphismes du A -module $B = A[X_1, X_2, \dots, X_n]$.

1. La sous-algèbre unitaire \mathfrak{D} de $\mathfrak{L}(B)$ engendrée par les dérivations partielles D_1, D_2, \dots, D_n est commutative: les éléments de \mathfrak{D} s'appellent opérateurs différentiels à coefficients constants sur B .

Soit donc S l'ensemble des applications de $[1, n]$ dans \mathbb{N} . Si, pour tout élément s de S , on pose

$$D^s = \prod_{i=1}^n D_i^{s(i)},$$

tout opérateur différentiel H sur $A[X_1, X_2, \dots, X_n]$ s'écrit sous la forme

$$H = \sum_{s \in S} \alpha_s D^s,$$

où, pour tout $s \in S$, α_s appartient à A .

Lorsqu'on note $\frac{\partial P}{\partial X_i}$ le polynôme $D_i P$, le polynôme $D^s P$ se note

$$\frac{\partial^p P}{\partial X_1^{p_1} \partial X_2^{p_2} \dots \partial X_n^{p_n}},$$

où, pour tout $i \in [1, n]$, $p_i = s(i)$, et où $p = \sum_{i=1}^n p_i = |s|$.

2. Plus particulièrement, lorsque A est de caractéristique nulle, l'unique morphisme f de l'algèbre unitaire $A[Y_1, Y_2, \dots, Y_n]$ dans l'algèbre unitaire \mathfrak{D} tel que, pour tout $i \in [1, n]$, $f(Y_i) = D_i$, est un isomorphisme.

Assertion 1. — Nous allons prouver que, pour tout couple (i, j) d'éléments distincts de $[1, n]$, les endomorphismes D_i et D_j commutent, c'est-à-dire que

$$D_i D_j = D_j D_i.$$

Désignons par C l'algèbre des polynômes construits sur l'ensemble $[1, n] - \{i, j\}$. Nous savons que D_i et D_j sont des endomorphismes du C -module $C[X_i, X_j]$. Il suffit donc de prouver que, pour tout couple (p, q) d'entiers naturels,

$$(D_i D_j)(X_i^p X_j^q) = (D_j D_i)(X_i^p X_j^q),$$

ce qui est immédiat.

Le reste de l'assertion résulte immédiatement de la proposition 2.5.

Assertion 2. — L'existence et l'unicité du morphisme f découlent alors de la propriété universelle de l'algèbre $A[Y_1, Y_2, \dots, Y_n]$. D'après la définition de \mathfrak{D} , f est surjectif. Il reste donc à prouver que les éléments D_1, D_2, \dots, D_n sont algébriquement indépendants. Raisonnons par récurrence sur l'entier n . Lorsque $n = 1$, considérons un élément non nul P de $A[X]$; il est clair que $P(D_1)X^r$, où $r = v_0(P)$, est un élément non nul de A , puisque A est de caractéristique nulle; il en découle que $P(D_1)$ n'est pas nul. Supposons l'assertion démontrée pour les polynômes à $n - 1$ indéterminées, et considérons un élément non nul P de $A[X_1, X_2, \dots, X_n]$, que nous écrivons sous la forme

$$P = \sum_{p=r}^{+\infty} Q_p(Y_1, Y_2, \dots, Y_{n-1}) Y_n^p,$$

où $Q_r(Y_1, Y_2, \dots, Y_{n-1}) \neq 0$. Alors, pour tout élément R de $A[X_1, X_2, \dots, X_{n-1}]$,

$$[P(D_1, D_2, \dots, D_n)](RX_n^r) = r! [Q_r(D_1, D_2, \dots, D_{n-1})](R).$$

Par suite, si $P(D_1, D_2, \dots, D_n)$ était nul, il en serait de même de $Q_r(D_1, D_2, \dots, D_{n-1})$, ce qui contredit l'hypothèse de récurrence.

REMARQUE 1. — Lorsque l'anneau A est de caractéristique p , le résultat précédent tombe en défaut, puisque, pour tout $i \in [1, n]$, $D_i^p = 0$. On pourra consulter à ce sujet l'exercice 20.

REMARQUE 2. — Lorsque A est de caractéristique zéro, l'isomorphisme f permet de définir pour les opérateurs différentiels à coefficients constants sur B les mêmes notions que pour les éléments de $A[Y_1, Y_2, \dots, Y_n]$. On peut ainsi définir le degré d'un tel opérateur différentiel, les opérateurs différentiels p -homogènes, etc.

REMARQUE 3. — Les opérateurs différentiels à coefficients constants 1-homogènes, c'est-à-dire les combinaisons linéaires des dérivations partielles D_1, D_2, \dots, D_n , sont évidemment des dérivations de l'algèbre B ; mais il n'en est pas de même des opérateurs différentiels de degré strictement supérieur à 1.

COROLLAIRE. — Formule de Maclaurin. — Soit $P = \sum_{s \in S} \alpha_s X^s$ un élément de $A[X_1, X_2, \dots, X_n]$. Alors, pour tout élément s de S ,

$$(1) \quad (D^s P)(0) = s! \alpha_s,$$

où $s! = \prod_{j=1}^n s(j)!$

En particulier, si A est un corps de caractéristique 0,

$$(2) \quad P = \sum_{s \in S} \frac{(D^s P)(0)}{s!} X^s.$$

La formule (1) se démontre par récurrence sur la longueur de s , et la formule (2) s'en déduit.

Nous sommes maintenant en mesure d'expliciter le développement taylorien d'un polynôme à l'aide de ses dérivées partielles successives.

THÉORÈME 2.13. — Formule de Taylor. — *Soient A un anneau commutatif unitaire, P un élément de $A[X_1, X_2, \dots, X_n]$, et*

$$(1) \quad P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} T_p(P)$$

le développement taylorien de P . Alors les polynômes $T_p(P)$ sont liés aux dérivées partielles de P par les relations

$$(2) \quad H^p(P) = p! T_p(P),$$

où H désigne l'opérateur différentiel sur $A[X_1, X_2, \dots, X_n]$ défini par la relation

$$(3) \quad H = \sum_{i=1}^n Y_i D_i.$$

En particulier, lorsque A est un corps de caractéristique nulle,

$$(4) \quad P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} \frac{H^p(P)}{p!}.$$

On notera que l'opérateur H^p peut s'expliciter à l'aide de la généralisation de la formule du binôme (cf. prop. I.2.37). Ainsi,

$$H^0(P) = P(X_1, X_2, \dots, X_n)$$

$$H^1(P) = \sum_{i=1}^n Y_i \frac{\partial P}{\partial X_i}(X_1, X_2, \dots, X_n)$$

$$H^2(P) = \sum_{i=1}^n Y_i^2 \frac{\partial^2 P}{\partial X_i^2}(X_1, X_2, \dots, X_n) + 2 \sum_{i < j} Y_i Y_j \frac{\partial^2 P}{\partial X_i \partial X_j}(X_1, X_2, \dots, X_n).$$

Considérons l'élément $P(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n)$ de $A[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n, X]$ obtenu en substituant les polynômes $X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n$ aux indéterminées X_1, X_2, \dots, X_n dans le polynôme P , et désignons par Q le polynôme à une

indéterminée X à coefficients dans $A[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]$ défini par la formule

$$Q(X) = P(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n).$$

Lorsqu'on substitue dans les deux membres de la relation (1) les polynômes XY_1, XY_2, \dots, XY_n aux indéterminées Y_1, Y_2, \dots, Y_n , nous voyons que

$$(5) \quad Q(X) = P(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n) = \sum_{p=0}^{+\infty} T_p(P)X^p,$$

car $T_p(P)$ est p -homogène relativement aux indéterminées Y_1, Y_2, \dots, Y_n .

Désignons par D l'opérateur de dérivation partielle par rapport à X , et, pour tout $i \in [1, n]$, par D_i l'opérateur de dérivation partielle par rapport à X_i .

Il résulte de la formule (5) que

$$(6) \quad (D^p Q)(0) = p! T_p(P).$$

Or, d'après la formule de dérivation des polynômes composés, pour tout élément R de $B[X_1, X_2, \dots, X_n]$, où $B = A[Y_1, Y_2, \dots, Y_n]$,

$$\begin{aligned} (7) \quad DR(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n) \\ = \sum_{i=1}^n Y_i \frac{\partial R}{\partial X_i}(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n) \\ = (HR)(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n). \end{aligned}$$

Par suite, pour tout entier naturel p ,

$$(8) \quad (D^p Q)(X) = (H^p P)(X_1 + XY_1, X_2 + XY_2, \dots, X_n + XY_n).$$

En substituant 0 à X dans cette dernière formule, nous obtenons la relation

$$(9) \quad (D^p Q)(0) = H^p P.$$

En comparant les relations (6) et (9), nous voyons que, pour tout entier naturel p ,

$$(2) \quad H^p P = p! T_p(P),$$

ce qui achève la démonstration.

PROPOSITION 2.19. — Différentielle d'une fraction rationnelle. — Soient $B = K(X_1, X_2, \dots, X_n)$ le corps des fractions rationnelles à n indéterminées à coefficients dans K , et M le sous-espace vectoriel constitué des éléments 1-homogènes du K -espace vectoriel $B[Y_1, Y_2, \dots, Y_n]$. Pour tout élément P de $K[X_1, X_2, \dots, X_n]$, la différentielle de P peut être considérée comme un élément de M .

Il existe une application K -linéaire d et une seule du K -espace vectoriel $K(X_1, X_2, \dots, X_n)$ dans l'espace vectoriel M prolongeant la différentiation des polynômes et telle que, pour tout couple (R, S) d'éléments de $K(X_1, X_2, \dots, X_n)$,

$$(1) \quad d(RS) = dR S + R dS.$$

Si un élément R de $K(X_1, X_2, \dots, X_n)$ est mis sous la forme $R = \frac{P}{Q}$, où P et Q sont deux éléments de $K[X_1, X_2, \dots, X_n]$, $Q \neq 0$, alors dR est donné par la formule

$$(2) \quad dR = \frac{dP Q - P dQ}{Q^2}.$$

*La fraction rationnelle dR s'appelle différentielle de R .
Lorsque $n = 1$, dR et $D(R)$ sont liées par la relation*

$$dR = D(R)Y.$$

La démonstration est calquée sur celle de la proposition 2.15.

PROPOSITION 2.20. — Propriétés de la différentiation des fractions rationnelles.

1. *Pour tout couple (R, S) d'éléments de $K(X_1, X_2, \dots, X_n)$, $S \neq 0$,*

$$(3) \quad d\left(\frac{R}{S}\right) = \frac{dR S - R dS}{S^2}.$$

2. *Pour tout élément non nul R de $K(X_1, X_2, \dots, X_n)$ et pour tout entier rationnel m ,*

$$(4) \quad d(R^m) = m R^{m-1} dR.$$

3. *Pour toute suite (R_1, R_2, \dots, R_p) d'éléments non nuls de $K(X_1, X_2, \dots, X_n)$ et pour toute suite (n_1, n_2, \dots, n_p) d'entiers rationnels, la différentielle logarithmique $\frac{dR}{R}$ de la fraction rationnelle $R = \prod_{j=1}^p R_j^{n_j}$ est donnée par la formule*

$$(5) \quad \frac{dR}{R} = \sum_{j=1}^p n_j \frac{dR_j}{R_j}.$$

4. *Soient R un élément de $K(X_1, X_2, \dots, X_n)$ et (S_1, S_2, \dots, S_n) une suite d'éléments de $K(X'_1, X'_2, \dots, X'_p)$ substituables dans R . Alors la différentielle de la fraction rationnelle $T = R(S_1, S_2, \dots, S_n)$ est donnée par la formule*

$$(6) \quad dT = dR(S_1, S_2, \dots, S_n, dS_1, dS_2, \dots, dS_n).$$

La démonstration est calquée sur celles des propositions 1.28, 2.15 et 2.16.

PROPOSITION 2.21. — Dérivées partielles. — *Pour tout élément i de $[1, n]$, il existe une dérivation D_i et une seule de la K -algèbre $K(X_1, X_2, \dots, X_n)$ telle que, pour tout élément j de $[1, n]$,*

$$(7) \quad D_i(X_j) = \delta_{ij}.$$

La dérivation D_i n'est autre que la dérivation canonique de la B -algèbre $B(X_i)$, où $B = K(X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$.

La démonstration est calquée sur celles des propositions 1.27 et 2.17.

La proposition 2.18 et ses corollaires s'étendent :

— Pour tout élément R de $K(X_1, X_2, \dots, X_n)$,

$$(8) \quad dR = \sum_{i=1}^n D_i(R) Y_i.$$

— Si le corps K est de caractéristique nulle, les fractions rationnelles constantes sont les seuls éléments R de $K(X_1, X_2, \dots, X_n)$ tels que $dR = 0$.

— Soient R un élément de $K(X_1, X_2, \dots, X_n)$, (S_1, S_2, \dots, S_n) une suite d'éléments de $K(X'_1, X'_2, \dots, X'_p)$, et $T = R(S_1, S_2, \dots, S_n)$. Alors, pour tout élément j de $[1, p]$,

$$(9) \quad \frac{\partial T}{\partial X'_j} = \sum_{i=1}^n \frac{\partial R}{\partial X_i}(S_1, S_2, \dots, S_n) \frac{\partial Q_i}{\partial X'_j}.$$

— Soient R un élément non constant de $K(X_1, X_2, \dots, X_n)$ et p un entier rationnel. Si R est p -homogène, alors, pour tout élément i de $[1, n]$, $\frac{\partial R}{\partial X_i}$ est $(p-1)$ -homogène.

Lorsque K est de caractéristique nulle, pour que R soit p -homogène, il faut et il suffit que

$$(10) \quad \sum_{i=1}^n X_i \frac{\partial R}{\partial X_i} = pR$$

(identité d'Euler).

Enfin, le théorème de Schwarz s'étend aussitôt au cas des fractions rationnelles.

On trouvera dans l'exercice 26 la formule de Taylor pour les fractions rationnelles.

Exercices conseillés : 18 à 22.

§ 5. POLYNÔMES ET FRACTIONS RATIONNELLES SYMÉTRIQUES

1. GROUPE SYMÉTRIQUE

On rappelle (cf. § I.2.2) que l'ensemble des permutations d'un ensemble non vide E , muni de la composition des applications, est un groupe, appelé

groupe symétrique de E , et noté \mathfrak{S}_E . Lorsque E est un ensemble fini à n éléments, l'ordre du groupe \mathfrak{S}_E est $n!$ (cf. cor. 2 de la prop. I.1.47). Lorsque $E = [1, n]$, \mathfrak{S}_E s'appelle groupe symétrique de degré n , et se note \mathfrak{S}_n .

PROPOSITION 2.22. — Isomorphismes d'équipotence. — Soient E et F deux ensembles équipotents, et φ une bijection de E sur F . Alors l'application $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ est un isomorphisme du groupe \mathfrak{S}_E sur le groupe \mathfrak{S}_F , dit canonicquement associé à φ .

En particulier, lorsque F est un ensemble fini ayant n éléments et que $E = [1, n]$, toute bijection φ de $[1, n]$ sur F définit un isomorphisme de \mathfrak{S}_n sur \mathfrak{S}_F . Autrement dit, lorsque l'ensemble F est rangé en une suite (a_1, a_2, \dots, a_n) , où, pour tout $j \in [1, n]$, $a_j = \varphi(j)$, alors, pour toute permutation σ de F , il existe une permutation τ de $[1, n]$ et une seule telle que, pour tout j , $\sigma(a_j) = a_{\tau(j)}$. C'est pourquoi, dans ces conditions, une permutation σ de F se note souvent de la manière suivante :

$$\sigma = \left\{ \begin{array}{cccc} a_1 & a_2 & \dots & a_n \\ a_{\tau(1)} & a_{\tau(2)} & \dots & a_{\tau(n)} \end{array} \right\}.$$

Plus particulièrement encore, lorsque $F = [1, n]$, on prend pour φ l'application identique de $[1, n]$, et on écrit toute permutation σ de $[1, n]$ de la manière suivante :

$$\sigma = \left\{ \begin{array}{cccc} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{array} \right\}.$$

En effet, dans ce cas particulier, $\tau = \sigma$.

On rappelle d'autre part qu'une opération d'un groupe G sur un ensemble X est une application $(g, x) \mapsto gx$ de $G \times X$ dans X satisfaisant aux deux conditions suivantes :

a) pour tout couple (g, h) d'éléments de G et pour tout élément x de X ,

$$g(hx) = (gh)x;$$

b) pour tout élément x de X ,

$$ex = x,$$

où e désigne l'élément neutre de G .

On dit alors que le groupe G opère sur l'ensemble X . Dans ces conditions, l'application $x \mapsto gx$ est une bijection φ_g de X sur lui-même, et l'application $g \mapsto \varphi_g$ est un morphisme du groupe G dans le groupe des bijections de X sur lui-même.

On rappelle enfin qu'étant donné un groupe G opérant sur un ensemble X , la relation binaire définie par les couples (x, y) d'éléments de X pour lesquels il existe un élément g de G tel que $y = gx$ est une relation d'équivalence. La classe d'équivalence d'un élément x de X s'appelle orbite de x sous G , ou,

plus simplement, orbite de x ; elle est constituée des éléments de X de la forme gx , où g parcourt G .

Les classes d'équivalence s'appellent orbites de G dans X . L'ensemble des orbites constitue une partition de X . Toute orbite P est stable par G , c'est-à-dire que, pour tout élément x de P et pour tout élément g de G , gx appartient à P . De plus, pour tout élément x de P , $P = Gx$.

S'il n'y a qu'une seule orbite, à savoir X , on dit que G opère *transitivement* sur X ; cela revient à dire que, pour tout couple (x, y) d'éléments de X , il existe un élément g de G tel que $y = gx$, ou encore que, pour tout élément x de X , l'application $g \mapsto gx$ est une surjection de G sur X .

Si, pour tout élément x de X , l'application $g \mapsto gx$ est une bijection de G sur X , on dit que G opère *simplement transitivement* sur X . Cela signifie encore que, pour tout couple (x, y) d'éléments de X , il existe un élément g de G et un seul tel que $y = gx$.

Dans toute la suite, on désigne par E un ensemble fini non réduit à un point, et on note n le cardinal de E .

PROPOSITION 2.23. — Opération canonique de \mathfrak{S}_E sur E .

1. L'application $(\sigma, x) \mapsto \sigma x$ est une opération du groupe \mathfrak{S}_E sur l'ensemble E , dite canonique. De plus, \mathfrak{S}_E opère transitivement sur E .

2. Soient σ un élément de \mathfrak{S}_E et G_σ le sous-groupe cyclique de \mathfrak{S}_E engendré par σ . L'application $(\tau, x) \mapsto \tau x$ est une opération du groupe cyclique G_σ sur l'ensemble E , dite canoniquement associée à σ . Les orbites de G_σ dans E s'appellent orbites associées à σ dans E , et l'ensemble de ces orbites se note O'_σ .

PROPOSITION 2.24. — Structure d'une orbite associée à une permutation. Soient σ une permutation de E , P une orbite associée à σ dans E , x un élément de P et $p = \text{card}(P)$. Alors le plus petit des entiers r tels que $\sigma^r x = x$ n'est autre que p , et l'orbite P est constituée des éléments distincts deux à deux $x, \sigma x, \dots, \sigma^{p-1} x$.

Soit q le plus petit des entiers r tels que $\sigma^r x = x$. Alors les éléments $x, \sigma x, \dots, \sigma^{q-1} x$ sont distincts deux à deux : en effet, la relation $\sigma^s x = \sigma^t x$ équivaut à la relation $\sigma^{s-t} x = x$. De plus, P , étant l'orbite de x sous G_σ , est constituée des éléments $x, \sigma x, \dots, \sigma^{q-1} x$. La proposition en découle.

Pour étudier l'ensemble O'_σ , nous allons considérer d'abord certains cas particuliers.

DÉFINITION 2.19. — Cycles, transpositions. — On dit qu'un élément σ de \mathfrak{S}_E est un cycle s'il existe au plus une orbite P associée à σ dans E telle que $\text{card}(P) > 1$. Deux cas peuvent se présenter :

— Ou bien $\sigma \neq I_E$; il existe alors une orbite P et une seule telle que $\text{card}(P) > 1$. Cette orbite s'appelle support du cycle σ . Les orbites ne sont autres

que P et les parties de E constituées d'un point du complémentaire de P dans E . Le nombre card (P) s'appelle longueur du cycle σ .

— Ou bien $\sigma = I_E$; les orbites ne sont autres que les parties de E réduites à un point. On convient de dire que la longueur du cycle I_E est égale à 1.

Les cycles de longueur 2 s'appellent transpositions.

PROPOSITION 2.25. — Structure des cycles.

1. Soient σ un cycle de longueur p strictement supérieure à 1 et de support P , x un élément de P , et, pour tout $j \in [1, p]$, $x_j = \sigma^{j-1}x$. Alors σ n'est autre que la permutation définie par les formules suivantes:

$$(1) \quad \begin{aligned} \sigma x_j &= x_{j+1} & \text{si } j \in [1, p-1] \\ \sigma x_p &= x_1 \\ \sigma z &= z & \text{si } z \in \complement_E P. \end{aligned}$$

2. Réciproquement, soient p un entier strictement supérieur à 1, et (x_1, x_2, \dots, x_p) une suite d'éléments de E distincts deux à deux. Alors la permutation σ de E définie par les formules (1) est un cycle, dont le support est la partie $P = \{x_1, x_2, \dots, x_p\}$. Ce cycle se note $\sigma = [x_1, x_2, \dots, x_p]$.

En particulier, pour tout élément p de $[1, n]$, il existe des cycles de longueur p .

L'assertion 1 découle aussitôt de la proposition précédente.

Assertion 2. — Considérons une orbite Q associée à σ telle que $\text{card}(Q) > 1$, et un élément y de Q . Il est clair que y appartient à P ; donc Q est contenue dans P . De plus, il existe un entier $j \in [0, p-1]$ tel que $y = x_{j+1} = \sigma^j x_1$. Par suite, x_1 appartient à Q , et, pour tout $r \in [0, p-1]$, $x_{r+1} = \sigma^r x_1$ appartient à Q . Ainsi, P est contenue dans Q , ce qui montre que $Q = P$.

REMARQUE. — Supposons donnée une bijection φ de $[1, n]$ sur E , c'est-à-dire une suite (a_1, a_2, \dots, a_n) d'éléments de E distincts deux à deux. Alors, pour tout cycle σ de E de longueur $p > 1$, il existe une injection ψ de $[1, p]$ dans $[1, n]$ et une seule satisfaisant aux conditions suivantes :

$$\sigma = [a_{\psi(1)}, a_{\psi(2)}, \dots, a_{\psi(p)}]$$

et, pour tout élément j de $[2, p]$, $\psi(1) < \psi(j)$. Le support de P n'est autre que $\{a_{\psi(1)}, a_{\psi(2)}, \dots, a_{\psi(p)}\}$, et $\psi(1)$ est encore le plus petit des entiers i tels que a_i appartienne à P .

Ainsi, la donnée d'une bijection de $[1, n]$ sur E permet d'écrire tout cycle σ de E de longueur strictement supérieure à 1 d'une manière *canonique* sous la forme $\sigma = [x_1, x_2, \dots, x_p]$.

COROLLAIRE 1. — La longueur d'un cycle σ est égale à l'ordre de l'élément σ dans le groupe \mathfrak{S}_E .

Écartons le cas trivial où $\sigma = I_E$. Soient alors P le support de σ , p sa longueur et x un élément de P . Soit d'autre part m l'ordre de σ dans le groupe \mathfrak{S}_E .

Par définition des orbites, P est constituée des éléments $\sigma^r x$, où r parcourt $[0, m-1]$. Donc p est inférieur ou égal à m .

D'après la proposition précédente, pour tout élément x de P , $\sigma^p x = x$. Ainsi, la permutation σ^p induit l'identité sur P . Comme, par hypothèse, elle induit l'identité sur le complémentaire de P , $\sigma^p = I_E$. Il en découle (cf. prop. I.2.29) que m divise p . Comme, d'autre part, $p \leq m$, nous voyons que $m = p$.

COROLLAIRE 2. — Structure des transpositions. — *Soient x et y deux éléments distincts de E . Alors le cycle $[x, y]$ est une transposition: c'est la seule transposition dont le support est égal à $\{x, y\}$.*

REMARQUE. — Lorsque $n \geq 3$, le groupe \mathfrak{S}_E n'est pas commutatif. En effet, pour tout triplet (a, b, c) d'éléments de E distincts deux à deux,

$$[a, b] \cdot [b, c] \neq [b, c] \cdot [a, b].$$

On notera qu'étant donné un cycle τ de longueur n et un entier naturel r , τ^r n'est pas nécessairement un cycle, ce qui conduit à la

DÉFINITION 2.20. — Permutations circulaires. — *Soit σ une permutation de E . On dit que σ est une permutation circulaire s'il existe un cycle τ de E de longueur n et un entier naturel r tels que $\sigma = \tau^r$. On dit alors que σ est une permutation circulaire associée au cycle τ .*

PROPOSITION 2.26. — Propriétés des permutations circulaires. — *Soit τ un cycle de longueur n .*

1. *Les permutations circulaires associées à τ ne sont autres que les éléments du groupe cyclique G_τ engendré par τ ; elles constituent un groupe cyclique à n éléments, et s'écrivent d'une manière et d'une seule sous la forme $\sigma = \tau^r$, où $r \in [0, n-1]$.*

2. *L'ordre de la permutation circulaire $\sigma = \tau^r$ dans le groupe \mathfrak{S}_E n'est autre que $\frac{n}{d}$, où d est le P. G. C. D. de r et de n . En particulier, σ est un cycle si et seulement si r et n sont premiers entre eux.*

3. *Toutes les orbites associées à σ dans E ont le même cardinal, à savoir $\frac{n}{d}$.*

Assertion 1. — Nous savons que l'ordre de τ est égal à sa longueur (cf. cor. 1 de la prop. 2.25); par suite, le groupe cyclique G_τ a n éléments.

L'assertion 2 en découle, grâce à la proposition I.2.30.

Assertion 3. — Soient P une orbite de E associée à $\sigma = \tau^r$ et a un point de P . Posons $m = \frac{n}{d}$ et $p = \text{card}(P)$. Puisque σ est d'ordre m , P est constituée des points $a, \sigma a, \dots, \sigma^{m-1} a$, donc $p \leq m$. D'autre part, d'après la proposition 2.24, $\sigma^p a = a$. Soit maintenant z un élément de E . Il existe un entier s tel que $z = \tau^s a$; alors $\sigma^p z = \tau^{pr+s} a = \tau^s a = z$. Ainsi, $\sigma^p = I_E$, ce qui montre que l'ordre m de cette permutation divise p . Comme $p \leq m$, nous voyons que $m = p$.

PROPOSITION 2.27. — Structure des permutations circulaires.

1. Soient σ une permutation circulaire de E , τ un cycle de E de longueur n , et r un élément de $[0, n - 1]$ tel que $\sigma = \tau^r$. Alors, pour tout élément x de E , il existe une suite (x_1, x_2, \dots, x_n) d'éléments de E et une seule telle que $x_1 = x$ et que $\tau = [x_1, x_2, \dots, x_n]$. La permutation circulaire σ satisfait donc aux conditions suivantes;

$$(1) \quad \begin{aligned} \sigma(x_j) &= x_{j+r} && \text{si } j \in [1, n - r] \\ &= x_{j+r-n} && \text{si } j \in [n - r + 1, n]. \end{aligned}$$

Ainsi, pour toute permutation circulaire σ de E , il existe une suite (x_1, x_2, \dots, x_n) d'éléments de E distincts deux à deux et un élément r de $[0, n - 1]$ tels que σ soit définie par les formules (1).

2. Réciproquement, pour toute suite (x_1, x_2, \dots, x_n) d'éléments de E distincts deux à deux et pour tout élément r de $[0, n - 1]$, il existe une permutation circulaire σ de E et une seule satisfaisant aux relations (1); elle n'est autre que $[x_1, x_2, \dots, x_n]^r$.

THÉORÈME 2.14. — Décomposition d'une permutation en produit de cycles. — Soit σ une permutation de E différente de I_E .

1. Soit O_σ l'ensemble des orbites associées à σ dans E non réduites à un point. Pour tout élément P de O_σ , la permutation σ_P coïncidant avec σ sur P et avec l'identité sur le complémentaire de P est un cycle de support P ; les cycles σ_P commutent deux à deux, et

$$(1) \quad \sigma = \prod_{P \in O_\sigma} \sigma_P$$

(formule de décomposition d'une permutation en produit de cycles).

Pour tout élément P de O_σ , σ_P s'appelle le composant de σ associé à l'orbite P .

2. Une telle décomposition est unique, c'est-à-dire que s'il existe une famille finie $(\sigma'_i)_{i \in I}$ de cycles différents de I_E dont les supports sont disjoints deux à deux, telle que

$$\sigma = \prod_{i \in I} \sigma'_i,$$

il existe une bijection φ de O_σ sur I telle que, pour tout élément P de O_σ , $\sigma'_{\varphi(P)} = \sigma_P$. En particulier, les orbites associées à σ non réduites à un point ne sont autres que les supports des cycles σ'_i , où i parcourt I .

Assertion 1. — Il est immédiat que les orbites associées à σ_P sont P et les parties du complémentaire de P réduites à un point. Puisque $\text{card}(P) > 1$, σ_P est donc un cycle de support P . Les cycles σ_P commutent deux à deux, car leurs supports sont disjoints deux à deux. Enfin, la formule (1) résulte du fait que les orbites associées à σ constituent une partition de E .

Assertion 2. — Soit $(P'_i)_{i \in I}$ la famille des supports des cycles σ'_i . Il est immédiat qu'un point x de E appartient à la réunion des parties P'_i si et seulement

si $\sigma x \neq x$. Il en découle que la réunion des orbites associées à σ non réduites à un point est égale à la réunion des parties P'_i . Soient maintenant P un élément de O_σ et x un élément de P . Il existe un élément i de I tel que x appartienne à P'_i . Alors, pour tout entier naturel r , $\sigma^r x = \sigma_P^r x = \sigma_i'^r x$. Par suite, P , qui est constituée des éléments $\sigma^r x$, est égale à P'_i , qui est constituée des éléments $\sigma_i'^r x$. Par conséquent, pour tout élément P de O_σ , il existe un élément i de I tel que $P = P'_i$. Cet élément est unique, puisque les parties P'_i sont disjointes deux à deux. L'application φ de O_σ dans I ainsi définie est bijective, et, pour tout élément P de O_σ , $P'_{\varphi(P)} = P$. Enfin, pour tout élément x de P , $\sigma'_{\varphi(P)} x = \sigma x = \sigma_P x$, ce qui prouve que $\sigma'_{\varphi(P)} = \sigma_P$.

COROLLAIRE. — Calcul de l'ordre d'une permutation. — Soit σ une permutation de E différente de I_E . L'ordre de σ dans \mathfrak{S}_E est égal au P. P. C. M. des entiers m_P , où, pour tout élément P de O_σ , m_P est la longueur du cycle σ_P composant de σ .

En effet, σ s'écrit sous la forme $\sigma = \prod_{P \in O_\sigma} \sigma_P$. Puisque les éléments σ_P commutent deux à deux, l'ordre de σ est égal au P. P. C. M. des ordres des éléments σ_P . Le corollaire en découle, puisque l'ordre de σ_P est égal à m_P (cf. cor. de la prop. 2.25).

REMARQUE 1. — Supposons donnée une bijection φ de $[1, n]$ sur E , c'est-à-dire une suite (a_1, a_2, \dots, a_n) d'éléments de E distincts deux à deux. Soient σ une permutation de E différente de I_E et q le cardinal de l'ensemble O_σ des orbites associées à σ dans E non réduites à un point. Considérons maintenant l'injection de O_σ dans $[1, n]$ qui à toute orbite P associe le plus petit des entiers i tels que $a_i \in P$, noté j_P , et la relation d'ordre sur O_σ définie par les couples (P, Q) tels que $j_P \leq j_Q$. Il existe une bijection strictement croissante ψ et une seule de $[1, q]$ sur O_σ , dite canoniquement associée à σ . La décomposition de σ en cycles peut alors s'écrire

$$\sigma = \prod_{i=1}^q \sigma_{\psi(i)}.$$

REMARQUE 2. — Le théorème précédent fournit un moyen pratique de calcul de la décomposition d'une permutation en cycles.

Considérons par exemple la permutation σ de $[1, 11]$ suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 9 & 10 & 1 & 5 & 11 & 4 & 6 & 3 & 2 & 8 \end{pmatrix}.$$

On commence par chercher le composant de σ associé à l'orbite de 1, en écrivant les transformés successifs de 1 par σ ; on obtient ainsi le cycle $[1, 7, 4]$. On considère alors le plus petit des entiers i n'appartenant pas à $\{1, 7, 4\}$, c'est-à-dire 2, et on détermine le composant de σ associé à l'orbite de 2; on obtient ainsi le cycle $[2, 9, 3, 10]$. On considère ensuite le plus petit des entiers i n'appartenant pas à $\{1, 7, 4\} \cup \{2, 9, 3, 10\}$, c'est-à-dire 5; comme l'orbite de 5 est réduite à l'élément 5, $\{5\}$ n'appartient pas à O_σ . On considère donc le plus petit des entiers i n'appartenant pas à $\{1, 7, 4\} \cup \{2, 9, 3, 10\} \cup \{5\}$, c'est-à-dire 6; le composant de σ associé à l'orbite de 6 est le cycle $[6, 11, 8]$. Finalement, la décomposition de σ en cycles s'écrit

$$\sigma = [1, 7, 4] \cdot [2, 9, 3, 10] \cdot [6, 11, 8].$$

L'ordre de σ est égal au P. P. C. M. des nombres 3, 3 et 4, c'est-à-dire 12.

Étudions maintenant les classes de conjugaison dans le groupe \mathfrak{S}_E , c'est-à-dire les orbites de \mathfrak{S}_E sous \mathfrak{S}_E , le groupe \mathfrak{S}_E opérant sur lui-même par automorphismes intérieurs. Autrement dit, la classe de conjugaison d'une permutation σ de E est l'ensemble H_σ des permutations de la forme $\tau\sigma\tau^{-1}$, où τ parcourt \mathfrak{S}_E .

Nous allons caractériser les éléments de H_σ à l'aide de la décomposition de σ en cycles.

PROPOSITION 2.28. — Soient σ une permutation de E , O_σ l'ensemble des orbites associées à σ dans E non réduites à un point, et $\sigma = \prod_{P \in O_\sigma} \sigma_P$ la décomposition de σ en produit de cycles. Alors, pour toute permutation τ , les orbites associées à $\sigma' = \tau\sigma\tau^{-1}$ dans E non réduites à un point ne sont autres que les parties $\tau(P)$, où P parcourt O_σ . De plus, pour tout élément P de O_σ , $\sigma'_P = \tau\sigma_P\tau^{-1}$ est un cycle de support $\tau(P)$. Plus précisément, si $\sigma = [a_1, a_2, \dots, a_p]$, $\tau\sigma\tau^{-1}$ n'est autre que le cycle $[\tau(a_1), \tau(a_2), \dots, \tau(a_p)]$.

Enfin, la décomposition de σ' en produit de cycles n'est autre que $\sigma' = \prod_{P \in O_{\sigma'}} \sigma'_P$.

En particulier, la permutation τ transforme la partition de E constituée des orbites associées à σ en la partition de E constituée des orbites associées à σ' .

Nous sommes ainsi amené à poser la

DÉFINITION 2.21. — **Système des invariants d'une permutation.** — Soient σ une permutation de E et r le cardinal de l'ensemble O'_σ des orbites associées à σ . Il existe une suite croissante $(m_j)_{1 \leq j \leq r}$ d'entiers naturels non nuls et une seule satisfaisant à la condition suivante : il existe une bijection φ de $[1, r]$ sur O'_σ telle que, pour tout élément j de $[1, r]$, $m_j = \text{card}(\varphi(j))$. Cette suite s'appelle système des invariants de σ , ou encore type de σ , et se note I_σ .

EXEMPLE. — Reprenons la permutation σ de $[1, 11]$ introduite plus haut. Alors $I_\sigma = (1, 3, 3, 4)$.

THÉORÈME 2.15. — **Caractérisation des classes d'éléments conjugués.** — Soient σ et σ' deux permutations de E . Pour que σ et σ' soient conjuguées dans \mathfrak{S}_E , il faut et il suffit qu'elles aient le même système d'invariants.

D'après la proposition précédente, nous savons que deux permutations conjuguées ont le même système d'invariants.

Réciproquement, considérons deux permutations σ et σ' de E ayant le même système d'invariants. Il en découle qu'il existe une permutation τ' de E transformant la partition de E constituée des orbites associées à σ' en la partition de E constituée des orbites associées à σ . Posons alors $\sigma'' = \tau'\sigma'\tau'^{-1}$; les permutations σ et σ'' définissent les mêmes orbites dans E . Il suffit donc de démontrer que deux permutations σ et σ'' ayant même ensemble d'orbites sont conjuguées. Pour cela, nous utiliserons le

LEMME. — Soient ρ et ρ' deux cycles différents de I_E , ayant le même support P . Il existe alors une permutation τ de E laissant fixes tous les points du complémentaire de P dans E et telle que $\rho' = \tau\rho\tau^{-1}$.

Soient en effet x et x' deux points de P , et, pour tout $j \in [1, p]$, $x_j = \rho x^{j-1}$ et $x'_j = \rho'^{j-1} x'$. Il existe une permutation τ de E et une seule laissant fixes les points du complémentaire de P et telle que, pour tout $j \in [1, p]$, $\tau x_j = x'_j$. Il est immédiat que τ convient, ce qui achève la démonstration du lemme.

Les permutations σ et σ'' ont le même ensemble d'orbites non réduites à un point. Notons O cet ensemble, et décomposons σ et σ'' en cycles :

$$\sigma = \prod_{P \in O} \sigma_P \quad \sigma'' = \prod_{P \in O} \sigma''_P.$$

D'après le lemme, pour tout élément P de O , il existe une permutation τ_P de E laissant fixes les éléments du complémentaire de P dans E et telle que $\sigma''_P = \tau_P \sigma_P \tau_P^{-1}$. Puisque les orbites sont disjointes deux à deux, il est immédiat que les permutations τ_P commutent deux à deux. Par suite, la permutation $\tau = \prod_{P \in O} \tau_P$ satisfait à la relation $\sigma'' = \tau \sigma \tau^{-1}$, ce qui montre que σ et σ'' sont conjuguées.

COROLLAIRE. — Caractérisation des permutations circulaires.

1. Soit σ une permutation circulaire de E . L'ordre m de σ divise n , toute orbite associée à σ dans E a m éléments, et l'ensemble O'_σ de ces orbites a $q = \frac{n}{m}$ éléments. Autrement dit, le système des invariants de σ est (p_1, p_2, \dots, p_q) , où, pour tout élément j de $[1, q]$, $p_j = m$.

En particulier, deux permutations circulaires ayant le même ordre sont conjuguées.

2. Réciproquement, soient m un diviseur de n et $q = \frac{n}{m}$. Il existe alors une permutation circulaire σ d'ordre m , et l'ensemble des permutations de E dont le système d'invariants est (p_1, p_2, \dots, p_q) , où, pour tout $j \in [1, q]$, $p_j = m$, n'est autre que l'ensemble des permutations circulaires de E conjuguées de σ .

Assertion 1. — Il suffit d'appliquer la proposition 2.26 et le théorème précédent.

Assertion 2. — Considérons un cycle τ de longueur n (cf. prop. 2.25). Alors la permutation circulaire $\sigma = \tau^q$ est d'ordre $\frac{n}{d}$, où $d = \text{P. G. C. D.}(n, q) = q$. Donc l'ordre de σ est égal à $\frac{n}{q} = m$. Le reste de l'assertion résulte du théorème précédent.

2. SIGNATURE D'UNE PERMUTATION

THÉORÈME 2.16. — Soit E un ensemble fini ayant n éléments, $n \geq 2$. Les transpositions de E engendrent le groupe symétrique \mathfrak{S}_E .

Pour toute permutation σ de E , désignons par $q(\sigma)$ le cardinal de l'ensemble des éléments x de E tels que $\sigma x \neq x$. Lorsque $q(\sigma) = 0$, $\sigma = I_E = \tau^2$, pour toute transposition τ de E . (Il existe une transposition de E , car $n \geq 2$.)

Supposons donc le théorème démontré pour toutes les permutations σ de E telles que $q(\sigma) < p$, où $p \geq 1$, considérons une permutation σ telle que $q(\sigma) = p$, et notons Q l'ensemble des points de E fixes par σ . Il existe un point x de E tel que $\sigma x \neq x$. Soient τ la transposition $[x, \sigma x]$ et $\sigma' = \tau\sigma$. Puisque σx appartient à l'orbite de x associée à σ dans E , et que cette orbite n'est pas réduite à un point, σx n'appartient pas à Q . Par suite, τ induit l'identité sur Q . Il en découle que l'ensemble Q' des points de E fixes par σ' est égal à $Q \cup \{x\}$; donc $q(\sigma') = p - 1$, et l'hypothèse de récurrence s'applique à σ' ; l'assertion en résulte, puisque $\sigma = \tau\sigma'$.

Lorsqu'on donne une bijection φ de $[1, n]$ sur E , on peut préciser le théorème précédent, grâce à la notion suivante :

DÉFINITION 2.22. — Transpositions élémentaires. — Soit φ une bijection de $[1, n]$ sur E , c'est-à-dire une suite (a_1, a_2, \dots, a_n) d'éléments de E distincts deux à deux. On appelle transpositions élémentaires les transpositions $\tau_j = [a_j, a_{j+1}]$, où $j \in [1, n - 1]$.

COROLLAIRE. — Dans ces conditions, les transpositions élémentaires engendrent le groupe symétrique \mathfrak{S}_E .

Soit en particulier τ une transposition. Il existe un couple (i, j) d'entiers et un seul tel que $i < j$ et que $\tau = [a_i, a_j]$. Alors

$$(1) \quad \tau = \tau_{j-1}\tau_{j-2} \dots \tau_{i+1}\tau_i\tau_{i+1} \dots \tau_{j-2}\tau_{j-1}.$$

Il suffit évidemment de démontrer la formule (1). L'entier i étant fixé, on la démontre par récurrence sur $j - i$. Lorsque $j - i = 1$, $\tau = \tau_i$, et la formule (1) est satisfaite. Supposons donc que la formule est vraie si $j - i = p - 1$, où $p \geq 2$, et considérons la transposition $\tau = [a_i, a_j]$, où $j - i = p$. Alors $\tau' = \tau_{j-1}\tau\tau_{j-1}$ est égale à $[a_i, a_{j-1}]$: en effet, les éléments de E différents de a_i, a_j et a_{j-1} sont fixes par τ et τ_{j-1} , $\tau'(a_i) = a_{j-1}$, $\tau'(a_{j-1}) = a_i$ et $\tau'(a_j) = a_j$. On en déduit la formule (1) en appliquant l'hypothèse de récurrence à τ' .

On rappelle qu'un caractère d'un groupe G à valeurs dans un anneau commutatif unitaire A (dont l'élément neutre est noté 1) est un morphisme χ du groupe G dans le groupe multiplicatif A^* des éléments inversibles de A , et que χ est dit trivial si $\chi(g) = 1$ pour tout élément g de G .

PROPOSITION 2.29. — Caractères du groupe symétrique. — Soient A un anneau intègre unitaire de caractéristique 0 et χ un caractère de \mathfrak{S}_E à valeurs dans A . L'ensemble des valeurs de χ est contenu dans le sous-groupe $\mathbf{G}_2 = \{-1, 1\}$ de A^* . De plus, si χ n'est pas trivial, alors, pour toute transposition τ , $\chi(\tau) = -1$.

Soient χ un caractère et τ une transposition de E . Puisque $\tau^2 = I_E$, $(\chi(\tau))^2 = 1$. Comme A est intègre, il en découle que $\chi(\tau) \in \mathbf{G}_2$. Par suite, χ est à valeurs dans \mathbf{G}_2 , puisque les transpositions engendrent le groupe \mathfrak{S}_E . Si

χ n'est pas trivial, il existe au moins une transposition τ telle que $\chi(\tau) = -1$. Soit maintenant τ' une transposition de E . Nous savons (cf. th. 2.15) que τ et τ' sont conjuguées, d'où il résulte aussitôt que $\chi(\tau') = \chi(\tau) = -1$.

Pour étudier l'existence d'un caractère non trivial du groupe \mathfrak{S}_E à valeurs dans A , nous utiliserons la

PROPOSITION 2.30. — Opérations du groupe symétrique sur les fonctions de n variables. — Soient E un ensemble fini non vide ayant n éléments, X un ensemble non vide, et A un anneau commutatif unitaire. Soit F la A -algèbre unitaire constituée des applications de X^E dans A . Pour tout élément f de F et pour toute permutation σ de E , on note σf l'application de X^E dans A qui à toute famille $(x_a)_{a \in E}$ d'éléments de X associe l'élément $f[(x_{\sigma(a)})_{a \in E}]$.

1. L'application $(\sigma, f) \mapsto \sigma f$ est une opération du groupe \mathfrak{S}_E sur l'ensemble F , dite canonique.

2. L'application $f \mapsto \sigma f$ est un automorphisme de l'algèbre unitaire F . En particulier, pour tout couple (f, g) d'éléments de F et pour tout élément α de A ,

$$\sigma(f + g) = \sigma f + \sigma g \quad \sigma(fg) = (\sigma f)(\sigma g) \quad \sigma(\alpha f) = \alpha(\sigma f).$$

EXEMPLE. — Prenons $E = [1, n]$ et $A = \mathbf{Z}$. Alors le groupe \mathfrak{S}_n opère canoniquement sur l'anneau unitaire $F = \mathcal{F}(X^n, \mathbf{Z})$: pour tout élément f de F et pour tout élément σ de \mathfrak{S}_n ,

$$(\sigma f)(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

DÉFINITION 2.23. — Poids. — On dit qu'une application non nulle f de X^E dans A est un poids pour le groupe \mathfrak{S}_E si, pour toute permutation σ de E , il existe un élément λ_σ de A tel que $\sigma f = \lambda_\sigma f$.

PROPOSITION 2.31. — Caractère associé à un poids. — On suppose que l'anneau A est intègre unitaire. Soit f un poids pour le groupe \mathfrak{S}_E . Alors, pour tout élément σ de \mathfrak{S}_E , il existe un élément λ_σ de A et un seul tel que $\sigma f = \lambda_\sigma f$. De plus, l'application $\chi : \sigma \mapsto \lambda_\sigma$ est un caractère de \mathfrak{S}_E à valeurs dans A .

Puisque f n'est pas nul et que A est intègre, λ_σ est unique. Considérons maintenant deux éléments σ et τ de \mathfrak{S}_E ; alors $(\tau\sigma)f = \chi(\tau\sigma)f$. D'autre part, $(\tau\sigma)f = \tau(\sigma f) = \tau[\chi(\sigma)f] = \chi(\sigma)(\tau f) = \chi(\sigma)\chi(\tau)f$. Par unicité, nous en déduisons que $\chi(\tau\sigma) = \chi(\tau)\chi(\sigma)$.

THÉORÈME 2.17. — Signature d'une permutation. — Soit A un anneau intègre unitaire de caractéristique 0.

1. Il existe un caractère non trivial ε et un seul, appelé signature, du groupe \mathfrak{S}_E à valeurs dans A . Pour toute transposition τ ,

$$(1) \quad \varepsilon(\tau) = -1.$$

Plus généralement, pour toute permutation σ de E et pour toute suite $(\tau_1, \tau_2, \dots, \tau_p)$ de p transpositions telle que $\sigma = \tau_1 \tau_2 \dots \tau_p$,

$$\varepsilon(\sigma) = (-1)^p.$$

C'est pourquoi les permutations de signature égale à 1 sont dites paires, et celles de signature égale à -1 sont dites impaires.

De plus, la signature est le seul morphisme ε du groupe \mathfrak{S}_E dans le groupe multiplicatif $\mathbf{G}_2 = \{-1, 1\}$ tel que, pour toute transposition τ , $\varepsilon(\tau) = -1$.

2. Soit φ une bijection de $[1, n]$ sur E , définissant une relation d'ordre total sur E . Alors l'élément v de $F = \mathcal{F}(A^E, A)$ qui à toute famille $(x_a)_{a \in E}$ associe l'élément $\prod_{b < c} (x_c - x_b)$ est un poids pour le groupe \mathfrak{S}_E dont le caractère associé n'est autre que ε . La fonction v s'appelle fonction de Vandermonde sur A^E .

Dans ces conditions, pour toute permutation σ de E , la signature $\varepsilon(\sigma)$ est égale à $(-1)^{n(\sigma)}$, où $n(\sigma)$ est le cardinal de l'ensemble des couples (b, c) d'éléments de E tels que $b < c$ et $\sigma b > \sigma c$. (Un tel couple s'appelle une inversion de la permutation σ .)

Unicité de la signature. — Soit ε un caractère non trivial de \mathfrak{S}_E à valeurs dans A . Alors, pour toute transposition τ , $\varepsilon(\tau) = -1$ (cf. prop. 2.29). Pour toute permutation σ de E , il existe une suite $(\tau_1, \tau_2, \dots, \tau_p)$ de transpositions de E telle que $\sigma = \tau_1 \tau_2 \dots \tau_p$ (cf. th. 2.16). Puisque ε est un caractère et que, pour tout $j \in [1, p]$, $\varepsilon(\tau_j) = -1$, $\varepsilon(\sigma) = (-1)^p$. L'unicité de ε en résulte.

Existence de la signature et assertion 2. — La démonstration s'effectue en plusieurs étapes.

a) Nous allons prouver que, pour toute permutation σ de E , la fonction de Vandermonde sur A^E satisfait à la relation

$$(2) \quad \sigma v = (-1)^{n(\sigma)} v,$$

où $n(\sigma)$ désigne le cardinal de l'ensemble Q_σ des inversions de σ . Considérons pour cela la partie P de $E \times E$ constituée des couples (b, c) tels que $b < c$, et la symétrie canonique $\delta : (b, c) \mapsto (c, b)$ de $E \times E$. Soit σ une permutation de E . Puisque l'application $f \mapsto \sigma f$ est un endomorphisme d'algèbre,

$$(3) \quad \sigma v((x_a)_{a \in E}) = \prod_{(b, c) \in P} (x_{\sigma c} - x_{\sigma b}).$$

L'application $\tilde{\sigma} : (b, c) \mapsto (\sigma b, \sigma c)$ est une bijection de $E \times E$ sur lui-même, transformant P en une partie $\tilde{\sigma}P$. Donc

$$(4) \quad \sigma v((x_a)_{a \in E}) = \prod_{(b, c) \in \tilde{\sigma}P} (x_c - x_b).$$

Introduisons les ensembles $R_\sigma = \tilde{\sigma}P \cap P$ et $T_\sigma = \tilde{\sigma}P \cap \delta P$. Il est immédiat que R_σ et T_σ sont complémentaires dans $\tilde{\sigma}P$. De plus, puisque $\tilde{\sigma}\delta = \delta\tilde{\sigma}$, R_σ et δT_σ sont complémentaires dans P . Enfin, $\tilde{\sigma}$ transforme Q_σ en T_σ . Par suite,

$$\begin{aligned}
 (5) \quad \sigma v((x_a)_{a \in E}) &= \prod_{(b,c) \in R_\sigma} (x_c - x_b) \prod_{(b,c) \in T_\sigma} (x_c - x_b) \\
 &= \prod_{(b,c) \in R_\sigma} (x_c - x_b) \prod_{(b,c) \in \delta T_\sigma} (x_b - x_c) \\
 &= (-1)^{\text{card}(Q_\sigma)} \prod_{(b,c) \in P} (x_c - x_b) \\
 &= (-1)^{\text{card}(Q_\sigma)} v((x_a)_{a \in E}),
 \end{aligned}$$

ce qui démontre la formule (2), puisque $n(\sigma) = \text{card}(Q_\sigma)$.

b) Prouvons maintenant l'existence de ε et la formule (1). Comme l'anneau A est infini, la fonction v n'est pas nulle. La formule (2) montre alors que v est un poids pour \mathfrak{S}_E , dont le caractère associé ε est à valeurs dans $\mathbf{G}_2 = \{-1, 1\}$; de plus, pour toute permutation σ de E ,

$$\varepsilon(\sigma) = (-1)^{n(\sigma)}.$$

Le caractère σ est donc non trivial, puisque, pour toute transposition élémentaire τ , $n(\tau) = -1$, et, par suite, $\varepsilon(\tau) = (-1)^{n(\tau)} = -1$.

c) Enfin, comme il existe des anneaux intègres unitaires de caractéristique 0 (par exemple \mathbf{Z}), ce qui précède établit l'existence d'un morphisme du groupe \mathfrak{S}_E dans le groupe multiplicatif \mathbf{G}_2 tel que, pour toute transposition τ , $\varepsilon(\tau) = -1$. Un tel morphisme est unique, puisque les transpositions engendrent \mathfrak{S}_E .

COROLLAIRE 1. — Signature d'un cycle, d'une permutation circulaire. — La signature d'un cycle τ de longueur p est égale à $(-1)^{p-1}$. Par suite, pour toute permutation circulaire $\sigma = \tau^q$, où τ est un cycle de longueur n ,

$$\varepsilon(\sigma) = (-1)^{(n-1)q}.$$

En particulier, si n est impair, toute permutation circulaire est paire.

Il suffit de remarquer que

$$[a_1, a_2, \dots, a_n] = [a_1, a_2] \cdot [a_2, a_3] \dots [a_{n-1}, a_n]$$

et que, dans le second membre, figurent $n - 1$ transpositions. Comme la signature d'une transposition est égale à -1 , l'assertion en découle.

COROLLAIRE 2. — Calcul de la signature à l'aide des orbites. — Soient σ une permutation de E et r le cardinal de l'ensemble O'_σ des orbites associées à σ dans E . Alors

$$\varepsilon(\sigma) = (-1)^{n-r}.$$

En particulier, pour toute permutation circulaire σ d'ordre m ,

$$\varepsilon(\sigma) = (-1)^{n-q},$$

où $q = \frac{n}{m}$.

La formule de décomposition de σ en cycles $\sigma = \prod_{P \in O_\sigma} \sigma_P$ montre que

$$\varepsilon(\sigma) = \prod_{P \in O_\sigma} \varepsilon(\sigma_P).$$

Or, d'après le corollaire 1, $\varepsilon(\sigma_P) = (-1)^{\text{card}(P)-1}$. Lorsque P est une orbite réduite à un point, $(-1)^{\text{card}(P)-1} = 1$. Par suite,

$$\varepsilon(\sigma) = (-1)^p,$$

où $p = \sum_{P \in O'_\sigma} [\text{card}(P) - 1]$. Comme O'_σ est une partition de E ,

$$\sum_{P \in O'_\sigma} \text{card}(P) = n.$$

Donc $p = n - r$.

EXEMPLE. — Reprenons la permutation σ de $[1, 11]$ définie dans la remarque 2 suivant le corollaire du théorème 2.14. Puisque $n = 11$ et que σ est de type $(1, 3, 3, 4)$, le nombre r d'orbites est égal à 4, et

$$\varepsilon(\sigma) = (-1)^{11-4} = (-1)^7 = -1.$$

Le lecteur pourra retrouver ce résultat en déterminant les inversions de σ , et vérifier que $n(\sigma) = 33$.

COROLLAIRE 3. — Groupe alterné. — Soit E un ensemble fini ayant n éléments, $n \geq 2$. La signature ε est un morphisme surjectif de \mathfrak{S}_E sur \mathbf{G}_2 , dont le noyau est un sous-groupe distingué de \mathfrak{S}_E , appelé groupe alterné de E , et noté \mathfrak{A}_E . Le groupe alterné de E est donc constitué des permutations paires de E . Pour toute permutation impaire σ_0 , les ensembles \mathfrak{A}_E et $\sigma_0 \mathfrak{A}_E$ constituent une partition de \mathfrak{S}_E . L'ordre de \mathfrak{A}_E est donc égal à $\frac{n!}{2}$.

Lorsque $E = [1, n]$, le groupe alterné de E s'appelle groupe alterné de degré n , et se note \mathfrak{A}_n .

EXEMPLES. — Nous allons étudier le groupe alterné \mathfrak{A}_n et, plus généralement, tous les sous-groupes distingués de \mathfrak{S}_n . Remarquons à cet effet qu'un sous-groupe distingué G de \mathfrak{S}_n contenant une transposition est égal à \mathfrak{S}_n , car deux transpositions quelconques sont conjuguées, et que les transpositions engendrent le groupe symétrique.

Dans ce qui suit, on note G_n le groupe cyclique à n éléments, et on appelle groupe de Klein le groupe $G_2 \times G_2$.

1. *Cas où $n = 2$.* Alors \mathfrak{S}_2 est isomorphe à G_2 , et \mathfrak{A}_2 est réduit à l'élément neutre.

2. *Cas où $n = 3$.* Alors \mathfrak{S}_3 est constitué de l'application identique, de trois transpositions et de deux cycles de longueur 3. Le groupe \mathfrak{A}_3 est isomorphe au groupe cyclique G_3 ; c'est le seul sous-groupe distingué non trivial G de \mathfrak{S}_3 .

En effet, un tel sous-groupe G ne contient aucune transposition. Le sous-groupe G contient donc l'un des deux cycles de longueur 3; il contient l'autre, car ces cycles sont conjugués (cf. th. 2.15). Le sous-groupe G est donc égal à \mathfrak{A}_3 .

3. *Cas où $n = 4$.* Alors \mathfrak{S}_4 est constitué de l'application identique, de six transpositions, de huit cycles de longueur 3, de six cycles de longueur 4, et de trois permutations de type (2, 2). Le groupe \mathfrak{A}_4 est constitué de l'application identique, des huit cycles de longueur 3 et des trois permutations de type (2, 2). Le groupe \mathfrak{A}_4 n'est pas commutatif; il possède un sous-groupe distingué \mathfrak{K}_4 d'ordre 4, constitué de I_E et des trois permutations de type (2, 2). Le groupe \mathfrak{K}_4 est isomorphe au groupe de Klein, et $\mathfrak{A}_4/\mathfrak{K}_4$ est isomorphe au groupe cyclique G_3 . De plus, \mathfrak{K}_4 est le seul sous-groupe distingué non trivial de \mathfrak{A}_4 ; enfin, \mathfrak{K}_4 et \mathfrak{A}_4 sont les seuls sous-groupes distingués non triviaux de \mathfrak{S}_4 .

Il est immédiat que \mathfrak{K}_4 est distingué, puisque le type d'une permutation est invariant par automorphismes intérieurs. Comme \mathfrak{K}_4 a quatre éléments et n'est pas cyclique, \mathfrak{K}_4 est isomorphe au groupe de Klein.

Soit G un sous-groupe distingué non trivial de \mathfrak{A}_4 . Le groupe G ne contient aucun cycle d'ordre 3, car, sinon, il les contiendrait tous, et serait d'ordre supérieur ou égal à 9, ce qui est impossible, puisque l'ordre de G doit diviser strictement l'ordre de \mathfrak{A}_4 , à savoir 12. Le groupe G contient donc au moins un élément de type (2, 2), et, par suite, $G = \mathfrak{K}_4$.

Soit maintenant H un sous-groupe distingué non trivial de \mathfrak{S}_4 . Le groupe $G = H \cap \mathfrak{A}_4$ est un sous-groupe distingué de \mathfrak{A}_4 . Le groupe G n'est pas réduit à $\{I_E\}$: sinon, pour tout élément σ de H , σ^2 serait égal à I_E ; les seuls éléments de \mathfrak{S}_4 satisfaisant à cette relation étant les éléments de \mathfrak{K}_4 et les transpositions, et H n'étant pas réduit à $\{I_E\}$, H contiendrait une transposition, et serait donc égal à \mathfrak{S}_4 , ce qui est absurde. Ainsi, G est un sous-groupe distingué de \mathfrak{A}_4 non réduit à $\{I_E\}$, et, par suite, G contient \mathfrak{K}_4 . Distinguons deux cas :

— Le groupe G contient strictement \mathfrak{K}_4 ; alors $G = \mathfrak{A}_4$. Le groupe H est réduit à \mathfrak{A}_4 , car l'ordre de H doit diviser strictement l'ordre de \mathfrak{S}_4 , égal à 24.

— Le groupe G est égal à \mathfrak{K}_4 ; alors $H = \mathfrak{K}_4$. En effet, dans le cas contraire, H contiendrait au moins un cycle d'ordre 4, et, par suite, tous les cycles d'ordre 4; donc H aurait 10 éléments, ce qui est impossible, puisque l'ordre de H divise 24.

4. *Cas où $n \geq 5$.* On montre alors (cf. exercice 35) que le groupe \mathfrak{A}_n est simple (c'est-à-dire qu'il admet aucun sous-groupe distingué non trivial), et que \mathfrak{A}_n est le seul sous-groupe distingué de \mathfrak{S}_n .

3. POLYNÔMES ET FRACTIONS RATIONNELLES SYMÉTRIQUES

Dans ce sous-paragraphe, n désigne un entier naturel non nul.

PROPOSITION 2.32. — Opérations du groupe symétrique sur les polynômes.

1. L'application qui à tout couple (σ, P) constitué d'un élément σ de \mathfrak{S}_n et d'un élément P de $A[X_1, X_2, \dots, X_n]$ associe le polynôme σP défini par la formule

$$\sigma P(X_1, X_2, \dots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$$

est une opération du groupe \mathfrak{S}_n sur $A[X_1, X_2, \dots, X_n]$. En particulier, pour tout couple (σ, τ) d'éléments de \mathfrak{S}_n ,

$$(\tau\sigma)P = \tau(\sigma P).$$

2. Soit σ un élément de \mathfrak{S}_n . L'application $P \mapsto \sigma P$ est un automorphisme de la A -algèbre unitaire $A[X_1, X_2, \dots, X_n]$. En particulier, pour tout couple (P, Q) d'éléments de $A[X_1, X_2, \dots, X_n]$ et pour tout scalaire α ,

$$\sigma(P + Q) = \sigma P + \sigma Q$$

$$\sigma(\alpha P) = \alpha \sigma P$$

$$\sigma(PQ) = \sigma P \sigma Q.$$

3. Soit U un polynôme p -homogène, où $p \in \mathbb{N}$. Alors, pour tout élément σ de \mathfrak{S}_n , σU est encore un polynôme p -homogène. Par suite, si P est un élément de $A[X_1, X_2, \dots, X_n]$, décomposé en ses composantes homogènes sous la forme

$$P = \sum_{p=0}^{+\infty} U_p, \text{ la décomposition de } \sigma P \text{ en ses composantes homogènes n'est autre que } \sigma P = \sum_{p=0}^{+\infty} \sigma U_p.$$

Les assertions 1 et 2 sont immédiates.

Assertion 3. — On se ramène à prouver que si U est un monôme de degré p , σU en est un, ce qui est évident.

PROPOSITION 2.33. — Poids du groupe symétrique dans les polynômes. — On suppose que l'anneau A est intègre et de caractéristique 0. Alors les poids de \mathfrak{S}_n dans l'espace vectoriel $A[X_1, X_2, \dots, X_n]$ sont

- a) les polynômes non nuls P tels que, pour tout élément σ de \mathfrak{S}_n , $\sigma P = P$;
- b) les polynômes non nuls P tels que, pour tout élément σ de \mathfrak{S}_n , $\sigma P = \varepsilon(\sigma)P$.

Soit en effet P un poids de \mathfrak{S}_n . D'après la proposition 2.31, il existe un caractère χ du groupe symétrique tel que, pour tout élément σ de \mathfrak{S}_n , $\sigma P = \chi(\sigma)P$. Les seuls caractères du groupe symétrique à valeurs dans A étant le caractère trivial et la signature (cf. th. 2.17), le résultat annoncé en découle.

Nous sommes ainsi amené à poser la

DÉFINITION 2.24. — **Polynômes symétriques, polynômes antisymétriques.** On dit qu'un élément P de $A[X_1, X_2, \dots, X_n]$ est symétrique (resp. antisymétrique) si, pour tout élément σ de \mathfrak{S}_n , $\sigma P = P$ (resp. $\sigma P = \varepsilon(\sigma)P$).

PROPOSITION 2.34. — **Propriétés des polynômes symétriques et antisymétriques.**

1. Les polynômes symétriques constituent une sous-algèbre unitaire de l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$, notée \mathcal{S} ; les polynômes antisymétriques constituent un sous-espace vectoriel de l'espace vectoriel $A[X_1, X_2, \dots, X_n]$, noté \mathcal{A} . Le produit de deux polynômes antisymétriques est symétrique, le produit d'un polynôme symétrique et d'un polynôme antisymétrique est antisymétrique.

Si la caractéristique de A est différente de 2, la somme $\mathcal{S} + \mathcal{A}$ est directe; si la caractéristique de A est 2, alors $\mathcal{A} = \mathcal{S}$.

2. Pour qu'un polynôme soit symétrique, ou antisymétrique, il faut et il suffit que toutes ses composantes homogènes le soient.

REMARQUE. — Lorsque $n = 1$, $\mathcal{S} = A[X]$; si, de plus, la caractéristique de A est différente de 2, $\mathcal{A} = \{0\}$.

Dans ce qui suit, nous nous proposons de déterminer tous les polynômes symétriques et antisymétriques.

Pour construire des polynômes symétriques, on utilise le procédé général suivant :

PROPOSITION 2.35. — **Construction d'invariants d'un groupe fini.** — Soient E un A -module, G un groupe fini, H un sous-groupe de G , et $(g, x) \mapsto gx$ une opération de G sur E telle que, pour tout élément g de G , l'application $x \mapsto gx$ soit un automorphisme de E .

On désigne par E^G (resp. par E^H) le sous-module de E constitué des éléments x de E invariants par G (resp. par H), c'est-à-dire tels que $gx = x$ pour tout élément g de G (resp. de H).

1. Le sous-module E^G est contenu dans le sous-module E^H . Pour tout élément x de E^H et pour tout élément g de G , l'élément gx ne dépend que de la classe à gauche $\gamma = gH$ de g suivant H ; on le note γx . L'application $x \mapsto \sum_{\gamma \in G/H} \gamma x$ est une application linéaire, notée $I_{G,H}$, de E^H dans E^G . De plus,

$$(I_{G,H})^2 = nI_{G,H},$$

où
$$n = \text{card}(G/H) = \frac{\text{card}(G)}{\text{card}(H)}.$$

2. Soient H' un sous-groupe de H , et $E^{H'}$ le sous-module de E constitué des éléments de E invariants par H' . Alors

$$I_{G,H'} = I_{G,H} \circ I_{H,H'}.$$

L'assertion 1 est immédiate.

Assertion 2. — Soient Q un système de représentants de G/H dans G , et Q' un système de représentants de H/H' dans H . Alors l'ensemble $P = QQ'$ des éléments de G de la forme gg' où $g \in Q$ et $g' \in Q'$, est un système de représentants de G/H' dans G . L'assertion en découle aussitôt.

REMARQUE. — Lorsque H est réduit à l'élément neutre de G , l'application $I_{G,H}$ se note plus simplement I_G .

Voici un exemple fondamental :

PROPOSITION 2.36. — **Polynômes symétriques élémentaires.**

1. Pour tout entier $p \in [1, n]$, le monôme $M_p = X_1 X_2 \dots X_p$ est invariant par le sous-groupe H_p de $G = \mathfrak{S}_n$ laissant stables les intervalles $[1, p]$ et $[p + 1, n]$. L'ensemble F_p des permutations σ de $[1, n]$ telles que

$$(1) \quad \sigma(1) < \sigma(2) < \dots < \sigma(p) \quad \text{et} \quad \sigma(p+1) < \sigma(p+2) < \dots < \sigma(n)$$

est un système de représentants dans G de G/H_p .

2. Le polynôme

$$(2) \quad S_p = I_{G,H_p}(X_1 X_2 \dots X_p) = \sum_{\sigma \in F_p} X_{\sigma(1)} X_{\sigma(2)} \dots X_{\sigma(p)}$$

est symétrique et homogène de degré p ; on l'appelle polynôme symétrique élémentaire de degré p .

De plus, l'application qui à tout élément σ de F_p associe sa restriction φ à $[1, p]$ est une bijection de F_p sur l'ensemble \mathcal{F}_p des applications strictement croissantes de $[1, p]$ dans $[1, n]$. La formule (2) peut donc encore s'écrire sous la forme

$$(2') \quad S_p = \sum_{\varphi \in \mathcal{F}_p} X_{\varphi(1)} X_{\varphi(2)} \dots X_{\varphi(p)}.$$

Ainsi, le polynôme S_p est une somme de C_n^p monômes; en outre, les monômes $X_{\varphi(1)} X_{\varphi(2)} \dots X_{\varphi(n)}$, où φ parcourt \mathcal{F}_p , sont distincts deux à deux.

En particulier,

$$(3) \quad S_1 = \sum_{j=1}^n X_j$$

$$(4) \quad S_2 = \sum_{i < j} X_i X_j$$

$$(5) \quad S_{n-1} = \sum_{j=1}^n X_1 \dots X_{j-1} X_{j+1} \dots X_n$$

$$(6) \quad S_n = X_1 X_2 \dots X_n.$$

Assertion 1. — Il est immédiat que le sous-groupe des éléments σ de \mathfrak{S}_n tels que $\sigma M_p = M_p$ est égal au sous-groupe H_p . Tout élément σ' de \mathfrak{S}_n peut s'écrire sous la forme $\sigma' = \sigma\tau$, où $\sigma \in F_p$ et où $\tau \in H_p$. D'autre part, deux éléments distincts de F_p ne sont pas congrus modulo H_p , ce qui prouve que F_p est un système de représentants dans G de G/H_p .

Assertion 2. — L'application $\sigma \mapsto \varphi$ est injective : soient en effet σ et σ' deux éléments de F_p ayant même restriction à $[1, p]$; alors, par passage aux complémentaires, nous en déduisons que $\sigma([p+1, n]) = \sigma'([p+1, n])$. Puisque σ et σ' appartiennent à F_p , il en découle que, pour tout élément j de $[p+1, n]$, $\sigma(j) = \sigma'(j)$, et donc que $\sigma = \sigma'$.

L'application $\sigma \mapsto \varphi$ est surjective : soit en effet φ une application strictement croissante de $[1, p]$ dans $[1, n]$; il existe une application strictement croissante ψ et une seule de $[p+1, n]$ dans $[1, n] - \varphi([1, p])$. L'application φ est alors l'image de la permutation σ dont les restrictions à $[1, p]$ et à $[p+1, n]$ sont respectivement φ et ψ .

Il reste à prouver que si φ et φ' sont deux éléments de \mathcal{F}_p tels que

$$(7) \quad X_{\varphi(1)} X_{\varphi(2)} \dots X_{\varphi(p)} = X_{\varphi'(1)} X_{\varphi'(2)} \dots X_{\varphi'(p)},$$

alors $\varphi = \varphi'$, ce qui est immédiat, puisque la relation (7) équivaut à la relation $\varphi([1, p]) = \varphi'([1, p])$.

L'intérêt des polynômes symétriques élémentaires apparaît dans la

PROPOSITION 2.37. — Relations entre coefficients et racines d'un polynôme. — Soit $B = A[X_1, X_2, \dots, X_n]$ l'algèbre des polynômes à n indéterminées. Alors, dans l'algèbre $B[X] = A[X_1, X_2, \dots, X_n, X]$,

$$(8) \quad \prod_{i=1}^n (X - X_i) = X^n - S_1 X^{n-1} + \dots + (-1)^{n-p} S_{n-p} X^p + \dots + (-1)^n S_n,$$

où S_1, S_2, \dots, S_n désignent les polynômes symétriques élémentaires de B .

Pour tout élément p de $[1, n]$, notons \mathcal{P}_p l'ensemble des parties de $[1, n]$ ayant p éléments, et \mathcal{F}_p l'ensemble des applications strictement croissantes de $[1, p]$ dans $[1, n]$. Alors

$$(9) \quad \prod_{i=1}^n (X - X_i) = X^n - Q_1 X^{n-1} + \dots + (-1)^{n-p} Q_{n-p} X^p + \dots + (-1)^n Q_n,$$

où, pour tout élément p de $[1, n]$,

$$(10) \quad Q_p = \sum_{P \in \mathcal{P}_p} \left(\prod_{i \in P} X_i \right).$$

Puisque l'application $\varphi \mapsto \varphi([1, p])$ est une bijection de \mathcal{F}_p sur \mathcal{P}_p et que

$$X_{\varphi(1)} X_{\varphi(2)} \dots X_{\varphi(p)} = \prod_{i \in \varphi([1, p])} X_i,$$

la formule (10) s'écrit encore

$$(11) \quad Q_p = \sum_{\varphi \in \mathcal{F}_p} X_{\varphi(1)} X_{\varphi(2)} \dots X_{\varphi(p)} = S_p.$$

La formule (8) découle alors des formules (9) et (11).

COROLLAIRE. — Soient S_1, S_2, \dots, S_n les polynômes symétriques élémentaires de $A[X_1, X_2, \dots, X_n]$ et $S'_1, S'_2, \dots, S'_{n-1}$ les polynômes symétriques élémentaires de $A[X_1, X_2, \dots, X_{n-1}]$. Alors, pour tout élément p de $[1, n-1]$,

$$(12) \quad S_p(X_1, X_2, \dots, X_{n-1}, 0) = S'_p(X_1, X_2, \dots, X_{n-1}).$$

De plus,

$$(13) \quad S_n(X_1, X_2, \dots, X_{n-1}, 0) = 0.$$

En effet,

$$(8) \quad \prod_{i=1}^n (X - X_i) = X^n - S_1 X^{n-1} + \dots + (-1)^{n-p} S_{n-p} X^p + \dots + (-1)^n S_n$$

$$(8') \quad \prod_{i=1}^{n-1} (X - X_i) = X^{n-1} - S'_1 X^{n-2} + \dots + (-1)^{n-p-1} S'_{n-p-1} X^p + \dots + (-1)^{n-1} S'_{n-1}.$$

La formule (13) est évidente. La relation (12) s'obtient en substituant 0 à X_n dans la relation (8) et en comparant le résultat à la relation (8'), compte tenu de la formule (13).

Nous allons démontrer maintenant que tout polynôme symétrique peut s'exprimer à l'aide des polynômes symétriques élémentaires. Remarquons tout d'abord que si, dans un monôme $Y_1^{p_1} Y_2^{p_2} \dots Y_n^{p_n}$ nous substituons les polynômes S_1, S_2, \dots, S_n aux indéterminées Y_1, Y_2, \dots, Y_n , nous obtenons un polynôme homogène de degré $p_1 + 2p_2 + \dots + np_n$, ce qui nous amène à poser la

DÉFINITION 2.25. — Polynômes isobares. — Pour tout élément s de $S = \mathbb{N}^n$, on appelle norme de s le nombre entier $\|s\| = \sum_{j=1}^n j s(j)$; pour tout entier naturel p , on note L_p l'ensemble des éléments s de S tels que $\|s\| = p$. Les ensembles L_p constituent une partition de S . Les éléments du sous-module B_p de $A[X_1, X_2, \dots, X_n]$ engendré par les monômes X^s tels que $\|s\| = p$ s'appellent polynômes p -isobares. On dit qu'un polynôme est isobare s'il appartient à l'un des sous-modules B_p .

Le A -module $A[X_1, X_2, \dots, X_n]$ est somme directe des sous-modules B_p , où p parcourt \mathbb{N} . Ainsi, tout élément P de $A[X_1, X_2, \dots, X_n]$ peut s'écrire

d'une manière et d'une seule sous la forme $P = \sum_{p=0}^{+\infty} W_p$, où, pour tout entier p , W_p est p -isobare (cf. prop. I.3.23).

DÉFINITION 2.26. — Poids d'un polynôme. — Soit P un élément de $A[X_1, X_2, \dots, X_n]$, écrit sous la forme $P = \sum_{p=0}^{+\infty} W_p$, où, pour tout entier p , W_p est p -isobare.

Si P est non nul, on appelle poids de P le plus grand des entiers p tels que W_p soit non nul.

Si P est nul, on appelle poids de P l'élément $-\infty$.

Les polynômes p -isobares non nuls sont donc de poids p . Le poids d'un polynôme P se note $\pi(P)$.

THÉORÈME 2.18. — Structure des polynômes symétriques. — Soit A un anneau intègre. Pour tout polynôme symétrique P appartenant à $A[X_1, X_2, \dots, X_n]$, il existe un élément Q et un seul de $A[Y_1, Y_2, \dots, Y_n]$ tel que

$$(1) \quad P(X_1, X_2, \dots, X_n) = Q(S_1, S_2, \dots, S_n),$$

où S_1, S_2, \dots, S_n sont les polynômes symétriques élémentaires de l'algèbre $A[X_1, X_2, \dots, X_n]$.

De plus, pour que P soit homogène de degré p , il faut et il suffit que Q soit isobare de poids p .

Pour tout entier $n > 1$, notons $S'_1, S'_2, \dots, S'_{n-1}$ les polynômes symétriques élémentaires de l'algèbre $A[X_1, X_2, \dots, X_{n-1}]$.

Unicité de Q . — Par différence, on se ramène aussitôt à démontrer que si Q est un élément de $A[Y_1, Y_2, \dots, Y_n]$ tel que

$$(2) \quad Q(S_1, S_2, \dots, S_n) = 0,$$

alors $Q = 0$.

Nous allons démontrer ce résultat par récurrence sur n . Lorsque $n = 1$, l'assertion est évidente, puisque $S_1 = X_1$. Supposons donc l'assertion démontrée pour tous les polynômes à $n - 1$ indéterminées, et considérons un polynôme Q à n indéterminées, $n > 1$, satisfaisant à la relation (2). Supposons par l'absurde $Q \neq 0$, et écrivons Q sous la forme

$$(3) \quad Q = \sum_{r=p}^{+\infty} Q_r Y_n^r,$$

où, pour tout entier r , $Q_r \in A[Y_1, Y_2, \dots, Y_{n-1}]$, et où $Q_p \neq 0$. En substituant S_1, S_2, \dots, S_n aux indéterminées Y_1, Y_2, \dots, Y_n dans cette relation, et en tenant compte de la relation (2), nous obtenons

$$(4) \quad \sum_{r=p}^{+\infty} Q_r(S_1, S_2, \dots, S_{n-1}) S_n^r = 0.$$

Comme $S_n \neq 0$ et que l'anneau A est intègre, nous en déduisons que

$$(5) \quad \sum_{r=p}^{+\infty} Q_r(S_1, S_2, \dots, S_{n-1}) S_n^{r-p} = 0.$$

En substituant 0 à X_n dans cette dernière relation, nous obtenons

$$(6) \quad Q_p(S'_1, S'_2, \dots, S'_{n-1}) = 0.$$

En effet, $S_n(X_1, X_2, \dots, X_{n-1}, 0) = 0$ et, pour tout $j \in [1, n]$,

$$(7) \quad S_j(X_1, X_2, \dots, X_{n-1}, 0) = S'_j(X_1, X_2, \dots, X_{n-1})$$

(cf. cor. de la prop. 2.37). L'hypothèse de récurrence montre alors que $Q_p = 0$, ce qui est absurde.

Existence de Q . — Puisque tout polynôme symétrique est somme de polynômes symétriques p -homogènes (cf. prop. 2.34), il suffit de prouver que, pour tout polynôme symétrique p -homogène P , il existe un élément Q de $A[Y_1, Y_2, \dots, Y_n]$ isobare de poids p satisfaisant à la relation (1). La démonstration de cette assertion va s'effectuer par double récurrence sur les entiers n et p .

Lorsque $n = 1$, cette assertion est évidente pour tout entier p , puisque $S_1 = X_1$; lorsque $p = 0$, cette assertion est évidente pour tout entier n . Supposons donc l'assertion démontrée pour tous les polynômes p -homogènes à $n - 1$ indéterminées, où p parcourt \mathbb{N} , et pour tous les polynômes q -homogènes à n indéterminées, pour tout entier $q < p$. Considérons alors un polynôme p -homogène P à n indéterminées, où $n > 1$ et $p > 1$, et introduisons l'élément P' de $A[X_1, X_2, \dots, X_{n-1}]$ défini par la relation

$$(8) \quad P'(X_1, X_2, \dots, X_{n-1}) = P(X_1, X_2, \dots, X_{n-1}, 0).$$

Puisque P est p -homogène, il en est de même de P' . De plus, pour toute permutation σ' de $[1, n - 1]$, il existe une permutation σ de $[1, n]$ (et une seule) prolongeant σ' ; puisque P est symétrique, il en est de même de P' . L'hypothèse de récurrence s'applique donc à P' , et montre qu'il existe un élément Q' de $A[Y_1, Y_2, \dots, Y_{n-1}]$ isobare de poids p tel que

$$(9) \quad P'(X_1, X_2, \dots, X_{n-1}) = Q'(S'_1, S'_2, \dots, S'_{n-1}).$$

Introduisons maintenant l'élément R de $A[X_1, X_2, \dots, X_n]$ défini par la formule

$$(10) \quad R = P(X_1, X_2, \dots, X_n) - Q'(S_1, S_2, \dots, S_{n-1}).$$

Puisque P est symétrique, il en est de même de R . D'autre part, puisque Q' est isobare de poids p , R est p -homogène. De plus, compte tenu des formules (8) et (9),

$$(11) \quad R(X_1, X_2, \dots, X_{n-1}, 0) = 0.$$

Le polynôme R , considéré comme élément de $B[X_n]$, où

$$B = A[X_1, X_2, \dots, X_{n-1}],$$

s'annule donc à l'origine, ce qui prouve qu'il est divisible par X_n . Par suite, X_n divise R dans $A[X_1, X_2, \dots, X_n]$. Il en découle que, pour toute permutation σ de $[1, n]$, $\sigma X_n = X_{\sigma(n)}$ divise $\sigma R = R$. Ainsi, pour tout élément j de $[1, n]$, X_j divise R . Le corollaire 4 de la proposition 2.10 montre alors que $S_n = X_1 X_2 \dots X_n$ divise R . Autrement dit, il existe un élément T de $A[X_1, X_2, \dots, X_n]$ tel que

$$(12) \quad R = S_n T.$$

Distinguons deux cas : ou bien $p < n$; alors $T = R = 0$, et l'existence de Q découle de la formule (10). Ou bien $p \geq n$; alors, puisque R et S_n sont symétriques, T l'est aussi; puisque R est p -homogène et que S_n est n -homogène, T est $(p - n)$ -homogène. L'hypothèse de récurrence s'applique donc à T : il existe un élément Q'' de $A[Y_1, Y_2, \dots, Y_n]$ isobare de poids $p - n$ tel que

$$(13) \quad T(X_1, X_2, \dots, X_n) = Q''(S_1, S_2, \dots, S_n).$$

Il résulte des formules (10), (12) et (13) que

$$(14) \quad P(X_1, X_2, \dots, X_n) = Q'(S_1, S_2, \dots, S_{n-1}) + S_n Q''(S_1, S_2, \dots, S_n).$$

Donc

$$P(X_1, X_2, \dots, X_n) = Q(S_1, S_2, \dots, S_n),$$

où

$$Q(Y_1, Y_2, \dots, Y_n) = Q'(Y_1, Y_2, \dots, Y_{n-1}) + Y_n Q''(Y_1, Y_2, \dots, Y_n).$$

Le polynôme Q convient, car il est isobare de poids p .

Nous allons voir maintenant que le degré de Q peut se calculer facilement :

PROPOSITION 2.38. — Degré partiel d'un polynôme symétrique. — Soient A un anneau intègre et P un polynôme symétrique à n indéterminées.

1. Le degré partiel de P relativement à X_i est indépendant de i ; on l'appelle degré partiel de P .

2. Soit Q l'unique élément de $A[Y_1, Y_2, \dots, Y_n]$ tel que

$$P(X_1, X_2, \dots, X_n) = Q(S_1, S_2, \dots, S_n).$$

Alors le degré total de Q est égal au degré partiel de P .

L'assertion 1 est immédiate, puisque, pour toute permutation σ , le degré partiel de $\sigma P = P$ relativement à $X_{\sigma(i)}$ est égal au degré partiel de P relativement à X_i .

Assertion 2. — Soient q le degré total de Q et r le degré partiel de P . Soit $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite d'entiers naturels telle que $\alpha_1 + \alpha_2 + \dots + \alpha_n = q$. Alors le degré partiel de $S_1^{\alpha_1} S_2^{\alpha_2} \dots S_n^{\alpha_n}$ est égal à q . Il en découle que $r \leq q$.

Nous allons prouver que $q \leq r$ en nous inspirant de la démonstration du théorème 2.18, c'est-à-dire en procédant par double récurrence sur n et r . Lorsque $n = 1$, ou $r = 0$, l'assertion est évidente. Supposons donc l'assertion démontrée pour tous les polynômes symétriques à $n - 1$ indéterminées, de degré partiel quelconque, et pour tous les polynômes symétriques à n indéterminées de degré partiel strictement inférieur à r , et considérons un polynôme symétrique P à n indéterminées, de degré partiel r , où $n > 1$ et $r > 0$.

Distinguons deux cas :

a) $P(X_1, X_2, \dots, X_{n-1}, 0) = 0$; on écrit P sous la forme $P = S_n P_1$, où P_1 est symétrique, et on applique l'hypothèse de récurrence à P_1 .

b) $P'(X_1, X_2, \dots, X_{n-1}) = P(X_1, X_2, \dots, X_{n-1}, 0) \neq 0$; il est immédiat que P' est symétrique, et que son degré partiel est inférieur ou égal à r . Il existe donc un polynôme Q' de degré inférieur ou égal à r tel que

$$P'(X_1, X_2, \dots, X_{n-1}) = Q'(S'_1, S'_2, \dots, S'_{n-1}).$$

Alors $R = P - Q(S_1, S_2, \dots, S_{n-1})$ est de degré partiel inférieur ou égal à r , et $R(X_1, X_2, \dots, X_{n-1}, 0) = 0$. On est ainsi ramené au cas a) : il existe un polynôme Q'' de degré total inférieur ou égal à r tel que

$$R(X_1, X_2, \dots, X_n) = Q''(S_1, S_2, \dots, S_n).$$

Alors $Q''' = Q' + Q''$ est de degré total inférieur ou égal à r , et

$$P(X_1, X_2, \dots, X_n) = Q'''(X_1, X_2, \dots, X_n).$$

Par unicité de Q , $Q = Q'''$, donc le degré total q de Q est inférieur ou égal à r .

PROPOSITION 2.39. — Polynômes de Newton. — *Pour tout entier p appartenant à $[1, n]$, le monôme X_1^p est invariant par le sous-groupe H_1 de $G = \mathfrak{S}_n$ laissant fixe le point 1. L'ensemble F_1 des permutations σ de $[1, n]$ telles que $\sigma(2) < \sigma(3) < \dots < \sigma(n)$ est un système de représentants dans G de G/H_1 . Par suite, le polynôme*

$$N_p = I_{G, H_1}(X_1^p) = \sum_{\sigma \in F_1} X_{\sigma(1)}^p$$

est symétrique, et homogène de degré p ; on l'appelle polynôme de Newton de degré p . Ainsi,

$$N_p = \sum_{j=1}^n X_j^p.$$

Voici comment, grâce à des formules de récurrence, on peut calculer les polynômes de Newton à l'aide des polynômes symétriques élémentaires et réciproquement :

PROPOSITION 2.40. — Relations entre polynômes de Newton et polynômes symétriques élémentaires.

1. Pour tout entier p appartenant à $[1, n]$,

$$(1) \quad N_p - S_1 N_{p-1} + \dots + (-1)^j S_j N_{p-j} + \dots + (-1)^p p S_p = 0.$$

En particulier,

$$(2) \quad N_1 - S_1 = 0, \quad \text{soit } N_1 = S_1$$

$$(3) \quad N_2 - S_1 N_1 + 2S_2 = 0, \quad \text{soit } N_2 = S_1^2 - 2S_2$$

$$(4) \quad N_3 - S_1 N_2 + S_2 N_1 - 3S_3 = 0, \quad \text{soit } N_3 = S_1^3 - 3S_1 S_2 + 3S_3.$$

2. Pour tout entier $p > n$,

$$(5) \quad N_p - S_1 N_{p-1} + \dots + (-1)^j S_j N_{p-j} + \dots + (-1)^n S_n N_{p-n} = 0.$$

Pour effectuer la démonstration, nous introduisons le corps $B(Y)$, où

$$B = K(X_1, X_2, \dots, X_n).$$

Assertion 1. — Considérons le polynôme

$$(6) \quad P = \prod_{i=1}^n (X - X_i) = X^n - S_1 X^{n-1} + \dots + (-1)^n S_n.$$

Donc

$$(7) \quad D(P) = nX^{n-1} - (n-1)S_1 X^{n-2} + \dots + (-1)^{n-1} S_{n-1}.$$

D'autre part,

$$(8) \quad \frac{D(P)}{P} = \sum_{i=1}^n \frac{1}{X - X_i}.$$

En substituant $\frac{1}{Y}$ à X dans les relations (6), (7) et (8), nous obtenons la formule suivante :

$$(9) \quad (1 - S_1 Y + S_2 Y^2 + \dots + (-1)^n S_n Y^n) \left[\sum_{i=1}^n \frac{1}{1 - X_i Y} \right] \\ = n - (n-1)S_1 Y + (n-2)S_2 Y^2 + \dots + (-1)^{n-1} S_{n-1} Y^{n-1}.$$

Or, pour tout élément i de $[1, n]$,

$$(10) \quad \frac{1}{1 - X_i Y} \equiv 1 + X_i Y + X_i^2 Y^2 + \dots + X_i^n Y^n \pmod{Y^{n+1}}.$$

Donc

$$(11) \quad \sum_{i=1}^n \frac{1}{1 - X_i Y} \equiv n + N_1 Y + N_2 Y^2 + \dots + N_n Y^n \pmod{Y^{n+1}}.$$

En reportant la formule (11) dans la formule (9) et en identifiant, pour tout élément p de $[1, n]$, les coefficients de Y^p dans la congruence ainsi obtenue, nous en déduisons la formule (1).

Assertion 2. — Écrivons que, pour tout élément i de $[1, n]$, le polynôme obtenu en substituant X_i à X dans P est nul :

$$(12) \quad X_i^n - S_1 X_i^{n-1} + \dots + (-1)^n S_n = 0.$$

Par suite, pour tout entier $p > n$,

$$(13) \quad X_i^p - S_1 X_i^{p-1} + \dots + (-1)^n S_n X_i^{p-n} = 0.$$

La relation (5) s'obtient alors en ajoutant les égalités (13), lorsque i parcourt $[1, n]$.

COROLLAIRE. — *Si la caractéristique de K est nulle, pour tout entier appartenant à $[1, n]$, il existe un élément Q_p de $K[Y_1, Y_2, \dots, Y_n]$ tel que*

$$S_p = Q_p(N_1, N_2, \dots, N_p).$$

De plus, pour tout polynôme symétrique P , il existe un élément Q de $K[Y_1, Y_2, \dots, Y_n]$ tel que

$$P = Q(N_1, N_2, \dots, N_n).$$

L'existence de Q_p se déduit des relations (1), et l'existence de Q en résulte, grâce au théorème 2.18.

On peut même trouver, en utilisant la théorie des séries entières formelles, des formules explicites donnant les polynômes de Newton à l'aide des polynômes symétriques élémentaires, et réciproquement.

PROPOSITION 2.41. — Formules de Waring. — *Soient p un entier supérieur ou égal à 1 et \mathcal{E}_p l'ensemble des applications s de $[1, n]$ dans \mathbf{N} telles que*

$\sum_{j=1}^n j s(j) = p$. Pour tout élément j de $[1, n]$, on pose $S'_j = (-1)^j S_j$. Alors

$$(1) \quad \frac{1}{p} N_p = \sum_{s \in \mathcal{E}_p} \frac{(-1)^{|s|}}{|s|} \frac{|s|!}{s!} S_1'^{s(1)} S_2'^{s(2)} S_n'^{s(n)}.$$

Introduisons le polynôme

$$(2) \quad Q = \prod_{i=1}^n (1 - X_i Y) = 1 + S'_1 Y + S'_2 Y^2 + \dots + S'_n Y^n.$$

Ce polynôme peut être considéré comme un élément de $B[[Y]]$, où $B = K(X_1, X_2, \dots, X_n)$. D'après le théorème 1.17,

$$(3) \quad \log Q = \sum_{i=1}^n \log(1 - X_i Y) = - \sum_{p=1}^{+\infty} \frac{1}{p} N_p Y^p.$$

D'autre part, d'après la formule (3),

$$(4) \quad \log Q = \sum_{q=1}^{+\infty} \frac{(-1)^{q-1}}{q} (S'_1 Y + S'_2 Y^2 + \dots + S'_n Y^n)^q.$$

On en déduit la formule (1) en identifiant les coefficients des séries entières formelles (3) et (4), compte tenu de la formule du binôme généralisée (cf. prop. I.2.37).

REMARQUE. — Réciproquement, on peut trouver des formules explicites donnant S'_1, S'_2, \dots, S'_n en fonction de N_1, N_2, \dots, N_n en écrivant la formule (2) sous la forme

$$1 + S'_1 Y + S'_2 Y^2 + \dots + S'_n Y^n = \exp(\log Q),$$

et en développant la série exponentielle figurant au second membre.

Pour étudier les symétrisés des monômes les plus généraux, nous utiliserons la

PROPOSITION 2.42. — **Opération du groupe symétrique sur les monômes.**

1. Pour tout élément s de $S = \mathcal{F}([1, n], \mathbf{N})$ et pour tout élément σ de \mathfrak{S}_n ,

$$\sigma X^s = X^{s \circ \sigma^{-1}}.$$

2. L'application $(\sigma, X^s) \mapsto \sigma X^s$ est une opération de \mathfrak{S}_n sur l'ensemble des monômes.

3. Toute orbite de \mathfrak{S}_n dans l'ensemble des monômes contient un monôme X^s et un seul tel que s soit une application décroissante de $[1, n]$ dans \mathbf{N} .

Les assertions 1 et 2 sont immédiates.

Assertion 3. — Posons $G = \mathfrak{S}_n$. Soient s_1 et s_2 deux applications décroissantes telles que $G X^{s_1} = G X^{s_2}$. Alors X^{s_1} et X^{s_2} appartiennent à une même orbite, c'est-à-dire qu'il existe une permutation σ de $[1, n]$ telle que $s_2 = s_1 \circ \sigma$. Comme s_1 et s_2 sont décroissantes, nous en déduisons que $s_1 = s_2$.

Réciproquement, pour toute orbite $G X^s$ de G , il existe une permutation σ telle que $s' = s \circ \sigma^{-1}$ soit décroissante; l'application s' convient.

Nous sommes ainsi amené à poser la

DÉFINITION 2.27. — **Polynômes symétriques fondamentaux.** — Soit S' l'ensemble des applications décroissantes de $[1, n]$ dans \mathbf{N} . Pour tout élément s de S' , soit H_s le sous-groupe de $G = \mathfrak{S}_n$ laissant invariant X^s . Le symétrisé

$$F_s = I_{G, H_s}(X^s)$$

s'appelle polynôme symétrique fondamental associé à s .

EXEMPLES. — Lorsque $s(j) = 1$ si $j \in [1, p]$ et $s(j) = 0$ si $j > p$, $F_s = S_p$. Lorsque $s(1) = p$ et $s(j) = 0$ si $j \geq 2$, $F_s = N_p$.

PROPOSITION 2.43. — **Propriétés des polynômes symétriques fondamentaux.**

1. Pour tout élément s de S' , il existe un polynôme Q_s à coefficients entiers rationnels et un seul tel que

$$F_s = Q_s(S_1, S_2, \dots, S_n).$$

Le poids de Q_s est égal à $|s|$, et le degré total de Q_s est égal à $s(1)$.

2. Pour tout élément s de S' ,

$$F_s = \sum_{X^t \in GX^s} X^t,$$

où GX^s est l'orbite de X^s sous G .

3. Les polynômes symétriques fondamentaux F_s , où s parcourt S' , constituent une base de l'espace vectoriel des polynômes symétriques.

L'assertion 1 résulte aussitôt du théorème 2.18 et de la proposition 2.38.

L'assertion 2 résulte aussitôt de ce que l'application $\gamma \mapsto \gamma X^s$ est une bijection de l'ensemble des classes à gauche de G modulo H_s sur l'orbite GX^s .

Assertion 3. — Les polynômes F_s sont linéairement indépendants, car les orbites GX^s , où s parcourt S' , sont disjointes deux à deux (cf. prop. 2.49).

Soit enfin $P = \sum_{s \in S} \alpha_s X^s$ un polynôme symétrique, c'est-à-dire tel que, pour tout élément σ de \mathfrak{S}_n ,

$$\sigma^{-1}P = \sum_{s \in S} \alpha_s X^{s \circ \sigma} = \sum_{s \in S} \alpha_s X^s.$$

Alors, pour tout élément s de S , $\alpha_{s \circ \sigma} = \alpha_s$, donc

$$P = \sum_{s \in S'} \alpha_s \left(\sum_{X^t \in GX^s} X^t \right) = \sum_{s \in S'} \alpha_s F_s,$$

ce qui prouve que la famille $(F_s)_{s \in S'}$ est génératrice.

REMARQUE. — Calcul pratique d'un polynôme symétrique en fonction des polynômes symétriques élémentaires. — Grâce à la proposition 2.43, on se ramène aussitôt au cas des polynômes symétriques fondamentaux F_s , où s est une application décroissante de $[1, n]$ dans \mathbb{N} .

On dit que F_s est r -uple si l'ensemble des entiers j tels que $s(j) \neq 0$ possède r éléments.

Voici deux méthodes pour déterminer le polynôme Q_s tel que

$$(1) \quad F_s = Q_s(S_1, S_2, \dots, S_n).$$

a) Méthode des poids. — On sait *a priori* que Q_s est isobare de poids $|s|$. Si F_s est r -uple, où r est assez grand, et si le poids r de F_s est petit, on écrit Q_s avec des coefficients indéterminés, en tenant compte du fait que le degré total de Q_s est égal au degré partiel de F_s ; on calcule ces coefficients en substituant des valeurs particulières aux indéterminées dans la relation (1).

EXEMPLE. — Considérons le cas où $s(1) = 2$, $s(2) = 1$, $s(j) = 0$ si $j \geq 3$. Alors

$$F_s = \sum_{\sigma \in \mathfrak{S}_s} X_{\sigma(1)}^2 X_{\sigma(2)} = X_1 X_2^2 + X_1 X_3^2 + X_2 X_1^2 + X_2 X_3^2 + X_3 X_1^2 + X_3 X_2^2.$$

A priori, Q_s est de poids 3, donc de la forme

$$Q_s = \alpha Y_1^3 + \beta Y_2 Y_1 + \gamma Y_3.$$

En remarquant que le degré partiel de P est égal à 2, nous voyons que $\alpha = 0$; en identifiant les coefficients de $X_1 X_2^2$, nous voyons que $\beta = 1$. Enfin, en substituant X à X_1 , X_2 , X_3 et en identifiant les coefficients de X^3 , nous voyons que $\gamma = -3$.

b) Méthode de Newton. — Si P est r -uple, où r est petit, on peut évaluer F_s à l'aide des polynômes de Newton N_p .

EXEMPLE. — Considérons le cas où $s(1) = p$, $s(2) = q$, $s(j) = 0$ si $j \geq 3$. Alors

$$F_s = \sum_{i \neq j} X_i^p X_j^q.$$

D'autre part,

$$N_p N_q = N_{p+q} + F_s,$$

ce qui donne F_s en fonction des sommes de Newton.

En particulier,

$$\sum_{\sigma \in \mathfrak{S}_3} X_{\sigma(1)}^2 X_{\sigma(2)} = N_1 N_2 - N_3.$$

Nous allons ramener maintenant l'étude des polynômes antisymétriques à celle des polynômes symétriques :

PROPOSITION 2.44. — Structure des polynômes antisymétriques. — *On suppose que l'anneau A est de caractéristique différente de 2 et que $n > 1$.*

1. *Le polynôme $V = \prod_{i < j} (X_j - X_i)$ est un polynôme antisymétrique homogène de degré $\frac{n(n-1)}{2}$. Le polynôme V s'appelle polynôme de Vandermonde à n indéterminées.*

2. *Lorsque l'anneau A est intègre, tout polynôme antisymétrique P à n indéterminées est divisible par V . Plus précisément, P peut s'écrire sous la forme $P = VQ$, où Q est un polynôme symétrique.*

Assertion 1. — Puisque les transpositions élémentaires engendrent le groupe \mathfrak{S}_n (cf. cor. du th. 2.16), il suffit de démontrer que, pour toute transposition élémentaire τ , $\tau V = -V$, ce qui est immédiat.

Assertion 2. — Soient P un polynôme antisymétrique non nul, et (i, j) un couple d'éléments distincts de $[1, n]$. Considérons P comme un élément de $A_j[X_j]$, où $A_j = A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$. Puisque P est antisymétrique, le polynôme P_1 obtenu en substituant X_i à X_j dans P est un élément de A_j satisfaisant à la relation $P_1 = -P$. Puisque la caractéristique de A est différente de 2, il en résulte que $P_1 = 0$. D'après le corollaire 4 de la proposition 2.10, nous en déduisons que P est divisible par $X_j - X_i$. D'après ce même corollaire, il en découle que P est divisible par V . Il existe donc un élément Q de $A[X_1, X_2, \dots, X_n]$ tel que $P = VQ$. Pour démontrer que Q est symétrique, notons que, pour tout élément σ de \mathfrak{S}_n , $\sigma P = \varepsilon(\sigma)P$, $\sigma V = \varepsilon(\sigma)V$ et $\sigma P = \sigma V \cdot \sigma Q$; donc $P = V \cdot \sigma Q$. Comme $P = VQ$, que V est non nul et que A est intègre, il s'ensuit que $\sigma Q = Q$, ce qui achève la démonstration.

Les résultats précédents se généralisent facilement au cas où l'on fait opérer le groupe symétrique sur les fractions rationnelles :

PROPOSITION 2.45. — Opérations du groupe symétrique sur les fractions rationnelles.

1. Soit R un élément de $K(X_1, X_2, \dots, X_n)$. Alors, pour tout élément σ de \mathfrak{S}_n , la suite $(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$ est substituable dans R . De plus, l'application

$$(\sigma, R) \mapsto \sigma R = R(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$$

est une opération du groupe \mathfrak{S}_n sur $K(X_1, X_2, \dots, X_n)$.

2. Soit σ un élément de \mathfrak{S}_n . L'application $R \mapsto \sigma R$ est un automorphisme de la K -algèbre unitaire $K(X_1, X_2, \dots, X_n)$. De plus, si R est un élément non nul de $K(X_1, X_2, \dots, X_n)$, écrit sous forme réduite $R = \frac{P}{Q}$, alors σR admet $\frac{\sigma P}{\sigma Q}$ pour forme réduite.

De même, pour tout polynôme irréductible P , σP est irréductible, et

$$v_{\sigma P}(\sigma R) = v_P(R).$$

Par suite, si la décomposition de R en facteurs irréductibles s'écrit sous la forme

$$R = \alpha \prod_{P \in E} P^{v_P(R)},$$

il existe un scalaire non nul β tel que

$$\sigma^{-1} R = \beta \prod_{P \in E} P^{v_{\sigma P}(R)}.$$

Assertion 1. — Écrivons R sous la forme $R = \frac{P}{Q}$, où P et Q appartiennent à $K[X_1, X_2, \dots, X_n]$, Q étant non nul. Alors σQ n'est pas nul, ce qui signifie que $(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$ est substituable dans R . Le reste de l'assertion est immédiat.

Assertion 2. — L'application $P \mapsto \sigma P$ est un automorphisme de l'anneau unitaire $K[X_1, X_2, \dots, X_n]$. Ainsi, pour que P et Q soient premiers entre eux, il faut et il suffit que σP et σQ le soient. De même, pour que P soit irréductible, il faut et il suffit que σP le soit. L'assertion en découle facilement.

La proposition 2.33 s'étend aussitôt à ce cas plus général, ce qui conduit à poser la

DÉFINITION 2.28. — Fractions rationnelles symétriques, fractions rationnelles antisymétriques. — On dit qu'un élément R de $K(X_1, X_2, \dots, X_n)$ est symétrique (resp. antisymétrique) si, pour tout élément σ de \mathfrak{S}_n , $\sigma R = R$ (resp. $\sigma R = \varepsilon(\sigma)R$).

Les fractions rationnelles symétriques constituent un sous-corps de $K(X_1, X_2, \dots, X_n)$.

PROPOSITION 2.46. — **Structure des fractions rationnelles symétriques et antisymétriques.**

1. *Pour qu'une fraction rationnelle R soit symétrique, il faut et il suffit que R puisse s'écrire sous la forme $R = \frac{P'}{Q'}$, où P' et Q' sont deux polynômes symétriques, Q' étant non nul. Plus précisément, soit R une fraction rationnelle non nulle, écrite sous la forme réduite $R = \frac{P}{Q}$. Pour que R soit symétrique, il faut et il suffit que P et Q le soient.*

2. *Pour qu'une fraction rationnelle R soit antisymétrique, il faut et il suffit que R puisse s'écrire sous la forme $R = \frac{P'}{Q'}$, où P' est un polynôme antisymétrique et Q' un polynôme symétrique non nul. Plus précisément, soit R une fraction rationnelle non nulle, écrite sous la forme réduite $R = \frac{P}{Q}$. Si R est antisymétrique, ou bien P est antisymétrique et Q symétrique, ou bien P est symétrique et Q antisymétrique. Dans le premier cas, R s'écrit sous la forme $R = V \frac{P_1}{Q}$, où P_1 et Q sont deux polynômes symétriques premiers entre eux, Q étant premier avec V ; dans le second cas, R s'écrit sous la forme $R = \frac{P}{VQ_1}$, où P et Q_1 sont deux polynômes symétriques, P étant premier avec V .*

Assertion 1. — Il est évident que si P' et Q' sont symétriques, $R = \frac{P'}{Q'}$ l'est aussi. Considérons donc une fraction rationnelle symétrique non nulle, écrite sous la forme réduite $R = \frac{P}{Q}$. Puisque σP et σQ sont premiers entre eux et que $\sigma R = R$, il existe un scalaire non nul α_σ tel que $\sigma P = \alpha_\sigma P$ et $\sigma Q = \alpha_\sigma Q$. Donc P et Q sont des poids de \mathfrak{S}_n . Il en découle que P et Q sont soit symétriques, soit antisymétriques (cf. prop. 2.33).

Ou bien P est symétrique; alors Q l'est aussi, et l'assertion est démontrée.

Ou bien P est antisymétrique; alors Q l'est aussi. D'après la proposition 2.44, le polynôme de Vandermonde V divise P et Q , ce qui est impossible, puisque P et Q sont premiers entre eux.

L'assertion 2 se démontre de la même manière. Cette fois, on prouve qu'il existe un scalaire α_σ tel que $\sigma P = \alpha_\sigma P$ et $\sigma Q = \varepsilon(\sigma)\alpha_\sigma Q$.

REMARQUE 1. — La construction de fractions rationnelles symétriques s'effectue exactement comme dans le cas des polynômes (cf. prop. 2.35). En particulier, pour tout entier $p < 0$, le symétrisé de X_1^p s'appelle $p^{\text{ième}}$ fraction rationnelle de Newton, et se note N_p . Ainsi,

$$N_p = \sum_{j=1}^n X_j^p.$$

REMARQUE 2. — Lorsque p est strictement négatif, le calcul des fractions rationnelles N_p en fonction des polynômes symétriques élémentaires s'effectue comme dans le cas où p est

strictement positif (cf. prop. 2.40) : lorsque $-n \leq p \leq -1$, on commence par écrire les formules (6), (7) et (8) donnant P , $D(P)$ et $\frac{D(P)}{P}$, mais, cette fois, on remplace la formule (10) par la suivante :

$$(10') \quad \frac{1}{X - X_i} = - \frac{1}{X_i \left(1 - \frac{X}{X_i}\right)} \equiv - \frac{1}{X_i} - \frac{X}{X_i^2} - \dots - \frac{X^{n-1}}{X_i^n} \quad (\text{mod. } X^n).$$

Donc

$$(11') \quad \sum_{i=1}^n \frac{1}{X - X_i} \equiv -N_{-1} - N_{-2}X - \dots - N_{-n}X^{n-1} \quad (\text{mod. } X^n).$$

Le calcul s'achève alors comme dans le cas où p est positif.

Par exemple, on obtient la formule

$$(2') \quad N_{-1}S_n - S_{n-1} = 0, \quad \text{soit} \quad N_{-1} = \frac{S_{n-1}}{S_n}.$$

Enfin, le cas où $p < -n$ se traite comme celui où $p > n$.

Exercices conseillés : 36 à 43.

§ 6. SÉRIES ENTIÈRES FORMELLES A PLUSIEURS INDÉTERMINÉES

Dans ce paragraphe, on désigne par A un anneau commutatif unitaire, par I un ensemble fini non vide et par S l'ensemble \mathbf{N}^I des applications de I dans \mathbf{N} , muni de la loi de composition $(s, t) \mapsto s + t$.

1. SÉRIES ENTIÈRES FORMELLES

DÉFINITION 2.29. — Algèbre des séries entières formelles. — On considère l'application qui à tout couple d'éléments $B = (\beta_s)_{s \in S}$ et $C = (\gamma_s)_{s \in S}$ de A^S associe l'élément $D = (\delta_s)_{s \in S}$ défini par la relation

$$\delta_s = \sum_{t+u=s} \beta_t \gamma_u.$$

Muni de cette application, le A -module A^S est une A -algèbre, notée $S_I(A)$. Les scalaires β_s s'appellent coefficients de $B = (\beta_s)_{s \in S}$. Les éléments de $S_I(A)$ s'appellent séries entières formelles à coefficients dans A construites sur I .

L'algèbre $S_I(A)$ est évidemment commutative et unitaire. Son élément unité, qu'on identifie à 1, n'est autre que $(\delta_{0,s})_{s \in S}$. L'algèbre unitaire $\mathbf{P}_I(A)$ des polynômes à coefficients dans A construite sur I est une sous-algèbre unitaire de $S_I(A)$; elle est constituée des séries entières formelles à support fini. En particulier, lorsqu'on note $A[X_i]_{i \in I}$ l'algèbre $\mathbf{P}_I(A)$, on note $A[[X_i]]_{i \in I}$

l'algèbre $S_I(A)$. Lorsque $I = [1, n]$, l'algèbre $S_I(A)$ se note encore $A[[X_1, X_2, \dots, X_n]]$, et s'appelle algèbre des séries entières formelles à n indéterminées à coefficients dans A .

REMARQUE. — L'algèbre $S_I(A)$ n'est autre que l'algèbre de convolution du monoïde additif \mathbf{N}^I .

DÉFINITION 2.30. — **Valuation d'une série entière formelle.** — On appelle valuation d'une série entière formelle non nulle $B = (\beta_s)_{s \in S}$ le plus petit des entiers n satisfaisant à la condition suivante : il existe un élément s de S tel que $|s| = n$ et que $\beta_s \neq 0$. On convient que la valuation de 0 est égale à $+\infty$. La valuation d'une série entière formelle B se note $v_0(B)$.

PROPOSITION 2.47. — **Valuation d'une somme, valuation d'un produit.** — Soient B et C deux éléments de $A[[X_i]]_{i \in I}$. Alors

$$v_0(B + C) \geq \inf [v_0(B), v_0(C)],$$

avec égalité si $v_0(B) \neq v_0(C)$;

$$v_0(BC) \geq v_0(B) + v_0(C).$$

DÉFINITION 2.31. — **Troncatures d'une série entière formelle.** — Soit p un entier naturel. On appelle troncature à l'ordre p , et on note T_p , l'application qui à tout élément $B = (\beta_s)_{s \in S}$ de $A[[X_i]]_{i \in I}$ associe l'élément $(\gamma_s)_{s \in S}$ défini par les formules suivantes :

$$\begin{aligned} \gamma_s &= \beta_s & \text{si} & \quad |s| \leq p \\ &= 0 & \text{si} & \quad |s| > p. \end{aligned}$$

PROPOSITION 2.48. — **Propriétés de la troncature.** — La troncature à l'ordre p est un projecteur de $A[[X_i]]_{i \in I}$, dont l'image est le sous-espace vectoriel de $A[[X_i]]_{i \in I}$ constitué des polynômes dont le degré total est inférieur ou égal à p , et dont le noyau \mathfrak{S}_p est l'idéal des séries entières formelles de valuation strictement supérieure à p .

Ainsi, l'intersection des noyaux \mathfrak{S}_p des endomorphismes T_p , où p parcourt \mathbf{N} , est réduite à $\{0\}$.

Comme dans le cas des séries entières formelles à une indéterminée à coefficients dans un corps (cf. prop. 1.40), on en déduit les résultats suivants :

COROLLAIRE 1. — **Critère d'égalité de deux applications linéaires dans les séries entières formelles.** — Soient I et J deux ensembles finis non vides, S l'ensemble des applications de I dans \mathbf{N} , U et V deux applications linéaires de $A[[X_i]]_{i \in I}$ dans $S_J(A)$ satisfaisant à la condition suivante : pour toute suite (B_n) d'éléments de $S_I(A)$ telle que $v_0(B_n)$ tende vers $+\infty$, $v_0[U(B_n)]$ et $v_0[V(B_n)]$ tendent vers $+\infty$ avec n . Alors, pour que $U = V$, il faut et il suffit que, pour tout élément s de S , $U(X^s) = V(X^s)$.

COROLLAIRE 2. — Critère d'égalité de deux applications multilinéaires dans les séries entières formelles. — Soient r un entier naturel non nul, I et J deux ensembles finis non vides, S l'ensemble des applications de I dans \mathbb{N} , U et V deux applications multilinéaires de $(A[[X_i]]_{i \in I})^r$ dans $S_J(A)$ satisfaisant à la condition suivante : pour tout élément j de $[1, r]$, pour toute suite $(C_1, \dots, C_{j-1}, C_{j+1}, \dots, C_r)$ d'éléments de $A[[X_i]]_{i \in I}$ et pour toute suite (B_n) d'éléments de $A[[X_i]]_{i \in I}$ telle que $v_0(B_n)$ tende vers $+\infty$,

$$v_0[U(C_1, \dots, C_{j-1}, B_n, C_{j+1}, \dots, C_r)]$$

et

$$v_0[V(C_1, \dots, C_{j-1}, B_n, C_{j+1}, \dots, C_r)]$$

tendent vers $+\infty$ avec n . Alors, pour que $U = V$, il faut et il suffit que, pour toute suite (s_1, s_2, \dots, s_r) d'éléments de S ,

$$U(X^{s_1}, X^{s_2}, \dots, X^{s_r}) = V(X^{s_1}, X^{s_2}, \dots, X^{s_r}).$$

En particulierisant ces deux corollaires, on obtient les trois énoncés suivants :

COROLLAIRE 3. — Propriétés de la multiplication des séries entières formelles.

1. L'application $(B, C) \mapsto BC$ est la seule application bilinéaire symétrique M de $A[[X_i]]_{i \in I} \times A[[X_i]]_{i \in I}$ dans $A[[X_i]]_{i \in I}$ prolongeant la multiplication des polynômes et satisfaisant à la condition suivante : pour toute série entière formelle C et pour toute suite (B_n) de séries entières formelles telle que $v_0(B_n)$ tende vers $+\infty$, $v_0[M(B_n, C)]$ tend vers $+\infty$ avec n .

2. L'algèbre $A[[X_i]]_{i \in I}$ est associative.

COROLLAIRE 4. — Isomorphismes d'équipotence. — Soient I et J deux ensembles finis non vides ayant même cardinal. Alors les algèbres unitaires $A[[X_i]]_{i \in I}$ et $A[[Y_j]]_{j \in J}$ sont isomorphes. Plus précisément, soit φ une bijection de I sur J ; il existe un morphisme f et un seul de $A[[X_i]]_{i \in I}$ sur $A[[Y_j]]_{j \in J}$ tel que, pour tout élément i de I , $f(X_i) = Y_{\varphi(i)}$ et satisfaisant à la condition suivante : pour toute suite (B_n) d'éléments de $A[[X_i]]_{i \in I}$ telle que $v_0(B_n)$ tende vers $+\infty$ avec n , $v_0[f(B_n)]$ tend vers $+\infty$.

COROLLAIRE 5. — Isomorphismes d'associativité. — Soient H un ensemble fini non vide et (I, J) une partition de H . Il existe alors un morphisme f et un seul de la A -algèbre unitaire $A[[X_h]]_{h \in H}$ sur la A -algèbre unitaire sous-jacente à la A_J -algèbre unitaire $A_J[[Y_i]]_{i \in I}$, où $A_J = A[[Z_j]]_{j \in J}$, satisfaisant aux trois conditions suivantes : pour tout élément i de I , $f(X_i) = Y_i$; pour tout élément j de J , $f(X_j) = Z_j$; pour toute suite (B_n) d'éléments de $A[[X_h]]_{h \in H}$ telle que $v_0(B_n)$ tende vers $+\infty$ avec n , $v_0[f(B_n)]$ tend vers $+\infty$. De plus, f est un isomorphisme de A -algèbres unitaires, dit canonique.

On construit de même un isomorphisme canonique de $A[[X_h]]_{h \in H}$ sur $A_I[[Z_j]]_{j \in J}$, où $A_I = A[[Y_i]]_{i \in I}$. Grâce à ces isomorphismes, on identifie les A -algèbres unitaires $A[[X_h]]_{h \in H}$, $A_J[[Y_i]]_{i \in I}$ et $A_I[[Z_j]]_{j \in J}$.

Pour tout couple (n, p) d'entiers naturels non nuls, on identifie donc les A -algèbres unitaires $A[[X_1, X_2, \dots, X_{n+p}]]$ et $A_n[[X_{n+1}, X_{n+2}, \dots, X_{n+p}]]$, où $A_n = A[[X_1, X_2, \dots, X_n]]$.

Plus particulièrement encore, l'algèbre unitaire $A[[X_1, X_2, \dots, X_{n+1}]]$ s'identifie à l'algèbre unitaire $A_n[[X_{n+1}]]$.

REMARQUE. — Changement d'anneau de base. — Soient B et B' deux A -algèbres commutatives unitaires, et j un morphisme de B dans B' . Il existe un morphisme \tilde{j} et un seul de la A -algèbre unitaire $B[[X_i]]_{i \in I}$ dans la A -algèbre unitaire $B'[[X_i]]_{i \in I}$ prolongeant j et satisfaisant aux deux conditions suivantes : pour tout élément i de I , $\tilde{j}(X_i) = X_i$; pour toute suite (C_n) d'éléments de $B[[X_i]]_{i \in I}$ telle que $v_0(C_n)$ tende vers $+\infty$, $v_0[\tilde{j}(C_n)]$ tend vers $+\infty$ avec n . La valeur de \tilde{j} sur une série entière formelle $C = \sum_{s \in S} \beta_s X^s$ est donnée par la formule

$$(1) \quad \tilde{j} \left(\sum_{s \in S} \beta_s X^s \right) = \sum_{s \in S} j(\beta_s) X^s.$$

Il est immédiat que l'application \tilde{j} définie par la formule (1) convient. Pour démontrer l'unicité de \tilde{j} , on se ramène, par différence, à prouver que 0 est la seule application A -linéaire U du A -module $B[[X_i]]_{i \in I}$ dans le A -module $B'[[X_i]]_{i \in I}$ s'annulant sur les polynômes et satisfaisant à la condition suivante : pour toute suite (C_n) d'éléments de $B[[X_i]]_{i \in I}$ telle que $v_0(C_n)$ tende vers $+\infty$, $v_0[U(C_n)]$ tend vers $+\infty$ avec n . Pour cela, on procède comme dans le corollaire 1 de la proposition 1.40.

DÉFINITION 2.32. — Familles sommables de séries entières formelles. — Soit H un ensemble non vide. On dit qu'une famille $(B_h)_{h \in H}$ d'éléments de $A[[X_i]]_{i \in I}$ est sommable si, pour tout entier naturel p l'ensemble des éléments h de H tels que $v_0(B_h) \leq p$ est fini. La somme d'une telle famille est la série entière formelle, notée $\sum_{h \in H} B_h$, dont les coefficients sont définis par la formule

$$\gamma_s = \sum_{h \in H} \beta_{s,h},$$

où, pour tout élément h de H , $\beta_{s,h}$ désigne le $s^{\text{ième}}$ coefficient de B_h .

REMARQUE. — Comme dans le cas des séries entières formelles à une indéterminée, on voit que cette notation coïncide avec la notation algébrique d'une somme lorsque la famille $(B_h)_{h \in H}$ est à support fini. D'autre part, pour tout élément $B = (\beta_s)_{s \in S}$ de $A[[X_i]]_{i \in I}$, la famille $(\beta_s X^s)_{s \in S}$ est sommable, et

$$B = \sum_{s \in S} \beta_s X^s.$$

Lorsque B est un polynôme, cette dernière notation est compatible avec celle qui a été introduite au § 2.

La proposition 1.41 et son corollaire s'étendent aussitôt au cas des séries entières formelles à plusieurs indéterminées.

Les propositions 1.42 et 1.43 s'étendent aussitôt en la

PROPOSITION 2.49. — Propriétés de la sommation des séries entières formelles.

1. Soient H un ensemble non vide, $(B_h)_{h \in H}$ une famille d'éléments de $A[[X_i]]_{i \in I}$ et σ une permutation de H . Pour que la famille $(B_{\sigma(h)})_{h \in H}$ soit sommable, il faut et il suffit que la famille $(B_h)_{h \in H}$ le soit. Dans ces conditions,

$$\sum_{h \in H} B_{\sigma(h)} = \sum_{h \in H} B_h.$$

2. Soient H un ensemble non vide, $(H_j)_{j \in J}$ une famille de parties de H disjointes deux à deux dont la réunion est égale à H , et $(B_h)_{h \in H}$ une famille d'éléments de $A[[X_i]]_{i \in I}$. Si la famille $(B_h)_{h \in H}$ est sommable, alors, pour tout élément j de J , la famille $(B_h)_{h \in H_j}$ est sommable. De plus, la famille $\left(\sum_{h \in H_j} B_h\right)_{j \in J}$ est sommable, et

$$\sum_{h \in H} B_h = \sum_{j \in J} \left(\sum_{h \in H_j} B_h \right).$$

3. Soient $(B_h)_{h \in H}$ et $(C_k)_{k \in K}$ deux familles sommables d'éléments de $A[[X_i]]_{i \in I}$. Alors la famille $(B_h C_k)_{(h,k) \in H \times K}$ est sommable, et

$$\left(\sum_{h \in H} B_h \right) \left(\sum_{k \in K} C_k \right) = \sum_{(h,k) \in H \times K} B_h C_k.$$

PROPOSITION 2.50. — Composantes homogènes d'une série entière formelle. Pour toute série entière formelle $B = \sum_{s \in S} \beta_s X^s$, il existe une famille sommable $(U_p)_{p \in \mathbb{N}}$ et une seule de polynômes p -homogènes telle que

$$B = \sum_{p=0}^{+\infty} U_p.$$

Pour tout entier naturel p , le polynôme U_p s'appelle composante p -homogène de la série entière formelle B .

En utilisant la sommabilité de la famille $(U_p)_{p \in \mathbb{N}}$ et une troncature, on voit aussitôt que, pour tout entier naturel p , U_p est nécessairement donné par la formule

$$(1) \quad U_p = \sum_{|s|=p} \beta_s X^s.$$

Réciproquement, il est immédiat que la famille $(U_p)_{p \in \mathbb{N}}$ définie par la formule (1) convient.

REMARQUE. — Lorsque B est un polynôme, la notation $B = \sum_{p=0}^{+\infty} U_p$ est compatible avec celle qui a été introduite au § 2.

De même, la proposition 1.44 s'étend en la

PROPOSITION 2.51. — Substitution de séries entières formelles dans une série entière formelle.

1. Soient $B = \sum_{s \in S} \beta_s X^s$ un élément de $A[[X_1, X_2, \dots, X_n]]$ et $C = (C_1, C_2, \dots, C_n)$ une suite d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ de valuations strictement positives. Alors la famille $(D_s)_{s \in S}$ d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ définie par la relation

$$D_s = \beta_s C_1^{s(1)} C_2^{s(2)} \dots C_n^{s(n)} = \beta_s C^s$$

est sommable. Sa somme s'appelle série entière formelle obtenue par substitution des séries entières formelles C_1, C_2, \dots, C_n dans la série entière formelle B , et se note $B(C_1, C_2, \dots, C_n)$.

2. Soit (C_1, C_2, \dots, C_n) une suite d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ de valuations strictement positives. L'application $B \mapsto B(C_1, C_2, \dots, C_n)$ est un morphisme de l'algèbre unitaire $A[[X_1, X_2, \dots, X_n]]$ dans l'algèbre unitaire $A[[Y_1, Y_2, \dots, Y_p]]$.

3. La substitution dans les séries entières formelles est associative. Plus précisément, soient B un élément de $A[[X_1, X_2, \dots, X_n]]$, (C_1, C_2, \dots, C_n) une suite d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ de valuations strictement positives et (D_1, D_2, \dots, D_p) une suite d'éléments de $A[[Z_1, Z_2, \dots, Z_p]]$ de valuations strictement positives. Alors

$$\begin{aligned} [B(C_1, C_2, \dots, C_n)](D_1, D_2, \dots, D_p) \\ = B[C_1(D_1, D_2, \dots, D_p), C_2(D_1, D_2, \dots, D_p), \dots, C_n(D_1, D_2, \dots, D_p)]. \end{aligned}$$

4. Soient $(B_i)_{i \in I}$ une famille sommable d'éléments de $A[[X_1, X_2, \dots, X_n]]$, B la somme de cette famille, et $C = (C_1, C_2, \dots, C_n)$ une suite d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ de valuations strictement positives. Alors $(B_i(C_1, C_2, \dots, C_n))_{i \in I}$ est une famille sommable d'éléments de $A[[Y_1, Y_2, \dots, Y_p]]$ dont la somme est égale à $B(C_1, C_2, \dots, C_n)$:

$$\left(\sum_{i \in I} B_i \right) (C_1, C_2, \dots, C_n) = \sum_{i \in I} B_i(C_1, C_2, \dots, C_n).$$

Bien évidemment, on ne peut pas en général substituer une famille de scalaires aux indéterminées d'une série entière formelle.

DÉFINITION 2.33. — Éléments substituables dans une série entière formelle. Soient n et p deux entiers naturels non nuls, $S = \mathcal{F}([1, n], \mathbb{N})$ et $T = \mathcal{F}([1, p], \mathbb{N})$. On dit qu'un élément $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ de A^n est substituable aux indéterminées X_1, X_2, \dots, X_n dans un élément $B = \sum_{(s,t) \in S \times T} \beta_{s,t} X^s Y^t$ de $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]]$ si la famille $(\beta_{s,t} \alpha^s Y^t)_{(s,t) \in S \times T}$ est sommable dans $A[[Y_1, Y_2, \dots, Y_p]]$. La somme de cette famille se note alors $B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p)$.

PROPOSITION 2.52. — Propriétés de la substitution des scalaires. — Soit $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de A^n . L'ensemble, noté

$$A[[\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p]]$$

des éléments de $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]]$ dans lesquels a est substituable est une sous-algèbre unitaire de l'algèbre unitaire

$$A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]].$$

De plus, l'application δ_a qui à tout élément B de

$$A[[\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p]]$$

associe $B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p)$ est un morphisme d'algèbres unitaires.

Soient $B = \sum_{s,t} \beta_{s,t} X^s Y^t$ et $B' = \sum_{s,t} \beta'_{s,t} X^s Y^t$ deux éléments de $A[[\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p]]$. Par hypothèse, les familles $(\beta_{s,t} a^s Y^t)$ et $(\beta'_{s,t} a^s Y^t)$ sont sommables dans $A[[Y_1, Y_2, \dots, Y_p]]$. D'après la proposition 2.49, il en est de même de la somme et du produit de ces deux familles. Par suite, a est substituable dans $B + B'$ et dans BB' . Comme a est évidemment substituable dans 1, il en découle que $A[[\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p]]$ est une sous-algèbre unitaire de $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]]$. Pour voir que δ_a est un morphisme, il suffit d'appliquer à nouveau la proposition 2.49.

EXEMPLE. — L'élément $a = (0, 0, \dots, 0)$ de A^n est substituable dans tout élément B de $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]]$. De plus, l'application δ_0 qui à B associe $B(0, 0, \dots, 0, Y_1, Y_2, \dots, Y_p)$ est un morphisme de l'algèbre unitaire $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]]$ dans l'algèbre unitaire $A[[Y_1, Y_2, \dots, Y_p]]$.

COROLLAIRE. — Soient n et p deux entiers naturels non nuls et A_n l'anneau $A[X_1, X_2, \dots, X_n]$.

1. L'ensemble des séries entières formelles appartenant à $A_n[[Y_1, Y_2, \dots, Y_p]]$ est une sous-algèbre unitaire de l'algèbre unitaire

$$A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_p]].$$

Tout élément $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ de A^n est substituable dans tout élément B de $A_n[[Y_1, Y_2, \dots, Y_p]]$; de plus, si B est écrit sous la forme $B = \sum_{s \in S} P_s Y^s$, la famille $(P_s(a) Y^s)_{s \in S}$ est sommable, et

$$B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p) = \sum_{s \in S} P_s(a) Y^s.$$

L'application $B \mapsto B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p)$ est un morphisme de la A -algèbre unitaire $A_n[[Y_1, Y_2, \dots, Y_p]]$ dans la A -algèbre unitaire $A[[Y_1, Y_2, \dots, Y_p]]$.

2. Si l'anneau A est intègre et infini et si, pour toute suite $(\alpha_1, \alpha_2, \dots, \alpha_n)$ d'éléments de A , $B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p) = 0$, alors $B = 0$.

L'assertion 1 résulte aussitôt de la proposition précédente.

Assertion 2. — Supposons que, pour toute suite $(\alpha_1, \alpha_2, \dots, \alpha_n)$ d'éléments de A , $B(\alpha_1, \alpha_2, \dots, \alpha_n, Y_1, Y_2, \dots, Y_p) = 0$, ou encore

$$\sum_{s \in S} P_s(a) Y^s = 0.$$

Cela implique que, pour tout élément s de S et pour tout élément a de A^n , $P_s(a) = 0$. En appliquant le théorème 2.10 (ce qui est licite, puisque l'anneau A est intègre et infini), nous en déduisons que, pour tout élément s de S , $P_s = 0$, et donc que $B = 0$.

Enfin, la proposition 1.45 s'étend en la

PROPOSITION 2.53. — Détermination d'une application linéaire dans les séries entières formelles. — Soient I et J deux ensembles finis non vides, S l'ensemble des applications de $[1, n]$ dans N et $(C_s)_{s \in S}$ une famille sommable d'éléments de $S_J(A)$. Il existe alors une application linéaire U et une seule de $A[[X_i]]_{i \in I}$ dans $S_J(A)$ satisfaisant aux deux conditions suivantes :

- a) Pour tout élément s de S , $U(X^s) = C_s$.
- b) Pour toute suite (B_n) d'éléments de $A[[X_i]]_{i \in I}$ telle que $v_0(B_n)$ tende vers $+\infty$, $v_0[U(B_n)]$ tend vers $+\infty$ avec n .

De plus, la valeur de U sur une série entière formelle $B = \sum_{s \in S} \beta_s X^s$ est donnée par la formule

$$(1) \quad U(B) = \sum_{s \in S} \beta_s C_s.$$

L'unicité de U a déjà été démontrée (cf. cor. 1 de la prop. 2.48). Puisque la famille (C_s) est sommable, il en est de même de la famille $(\alpha_s C_s)$, pour toute famille (α_s) de scalaires. Il est alors immédiat que l'application U définie par la formule (1) convient.

REMARQUE. — On laisse au lecteur le soin d'étendre cette proposition au cas des applications multilinéaires de $(A[[X_i]]_{i \in I})^r$ dans $S_J(A)$.

Les théorèmes 1.13 et 1.14 s'étendent de la manière suivante :

THÉORÈME 2.19. — Éléments inversibles de l'anneau des séries entières formelles. — Pour qu'une série entière formelle $B = (\beta_s)_{s \in S}$ soit inversible dans l'anneau $A[[X]]$, il faut et il suffit que son terme constant β_0 soit inversible dans l'anneau A .

S'il existe une série entière formelle $C = (\gamma_s)_{s \in S}$ telle que $BC = 1$, alors $\beta_0 \gamma_0 = 1$, et β_0 est inversible. Réciproquement, si β_0 est inversible, B peut s'écrire sous la forme $B = \beta_0(1 + N)$, où $v_0(N) > 0$. La série entière formelle N

est donc substituable dans la série formelle entière à une indéterminée $(1 + X)^{-1} = 1 - X + X^2 + \dots + (-1)^n X^n + \dots$. Il est immédiat que $C = \beta_0^{-1}(1 - N + N^2 + \dots + (-1)^n N^n + \dots)$ est inverse de B .

COROLLAIRE 1. — Groupe unipotent. — *L'ensemble \mathcal{U} des séries entières formelles dont le terme constant est égal à 1 est un sous-groupe du groupe multiplicatif des éléments inversibles de l'anneau $A[[X_i]]_{i \in I}$.*

COROLLAIRE 2. — Idéal maximal de l'anneau des séries entières formelles. *Lorsque l'anneau A est un corps, l'ensemble \mathfrak{M} des séries entières formelles de valuation strictement positive est l'unique idéal maximal de $A[[X_i]]_{i \in I}$. Tout idéal de $A[[X_i]]_{i \in I}$ distinct de $A[[X_i]]_{i \in I}$ est contenu dans \mathfrak{M} . La puissance $p^{\text{ième}}$ de \mathfrak{M} n'est autre que l'idéal constitué des séries entières formelles de valuation supérieure ou égale à p .*

REMARQUE. — Contrairement au cas des séries entières formelles à une indéterminée, les idéaux précédents ne sont pas les seuls idéaux de $A[[X_i]]_{i \in I}$. Ainsi, dans l'anneau $A[[X, Y]]$, l'idéal principal engendré par X n'est pas du type précédent.

THÉORÈME 2.20. — Intégrité de l'anneau des séries entières formelles. — *Si l'anneau A est intègre, il en est de même de l'anneau $A[[X_i]]_{i \in I}$. Plus précisément, pour tout couple (B, C) d'éléments de $A[[X_i]]_{i \in I}$,*

$$(1) \quad v_0(BC) = v_0(B) + v_0(C).$$

En particulier, soit K un corps commutatif. L'anneau $K[[X_i]]_{i \in I}$ est intègre; son corps des quotients est une K -algèbre, notée $K((X_i))_{i \in I}$.

Soient B et C deux éléments non nuls de $A[[X_i]]_{i \in I}$, de valuations respectives p et q . Décomposons B et C en leurs composantes homogènes :

$$B = \sum_{r=p}^{+\infty} U_r \quad \text{et} \quad C = \sum_{s=q}^{+\infty} V_s.$$

Alors, d'après la proposition 2.49,

$$BC = \sum_{n=p+q}^{+\infty} \left(\sum_{r+s=n} U_r V_s \right).$$

Ainsi, pour tout entier $n < p + q$, la composante n -homogène de BC est nulle, tandis que la composante $(p + q)$ -homogène de BC est égale à $U_p V_q$. Puisque $U_p \neq 0$, que $V_q \neq 0$ et que l'anneau $A[[X_i]]_{i \in I}$ est intègre (cf. th. 2.6), $U_p V_q \neq 0$. La formule (1) en résulte.

REMARQUE 1. — Lorsque $n > 1$, tout élément B de $K((X_1, X_2, \dots, X_n))$ ne s'écrit pas nécessairement sous la forme $B = X^s C$, où s est une application de $[1, n]$ dans \mathbb{Z} , et où $C \in K[[X_1, X_2, \dots, X_n]]$; cf. exercice 51. C'est pourquoi la notion de série entière formelle généralisée est inintéressante dans le cas de plusieurs indéterminées.

REMARQUE 2. — Le théorème de permanence de la factorialité (cf. th. 2.9) ne s'étend pas aux anneaux de séries entières formelles : il existe des anneaux factoriels A tels que $A[[X]]$ ne soit pas factoriel. Néanmoins, on peut démontrer que, pour tout corps commutatif K , $K[[X_1, X_2, \dots, X_n]]$ est un anneau factoriel (cf. exercice 57). La démonstration repose sur un résultat de division euclidienne (th. de préparation de Weierstrass), que l'on trouvera dans l'exercice 53.

Ainsi, les propriétés de divisibilité des polynômes à plusieurs indéterminées s'étendent au cas des séries entières formelles.

REMARQUE 3. — Le théorème de permanence de Hilbert (cf. th. 2.8) s'étend aux anneaux de séries entières formelles : si A est noethérien, $A[[X]]$ l'est aussi; cf. exercice 50.

Étudions maintenant la dérivation des séries entières formelles à plusieurs indéterminées.

DÉFINITION 2.34. — Développement taylorien d'une série entière formelle. — Soient $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]]$ l'algèbre des séries entières formelles à $2n$ indéterminées à coefficients dans un anneau commutatif unitaire A , et $A_n = A[X_1, X_2, \dots, X_n]$ la sous-algèbre unitaire engendrée par X_1, X_2, \dots, X_n . Pour tout élément B de $A[[X_1, X_2, \dots, X_n]]$, soit $B(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n)$ l'élément de

$$A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]]$$

obtenu en substituant les polynômes $X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n$ aux indéterminées X_1, X_2, \dots, X_n dans la série entière formelle B . Pour tout entier naturel p , on désigne par $T_p(B)$ la composante p -homogène de la série formelle $B(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n)$, considérée comme élément de $A_n[Y_1, Y_2, \dots, Y_n]$. Ainsi, $T_p(B)$ est un polynôme p -homogène, et

$$B(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} T_p(B).$$

La famille des polynômes $T_p(B)$, où p parcourt \mathbb{N} , s'appelle développement taylorien de la série entière formelle B .

En particulier, $T_1(B)$ est un élément 1-homogène du sous-module M constitué des éléments 1-homogènes du A -module $A_n[Y_1, Y_2, \dots, Y_n]$; on l'appelle différentielle de la série entière formelle B , et on le note dB .

REMARQUE. — Lorsque B est un polynôme, les définitions précédentes coïncident avec celles du § 4.

La proposition 2.14 s'étend aussitôt à ce cas. Quant à la proposition 2.15, elle se généralise en la

PROPOSITION 2.54. — Propriétés de la différentiation des séries entières formelles. — L'application $B \mapsto dB$ est la seule application A -linéaire de $A[[X_1, X_2, \dots, X_n]]$ dans M satisfaisant aux deux conditions suivantes :

a) pour tout couple (B, C) d'éléments de $A[[X_1, X_2, \dots, X_n]]$,

$$d(BC) = dB \cdot C + B \cdot dC;$$

b) pour tout élément i de $[1, n]$,

$$dX_i = Y_i.$$

De plus, pour toute famille sommable $(B_j)_{j \in J}$ d'éléments de $A[[X_1, X_2, \dots, X_n]]$, la famille $(dB_j)_{j \in J}$ est sommable dans M , et

$$(1) \quad d\left(\sum_{j \in J} B_j\right) = \sum_{j \in J} dB_j.$$

Il est clair que l'application $B \mapsto dB$ satisfait aux conditions a) et b). Réciproquement, soit d' une application A -linéaire de $A[[X_1, X_2, \dots, X_n]]$ dans M satisfaisant à ces deux conditions. Comme dans la proposition 2.15, on démontre que $d'(1) = 0$ et, par récurrence, que, pour tout élément s de S , $d'X^s = dX^s$. Soit maintenant B un élément non nul de $A[[X_1, X_2, \dots, X_n]]$, de valuation $p > 0$. Alors B peut s'écrire sous la forme $B = \sum_{|s|=p} X^s C_s$, où $C_s \in A[[X_1, X_2, \dots, X_n]]$. Par suite,

$$d'B = \sum_{|s|=p} (d'X^s C_s + X^s d'C_s) = \sum_{|s|=p} (dX^s C_s + X^s d'C_s),$$

ce qui prouve que les valuations de tous les coefficients de $d'B$, considérés comme éléments de $A[[X_1, X_2, \dots, X_n]]$, sont supérieures ou égales à $p - 1$. Il en découle que les applications $B \mapsto dB$ et $B \mapsto d'B$ sont deux applications linéaires de $A[[X_1, X_2, \dots, X_n]]$ dans $A[[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n]]$, coïncidant sur les monômes, et satisfaisant aux conditions du corollaire 2 de la proposition 2.48. Donc $d' = d$.

Enfin, la démonstration de la formule (1) est calquée sur le cas des séries entières formelles à une indéterminée (cf. assertion 3 du th. 1.15).

La proposition 2.16, concernant les différentielles des polynômes composés, s'étend aussitôt. Les propositions 2.17 et 2.18, concernant les dérivées partielles des polynômes, s'étendent au cas des séries entières formelles, l'unicité de la dérivation partielle D_i se démontrant comme ci-dessus.

Enfin, les théorèmes de Schwarz et de Taylor s'étendent facilement en les énoncés suivants :

THÉORÈME 2.21. — Théorème de Schwarz. — Soit \mathcal{E} l'algèbre des endomorphismes du A -module $A[[X_1, X_2, \dots, X_n]]$.

1. La sous-algèbre unitaire \mathcal{D} de \mathcal{E} engendrée par les dérivations partielles D_1, D_2, \dots, D_n est commutative; les éléments de \mathcal{D} s'appellent opérateurs différentiels à coefficients constants sur $A[[X_1, X_2, \dots, X_n]]$.

2. Lorsque A est de caractéristique nulle, l'unique morphisme f de l'algèbre unitaire $A[Y_1, Y_2, \dots, Y_n]$ dans l'algèbre unitaire \mathcal{D} tel que, pour tout $i \in [1, n]$, $f(Y_i) = D_i$, est un isomorphisme.

COROLLAIRE. — Formule de Maclaurin. — Soit $B = \sum_{s \in S} \beta_s X^s$ un élément de $A[[X_1, X_2, \dots, X_n]]$. Alors, pour tout élément s de S ,

$$(D^s B)(0) = s ! \beta_s.$$

En particulier, si A est un corps de caractéristique 0,

$$B = \sum_{s \in S} \frac{(D^s B)(0)}{s !} X^s.$$

THÉORÈME 2.22. — Formule de Taylor. — Soient A un anneau commutatif unitaire, B un élément de $A[[X_1, X_2, \dots, X_n]]$, et

$$B(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} T_p(B)$$

le développement taylorien de B . Alors les polynômes $T_p(B)$ sont liés aux dérivées partielles de B par les relations

$$H^p(B) = p ! T_p(B),$$

où H désigne l'opérateur différentiel sur $A[[X_1, X_2, \dots, X_n]]$ défini par la relation

$$H = \sum_{i=1}^n Y_i D_i.$$

En particulier, lorsque A est un corps de caractéristique 0,

$$B(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n) = \sum_{p=0}^{+\infty} \frac{H^p(B)}{p !}.$$

REMARQUE. — L'application $B \mapsto dB$ se prolonge d'une manière et d'une seule en une application linéaire de $K((X_1, X_2, \dots, X_n))$ dans le sous-module M' constitué des éléments 1-homogènes de $K'_n[Y_1, Y_2, \dots, Y_n]$, où

$$K'_n = A((X_1, X_2, \dots, X_n)).$$

De même, pour tout élément i de $[1, n]$, l'application $B \mapsto D_i B$ se prolonge d'une manière et d'une seule en une dérivation de l'algèbre $K((X_1, X_2, \dots, X_n))$.

Pour généraliser le théorème 1.16 concernant les séries entières formelles réciproques, nous utiliserons quelques notions sur les séries entières formelles à coefficients vectoriels, dont la théorie générale est esquissée dans les exercices 27 et 29.

Soit n un entier naturel non nul. Les suites $B = (B_1, B_2, \dots, B_n)$ d'éléments de l'anneau $A[[X_1, X_2, \dots, X_p]]$ s'appellent séries entières formelles à coefficients dans A^n ; elles constituent un $A[[X_1, X_2, \dots, X_p]]$ — module, noté $A^n[[X_1, X_2, \dots, X_p]]$. On appelle valuation de B , et on note $v_0(B)$, la plus petite des valuations $v_0(B_j)$, où j parcourt $[1, n]$.

On dit qu'une famille $(B_h)_{h \in H}$ de séries entières formelles

$$B_h = (B_{h1}, B_{h2}, \dots, B_{hp})$$

est sommable si, pour tout élément j de $[1, n]$, la famille $(B_{hj})_{h \in H}$ l'est. On appelle alors somme de la famille $(B_h)_{h \in H}$, et on note $\sum_{h \in H} B_h$, la série entière formelle à coefficients dans A^n ayant pour composantes $\sum_{h \in H} B_{hj}$, où j parcourt $[1, n]$. Les propriétés de la sommation des séries entières formelles s'étendent aussitôt à ce cas.

On définit de même la dérivée partielle $D_i(C) = (D_i(C_1), D_i(C_2), \dots, D_i(C_n))$ d'un élément $C = (C_1, C_2, \dots, C_n)$ de $A_n[[X_1, X_2, \dots, X_p]]$. L'application D_i est un endomorphisme du A -module $A^n[[X_1, X_2, \dots, X_p]]$. Pour tout élément B de $A[[X_1, X_2, \dots, X_p]]$ et pour tout élément C de $A^n[[X_1, X_2, \dots, X_p]]$,

$$D_i(BC) = (D_i B)C + B(D_i C).$$

Enfin, pour toute famille sommable $(C_h)_{h \in H}$ d'éléments de $A_n[[X_1, X_2, \dots, X_p]]$, la famille $(D_i(C_h))_{h \in H}$ est sommable, et

$$D_i\left(\sum_{h \in H} C_h\right) = \sum_{h \in H} D_i C_h.$$

Soit maintenant U une application A -linéaire de A^n dans A^m . A tout élément $B = (B_1, B_2, \dots, B_n)$ de $A^n[[X_1, X_2, \dots, X_p]]$ on associe l'élément $\tilde{U}(B) = (C_1, C_2, \dots, C_m)$ de $A^m[[X_1, X_2, \dots, X_p]]$ défini par la formule

$$C_i = \sum_{j=1}^n \alpha_{ij} B_j,$$

où (α_{ij}) désigne la matrice canoniquement associée à U . L'application \tilde{U} ainsi définie est $A[[X_1, X_2, \dots, X_p]]$ -linéaire; on l'appelle extension canonique de U . Il est immédiat que, pour tout élément B de $A^n[[X_1, X_2, \dots, X_p]]$, $v_0[\tilde{U}(B)] \geq v_0(B)$.

Nous pouvons alors énoncer le théorème suivant :

***THÉORÈME 2.23. — Séries entières formelles implicites.** — Soient (F_1, F_2, \dots, F_n) une suite de n éléments de $A[[Y_1, Y_2, \dots, Y_n, X_1, X_2, \dots, X_p]]$, de valuations strictement positives et, pour tout couple (i, j) d'éléments de $[1, n]$, E_{ij} le terme constant de la série entière formelle $\frac{\partial F_i}{\partial Y_j}$, considérée comme élément de $A_p[[Y_1, Y_2, \dots, Y_n]]$, où $A' = A[[X_1, X_2, \dots, X_p]]$. Si $\text{Det}(E_{ij})$ est inversible dans l'anneau $A[[X_1, X_2, \dots, X_p]]$, il existe une suite (B_1, B_2, \dots, B_n) et une seule d'éléments de $A[[X_1, X_2, \dots, X_p]]$ de valuations strictement positives telle que, pour tout élément i de $[1, n]$,

$$(1) \quad F_i(B_1, B_2, \dots, B_n, X_1, X_2, \dots, X_p) = 0.$$

Il résulte des hypothèses que, pour tout élément i de $[1, n]$, F_i s'écrit sous la forme

$$(2) \quad F_i = C_i + \sum_{j=1}^n E_{ij} Y_j + \sum_{|s| \geq 2} U_{s,i} Y^s,$$

où C_i et $U_{s,i}$ sont des éléments de A' , C_i étant de valuation strictement positive.

Soit \mathfrak{M}' l'idéal maximal de $A' = A[[X_1, X_2, \dots, X_p]]$. Considérons l'élément $C = (C_1, C_2, \dots, C_n)$ du A' -module \mathfrak{M}'^n et l'endomorphisme U de ce module canoniquement associé à la matrice (E_{ij}) . Introduisons enfin l'application V de \mathfrak{M}'^n dans lui-même qui à tout élément $G = (G_1, G_2, \dots, G_n)$ associe l'élément $G' = (G'_1, G'_2, \dots, G'_n)$ où, pour tout élément i de $[1, n]$,

$$G'_i = \sum_{|s| \geq 2} U_{s,i} G^s.$$

L'existence et l'unicité d'une suite (B_1, B_2, \dots, B_n) d'éléments de \mathfrak{M}' , satisfaisant à la relation (1) équivalent alors à l'existence et l'unicité d'un élément B de \mathfrak{M}'^n satisfaisant à la relation

$$(3) \quad C + U(B) + V(B) = 0.$$

Or, puisque D et $U = D$ et (E_{ij}) est inversible dans A' , U est un automorphisme de \mathfrak{M}'^n . L'équation (3) s'écrit donc encore

$$(4) \quad B = D + W(B),$$

où $D = -U^{-1}(C)$ et $W = -U^{-1} \circ V$.

De plus, pour tout couple (G, G') d'éléments distincts de \mathfrak{M}'^n ,

$$(5) \quad v_0[W(G) - W(G')] > v_0(G - G').$$

En effet, on voit aussitôt par récurrence sur $|s|$ que, pour tout élément s de S tel que $|s| \geq 2$,

$$v_0(G^s - G'^s) > v_0(G - G').$$

La formule (5) en résulte, puisque $W = -U^{-1} \circ V$ et que U^{-1} est linéaire.

Nous pouvons maintenant prouver l'existence et l'unicité de B par la méthode des approximations successives.

Unicité. — Soient B et B' deux éléments de \mathfrak{M}'^n satisfaisant à (4). Alors

$$B - B' = W(B) - W(B').$$

D'après la formule (5), il s'ensuit que $B = B'$.

Existence. — Considérons la suite (S_r) d'éléments de \mathfrak{M}'^n définie par les relations

$$(6) \quad \begin{aligned} S_0 &= 0 \\ S_r &= D + W(S_{r-1}) \quad \text{si } r \geq 1. \end{aligned}$$

D'après la relation (5), pour tout entier naturel r ,

$$v_0(\mathcal{S}_{r+1} - \mathcal{S}_r) \geq v_0(\mathcal{S}_r - \mathcal{S}_{r-1}) + 1.$$

Comme $v_0(\mathcal{S}_1 - \mathcal{S}_0) = v_0(\mathcal{D}) \geq 1$, nous en déduisons que

$$v_0(\mathcal{S}_r - \mathcal{S}_{r-1}) \geq r.$$

La suite $(\mathcal{S}_{r+1} - \mathcal{S}_r)$ est donc sommable; soit \mathcal{B} sa somme. Alors, pour tout entier naturel r ,

$$v_0(\mathcal{B} - \mathcal{S}_r) > r.$$

Il en découle que

$$v_0[\mathcal{B} - \mathcal{D} - W(\mathcal{B})] \geq v_0(\mathcal{B} - \mathcal{S}_{r+1}) + v_0[W(\mathcal{B}) - W(\mathcal{S}_r)] > r + 1,$$

ce qui prouve que \mathcal{B} satisfait à la relation (4).

REMARQUE. — L'algorithme (6) fournit un procédé explicite de construction de solutions approchées de l'équation (4).

Enfin, la définition et les propriétés des exponentielles formelles s'étendent sans changement au cas des séries entières formelles à une indéterminée à coefficients dans un anneau commutatif unitaire A de caractéristique 0 contenant \mathbb{Q} . En particulier, on peut prendre pour A l'anneau $K[X_1, X_2, \dots, X_n]$, ou l'anneau $K[[X_1, X_2, \dots, X_n]]$, où K est un corps de caractéristique 0.

Nous obtenons alors la

PROPOSITION 2.55. — **Équation fonctionnelle de l'exponentielle formelle.** — Soit A un anneau commutatif unitaire de caractéristique 0 contenant \mathbb{Q} .

1. La série entière formelle $E = \exp X$ satisfait aux conditions suivantes :

$$(1) \quad E(0) = 1$$

$$(2) \quad E(Y + Z) = E(Y)E(Z).$$

2. Réciproquement, soit E un élément de $A[[X]]$ satisfaisant à ces conditions. Il existe alors un scalaire α et un seul tel que $E = \exp(\alpha X)$, à savoir $\alpha = E'(0)$.

Assertion 1. — La démonstration est calquée sur celle de la formule $\exp(A + B) = (\exp A)(\exp B)$ (cf. th. 1.17). Inversement, cette dernière formule peut s'obtenir à partir de la formule (2) en substituant A à Y et B à Z (cf. prop. 2.51).

Assertion 2. — Soit E un élément de $A[[X]]$ satisfaisant aux conditions (1) et (2). En prenant les dérivées partielles des deux membres de (2) par rapport à Y , nous obtenons la relation

$$(3) \quad E'(Y + Z) = E'(Y)E(Z).$$

En substituant 0 à Y dans les deux membres de (3), nous en déduisons que

$$(4) \quad E'(Z) = \alpha E(Z), \quad \text{où } \alpha = E'(0).$$

En appliquant le théorème 1.17 (au cas des séries entières formelles à coefficients dans un anneau), nous déduisons alors des relations (1) et (4) que

$$(5) \quad E(Z) = \exp(\alpha Z).$$

Inversement, si $E(Z) = \exp(\beta Z)$, où $\beta \in A$, alors $\beta = E'(0)$, ce qui montre l'unicité de α .

Exercices conseillés : 44 à 47.

2. OPÉRATEURS DE COMPOSITION

Dans ce qui suit, K désigne un corps commutatif de caractéristique nulle. On note D la dérivation canonique de la K -algèbre $K[X]$.

PROPOSITION 2.56. — Opérateurs de translation. — *Pour tout élément α de K , l'application T_α qui à tout polynôme P associe le polynôme*

$$T_\alpha(P) = P(X + \alpha)$$

est un automorphisme de la K -algèbre unitaire $K[X]$, appelé opérateur de translation défini par α . De plus, l'application $\alpha \mapsto T_\alpha$ est un morphisme du groupe additif K dans le groupe G des automorphismes de la K -algèbre unitaire $K[X]$. En particulier, pour tout couple (α, β) d'éléments de K ,

$$T_{\alpha+\beta} = T_\alpha \circ T_\beta = T_\beta \circ T_\alpha.$$

DÉFINITION 2.35. — Opérateurs de composition. — *On dit qu'un endomorphisme U de l'espace vectoriel $K[X]$ est un opérateur de composition sur $K[X]$ si U commute avec tous les opérateurs de translation T_α , où α parcourt K :*

$$U \circ T_\alpha = T_\alpha \circ U.$$

Les opérateurs de composition constituent une sous-algèbre unitaire, notée $\widehat{\mathcal{D}}$, de l'algèbre des endomorphismes de l'espace vectoriel $K[X]$.

EXEMPLES.

1. Opérateurs aux différences finies. — Les combinaisons linéaires des opérateurs de translation constituent une sous-algèbre unitaire de $\widehat{\mathcal{D}}$, dont les éléments s'appellent *opérateurs aux différences finies*.

En particulier, l'endomorphisme $\Delta : P \mapsto P(X + 1) - P(X)$ est un opérateur aux différences finies, ainsi que $Q(\Delta)$, pour tout élément Q de $K[X]$.

L'étude de ces opérateurs, qui interviennent dans la théorie des fonctions définies sur \mathbf{Z} , sera effectuée au § 5.8. L'étude de Δ sera approfondie au chapitre 4.

2. Opérateurs différentiels. — L'ensemble \mathcal{D} des opérateurs différentiels à coefficients constants sur $K[X]$ est une sous-algèbre de $\widehat{\mathcal{D}}$.

En effet, pour tout élément α de K ,

$$(D \circ T_\alpha)(P) = D[P(X + \alpha)] = (DP)(X + \alpha) = (T_\alpha \circ D)(P).$$

Ainsi, D est un opérateur de composition. Par suite, pour tout élément Q de $K[X]$, l'endomorphisme $Q(D)$ est un opérateur de composition, ce qu'il fallait prouver.

L'étude de ces opérateurs sera effectuée au § 5.8.

3. Plus généralement encore, considérons un élément $A = \sum_{n=0}^{+\infty} \alpha_n X^n$ de $K[[X]]$. L'application $P \mapsto \sum_{n=0}^{+\infty} \alpha_n D^n(P)$ est un opérateur de composition, noté $\sum_{n=0}^{+\infty} \alpha_n D^n$, ou encore $A(D)$.

En effet, pour tout polynôme P et pour tout scalaire α , $D^n(P) = 0$ et $D^n[T_\alpha(P)] = 0$ dès que $n > d^0(P)$.

En fait, le dernier exemple constitue le cas le plus général. Plus précisément :

THÉORÈME 2.24. — Structure des opérateurs de composition. — *Soit U un endomorphisme de l'espace vectoriel $K[X]$. Il est équivalent de dire :*

1. *L'endomorphisme U est un opérateur de composition, c'est-à-dire qu'il commute avec tous les opérateurs de translation.*

2. *L'endomorphisme U commute avec D .*

3. *Il existe un élément A de $K[[X]]$ tel que $U = A(D)$.*

De plus, lorsque ces conditions équivalentes sont réalisées, pour tout élément P de $K[X]$,

$$(1) \quad U(P)(X + Y) = \sum_{n=0}^{+\infty} \frac{U(X^n)}{n!} [D^n(P)](Y)$$

(formule de Taylor généralisée).

En particulier,

$$(2) \quad U(P) = \sum_{n=0}^{+\infty} \frac{U(X^n)}{n!} [D^n(P)](0)$$

(formule de Maclaurin généralisée), et

$$(3) \quad U = \sum_{n=0}^{+\infty} \alpha_n D^n,$$

où α_n est la valeur au point 0 du polynôme $\frac{U(X^n)}{n!}$ (formule de structure de U).

1 \Leftrightarrow 2. En utilisant la formule de Taylor pour les polynômes à une indéterminée (cf. th. 1.9), nous voyons que, pour tout endomorphisme U de l'espace vectoriel $K[X]$,

$$(4) \quad (U \circ T_\alpha)(P) = U[P(X + \alpha)] = \sum_{n=0}^{+\infty} \frac{\alpha^n}{n!} (U \circ D^n)(P)$$

et

$$(5) \quad (T_\alpha \circ U)(P) = \sum_{n=0}^{+\infty} \frac{\alpha^n}{n!} (D^n \circ U)(P).$$

Si $U \circ D = D \circ U$, alors, pour tout entier naturel n , $U \circ D^n = D^n \circ U$, et $U \circ T_\alpha = T_\alpha \circ U$.

Réciproquement, si, pour tout élément α de K , $T_\alpha \circ U = U \circ T_\alpha$, alors, pour tout élément P de $K[X]$, les fonctions polynomiales

$$\alpha \mapsto \sum_{n=0}^{+\infty} \frac{\alpha^n}{n!} (U \circ D^n)(P) \quad \text{et} \quad \alpha \mapsto \sum_{n=0}^{+\infty} \frac{\alpha^n}{n!} (D^n \circ U)(P)$$

sont égales. Comme le corps K est infini, il en découle que, pour tout entier naturel n ,

$$(U \circ D^n)(P) = (D^n \circ U)(P),$$

ce qu'il fallait prouver.

3 \Rightarrow 2 est évident.

Pour démontrer que 2 \Rightarrow 3, il suffit évidemment de prouver que si $U \circ D = D \circ U$, la formule (1) est vraie, car les formules (2) et (3) s'en déduisent par substitution de 0 à Y et à X . Supposons donc que $U \circ D = D \circ U$ et appliquons la formule de Taylor au polynôme $U(P)$, où $P \in K[X]$:

$$(6) \quad [U(P)](X + Y) = \sum_{n=0}^{+\infty} \frac{Y^n}{n!} [(D^n \circ U)(P)](X).$$

Comme, pour tout entier n , U commute avec D^n ,

$$(7) \quad [U(P)](X + Y) = U \left[\sum_{n=0}^{+\infty} \frac{Y^n}{n!} (D^n P)(X) \right].$$

Or,

$$(8) \quad \sum_{n=0}^{+\infty} \frac{Y^n}{n!} (D^n P)(X) = P(X + Y) = \sum_{n=0}^{+\infty} \frac{X^n}{n!} (D^n P)(Y).$$

La formule (1) résulte alors des formules (7) et (8).

COROLLAIRE 1. — Propriétés des opérateurs de composition.

1. L'application $A \mapsto A(D)$ est un isomorphisme de la K -algèbre $K[[X]]$ sur l'algèbre $\widehat{\mathcal{D}}$ des opérateurs de composition sur $K[X]$. En particulier, $\widehat{\mathcal{D}}$ est commutative. C'est pourquoi l'algèbre $\widehat{\mathcal{D}}$ sera désormais notée $K[[D]]$.

Ainsi, tout opérateur de composition U sur $K[X]$ s'écrit d'une manière et d'une seule sous la forme $U = \sum_{n=0}^{+\infty} \alpha_n D^n$. La valuation de la série entière formelle $\sum_{n=0}^{+\infty} \alpha_n X^n$ s'appelle ordre de U .

2. Si U est d'ordre p , où $p \in \mathbb{N}$, U s'écrit d'une manière et d'une seule sous la forme $U = D^p V$, où V est un opérateur de composition d'ordre 0. Pour tout polynôme non nul P ,

$$\begin{aligned} U(P) &= 0 & \text{si } d^0(P) < p, \\ d^0[U(P)] &= d^0(P) - p & \text{si } d^0(P) \geq p. \end{aligned}$$

En particulier, le noyau de U est constitué des polynômes de degré strictement inférieur à p .

Soit φ l'application qui à tout élément A de $K[[X]]$ associe l'opérateur de composition $A(D)$. Il est évident que φ est linéaire. D'après la formule (3), φ est bijective. Soit maintenant U un opérateur de composition d'ordre p , écrit sous la forme $U = \sum_{n=p}^{+\infty} \alpha_n D^n$, où $\alpha_p \neq 0$. Il en découle aussitôt que U s'écrit d'une manière et d'une seule sous la forme $U = D^p V$, où V est d'ordre 0. De plus, pour tout entier naturel r ,

$$U(X^r) = \sum_{n=p}^{+\infty} \alpha_n D^n(X^r);$$

donc $U(X^r) = 0$ si $r < p$ et $d^0[U(X^r)] = r - p$ si $r \geq p$. L'assertion 2 en résulte.

Il nous reste à prouver que, pour tout couple (A, B) d'éléments de $K[[X]]$ et pour tout élément P de $K[X]$,

$$(9) \quad [\varphi(AB)](P) = [\varphi(A) \circ \varphi(B)](P).$$

Fixons pour cela B et P . Il est immédiat que la relation (9) est vraie lorsque $A = X^n$, où $n \in \mathbb{N}$. D'autre part, les applications $\psi : A \mapsto [\varphi(AB)](P)$ et $\chi : A \mapsto \varphi(A)[\varphi(B)(P)]$ sont des endomorphismes de l'espace vectoriel $K[[X]]$. Si $v_0(A) > d^0(P)$, $\psi(A) = [\varphi(AB)](P) = 0$, car $v_0(AB) > d^0(P)$. De même, $\chi(A) = \varphi(A)[\varphi(B)(P)] = 0$, car $v_0(A) > d^0(P) \geq d^0[\varphi(B)(P)]$. Ainsi, les endomorphismes ψ et χ satisfont aux hypothèses du corollaire 1 de la proposition 2.48. Par suite, $\psi = \chi$, ce qu'il fallait démontrer.

EXEMPLES.

1. **Structure des opérateurs de translation.** — Pour tout scalaire α ,

$$T_\alpha = \exp(\alpha D) = \sum_{n=0}^{+\infty} \frac{\alpha^n D^n}{n!}.$$

L'ordre de T_α est donc égal à 0.

En effet, la formule de Taylor montre que, pour tout élément P de $K[X]$,

$$T_\alpha(P) = P(X + \alpha) = \sum_{n=0}^{+\infty} \frac{\alpha^n}{n!} D^n(P).$$

2. Structure de l'opérateur de Bernoulli. — Soit $\Delta = T_1 - T_0$. Alors

$$\Delta = \exp D - I = \sum_{n=1}^{+\infty} \frac{D^n}{n!}.$$

En particulier, Δ est d'ordre 1.

COROLLAIRE 2. — Inversibilité des opérateurs de composition. — Soit U un opérateur de composition sur $K[X]$ associé à un élément A de $K[[X]]$. Pour que U soit inversible dans $\mathcal{L}(K[X])$, il faut et il suffit que l'ordre de U soit égal à 0. Dans ces conditions, U^{-1} est un opérateur de composition, à savoir l'opérateur associé à la série entière formelle A^{-1} .

En effet, si l'ordre de U n'est pas égal à 0, le noyau de U n'est pas réduit à $\{0\}$. Par suite, U n'est pas inversible dans $\mathcal{L}(K[X])$.

Si l'ordre de U est égal à 0, c'est-à-dire si la valuation de A est nulle, A est inversible dans $K[[X]]$ (cf. th. 1.13). Comme l'application $A \mapsto A(D)$ est un isomorphisme de $K[[X]]$ sur $\widehat{\mathcal{D}}$, l'opérateur de composition associé à A^{-1} est inverse de U .

Pour calculer de manière explicite l'inverse d'un opérateur de composition, nous introduisons la

DÉFINITION 2.36. — Polynômes d'Appell. — Soit U un opérateur de composition d'ordre p , où $p \in \mathbb{N}$, écrit sous la forme $U = D^p V$. Pour tout entier naturel n , le polynôme $P_n = V^{-1}(X^n)$ s'appelle $n^{\text{ième}}$ polynôme d'Appell associé à U , et le scalaire $\beta_n = P_n(0)$ s'appelle $n^{\text{ième}}$ nombre d'Appell associé à U .

PROPOSITION 2.57. — Propriétés des polynômes d'Appell. — Soient (P_n) la suite des polynômes d'Appell et (β_n) la suite des nombres d'Appell associées à U .

1. Pour tout entier naturel n , le polynôme P_n est de degré n et, pour tout entier naturel non nul n ,

$$(1) \quad D(P_n) = nP_{n-1}.$$

De plus,

$$(2) \quad \begin{array}{ll} U(P_n) = 0 & \text{si } 0 \leq n < p \\ U(P_n) = \frac{n!}{(n-p)!} X^{n-p} & \text{si } n \geq p. \end{array}$$

2. Pour tout scalaire α ,

$$(3) \quad T_\alpha \circ V^{-1} = V^{-1} \circ T_\alpha = \sum_{n=0}^{+\infty} \frac{P_n(\alpha)}{n!} D^n.$$

En particulier,

$$(4) \quad V^{-1} = \sum_{n=0}^{+\infty} \frac{\beta_n}{n!} D^n.$$

Enfin, pour tout entier naturel n ,

$$(5) \quad P_n(X) = \sum_{k=0}^n C_n^k \beta_{n-k} X^k.$$

3. Soit A l'élément de $K[[X]]$ canoniquement associé à U , écrit sous la forme $A = X^p B$, où B est inversible dans $K[[X]]$. Alors

$$(6) \quad B^{-1}(Y) \exp(XY) = \sum_{n=0}^{+\infty} \frac{P_n(X)}{n!} Y^n.$$

Autrement dit, le $n^{\text{ième}}$ polynôme d'Appell associé à U s'obtient en multipliant par $n!$ le coefficient de Y^n dans la série entière formelle à deux indéterminées $B^{-1}(Y) \exp(XY)$. C'est pourquoi cette série entière formelle à deux indéterminées s'appelle série génératrice des polynômes d'Appell associé à U .

Assertion 1. — Comme V^{-1} est d'ordre 0, $d^0(P_n) = d^0(X^n) = n$. Les formules (1) et (2) résultent respectivement des formules $UV^{-1} = D^p$ et $DV^{-1} = V^{-1}D$.

Assertion 2. — D'après le théorème 2.24,

$$V^{-1}(P)(X + Y) = \sum_{n=0}^{+\infty} \frac{V^{-1}(X^n)}{n!} (D^n P)(Y) = \sum_{n=0}^{+\infty} \frac{P_n(X)}{n!} (D^n P)(Y).$$

La formule (3) s'en déduit aussitôt, ainsi que la formule (4), qui correspond au cas où $\alpha = 0$. Enfin, la formule (5) s'obtient en appliquant les deux membres de la relation (4) au monôme X^n .

Assertion 3. — L'opérateur de composition V^{-1} n'est autre que $B^{-1}(D)$. D'autre part, pour tout scalaire α , $T_\alpha = \exp(\alpha D)$. La formule (3) s'écrit donc encore

$$(7) \quad B^{-1}(D) \exp(\alpha D) = \sum_{n=0}^{+\infty} \frac{P_n(\alpha)}{n!} D^n.$$

L'application $A \mapsto A(D)$ étant un isomorphisme de $K[[Y]]$ sur $\widehat{\mathcal{D}}$, nous en déduisons que, pour tout scalaire α ,

$$(8) \quad B^{-1}(Y) \exp(\alpha Y) = \sum_{n=0}^{+\infty} \frac{P_n(\alpha)}{n!} Y^n.$$

Considérons maintenant les deux séries entières formelles à deux indéterminées $B^{-1}(Y) \exp(XY)$ et $\sum_{n=0}^{+\infty} \frac{P_n(X)}{n!} Y^n$. Ces séries entières formelles appartiennent

nent à $K[X][[Y]]$. D'après le corollaire de la proposition 2.48, la formule (8) implique que ces deux séries entières formelles sont égales, c'est-à-dire que la formule (6) est vraie.

EXEMPLES.

1. **Polynômes d'Appell associés aux opérateurs de translation.** — Le $n^{\text{ième}}$ polynôme d'Appell associé à l'opérateur de translation T_α n'est autre que $(X - \alpha)^n$. La série génératrice de ces polynômes n'est autre que $\exp[(X - \alpha)Y]$.

En effet, T_α est d'ordre 0, et son inverse est $T_{-\alpha}$. Donc

$$P_n = T_{-\alpha}(X^n) = (X - \alpha)^n.$$

La série entière formelle B associée à T_α est égale à $\exp(\alpha Y)$; donc la série génératrice des polynômes P_n est égale à

$$[\exp(\alpha Y)]^{-1} \exp(XY) = \exp[(X - \alpha)Y].$$

2. **Polynômes de Bernoulli.** — Considérons l'opérateur de composition $\Delta = T_1 - T_0$. La série entière formelle associée à Δ est égale à $\exp Y - 1$. L'opérateur Δ est d'ordre 1, et s'écrit sous la forme $\Delta = DV$, où $V = B(D)$, B étant la série entière formelle définie par la formule

$$B(Y) = \frac{\exp Y - 1}{Y}.$$

Le $n^{\text{ième}}$ polynôme d'Appell associé à Δ s'appelle $n^{\text{ième}}$ polynôme de Bernoulli, et se note B_n ; le nombre $\beta_n = B_n(0)$ s'appelle $n^{\text{ième}}$ nombre de Bernoulli. Le théorème précédent montre que les polynômes de Bernoulli satisfont aux relations (1) à (5).

De plus, la série génératrice des polynômes de Bernoulli est $\frac{Y \exp(XY)}{\exp Y - 1}$.

Autrement dit,

$$(6') \quad \frac{Y \exp(XY)}{\exp Y - 1} = \sum_{n=0}^{+\infty} \frac{B_n(X)}{n!} Y^n.$$

En particulier,

$$(7') \quad \frac{Y}{\exp Y - 1} = \sum_{n=0}^{+\infty} \frac{\beta_n}{n!} Y^n.$$

En outre, d'après la formule (2), pour tout entier $n \geq 1$, $B_n(1) = B_n(0)$. En tenant compte de la formule (5), nous en déduisons que, pour tout entier $n \geq 1$,

$$(8') \quad \sum_{k=0}^{n-1} C_n^k \beta_k = 0$$

(formule de récurrence qui permet de calculer de proche en proche les nombres de Bernoulli, et de prouver que ces nombres sont rationnels).

Posons enfin

$$G(Y) = \frac{Y}{\exp Y - 1}.$$

Alors

$$G(Y) + G(-Y) = Y \frac{\exp Y + 1}{\exp Y - 1},$$

$$G(Y) - G(-Y) = -Y.$$

La série entière formelle $G(Y) + \frac{Y}{2}$ est donc paire; on en déduit que

$$(9') \quad \beta_{2n+1} = 0 \quad \text{si } n \geq 1.$$

Par suite,

$$(10') \quad \frac{Y \exp Y + 1}{2 \exp Y - 1} = 1 + \sum_{n=1}^{+\infty} \frac{\beta_{2n}}{(2n)!} Y^{2n}.$$

D'autre part,

$$\beta_0 = 1, \quad \beta_1 = -\frac{1}{2}, \quad \beta_2 = \frac{1}{6}, \quad \beta_4 = -\frac{1}{30}, \quad \beta_6 = \frac{1}{42}, \dots$$

Les nombres de Bernoulli interviennent dans les développements en série de nombreuses fonctions classiques :

PROPOSITION 2.58. — Calcul de certaines séries entières formelles hyperboliques et trigonométriques.

1. Les séries entières formelles $\text{th } X$ et $\text{tg } X$ sont inversibles dans l'algèbre $C((X))$ des séries entières formelles généralisées; leurs inverses s'appellent *cotangente hyperbolique formelle* et *cotangente formelle* de X , et se notent $\text{coth } X$ et $\text{cot } X$. De plus,

$$(1) \quad \text{coth } X = \frac{1}{X} + \sum_{n=1}^{+\infty} 2^{2n} \frac{\beta_{2n}}{(2n)!} X^{2n-1}$$

$$(1') \quad \text{cot } X = \frac{1}{X} + \sum_{n=1}^{+\infty} (-1)^n 2^{2n} \frac{\beta_{2n}}{(2n)!} X^{2n-1}.$$

2. Les séries entières formelles $\text{th } X$ et $\text{tg } X$ sont données par les formules suivantes :

$$(2) \quad \text{th } X = \sum_{n=1}^{+\infty} 2^{2n} (2^{2n} - 1) \frac{\beta_{2n}}{(2n)!} X^{2n-1}$$

$$(2') \quad \text{tg } X = \sum_{n=1}^{+\infty} (-1)^{n-1} 2^{2n} (2^{2n} - 1) \frac{\beta_{2n}}{(2n)!} X^{2n-1}.$$

3. Les séries entières formelles $\operatorname{sh} X$ et $\sin X$ sont inversibles dans l'algèbre $\mathbb{C}((X))$; leurs inverses sont donnés par les formules suivantes :

$$(3) \quad \frac{1}{\operatorname{sh} X} = \frac{1}{X} - \sum_{n=1}^{+\infty} 2(2^{2n-1} - 1) \frac{\beta_{2n}}{(2n)!} X^{2n-1}.$$

$$(3') \quad \frac{1}{\sin X} = \frac{1}{X} + \sum_{n=1}^{+\infty} (-1)^{n-1} 2(2^{2n-1} - 1) \frac{\beta_{2n}}{(2n)!} X^{2n-1}.$$

La formule (1) s'obtient en substituant $2X$ à Y dans la formule (10'), car

$$\operatorname{coth} X = \frac{\exp(2X) + 1}{\exp(2X) - 1}.$$

Les formules (2) et (3) découlent aussitôt de la formule (1) et des relations suivantes :

$$\operatorname{th} X = 2 \operatorname{coth} 2X - \operatorname{coth} X$$

$$\frac{1}{\operatorname{sh} X} = \operatorname{coth} \frac{X}{2} - \operatorname{coth} X.$$

Les formules (1'), (2') et (3') s'obtiennent alors en substituant iX à X dans les formules (1), (2) et (3).

REMARQUE 1. — En utilisant les relations

$$\begin{aligned} \frac{1}{\operatorname{ch}^2 X} &= D(\operatorname{th} X) = 1 - \operatorname{th}^2 X & \frac{1}{\cos^2 X} &= D(\operatorname{tg} X) = 1 + \operatorname{tg}^2 X \\ \frac{1}{\operatorname{sh}^2 X} &= -D(\operatorname{coth} X) = \operatorname{coth}^2 X - 1 & \frac{1}{\sin^2 X} &= -D(\cot X) = 1 + \cot^2 X, \end{aligned}$$

on déduit des formules (1), (1'), (2), (2'), (3) et (3') des formules explicitant les séries entières formelles $\frac{1}{\operatorname{ch}^2 X}$, $\frac{1}{\cos^2 X}$, $\frac{1}{\operatorname{sh}^2 X}$, $\frac{1}{\sin^2 X}$, $\operatorname{th}^2 X$, $\operatorname{tg}^2 X$, $\operatorname{coth}^2 X$ et $\cot^2 X$.

REMARQUE 2. — En utilisant la formule

$$D(\operatorname{tg} X) = 1 + \operatorname{tg}^2 X$$

et en raisonnant par récurrence, on voit que, pour tout entier naturel r , il existe un polynôme P_r de degré r et un polynôme Q_r de degré $r+1$, tous deux à coefficients entiers strictement positifs, tels que

$$D^{2r}(\operatorname{tg} X) = \operatorname{tg} X P_r(\operatorname{tg}^2 X) \quad D^{2r+1}(\operatorname{tg} X) = Q_r(\operatorname{tg}^2 X).$$

Par suite, les valeurs à l'origine des dérivées d'ordre impair de $\operatorname{tg} X$ sont des nombres entiers strictement positifs. En comparant la relation (2') à la formule de Maclaurin, nous en déduisons que, pour tout entier naturel n , $(-1)^{n-1} \beta_{2n}$ est un nombre rationnel strictement positif.

Exercice conseillé : 48.

EXERCICES

DIVISIBILITÉ

1. Polynômes primitifs.

Soient A un anneau factoriel, K son corps des fractions et P un polynôme primitif à coefficients dans A .

1. Prouver que P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$.

2. Soient Q_1, Q_2, \dots, Q_n des éléments de $A[X]$ tels que $P = Q_1 Q_2 \dots Q_n$. Prouver que Q_1, Q_2, \dots, Q_n sont primitifs.

2 A. Règle d'irréductibilité (Gauss).

On considère un nombre premier p , on désigne par F_p le corps $\mathbb{Z}/p\mathbb{Z}$, et, pour tout élément $P = \sum_{n=0}^{+\infty} a_n X^n$ de $\mathbb{Z}[X]$, on désigne par P_p l'élément $\sum_{n=0}^{+\infty} \dot{a}_n X^n$ de $F_p[X]$, où, pour tout élément a de \mathbb{Z} , \dot{a} désigne la classe de a modulo p .

Prouver que si le coefficient dominant de P n'est pas divisible par p et si P n'est pas irréductible sur \mathbb{Z} , P_p n'est pas irréductible sur F_p .

Application. — Examiner l'irréductibilité sur \mathbb{Z} des polynômes suivants :

$$\begin{aligned} X^5 - X^2 + 1 \\ X^4 + 3X^3 + 3X^2 - 5 \\ X^4 - X^2 + 1. \end{aligned}$$

*3 B. Méthode de décomposition en facteurs irréductibles (Kronecker).

Soient P un élément de $\mathbb{Z}[X]$, s un entier naturel strictement inférieur au degré de P , et (a_0, a_1, \dots, a_s) une suite d'entiers rationnels distincts deux à deux.

Prouver que si Q est un élément de $\mathbb{Z}[X]$ divisant P , alors, pour tout entier $i \in [0, s]$, $Q(a_i)$ divise $P(a_i)$. En déduire une méthode permettant de déterminer au bout d'un nombre fini d'opérations tous les diviseurs de P de degré inférieur ou égal à s . (On pourra utiliser les polynômes d'interpolation de Lagrange.)

Application. — Décomposer en facteurs irréductibles sur \mathbb{Q} les polynômes suivants :

$$\begin{aligned} X^5 + X^4 + X^3 + X + 2 \\ 4X^3 - 8X^2 + 5X - 3 \\ 6X^5 + 11X^4 - X^3 + 5X - 6. \end{aligned}$$

4 B. Irréductibilité des polynômes.

Soient K un corps de caractéristique 0, et p un entier strictement supérieur à 1.

1. Soient $\alpha_1, \alpha_2, \dots, \alpha_n$ des éléments non nuls de K , et β un élément de K . Prouver que le polynôme $\alpha_1 X_1 + \alpha_2 X_2 + \dots + \alpha_n X_n + \beta$ est irréductible sur K .

2. Soient q un entier naturel non nul, β un scalaire non nul, et Q un élément non constant de $K[Y_1, Y_2, \dots, Y_q]$ satisfaisant à la condition suivante : il existe un élément irréductible P de $K[Y_1, Y_2, \dots, Y_q]$ tel que $v_P(Q) = 1$. Prouver que le polynôme $X^p Q + \beta$ est irréductible dans $K[X, Y_1, Y_2, \dots, Y_q]$.

3. Soient n un entier strictement supérieur à 1, β un scalaire non nul, et R un élément p -homogène de $K[X_1, X_2, \dots, X_n]$ satisfaisant à la condition suivante : il existe un élément irréductible P de $K[X_1, X_2, \dots, X_n]$ tel que $v_P(R) = 1$. Prouver que $R + \beta$ est irréductible dans $K[X_1, X_2, \dots, X_n]$. En déduire que, pour tout couple (α_1, α_2) d'éléments non nuls de K , $\alpha_1 X_1^p + \alpha_2 X_2^p + \beta$ est irréductible dans $K[X_1, X_2]$.

4. Prouver que, si n est un entier strictement supérieur à 2, alors, pour toute suite $(\alpha_1, \alpha_2, \dots, \alpha_n)$ d'éléments non nuls de K , le polynôme $\alpha_1 X_1^p + \alpha_2 X_2^p + \dots + \alpha_n X_n^p$ est irréductible sur K .

En déduire que si P_1, P_2, \dots, P_n sont des polynômes homogènes de degré 1 linéairement indépendants dans $K[X_1, X_2, \dots, X_n]$, $n > 2$, alors, pour tout polynôme Q de degré strictement inférieur à p , le polynôme $\alpha_1 P_1^p + \alpha_2 P_2^p + \dots + \alpha_n P_n^p + Q$ est irréductible sur K .

En appliquant la méthode de Gauss de réduction des formes quadratiques, déduire de ce qui précède une méthode explicite pour déterminer l'irréductibilité des polynômes à n indéterminées de degré inférieur ou égal à 2.

5. Décomposer en produits de facteurs irréductibles dans $C[X, Y, Z]$ les polynômes suivants :

$$\begin{aligned} & X^3(Y - Z) + Y^3(Z - X) + Z^3(X - Y) \\ & X^3(Z - Y^2) + Y^3(X - Z^2) + Z^3(Y - X^2) + XYZ(XYZ - 1). \end{aligned}$$

6. *Sous-algèbres du corps des fractions rationnelles à une indéterminée.*

1. Soient B un anneau commutatif unitaire non réduit à $\{0\}$ et S une partie de B contenant 1, stable pour la multiplication et constituée d'éléments réguliers. Soit B_S l'anneau des fractions xs^{-1} , où $x \in B$ et $s \in S$ (cf. exercice I.2.32). Montrer que, pour tout idéal \mathfrak{J} de B_S ,

$$\mathfrak{J} = (\mathfrak{J} \cap B) \cdot B_S.$$

2. Soient S une partie de $B = K[X_1, X_2, \dots, X_n]$ contenant A et stable pour la multiplication et B_S l'anneau des fractions rationnelles $\frac{P}{Q}$, où $P \in K[X_1, X_2, \dots, X_n]$ et $Q \in S$. Montrer que tout idéal \mathfrak{J} de l'anneau B_S est de la forme $\mathfrak{J} = \mathfrak{J} B_S$, où \mathfrak{J} est un idéal de $K[X_1, X_2, \dots, X_n]$. En déduire que l'anneau B_S est noethérien.

3. Lorsque $n = 1$, montrer que toute sous-algèbre A de $K(X)$ contenant $B = K[X]$ est de la forme B_S . (On pourra prouver que si P et Q sont deux polynômes premiers entre eux tels que $\frac{P}{Q} \in A$, alors $\frac{1}{Q} \in A$.)

7 A. Idéaux des algèbres de type fini.

On dit qu'une A -algèbre unitaire B est de type fini s'il existe une suite finie (b_1, b_2, \dots, b_n) d'éléments de B telle que la sous-algèbre unitaire engendrée par cette suite soit égale à B .

1. Soit B une A -algèbre de type fini. On considère le morphisme f de l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$ dans l'algèbre unitaire B tel que, pour tout élément i de $[1, n]$, $f(X_i) = b_i$. Prouver que f définit par passage au quotient un isomorphisme de $A[X_1, X_2, \dots, X_n]/\text{Ker}(f)$ sur B .

2. A l'aide de l'exercice I.3.95, en déduire le résultat suivant :

Si l'anneau A est noethérien, il en est de même de toute A -algèbre de type fini.

8 A. Décomposition en facteurs irréductibles dans un anneau noethérien.

Soit A un anneau intègre unitaire.

1. On suppose que l'anneau A est noethérien. On considère un ensemble E de représentants des classes d'éléments irréductibles de A . Prouver que, pour tout élément non inversible a de A , il existe un élément irréductible de A divisant a . En déduire que tout élément non nul a de A peut s'écrire sous la forme

$$a = up_1p_2 \cdots p_n,$$

où u est inversible et où, pour tout $i \in [1, n]$, $p_i \in E$.

2. Soit a un élément de A . Prouver que si l'idéal Aa est premier (cf. exercice I.2.30), l'élément a est irréductible, et que la réciproque est vraie si l'anneau A est factoriel.

3. On considère l'anneau $A = \mathbb{Q}[\sqrt{-3}]$ (cf. exercice I.3.78). Cet anneau est intègre, unitaire et noethérien. Prouver qu'il n'est pas factoriel, en utilisant les relations $4 = 2 \times 2$ et $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, et en prouvant que les éléments 2 , $1 + i\sqrt{3}$ et $1 - i\sqrt{3}$ sont irréductibles. Montrer enfin que si a est égal à l'un des trois éléments précédents, l'idéal Aa n'est pas premier. (On voit ainsi que la notion d'élément irréductible est inadéquate pour étudier les anneaux non factoriels; on doit lui substituer celle d'idéal premier; cf. chap. III.3.)

4. On suppose que l'anneau A est noethérien et que, pour tout élément irréductible p de A , l'idéal Ap est premier. Prouver que l'anneau A est factoriel. (On pourra montrer l'unicité de la décomposition d'un élément en facteurs irréductibles.)

Ainsi, pour vérifier qu'un anneau intègre unitaire noethérien est factoriel, il suffit de prouver que si un élément irréductible p de A divise le produit ab de deux éléments de A , alors p divise l'un de ces éléments.

FONCTIONS POLYNOMIALES ET RATIONNELLES

9 A. Soient A un anneau intègre et infini, et (B_1, B_2, \dots, B_n) une suite de parties infinies de A . Prouver que, pour tout élément P non nul de $A[X_1, X_2, \dots, X_n]$, l'ensemble des éléments α de $\prod_{i=1}^n B_i$ tels que $\tilde{P}(\alpha)$ soit non nul est infini. (On pourra raisonner par récurrence sur n .)

10. 1. Soient A et B deux anneaux commutatifs unitaires, et f un morphisme de A dans B . Prouver qu'il existe un morphisme \tilde{f} et un seul de l'anneau unitaire $A[X_i]_{i \in I}$ dans l'anneau unitaire $B[Y_i]_{i \in I}$ prolongeant f , et tel que, pour tout $i \in I$, $\tilde{f}(X_i) = Y_i$. Déterminer le noyau et l'image de \tilde{f} en fonction du noyau et de l'image de f ; prouver que si f est injectif, surjectif, ou bijectif, il en est de même de \tilde{f} .

2. Soient K et L deux corps commutatifs, et f un morphisme de K dans L . Prouver de même qu'il existe un morphisme \tilde{f} et un seul du corps $K(X_i)_{i \in I}$ dans le corps $L(X_i)_{i \in I}$ prolongeant f , et tel que, pour tout $i \in I$, $\tilde{f}(X_i) = Y_i$.

11. Soient K un corps commutatif et n un entier strictement positif.

1. Soient $(\alpha_0, \alpha_1, \dots, \alpha_n)$ une suite de scalaires distincts deux à deux, et P un élément de $K[X]$ de degré n . Prouver que les polynômes $P(X + \alpha_0), P(X + \alpha_1), \dots, P(X + \alpha_n)$ constituent une base de l'espace vectoriel des polynômes de degré inférieur ou égal à n .

(On montrera que la famille considérée est libre. Pour cela, on pourra utiliser l'existence d'une suite (Q_0, Q_1, \dots, Q_n) de polynômes telle que

$$P(X + Y) = \sum_{p=0}^n Y^p Q_p(X).$$

On se ramènera alors à démontrer que les relations $\sum_{i=0}^n \lambda_i \alpha_i^p = 0$, où p parcourt $[0, n]$, impliquent que $\lambda_0 = \lambda_1 = \dots = \lambda_n = 0$. A cet effet, on pourra raisonner par récurrence sur l'entier n , ou encore employer la théorie des déterminants de Vandermonde; cf. § 3.3.)

2. On désigne par E_n le sous-espace vectoriel de $K[X_1, X_2, \dots, X_p]$ constitué des polynômes n -homogènes. Prouver que l'ensemble des polynômes de la forme P^n , où P est homogène de degré 1, est une partie génératrice de l'espace vectoriel E_n . (On pourra, en raisonnant par récurrence, se ramener au cas où $p = 2$, qu'on traitera à l'aide de la question 1.)

12. *Composé de polynômes homogènes.*

Soient P un élément p -homogène de $A[X_1, X_2, \dots, X_n]$ et $Q = (Q_1, Q_2, \dots, Q_n)$ une suite d'éléments q -homogènes de $A[Y_1, Y_2, \dots, Y_p]$. Prouver que $P \circ Q$ est pq -homogène.

Lorsque A est un corps, étendre ce résultat au cas des fractions rationnelles.

13 A. *Morphismes du groupe additif K dans le groupe multiplicatif K^* .*

1. Soit P un polynôme non nul à une indéterminée. Prouver que si P satisfait à la relation

$$P(X + Y) = P(X)P(Y),$$

alors $P = 1$.

2. Soit R une fraction rationnelle non nulle à une indéterminée, écrite sous la forme irréductible $R = \frac{P}{Q}$. Prouver que si R satisfait à la relation

$$R(X + Y) = R(X)R(Y),$$

alors $Q(X + Y)$ est divisible par $Q(X)Q(Y)$. En déduire que $Q(X + Y) = Q(X)Q(Y)$. Prouver finalement que $R = 1$.

3. Prouver que la fonction constante égale à 1 est la seule fonction rationnelle non nulle telle que, pour tout couple (α, β) d'éléments de K ,

$$f(\alpha + \beta) = f(\alpha)f(\beta).$$

(Lorsque le corps K est infini, on pourra appliquer la question 2. Lorsque K est fini de caractéristique p , ayant p^n éléments, on pourra utiliser l'exercice 1.9 et démontrer la relation $f(p^n \alpha) = [f(\alpha)]^{(p^n)}$.)

14 A. Morphismes du groupe multiplicatif K^* dans le groupe additif K .

1. Soit R une fraction rationnelle non nulle à une indéterminée, écrite sous la forme irréductible $R = \frac{P}{Q}$. Prouver que si R satisfait à la relation

$$(1) \quad R(XY) = R(X) + R(Y),$$

alors $Q(XY)$ est divisible par $Q(X)Q(Y)$. En déduire que $Q = 1$. Prouver finalement que 0 est la seule fraction rationnelle satisfaisant à la relation (1).

2. Prouver que la fonction nulle est la seule fonction rationnelle f définie sur K^* telle que, pour tout couple (α, β) d'éléments de K^* ,

$$f(\alpha\beta) = f(\alpha) + f(\beta).$$

(Lorsque le corps K est infini, on pourra appliquer la question 1. Lorsque K est fini de caractéristique p , ayant p^n éléments, on pourra utiliser l'exercice 1.9 et démontrer la relation $f(\alpha^{(p^n)}) = p^n f(\alpha)$.)

15 A. Endomorphismes du groupe additif K .

1. Soit R une fraction rationnelle non nulle à une indéterminée, écrite sous la forme irréductible $R = \frac{P}{Q}$. Prouver que si R satisfait à la relation

$$(1) \quad R(X + Y) = R(X) + R(Y),$$

alors $Q(X + Y)$ est divisible par $Q(X)Q(Y)$. En déduire que

$$Q(X + Y) = Q(X)Q(Y),$$

et, à l'aide de l'exercice 13, que $Q = 1$.

2. Soit donc P un polynôme à une indéterminée tel que

$$P(X + Y) = P(X) + P(Y).$$

Prouver que $P(0) = 0$ et que $D(P) = \alpha$, où $\alpha = [D(P)](0)$.

3. En déduire que si la caractéristique de K est nulle, les monômes αX sont les seules fractions rationnelles R satisfaisant à la relation (1).

En déduire aussi que si K est de caractéristique p non nulle, les polynômes

$$\alpha X + \sum_{n=1}^{+\infty} \alpha_n X^{np}$$

sont les seules fractions rationnelles R satisfaisant à la relation (1).

4. Prouver que si K est un corps infini de caractéristique zéro, les fonctions $\alpha \mapsto \gamma\alpha$ sont les seules fonctions rationnelles f définies sur K telles que, pour tout couple (α, β) de scalaires,

$$f(\alpha + \beta) = f(\alpha) + f(\beta).$$

Examiner aussi le cas où K est un corps infini de caractéristique p .

Soient enfin K un corps fini de caractéristique p , ayant p^n éléments, et K' le sous-corps premier de K (cf. exercice I.2.57). Prouver que les endomorphismes du K' -espace vectoriel K sont les seules fonctions polynomiales sur K satisfaisant à la condition précédente.

16¹A. *Endomorphismes du groupe multiplicatif K^* .*

1. Soient P un polynôme non nul à une indéterminée, et $p = v_0(P)$. Prouver que si P satisfait à la relation

$$(1) \quad P(XY) = P(X)P(Y)$$

et que si $p = 0$, alors $P = 1$. (On raisonnera par l'absurde, en montrant que P peut alors s'écrire sous la forme $P \equiv 1 + \alpha X^q \pmod{\mathfrak{J}_q}$, où $\alpha \neq 0$ et $q > 0$.)

En déduire que, pour tout entier naturel p , X^p est le seul polynôme P satisfaisant à la relation (1) et tel que $v_0(P) = p$.

2. Soient R une fraction rationnelle non nulle à une indéterminée, écrite sous la forme irréductible $R = \frac{P}{Q}$, et $p = v_0(R)$. Prouver que si R satisfait à la relation

$$(2) \quad R(XY) = R(X)R(Y),$$

alors $Q(XY)$ est divisible par $Q(X)Q(Y)$. En déduire que $Q(XY) = Q(X)Q(Y)$. En utilisant la question 1, prouver finalement que, pour tout entier rationnel p , X^p est la seule fraction rationnelle satisfaisant à la relation (2) et telle que $v_0(R) = p$.

3. Prouver que les fonctions $\alpha \mapsto \alpha^p$, où $p \in \mathbb{Z}$, sont les seules fonctions rationnelles non nulles f sur K^* telles que, pour tout couple (α, β) d'éléments de K^* ,

$$f(\alpha\beta) = f(\alpha)f(\beta).$$

(Lorsque K est infini, on pourra appliquer la question 2. Lorsque K est un corps fini de caractéristique p , ayant p^n éléments, on pourra utiliser le fait que le groupe multiplicatif de K^* est cyclique ; cf. exercice 1.9.)

17 A. *Automorphismes de l'algèbre $K[X_1, X_2, \dots, X_n]$.*

Soient $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de K^n , $M = (\beta_{ij})$ un élément inversible de $M_n(K)$, et U_{aM} l'endomorphisme de la K -algèbre unitaire $K[X_1, X_2, \dots, X_n]$ défini par les relations

$$U_{aM}(X_j) = \alpha_j + \sum_{i=1}^n \beta_{ij} X_i \quad j \in [1, n].$$

Montrer que U_{aM} est un automorphisme. Réciproquement, soit U un automorphisme de $K[X_1, X_2, \dots, X_n]$. Montrer qu'il existe un automorphisme U_{aM} de la forme précédente tel que, pour tout élément j de $[1, n]$,

$$(U_{aM} \circ U)(X_j) = X_j + P'_j,$$

où P'_j est une somme de polynômes p -homogènes, $p \geq 2$.

(En composant U avec un automorphisme de la forme U_{aI_n} , on se ramènera au cas où, pour tout $j \in [1, n]$ $U(X_j) = P_j + P'_j$, P_j étant 1-homogène et P'_j une somme de polynômes p -homogènes, $p \geq 2$. On considèrera l'unique polynôme Q_j tel que $U(Q_j) = X_j$, et l'on montrera que Q_j peut s'écrire sous la forme $Q_j = H_j + H'_j$, où H_j est 1-homogène et où H'_j est une somme de polynômes p -homogènes de degré $p \geq 2$.)

Soit U l'unique endomorphisme de $K[X, Y]$ tel que $U(X) = X$ et $U(Y) = Y + X^2$. Prouver que U est un automorphisme de K -algèbre unitaire. Plus généralement, soit V un endomorphisme nilpotent de la K -algèbre unitaire $E = K[X_1, X_2, \dots, X_n]$. Prouver que $U = I_E + V$ est un automorphisme de cette algèbre.

DÉRIVATION

18. Dérivée $r^{\text{ième}}$ d'un polynôme composé.

Soit K un corps de caractéristique nulle.

1. Prouver que, pour tout entier $r > 0$ et pour tout élément Q de $K[X]$, il existe une suite (Q_1, Q_2, \dots, Q_r) d'éléments de $K[X]$ et une seule telle que, pour tout élément R de $K[X]$,

$$(1) \quad D^r(R \circ Q) = \sum_{k=1}^r [(D^k R) \circ Q] Q_k,$$

et montrer que, pour tout élément k de $[1, r]$,

$$Q_k = D^r(Q_k) - C_k^1 Q D^r(Q^{k-1}) + \dots + (-1)^j C_k^j Q^j D^r(Q^{k-j}) + \dots + (-1)^{k-1} C_k^{k-1} Q^{k-1} D^r Q.$$

(On pourra expliciter la relation (1) en prenant successivement $R = X$, $R = X^2$, ..., $R = X^r$.)

2. Par récurrence sur r , montrer que, pour tout entier $r > 0$ et pour tout élément k de $[1, r]$, il existe un élément P_k de $K[X_1, X_2, \dots, X_{r-k+1}]$ à coefficients entiers naturels tel que, pour tout élément Q de $K[X]$,

$$Q_k = P_k(DQ, D^2Q, \dots, D^{r-k+1}Q).$$

A l'aide de l'exercice 21, prouver que P_k est le seul élément de $K[X_1, X_2, \dots, X_{r-k+1}]$ satisfaisant à ces conditions.

19. Dérivations de $K[X_1, X_2, \dots, X_n]$ et de $K(X_1, X_2, \dots, X_n)$.

1. Montrer que, pour toute suite (A_1, A_2, \dots, A_n) d'éléments de $K[X_1, X_2, \dots, X_n]$, il existe une dérivation U de l'algèbre $K[X_1, X_2, \dots, X_n]$ et une seule telle que, pour

tout $i \in [1, n]$, $U(X_i) = A_i$. Prouver que $U = \sum_{i=1}^n A_i D_i$. Déterminer toutes les dérivations de $K[X_1, X_2, \dots, X_n]$.

2. Montrer de même que, pour toute suite (B_1, B_2, \dots, B_n) d'éléments de $K(X_1, X_2, \dots, X_n)$, il existe une dérivation V de l'algèbre $K(X_1, X_2, \dots, X_n)$ et une

seule telle que, pour tout $i \in [1, n]$, $V(X_i) = B_i$. Prouver que $V = \sum_{i=1}^n B_i D_i$. Déterminer toutes les dérivations de $K(X_1, X_2, \dots, X_n)$.

20 A. Opérateurs différentiels, en caractéristique p .

Soit A un anneau commutatif unitaire de caractéristique p . Prouver que l'algèbre unitaire \mathcal{D} des opérateurs différentiels sur $A[X_1, X_2, \dots, X_n]$ est isomorphe au quotient de l'algèbre unitaire $A[Y_1, Y_2, \dots, Y_n]$ par l'idéal engendré par les monômes Y_i^p , où i parcourt $[1, n]$.

21 A. Équations différentielles algébriques.

Soit K un corps de caractéristique nulle. Pour tout entier naturel r , on désigne par E_r l'ensemble des polynômes à coefficients dans K de degré inférieur ou égal à r .

Pour tout élément $a = (\alpha_0, \alpha_1, \dots, \alpha_r)$ de K^{r+1} , on note P_a le polynôme $\sum_{k=0}^r \alpha_k X^k$.

1. Déterminer l'ensemble des points α de K^{r+1} tels que $D^r P_\alpha = 0$.
2. En utilisant le théorème de prolongement des identités algébriques, montrer que 0 est le seul élément P de $K[X, Y]$ tel que, pour tout élément Q de E_1 , $P(Q, DQ) = 0$.
3. Plus généralement, montrer, par récurrence sur l'entier r , que 0 est le seul élément P de $K[X_1, X_2, \dots, X_r, X_{r+1}]$ tel que, pour tout élément Q de E_r ,

$$P(Q, DQ, \dots, D^r Q) = 0.$$

(On pourra d'abord prouver que $P(X_1, X_2, \dots, X_r, 0) = 0$.)

En particulier, il n'existe aucune équation différentielle algébrique à coefficients constants non triviale satisfaite par tous les éléments de $K[X]$.

22 B. Noyaux des opérateurs différentiels décomposés à coefficients constants.

Soient K un corps de caractéristique zéro, n et p deux entiers naturels non nuls. Pour tout entier naturel r , on note $E_{n,r}$ l'espace vectoriel des polynômes à n indéterminées r -homogènes à coefficients dans K .

I. — Soit D un opérateur différentiel sur $K[X_1, X_2, \dots, X_n]$, à coefficients constants, 1-homogène.

1. Prouver que l'intersection du noyau de D avec le sous-espace vectoriel $E_{n,1}$ est de dimension $n - 1$.

2. Soient $(A_1, A_2, \dots, A_{n-1})$ une base de cette intersection, et B un élément de $E_{n,1}$ tel que $D(B) = 1$. Soit $F_{n,p}$ le sous-espace vectoriel de $E_{n,p}$ constitué des polynômes P tels que $D(P) = 0$. Prouver que si un élément Q de $K[X_1, X_2, \dots, X_n]$ est premier avec B , alors, pour tout entier naturel non nul m , $B^m Q$ n'appartient pas au noyau de D . En déduire que l'intersection de $F_{n,p}$ et de $BE_{n,p-1}$ est réduite à $\{0\}$. Montrer que, pour toute suite $(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ d'entiers dont la somme est égale à p , le polynôme $A_1^{\alpha_1} A_2^{\alpha_2} \dots A_{n-1}^{\alpha_{n-1}}$ appartient à $F_{n,p}$, et que les polynômes ainsi définis sont linéairement indépendants.

3. Déduire de tout ce qui précède que ces polynômes constituent une base de $F_{n,p}$, et que l'espace vectoriel $E_{n,p}$ est somme directe des sous-espaces vectoriels $F_{n,p}$ et $BE_{n,p-1}$. (On calculera les dimensions des espaces vectoriels considérés.)

4. Soient N un élément du noyau de D et r un entier naturel. Calculer $D(B^r N)$. En utilisant la question 3, prouver que, pour tout élément Q de $F_{n,p-1}$, il existe une suite $(N_0, N_1, \dots, N_{p-1})$ et une seule d'éléments du noyau de D telle que

$$Q = N_0 + BN_1 + B^2 N_2 + \dots + B^{p-1} N_{p-1}.$$

Déterminer l'ensemble des éléments P de $E_{n,p}$ tels que $D(P) = Q$, où Q est un élément donné de $F_{n,p-1}$.

5. Soit q un entier appartenant à $[1, p]$. Déterminer l'ensemble des éléments P de $E_{n,p}$ tels que $D^q(P) = 0$, et résoudre l'équation $D^q(P) = Q$, où Q est un élément donné de $E_{n,p-q}$.

II. — Soient m un entier appartenant à $[1, p]$, (D_1, D_2, \dots, D_m) une suite de m opérateurs différentiels sur $K[X_1, X_2, \dots, X_n]$ à coefficients constants et 1-homogènes. On suppose que ces opérateurs, considérés comme formes linéaires sur $E_{n,1}$, sont linéairement indépendants.

1. Prouver qu'il existe une suite $(B_1, B_2, \dots, B_m, A_{m+1}, \dots, A_n)$ d'éléments de $E_{n,1}$ telle que, pour tout élément i de $[1, m]$,

$$\begin{aligned} D_i(B_i) &= 1 \\ D_i(B_j) &= 0 \quad \text{si } j \neq i \\ D_i(A_k) &= 0 \quad \text{pour tout } k \in [m+1, n]. \end{aligned}$$

Indiquer comment on peut calculer les polynômes B_j et A_k à l'aide des composantes de D_1, D_2, \dots, D_m dans la base du dual de $E_{n,1}$ constituée des opérateurs de dérivation partielle.

2. Montrer que les opérateurs différentiels D_1, D_2, \dots, D_m sont algébriquement indépendants sur $K(X_1, X_2, \dots, X_n)$.

3. Soit $F_{n,p}$ le sous-espace vectoriel de $E_{n,p}$ ayant pour base la famille \mathcal{B} des polynômes

$$C_{\alpha, \beta} = \prod_{k=m+1}^n A_k^{\alpha_k} \prod_{i=1}^m B_i^{\beta_i},$$

où $\alpha = (\alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_n)$ et $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ sont deux suites d'entiers telles que

$$\sum_{k=m+1}^n \alpha_k + \sum_{i=1}^m \beta_i = p$$

et que $\beta_1 \beta_2 \dots \beta_n = 0$.

Déterminer la dimension de $F_{n,p}$, et prouver que $F_{n,p}$ est contenu dans le noyau de l'opérateur différentiel $D = D_1 D_2 \dots D_m$.

4. En utilisant la première partie, prouver que $F_{n,p}$ est égal à l'intersection de $E_{n,p}$ et du noyau de D , et que $E_{n,p}$ est somme directe de $F_{n,p}$ et du sous-espace vectoriel $B_1 B_2 \dots B_m E_{n,p-m}$.

5. En s'inspirant de la question I.4, déterminer l'ensemble des éléments P de $F_{n,p}$ tels que $D(P) = Q$, où Q est un élément donné de $F_{n,p-m}$.

6. Plus généralement, soient (q_1, q_2, \dots, q_m) une suite d'entiers naturels telle que $\sum_{i=1}^m q_i \in [1, p]$, et $D = \prod_{i=1}^m D_i^{q_i}$.

Déterminer l'ensemble des éléments P de $E_{n,p}$ tels que $D(P) = 0$, et résoudre l'équation $D(P) = Q$, où Q est un élément donné de $E_{n,p-q}$.

7. *Application.* — On suppose que $K = \mathbb{C}$, que $n = 2$, et que

$$D = \alpha D_X^2 + 2\beta D_X D_Y + \gamma D_Y^2.$$

Déterminer l'ensemble des éléments P de $E_{2,p}$ tels que $D(P) = 0$. Résoudre l'équation $D(P) = Q$, où Q est un élément donné de $E_{2,p-2}$. (On distinguera deux cas suivant que le polynôme $\alpha Z^2 + 2\beta Z + \gamma$ a deux racines distinctes ou non.)

Détailler les trois cas particuliers suivants :

$$D = D_X^2 + D_Y^2$$

$$D = D_X^2 - D_Y^2$$

$$D = D_X^2 + 2D_X D_Y + D_Y^2.$$

Résoudre dans ces trois cas les équations

$$\begin{array}{llll} D(P) = 0 & D(P) = 1 & D(P) = X & D(P) = Y \\ D(P) = XY & D(P) = X^2 + Y^2 & D(P) = X^2 - Y^2. \end{array}$$

23. Soit P un élément de $K[X, Y]$. Montrer que si P est homogène, $P(TX - D_Y P, TY + D_X P)$ est divisible par P dans $K[X, Y, T]$.

ÉTUDE LOCALE DES FRACTIONS RATIONNELLES

24 B. *Valuation en un point d'une fraction rationnelle.*

I. — Soit A un anneau intègre unitaire.

1. Soient P un élément non nul de $A[X_1, X_2, \dots, X_n]$ et $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de A^n . On appelle valuation de P au point a , et on note $v_a(P)$, le plus petit des entiers naturels p tels que la composante p -homogène du polynôme

$$P(\alpha_1 + X_1, \alpha_2 + X_2, \dots, \alpha_n + X_n)$$

soit non nulle. Montrer que lorsque $n = 1$, cette notion coïncide avec celle qui a été introduite au § 1.3. On convient que $v_a(0) = +\infty$. Prouver que, pour tout couple (P, Q) d'éléments de $A[X_1, X_2, \dots, X_n]$,

$$(1) \quad v_a(P + Q) \geq \inf [v_a(P), v_a(Q)],$$

avec égalité si $v_a(P) \neq v_a(Q)$,

$$(2) \quad v_a(PQ) = v_a(P) + v_a(Q).$$

Pour que $P(a) = 0$, il faut et il suffit que $v_a(P) > 0$. L'entier $v_a(P)$ s'appelle alors ordre de multiplicité du zéro a .

2. Soient P un élément de $A[X_1, X_2, \dots, X_n]$ et $Q = (Q_1, Q_2, \dots, Q_n)$ une suite d'éléments de $A[Y_1, Y_2, \dots, Y_p]$. On appelle valuation de Q en un point $a = (\alpha_1, \alpha_2, \dots, \alpha_p)$ de K^p , et on note $v_a(Q)$, la plus petite des valuations $v_a(Q_i)$. Prouver que si $Q \neq 0$,

$$v_a(P \circ Q) \geq v_{Q(a)}(P) \cdot v_a(Q).$$

3. On suppose que A est de caractéristique nulle. Prouver que, pour tout opérateur différentiel à coefficients constants p -homogène D , et pour tout élément P de $A[X_1, X_2, \dots, X_n]$,

$$v_a(DP) \geq v_a(P) - p.$$

II. — Soit K un corps commutatif.

1. Soient R un élément non nul de $K(X_1, X_2, \dots, X_n)$ et $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de K^n . Prouver que si R s'écrit sous les formes $\frac{P}{Q}$ et $\frac{P'}{Q'}$, où P, Q, P' et Q' sont des éléments non nuls de $K[X_1, X_2, \dots, X_n]$, $v_a(P) - v_a(Q) = v_a(P') - v_a(Q')$. La valeur commune de ces nombres s'appelle valuation de R au point a , et se note $v_a(R)$. Lorsque R est un polynôme, cette notion coïncide avec celle qui a été précédemment introduite.

Étendre les relations (1) et (2) au cas des fractions rationnelles. Prouver en outre que si $R \neq 0$, $v_a\left(\frac{1}{R}\right) = -v_a(R)$.

Lorsque a est substituable dans R , pour que $R(a) = 0$, il faut et il suffit que $v_a(R) > 0$; l'entier $v_a(R)$ s'appelle alors ordre de multiplicité du zéro a . Lorsque a est substituable dans R^{-1} , pour que $R^{-1}(a) = 0$, il faut et il suffit que $v_a(R) < 0$; l'entier $-v_a(R)$ s'appelle alors ordre de multiplicité du pôle a .

2. Soient R un élément de $K(X_1, X_2, \dots, X_n)$ et $S = (S_1, S_2, \dots, S_n)$ une suite d'éléments de $K(Y_1, Y_2, \dots, Y_p)$ substituable dans R . On appelle valuation de S en un point $a = (\alpha_1, \alpha_2, \dots, \alpha_p)$ de K^p , et on note $v_a(S)$, la plus petite des valuations $v_a(S_i)$. Prouver que si $S \neq 0$, si a est substituable dans S_1, S_2, \dots, S_n et si $S(a)$ est substituable dans R ,

$$v_a(R \circ S) \geq v_{S(a)}(R) \cdot v_a(S).$$

Montrer que ce résultat peut tomber en défaut si $S(a)$ n'est pas substituable dans R , en prenant par exemple $R = \frac{1}{X_1 + X_2 + X_1^2}$, $S_1 = Y$, $S_2 = -Y$ et $a = 0$.

3. Prouver que si K est de caractéristique nulle, alors, pour tout opérateur différentiel à coefficients constants p -homogène D , et pour tout élément R de $K(X_1, X_2, \dots, X_n)$,

$$v_a(DR) \geq v_a(R) - p.$$

25 A. Développements limités des fractions rationnelles.

On utilise les notations et les résultats de l'exercice précédent.

1. Soient R un élément de $K(X_1, X_2, \dots, X_n)$ et $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de K^n substituable dans R . Prouver que, pour tout entier naturel p , il existe un couple (P_p, T_p) et un seul constitué d'un élément P_p de $K[Y_1, Y_2, \dots, Y_n]$ et d'un élément T_p de $K(Y_1, Y_2, \dots, Y_n)$ tel que 0 soit substituable dans T_p et que

$$R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_n + Y_n) = P_p + T_p, \quad d^\circ(P_p) \leq p, \quad v_0(T_p) > p.$$

Le polynôme P_p s'appelle développement limité de R à l'ordre p au point a , et se note $\text{Pr}_{a,p}(R)$.

(Pour établir l'existence du couple (P_p, T_p) , on écrira

$$R' = R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_n + Y_n)$$

sous la forme $R' = \frac{P}{1+Q}$, où $P, Q \in K[Y_1, Y_2, \dots, Y_n]$, $Q(0) = 0$.)

2. Prouver que, pour tout couple (p, q) d'entiers naturels tels que $p < q$,

$$\text{Pr}_{a,q}(R) \equiv \text{Pr}_{a,p}(R), \quad (\text{mod. } \mathfrak{J}_p)$$

où \mathfrak{J}_p désigne l'idéal de $K[Y_1, Y_2, \dots, Y_n]$ constitué des polynômes P tels que $v_0(P) > p$.

En déduire qu'il existe une suite (H_r) et une seule d'éléments de $K[Y_1, Y_2, \dots, Y_n]$ tel que, pour tout entier naturel r , H_r soit r -homogène et que, pour tout entier p ,

$$\text{Pr}_{a,p}(R) = \sum_{r=0}^p H_r.$$

La famille des polynômes H_r s'appelle développement taylorien de R au point a , et H_r se note $T_{a,r}(R)$.

Montrer enfin que si l'on considère $R' = R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_n + Y_n)$ comme un élément de $K[[Y_1, Y_2, \dots, Y_n]]$,

$$R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_n + Y_n) = \sum_{r=0}^{+\infty} T_{a,r}(R).$$

3. Étendre à ce cas les résultats de l'exercice 1.56 concernant les développements limités d'une somme, d'un produit, d'une composée, de fractions rationnelles.

4. On suppose que K est de caractéristique nulle. Soient D un opérateur différentiel à coefficients constants p -homogène et R un élément de $K(X_1, X_2, \dots, X_n)$. Prouver que, pour tout entier $p \geq r$,

$$\text{Pr}_{a,p-r}(DR) = D[\text{Pr}_{a,p}(R)].$$

26 A. Formule de Taylor pour les fractions rationnelles.

On utilise les notations et les résultats de l'exercice précédent.

Soient R un élément de $K(X_1, X_2, \dots, X_n)$ et $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de K^n substituable dans R .

1. Soit $(T_{a,r}(R))$ le développement taylorien de R au point a . Soit d'autre part H l'opérateur différentiel sur $K(X_1, X_2, \dots, X_n)$ défini par la relation

$$H = \sum_{i=1}^n Y_i D_i.$$

Prouver que, pour tout entier naturel p ,

$$H^p(R)(a) = p! T_{a,p}(R).$$

Lorsque K est de caractéristique nulle, en déduire que, pour tout entier naturel p ,

$$R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_n + Y_n) = \sum_{r=0}^p \frac{H^r(R)(a)}{r!} + T_p,$$

où 0 est substituable dans T_p , et $v_0(T_p) > p$. En déduire aussi que dans $K[[Y_1, Y_2, \dots, Y_p]]$

$$R(\alpha_1 + Y_1, \alpha_2 + Y_2, \dots, \alpha_p + Y_p) = \sum_{r=0}^{+\infty} \frac{H^r(R)(a)}{r!}$$

(formule de Taylor pour les fractions rationnelles).

2. Soit p un entier naturel. Prouver que la valuation de R au point a est égale à p si et seulement si les deux conditions suivantes sont réalisées :

- a) pour tout élément s de \mathbb{N}^n tel que $|s| < p$, $(D^s R)(a) = 0$;
- b) il existe un élément t de \mathbb{N}^n tel que $|t| = p$ et que $(D^t R)(a) \neq 0$.

POLYNÔMES A COEFFICIENTS VECTORIELS

27 A. Polynômes et séries entières formelles à coefficients vectoriels.

Soient E un A -module, et S l'ensemble des applications de $[1, n]$ dans E , où $n \in \mathbb{N}^*$. On considère le module $E^S = \mathcal{F}(S, E)$ des applications de S dans E ,

et le sous-module $E^{(S)}$ de E^S constitué des applications à support fini. On note B l'anneau $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans A .

1. On considère l'application de $E^{(S)} \times B$ dans $E^{(S)}$ qui à tout couple constitué d'un élément $P = (a_s)_{s \in S}$ de $E^{(S)}$ et d'un élément $Q = \sum_{t \in S} \beta_t X^t$ de B associe l'élément $R = (c_u)_{u \in S}$ de $E^{(S)}$, noté PQ , défini par la relation

$$(1) \quad c_u = \sum_{s+t=u} \beta_t a_s.$$

Montrer que cette application définit sur $E^{(S)}$ une structure de B -module, et que si l'on identifie E à son image dans $E^{(S)}$ par l'application $a \mapsto (a_s)_{s \in S}$, où $a_s = 0$ si $s \neq 0$ et où $a_0 = a$, tout élément P de $E^{(S)}$ peut s'écrire d'une manière et d'une seule sous la forme $P = \sum_{s \in S} b_s X^s$. C'est pourquoi, muni de cette structure de B -module, $E^{(S)}$ s'appelle module des polynômes à n indéterminées à coefficients dans E , et se note

$$E[X_1, X_2, \dots, X_n].$$

L'élément $P = (a_s)_{s \in S}$ de $E^{(S)}$ se note alors $P = \sum_{s \in S} a_s X^s$.

2. Montrer que, pour toute suite $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ d'éléments de A , il existe une application A -linéaire f et une seule de $E[X_1, X_2, \dots, X_n]$ dans E telle que, pour tout élément P de B et pour tout élément b de E ,

$$f(bP) = P(a)b.$$

3. Généraliser à ce cas la définition et les propriétés des polynômes homogènes, ainsi que les notions de degré et de degré partiel d'un polynôme.

4. On considère trois A -modules E_1, E_2 et F , et une application bilinéaire T de $E_1 \times E_2$ dans F . Prouver qu'il existe une application B -bilinéaire \tilde{T} et une seule de $E_1^{(S)} \times E_2^{(S)}$ dans $F^{(S)}$ prolongeant T . Montrer que

$$(2) \quad \tilde{T}\left(\sum_{s \in S} a_s X^s, \sum_{t \in S} b_t X^t\right) = \sum_{u \in S} \left(\sum_{s+t=u} T(a_s, b_t) X^u\right).$$

5. On considère l'application de $E^S \times A[[X_1, X_2, \dots, X_n]]$ dans E^S définie par la formule (1). On appelle valuation d'un élément non nul $B = (b_s)_{s \in S}$ de E^S le plus petit des entiers $|s|$, où s est tel que $b_s \neq 0$. Étendre à ce cas les propriétés des valuations des séries entières formelles, la définition et les propriétés des familles sommables de séries entières formelles. En particulier, tout élément B de E^S peut s'écrire d'une manière et d'une seule sous la forme

$$B = \sum_{s \in S} b_s X^s.$$

Montrer que l'application $(B, P) \mapsto BP$ définit une structure de $A[[X_1, X_2, \dots, X_n]]$ module sur E^S . Muni de cette structure, E^S s'appelle module des séries entières formelles à n indéterminées à coefficients dans E , et se note $E[[X_1, X_2, \dots, X_n]]$.

6. On considère trois A -modules E_1, E_2 et F sur K , et une application bilinéaire T de $E_1 \times E_2$ dans F . Prouver qu'il existe une application B -bilinéaire \tilde{T} et une

seule de $E_1^S \times E_2^S$ dans F^S prolongeant T et satisfaisant à la condition suivante : pour tout élément B_1 de E_1^S et pour tout élément B_2 de E_2^S ,

$$\nu[\tilde{T}(B_1, B_2)] \geq \nu(B_1) + \nu(B_2).$$

Montrer que \tilde{T} est encore donnée par la formule (2), et généraliser à ce cas la propriété de distributivité dénombrable du produit de deux séries entières formelles.

7. Soient $Q = (Q_1, Q_2, \dots, Q_n)$ une suite de n éléments de $A[Y_1, Y_2, \dots, Y_p]$ et φ le morphisme de l'algèbre unitaire $A[X_1, X_2, \dots, X_n]$ dans l'algèbre unitaire $A[Y_1, Y_2, \dots, Y_p]$ tel que, pour tout élément i de $[1, n]$, $\varphi(X_i) = Y_i$. Montrer qu'il existe une application A -linéaire $\tilde{\varphi}$ et une seule de $E[X_1, X_2, \dots, X_n]$ dans $E[Y_1, Y_2, \dots, Y_p]$ telle que, pour tout élément P de $A[X_1, X_2, \dots, X_n]$ et pour tout élément b de E ,

$$\tilde{\varphi}(bP) = b\varphi(P).$$

La valeur de $\tilde{\varphi}$ sur un élément P de $E[X_1, X_2, \dots, X_n]$ s'appelle polynôme obtenu par substitution de Q_1, Q_2, \dots, Q_n à X_1, X_2, \dots, X_n dans P , et se note $P(Q_1, Q_2, \dots, Q_n)$, ou, plus simplement, $P \circ Q$. Généraliser à ce cas les propriétés de la composition des polynômes.

Étudier de même la substitution pour les séries entières à coefficients vectoriels.

28 A. Applications polynomiales.

On conserve les notations de l'exercice précédent.

Soient E un A -module, et p un entier naturel non nul.

1. Soient $P = \sum_{s \in S} b_s X^s$ un élément de $E[X_1, X_2, \dots, X_p]$ et \tilde{P} l'application de A^p dans E qui à tout élément $a = (\alpha_1, \alpha_2, \dots, \alpha_p)$ associe $\sum_{s \in S} b_s a^s$. Prouver que l'application $P \mapsto \tilde{P}$ est une application linéaire de $E[X_1, X_2, \dots, X_p]$ dans $\mathcal{F}(A^p, E)$, et que, pour tout élément P de $E[X_1, X_2, \dots, X_p]$ et pour tout élément Q de $A[X_1, X_2, \dots, X_p]$, $\widetilde{PQ} = \tilde{Q}\tilde{P}$.

2. On dit qu'une application f définie sur une partie B de A^p à valeurs dans E est polynomiale s'il existe un élément P de $E[X_1, X_2, \dots, X_p]$ tel que \tilde{P} coïncide avec f sur B . L'application $a \mapsto \tilde{P}(a)$ s'appelle application polynomiale de B dans E canoniquement associée à P .

3. On suppose que $p = 1$ et que A est intègre. Soient P un élément de $E[X]$ et α un élément de A . Prouver que $\tilde{P}(\alpha) = 0$ si et seulement si P est divisible par $X - \alpha$. (On dit que P est divisible par un élément Q de $K[X]$ s'il existe un élément R de $E[X]$ tel que $P = QR$.) Étendre la notion de valuation d'un polynôme en un point α au cas des polynômes à coefficients vectoriels, ainsi que le théorème 2.1 et ses conséquences.

4. Soient F un A -module et U une application linéaire de E dans F . Prouver que, pour toute application polynomiale f de B dans E , $U \circ f$ est une application polynomiale de B dans F . En particulier, pour toute forme linéaire y^* sur E , $y^* \circ f$ est une fonction polynomiale sur B .

En déduire à nouveau que si $p = 1$ et si B est une partie infinie de A , l'application $P \mapsto \tilde{P}$ est injective. Lorsque $p > 1$, étendre le théorème de prolongement des identités algébriques au cas des polynômes à coefficients vectoriels.

5. On suppose que A est un corps et que E est de dimension finie n . Soient (e_1, e_2, \dots, e_n) une base de E et $(e_1^*, e_2^*, \dots, e_n^*)$ sa base duale. Montrer qu'une application f de B dans E est polynomiale si et seulement si, pour tout élément i de $[1, n]$, $e_i^* \circ f$ est une fonction polynomiale sur B .

29 A. Différentielle d'un polynôme à coefficients vectoriels.

On conserve les notations de l'exercice 27.

Soient E un A -module, $E[X_1, X_2, \dots, X_p, Y_1, Y_2, \dots, Y_p]$ le module des polynômes à $2p$ indéterminées à coefficients dans E , et $F = E[X_1, X_2, \dots, X_p]$. On identifie $E[X_1, X_2, \dots, X_p, Y_1, Y_2, \dots, Y_p]$ au module $F[Y_1, Y_2, \dots, Y_p]$. Pour tout élément P de $E[X_1, X_2, \dots, X_p]$ et pour tout entier naturel n , on désigne par $T_n(P)$ la composante n -homogène du polynôme $P(X_1 + Y_1, X_2 + Y_2, \dots, X_n + Y_n)$, considéré comme élément de $F[Y_1, Y_2, \dots, Y_p]$. Ainsi, $T_n(P)$ est un polynôme n -homogène, et

$$P(X_1 + Y_1, X_2 + Y_2, \dots, X_p + Y_p) = \sum_{n=0}^{+\infty} T_n(P).$$

La famille des polynômes $T_n(P)$ s'appelle développement taylorien du polynôme P .

1. Prouver que l'application $P \mapsto T_n(P)$ est linéaire et que, pour tout élément P de $E[X_1, X_2, \dots, X_p]$ et pour tout élément Q de $A[X_1, X_2, \dots, X_p]$,

$$T_n(PQ) = \sum_{r+s=n} T_r(P)T_s(Q).$$

2. On appelle différentielle de P , et on note dP , le polynôme $T_1(P)$. Montrer que l'application $P \mapsto dP$ est la seule application A -linéaire de $E[X_1, X_2, \dots, X_p]$ dans $E[X_1, X_2, \dots, X_p, Y_1, Y_2, \dots, Y_p]$ telle que, pour tout élément Q de $A[X_1, X_2, \dots, X_p]$ et pour tout élément b de E ,

$$d(bQ) = b dQ,$$

où dQ désigne la différentielle du polynôme Q .

Montrer que, pour tout élément P de $E[X_1, X_2, \dots, X_p]$ et pour tout élément Q de $A[X_1, X_2, \dots, X_p]$,

$$d(PQ) = dPQ + PdQ.$$

Étendre à ce cas la formule donnant la différentielle d'un polynôme composé, de la forme $P(Q_1, Q_2, \dots, Q_p)$, où Q_1, Q_2, \dots, Q_p appartiennent à $A[X'_1, X'_2, \dots, X'_q]$.

3. Prouver que pour tout élément i de $[1, p]$, il existe un endomorphisme D_i et un seul du module $E[X_1, X_2, \dots, X_p]$ tel que, pour tout élément Q de $A[X_1, X_2, \dots, X_p]$ et pour tout élément b de E ,

$$D_i(bQ) = b D_i(Q),$$

où $D_i(Q)$ désigne la $i^{\text{ème}}$ dérivée partielle du polynôme Q . Étendre à ce cas les propriétés des dérivées partielles des polynômes. En particulier, prouver que

$$dP = \sum_{i=1}^p D_i(P) Y_i.$$

Étendre les théorèmes 2.11 et 2.12.

4. Soit H l'opérateur différentiel sur $E[X_1, X_2, \dots, X_p]$ défini par la relation

$$H(P) = \sum_{i=1}^p D_i(P) Y_i.$$

Prouver que si A est un corps de caractéristique nulle, alors, pour tout entier naturel n ,

$$T_n(P) = \frac{H^n(P)}{n!}.$$

En déduire que la formule de Taylor s'étend aux polynômes à coefficients vectoriels.

5. Généraliser les notions et résultats précédents au cas des séries entières à coefficients vectoriels.

GROUPE SYMÉTRIQUE, GROUPE ALTERNÉ

30. Soient E un ensemble fini ayant n éléments, où $n \geq 3$, p un entier naturel inférieur ou égal à $n - 2$, (a_1, a_2, \dots, a_p) et (b_1, b_2, \dots, b_p) deux suites d'éléments de E distincts deux à deux. Prouver qu'il existe un élément σ de \mathfrak{S}_E tel que, pour tout élément j de $[1, p]$, $\sigma(a_j) = b_j$, et que, si $p = n - 2$, cet élément est unique.

31. Soit G un groupe fini d'ordre n . Montrer que l'application de G dans \mathfrak{S}_G qui à tout élément a associe la translation à gauche ${}_a\sigma : x \mapsto ax$ définit un isomorphisme de G sur un sous-groupe de \mathfrak{S}_G .

Examiner le cas où G est cyclique, et celui où G est le groupe de Klein.

32. Pour tout élément σ de \mathfrak{S}_n , on note $v(\sigma)$ le cardinal de l'ensemble des orbites de $[1, n]$ sous σ . Établir la formule

$$\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) X^{v(\sigma)} = X(X-1) \dots (X-n+1).$$

(On pourra raisonner par récurrence sur l'entier n .)

33. Soit E un ensemble fini ayant n éléments, $n \geq 2$. Prouver que toute permutation de E est le produit d'au plus n transpositions de E . Plus précisément, soient σ une permutation de E différente de I_E et $q(\sigma)$ le cardinal de l'ensemble des points x de E tels que $\sigma x \neq x$. Prouver que σ est le produit d'au plus $q(\sigma) - 1$ transpositions.

34. *Générateurs des groupes symétrique et alterné.*

Soit E un ensemble fini ayant n éléments, $n \geq 2$.

1. Soit a un élément de E . Montrer que les $n - 1$ transpositions $\tau_{a,x}$, où x parcourt $E - \{a\}$, engendrent le groupe \mathfrak{S}_E . (On prouvera que toute transposition de E appartient au sous-groupe engendré par les transpositions précédentes.)

2. Soit T un ensemble de transpositions engendrant le groupe \mathfrak{S}_E . Montrer que, pour tout entier p appartenant à $[1, n - 1]$, il existe une partie P de T ayant p éléments telle que la réunion des supports des éléments de P ait $p + 1$ éléments. (On pourra raisonner par récurrence sur l'entier p .) En déduire que $\text{card}(T) \geq n - 1$.

3. On suppose que $n \geq 3$. Soient a et b deux éléments distincts de E . Montrer que les $n - 2$ cycles (a, b, x) , où x parcourt $E - \{a, b\}$, engendrent le groupe \mathfrak{A}_E (On prouvera que, pour tout élément x de E distinct de a et de b , $\tau_{a,b}\tau_{a,x}$ et $\tau_{a,x}\tau_{a,b}$ appartiennent au sous-groupe de \mathfrak{A}_E engendré par les cycles précédents).

35 B. Simplicité du groupe alterné.

Soit H un sous-groupe distingué du groupe alterné \mathfrak{A}_n .

1. On suppose que $n \geq 3$. A l'aide de l'exercice précédent, montrer que si H contient un cycle de longueur 3, alors $H = \mathfrak{A}_n$.

2. On suppose que $n \geq 4$ et que H contient une permutation σ ayant un cycle composant $\sigma' = (a_1, a_2, \dots, a_p)$ de longueur $p > 3$. Prouver que H contient un cycle de longueur 3 (On pourra calculer $\tau\sigma\tau^{-1}\sigma^{-1}$, où $\tau = (a_1, a_2, a_3)$).

3. On suppose que $n \geq 5$ et que H contient une permutation σ ayant un cycle composant $\tau_{a,b}$ de longueur 2. Prouver qu'il existe un autre cycle composant σ' de longueur $p \geq 2$. Soient c un élément du support de σ' , et $d = \sigma(c)$. On considère le cycle $\tau = (a, b, c)$, et on pose $\sigma_1 = \tau\sigma\tau^{-1}\sigma^{-1}$. Prouver que σ_1 appartient à H , et que $\sigma_1 = \tau_{a,c}\tau_{b,d}$. En déduire que H contient un cycle de longueur 3 (On considérera un élément e de $[1, n]$ distinct des éléments a, b, c et d . On posera $\tau' = (a, b, e)$, et on calculera $\tau'\sigma_1\tau'^{-1}$).

4. On suppose que $n \geq 6$ et que H contient une permutation σ ayant au moins deux cycles composants $\sigma' = (a, b, c)$ et $\sigma'' = (d, e, f)$ de longueur 3. On considère la permutation $\tau = \tau_{a,d}\tau_{b,e}$, et on pose $\sigma_1 = \tau\sigma\tau^{-1}\sigma^{-1}$. Prouver que σ_1 appartient à H , et que $\sigma_1 = \tau_{a,d}\tau_{c,f}$. En déduire que H contient un cycle de longueur 3.

5. Déduire des questions précédentes le résultat suivant :

Pour tout entier naturel $n \geq 5$, le groupe alterné \mathfrak{A}_n est simple (c'est-à-dire que \mathfrak{A}_n n'admet pas d'autres sous-groupes distingués que \mathfrak{A}_n et le sous-groupe réduit à l'élément neutre).

6. Soit σ un élément du centre de \mathfrak{S}_n , $n \geq 3$. En écrivant que, pour toute transposition τ , $\tau = \sigma\tau\sigma^{-1}$, prouver que σ laisse stable toute partie de $[1, n]$ à deux éléments. En déduire que le centre de \mathfrak{S}_n est réduit à l'élément neutre e .

De même, prouver que le centre de \mathfrak{A}_n est réduit à $\{e\}$ si $n \geq 4$.

7. Soient G un sous-groupe distingué non trivial de \mathfrak{S}_n , $n \geq 5$, et $H = G \cap \mathfrak{A}_n$. Prouver que $G = \mathfrak{A}_n$. (On distinguera deux cas suivant que $H = \mathfrak{A}_n$ ou que H est réduit à l'élément neutre. Dans le second cas, on prouvera que G contient un seul élément autre que e , et que cet élément appartient au centre de \mathfrak{S}_n . On aboutira alors à une contradiction.)

POLYNÔMES ET FRACTIONS RATIONNELLES SYMÉTRIQUES

Dans les exercices suivants, on désigne par S_1, S_2, \dots, S_p , les polynômes symétriques élémentaires et par N_1, N_2, \dots, N_p les polynômes de Newton.

36. Polynômes symétriques de faible degré.

On considère l'algèbre $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées. Calculer à l'aide des polynômes symétriques élémentaires les symétrisés des polynômes suivants :

- a) $(X_1 - X_2)^2, (X_1 - X_2)(X_1 - X_3), (X_1 + X_2)(X_1 + X_3)$;
 b) $X_1^3, X_1^2 X_2, (S_1 - X_1)^3, (X_1 - X_2)^3, X_3(X_1 - X_2)^2$;
 c) $X_1^4, X_1^3 X_2, X_1^2 X_2^2, X_1^2 X_2 X_3, (S_1 - X_1)^4, (X_1 - X_2)^4$;
 d) $X_1^3 X_2 X_3, X_1^3 X_2^2$.

37. On considère l'algèbre $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées. Calculer $(S_1 - \alpha X_1)(S_1 - \alpha X_2) \dots (S_1 - \alpha X_n)$, où $\alpha \in K$, à l'aide des polynômes symétriques élémentaires. (On pourra introduire le polynôme $(X - X_1)(X - X_2) \dots (X - X_n)$.)

Application. — Calculer

$$(X_1 + X_2 + X_3)(X_2 + X_3 + X_4)(X_3 + X_4 + X_1)(X_4 + X_1 + X_2).$$

38. *Polynômes symétriques à un petit nombre d'indéterminées.*

1. On considère l'algèbre $K[X, Y, Z]$ des polynômes à trois indéterminées. Calculer le symétrisé de $(X + Y - Z)^5$ à l'aide des polynômes symétriques élémentaires.

2. On considère l'algèbre $K[X, Y, Z, T]$ des polynômes à quatre indéterminées. Calculer à l'aide des polynômes symétriques élémentaires les polynômes suivants :

$$\begin{aligned} & (X + Y - Z - U)^2 + (X + Z - U - Y)^2 + (X + U - Y - Z)^2 \\ & (X + Y - Z - U)(X + Z - U - Y)(X + U - Y - Z) \\ & (XY - ZU)(XZ - UY)(XU - YZ). \end{aligned}$$

39. *Polynômes antisymétriques.*

On considère l'algèbre $K[X, Y, Z]$ des polynômes à trois indéterminées. Déterminer le quotient par le polynôme de Vandermonde des polynômes antisymétriques suivants :

$$\begin{aligned} & X(Y - Z)^3 + Y(Z - X)^3 + Z(X - Y)^3 \\ & X^2(Y - Z)^3 + Y^2(Z - X)^3 + Z^2(X - Y)^3 \\ & (X - Y)^5 + (Y - Z)^5 + (Z - X)^5 \\ & X^3(Y - Z) + Y^3(Z - X) + Z^3(X - Y) \\ & X^5(Y - Z) + Y^5(Z - X) + Z^5(X - Y) + XYZ(Y - Z)(Z - X)(X - Y). \end{aligned}$$

40. *Fractions rationnelles symétriques.*

On considère le corps $K(X, Y, Z)$ des fractions rationnelles à trois indéterminées. Calculer les fractions rationnelles symétriques suivantes à l'aide des polynômes symétriques élémentaires, et les mettre sous forme irréductible :

$$\begin{aligned} & \frac{X^3(Y^2 - Z^2) + Y^3(Z^2 - X^2) + Z^3(X^2 - Y^2)}{X^2(Y - Z) + Y^2(Z - X) + Z^2(X - Y)} \\ & \frac{X^2(X + Y)(X + Z)}{(X - Y)(X - Z)} + \frac{Y^2(Y + Z)(Y + X)}{(Y - Z)(Y - X)} + \frac{Z^2(Z + X)(Z + Y)}{(Z - X)(Z - Y)} \\ & \left(\frac{Y - Z}{X} + \frac{Z - X}{Y} + \frac{X - Y}{Z} \right) \left(\frac{X}{Y - Z} + \frac{Y}{Z - X} + \frac{Z}{X - Y} \right). \end{aligned}$$

41. *Polynômes symétriques triples.*

On considère l'algèbre $K[X_1, X_2, \dots, X_n]$ des polynômes à n indéterminées. Soient p, q et r trois entiers rationnels non nuls distincts deux à deux. Prouver que le symétrisé de $X_1^p X_2^q X_3^r$ est égal à

$$N_p N_q N_r - N_{p+q} N_r - N_{q+r} N_p - N_{r+p} N_q + 2N_{p+q+r}.$$

Calculer de même les symétrisés de $X_1^p X_2^p X_3^p$ et de $X_1^p X_2^p X_3^p$ à l'aide des polynômes de Newton.

42. Soient n un entier strictement supérieur à 1 et P un élément de $K[X_1, X_2, \dots, X_n]$. Montrer que si P est symétrique et divisible par $X_1 - X_2$, P est divisible par le carré du polynôme de Vandermonde.

- *43. Application des polynômes symétriques au calcul des déterminants.

Soient α, β et γ des scalaires. Calculer les déterminants suivants :

$$\begin{vmatrix} -2\alpha & \alpha+\beta & \alpha+\gamma \\ \beta+\alpha & -2\beta & \beta+\gamma \\ \gamma+\alpha & \gamma+\beta & -2\gamma \end{vmatrix} \quad \begin{vmatrix} (\beta+\gamma)^2 & \gamma^2 & \beta^2 \\ \gamma^2 & (\gamma+\alpha)^2 & \alpha^2 \\ \beta^2 & \alpha^2 & (\alpha+\beta)^2 \end{vmatrix} \quad \begin{vmatrix} (\beta+\gamma)^2 & \beta^2 & \gamma^2 \\ \alpha^2 & (\gamma+\alpha)^2 & \gamma^2 \\ \alpha^2 & \beta^2 & (\alpha+\beta)^2 \end{vmatrix}$$

$$\begin{vmatrix} \beta\gamma & \gamma\alpha & \alpha\beta \\ \alpha^2 & \beta^2 & \gamma^2 \\ \alpha & \beta & \gamma \end{vmatrix} \quad \begin{vmatrix} \beta+\gamma & \gamma+\alpha & \alpha+\beta \\ \beta^2+\gamma^2 & \gamma^2+\alpha^2 & \alpha^2+\beta^2 \\ \beta^3+\gamma^3 & \gamma^3+\alpha^3 & \alpha^3+\beta^3 \end{vmatrix} \quad \begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^4 & \beta^4 & \gamma^4 \end{vmatrix} \cdot *$$

SÉRIES ENTIÈRES FORMELLES

- 44 A. Caractérisation de l'exponentielle formelle.

Soit S une série entière formelle généralisée non nulle à une indéterminée.

1. Prouver que si S satisfait à la relation

$$(1) \quad S(X + Y) = S(X)S(Y),$$

alors $v_0(S) = 0$, $S(0) = 1$ et $D(S) = \alpha S$, où $\alpha = [D(S)](0)$.

En déduire que si la caractéristique de K n'est pas nulle, il n'existe aucune série entière formelle généralisée non nulle S satisfaisant à la relation (1).

(Lorsque α n'est pas nul, on prouvera que S est un polynôme, et on utilisera l'exercice 13. Lorsque $\alpha = 0$, on prouvera que S est de la forme $1 + \sum_{n=0}^{+\infty} \alpha_n X^{np}$ où p est la caractéristique de K ; on montrera à l'aide de la formule du binôme que tous les scalaires α_n sont nuls).

2. On suppose désormais que K est de caractéristique 0. Montrer que les séries entières formelles $\exp(\alpha X)$, où $\alpha \in K$, sont les seules séries entières formelles telles que $S(0) = 1$ et que, pour tout couple (A, B) d'éléments de M ,

$$S \circ (A + B) = (S \circ A) \cdot (S \circ B).$$

(En utilisant l'équation $S(2X) = [S(X)]^2$ et en posant $T = \frac{D(S)}{S}$, on montrera que $T(2X) = T(X)$, et que T est constante.)

45 A. Endomorphismes formels du groupe additif K .

En s'inspirant de la méthode de l'exercice 15, prouver que si K est de caractéristique nulle, les monômes αX sont les seules séries entières formelles généralisées A telles que

$$A(X + Y) = A(X) + A(Y).$$

Prouver de même que si K est de caractéristique p non nulle, les séries entières formelles $\alpha X + \sum_{n=1}^{+\infty} \alpha_n X^{np}$ sont les seules séries entières formelles généralisées A telles que

$$A(X + Y) = A(X) + A(Y).$$

46 A. Endomorphismes formels du groupe multiplicatif K^* .

1. En s'inspirant de la méthode de l'exercice 16, montrer que, pour tout entier rationnel p , X^p est la seule série entière formelle généralisée A satisfaisant aux relations

$$A(XY) = A(X)A(Y)$$

et $v_0(A) = p$.

2. Lorsque K est de caractéristique nulle, retrouver ce résultat en montrant qu'une série entière formelle non nulle A satisfaisant aux relations précédentes satisfait à la relation

$$XD(A) = pA.$$

47 A. Équations différentielles formelles linéaires du premier ordre.

1. Soient α un scalaire, B une série entière formelle et A l'unique primitive de B telle que $A(0) = 0$. Soit d'autre part S une série entière formelle. Montrer qu'il est équivalent de dire :

- a) La série entière formelle S satisfait aux relations $D(S) + BS = 0$ et $S(0) = \alpha$.
- b) La série entière formelle S est égale à $\alpha \exp(-A)$.

(Pour démontrer que $a) \Rightarrow b$), on dérivera la série entière formelle $S \exp A$.)

2. Plus généralement, déterminer les séries entières formelles S telles que

$$D(S) + BS = C,$$

où C est une série entière formelle donnée.

3. Plus généralement encore, déterminer les séries entières formelles S telles que

$$B_1 D(S) + B_2 S = C,$$

où B_1, B_2 et C sont des séries entières formelles données, B_1 étant inversible.

4. Soient B_1 et B_2 des séries entières formelles telles que $p = v_0(B_1) > 0$, $v_0(B_2) = 0$. On pose $B_1 = X^p B_1'$. Montrer que l'espace vectoriel des séries entières formelles généralisées S solutions de l'équation

$$B_1 D(S) + B_2 S = 0$$

est réduit à $\{0\}$ si $p \geq 2$ et que, si $p = 1$, il n'est pas réduit à $\{0\}$ si et seulement si $\frac{B_2(0)}{B_1'(0)}$

appartient à \mathbb{Z} . Prouver que cet espace vectoriel est alors de dimension 1, et en déterminer une base. Chercher à quelle condition cet espace vectoriel est constitué de séries entières formelles.

Soit maintenant C une série entière formelle. Montrer que si $p \geq 2$, il existe une série entière formelle S et une seule telle que

$$(1) \quad B_1 D(S) + B_2 S = C,$$

et qu'il en est de même lorsque $p = 1$ et que $\frac{B_2(0)}{B_1'(0)}$ n'appartient pas à \mathbb{Z} .

On suppose enfin que $p = 1$ et que $q = \frac{B_2(0)}{B_1'(0)}$ appartient à \mathbb{Z} . En étudiant l'équation

différentielle satisfaite par $T = SX^q$, déterminer une condition nécessaire et suffisante pour que l'équation (1) admette une solution. Montrer qu'il en est ainsi lorsque $v_0(C) + q \geq 1$.

- 48 A.** Soient U un opérateur de composition et E l'ensemble des séries entières formelles à deux indéterminées appartenant à $K[X][[Y]]$, considéré comme $K[[Y]]$ -module. Montrer qu'il existe un endomorphisme \tilde{U} et un seul du module E prolongeant U et tel que, pour tout élément A de E , considéré comme série entière formelle à deux indéterminées, $v_0[\tilde{U}(A)] = v_0(A)$.

Prouver que

$$\tilde{U}\left(\sum_{n=0}^{+\infty} P_n Y^n\right) = \sum_{n=0}^{+\infty} U(P_n) Y^n.$$

En particulier prouver que

$$\tilde{U}[\exp(XY)] = A(Y) \exp(XY),$$

où A est la série entière formelle associée à l'opérateur de composition U .

IDÉAUX DE L'ANNEAU DES SÉRIES ENTIÈRES FORMELLES

- 49 A.** *Ideaux gradués de $A[X_1, X_2, \dots, X_n]$.*

On dit qu'un idéal \mathfrak{J} de $A[X_1, X_2, \dots, X_n]$ est gradué s'il est somme directe des sous-espaces vectoriels $\mathfrak{J} \cap H_p$, où, pour tout entier naturel p , H_p désigne le sous-espace vectoriel de $A[X_1, X_2, \dots, X_n]$ constitué des polynômes p -homogènes.

1. Soit \mathfrak{J} un idéal de $A[X_1, X_2, \dots, X_n]$. Prouver que s'il existe une famille génératrice de l'idéal \mathfrak{J} constituée de polynômes homogènes, l'idéal \mathfrak{J} est gradué. Réciproquement, prouver que si \mathfrak{J} est gradué, alors, pour toute famille génératrice $(P_i)_{i \in I}$ de l'idéal \mathfrak{J} la famille des composantes homogènes des polynômes P_i engendre encore l'idéal \mathfrak{J} .

2. Soient \mathfrak{J} un idéal gradué de $A[X_1, X_2, \dots, X_n]$ et $(U_i)_{i \in I}$ une famille génératrice de l'idéal \mathfrak{J} constituée de polynômes homogènes. Prouver que, pour tout polynôme P p -homogène appartenant à \mathfrak{J} , P peut s'écrire sous la forme

$$P = \sum_{i \in J} Q_i U_i,$$

où J est une partie finie de I et où, pour tout élément i de I , Q_i est homogène de degré $d^\circ(P) - d^\circ(U_i)$.

50 B. *Théorème de Hilbert pour les séries entières formelles.*

Soient A un anneau noëthérien et \mathfrak{S} un idéal de $A[[X]]$.

1. Pour tout entier naturel p , on note \mathfrak{A}_p l'ensemble des éléments a de A tels qu'il existe un élément B de \mathfrak{S} satisfaisant à la condition suivante : $B \equiv aX^p \pmod{\mathfrak{S}_p}$, où \mathfrak{S}_p désigne l'idéal de $A[[X]]$ constitué des éléments de valuation supérieure ou égale à p . Prouver que \mathfrak{A}_p est un idéal de A , et que la suite (\mathfrak{A}_p) est croissante. En déduire qu'il existe un entier naturel r tel que, pour tout entier $p > r$, $\mathfrak{A}_p = \mathfrak{A}_r$.

2. Pour tout élément i de $[0, r]$, on considère une suite finie $(a_{ij})_{j \in [1, n_i]}$ engendrant l'idéal \mathfrak{A}_i , et un élément B_{ij} de \mathfrak{S} tel que $B_{ij} \equiv a_{ij}X^i \pmod{\mathfrak{S}_{i+1}}$. Soit \mathfrak{S}' l'idéal de $A[[X]]$ engendré par les éléments B_{ij} . Prouver que, pour tout élément C de \mathfrak{S} , il existe un élément B_0 de \mathfrak{S}' et un élément C_1 de $\mathfrak{S} \cap \mathfrak{S}_1$ tels que $C = B_0 + C_1$. Prouver de même que, pour tout entier naturel p et pour tout élément C_p de $\mathfrak{S} \cap \mathfrak{S}_p$, il existe un élément B_p de $\mathfrak{S}' \cap \mathfrak{S}_p$ et un élément C_{p+1} de $\mathfrak{S} \cap \mathfrak{S}_{p+1}$ tels que $C_p = B_p + C_{p+1}$. En déduire que, pour tout élément C de \mathfrak{S} , il existe un élément B de \mathfrak{S}' et un élément C_r de $\mathfrak{S} \cap \mathfrak{S}_r$ tels que $C = B + C_r$. Prouver que, pour tout entier $p \geq r$, tout élément C_p de $\mathfrak{S} \cap \mathfrak{S}_p$ peut s'écrire sous la forme

$$C_p = \sum_{j=1}^r D_{pj} B_{rj} + C_{p+1},$$

où $C_{p+1} \in \mathfrak{S} \cap \mathfrak{S}_{p+1}$ et où, pour tout $j \in [1, n_r]$, $v(D_{pj}) \geq p - r$ (On pourra utiliser l'exercice précédent).

En déduire que, pour tout élément j de $[1, n_r]$, la famille (D_{pj}) est sommable, et que C_r appartient à \mathfrak{S}' . Donc $\mathfrak{S} = \mathfrak{S}'$.

On obtient ainsi le résultat fondamental suivant :

Si l'anneau A est noëthérien, il en est de même de $A[[X]]$, et, plus généralement, de $A[[X_1, X_2, \dots, X_n]]$. En particulier, pour tout corps commutatif K , l'anneau $K[[X_1, X_2, \dots, X_n]]$ est noëthérien.

51. Soit P un élément de $K[X_1, X_2, \dots, X_n]$, homogène et non nul. Montrer que $\frac{1}{P}$ peut se mettre sous la forme $X^s C$, où s est une application de $[1, n]$ dans \mathbb{Z} et où C appartient à $K[[X_1, X_2, \dots, X_n]]$, si et seulement si P est de la forme X^t .

52 A. *Méthode des approximations successives dans l'algèbre des séries entières formelles.*

Soit U un endomorphisme de l'espace vectoriel $K[[X_1, X_2, \dots, X_n]]$ tel que, pour tout entier naturel p et pour tout élément T de $K[[X_1, X_2, \dots, X_n]]$, $v[U^p(T)] \geq p$. Prouver que, pour tout élément D de $K[[X_1, X_2, \dots, X_n]]$, il existe un élément S et un seul de $K[[X_1, X_2, \dots, X_n]]$ tel que

$$S = D + U(S),$$

à savoir
$$S = \sum_{p=0}^{+\infty} U^p(D).$$

53 B. Théorème préparatoire de Weierstrass.

Dans cet exercice, on considère les éléments de l'algèbre $K[[X_1, X_2, \dots, X_n]]$ comme des éléments de $A[[X_n]]$, où A désigne l'anneau $K[[X_1, X_2, \dots, X_{n-1}]]$. On note $a \mapsto \bar{a}$ l'application de A dans K qui à tout élément associe sa valeur à l'origine. Pour tout entier naturel p , on note \mathfrak{S}_p l'idéal de A constitué des éléments de valuation supérieure ou égale à p .

1. A tout élément $B = \sum_{p=0}^{+\infty} a_p X_n^p$ de $A[[X_n]]$ on associe l'élément \bar{B} de $K[[X_n]]$ défini par la formule $\bar{B} = \sum_{p=0}^{+\infty} \bar{a}_p X_n^p$. La série entière formelle \bar{B} s'appelle *série entière formelle réduite associée à B* , et sa valuation s'appelle *valuation réduite de B* .

Prouver que l'application $B \mapsto \bar{B}$ est un morphisme de la K -algèbre unitaire $A[[X_n]]$ dans la K -algèbre $K[[X_n]]$, dont le noyau est l'idéal de $A[[X_n]]$ constitué des séries entières formelles B dont tous les coefficients a_p appartiennent à l'idéal maximal $\mathfrak{M} = \mathfrak{S}_1$ de A .

2. Soient B un élément de $K[[X_1, X_2, \dots, X_n]]$ tel que $\bar{B} \neq 0$, et m la valuation réduite de B . Montrer que, pour tout élément C de $A[[X_n]]$, il existe un couple (Q, r) et un seul constitué d'un élément Q de $A[[X_n]]$ et d'une suite $r = (r_0, r_1, \dots, r_{m-1})$ d'éléments de A tels que

$$(1) \quad C = BQ + \sum_{p=0}^{m-1} r_p X_n^p.$$

Ce résultat est connu sous le nom de *théorème préparatoire de Weierstrass*; il est fondamental pour l'étude de la divisibilité dans les anneaux de séries entières formelles; cf. exercices 54 et 57. Pour le démontrer, on pourra utiliser les étapes suivantes :

a) Soit V l'endomorphisme du K -espace vectoriel $A[[X_n]]$ qui à tout élément $C = \sum_{p=0}^{+\infty} c_p X_n^p$ associe $\sum_{p=m}^{+\infty} c_p X_n^{p-m}$. Prouver qu'il existe un couple (Q, r) et un seul satisfaisant à la relation (1) si et seulement s'il existe un élément Q et un seul de $A[[X_n]]$ tel que

$$(2) \quad V(C) = V(BQ).$$

b) On écrit B sous la forme $B = \sum_{p=0}^{+\infty} a_p X_n^p$ et on pose

$$P = \sum_{p=0}^{m-1} a_p X_n^p \quad \text{et} \quad B' = \sum_{p=m}^{+\infty} a_p X_n^{p-m}.$$

Par hypothèse, B' est inversible dans $A[[X_n]]$, et $\bar{P} = 0$, c'est-à-dire que a_0, a_1, \dots, a_{m-1} appartiennent à l'idéal maximal \mathfrak{M} de A . En posant $S = B'Q$, montrer qu'il existe un élément Q et un seul de $A[[X_n]]$ satisfaisant à la relation (2) si et seulement s'il existe un élément S et un seul de $A[[X_n]]$ tel que

$$(3) \quad V(C) = V(PB'^{-1}S) + S.$$

c) On introduit l'endomorphisme U du K -espace vectoriel $A[[X_n]]$ défini par la relation $U(T) = -V(PB'^{-1}T)$. Prouver que si les coefficients de T , considéré comme élément de $A[[X_n]]$, appartiennent à l'idéal \mathfrak{J}_p , alors ceux de $U(T)$ appartiennent à \mathfrak{J}_{p+1} . En déduire, à l'aide de l'exercice 52, que l'équation (3) admet une solution S et une seule.

54 B. Polynômes distingués.

On utilise les notations et les résultats de l'exercice précédent.

On dit qu'un élément P de $A[[X_n]]$ est un polynôme distingué s'il est de la forme

$$P = X_n^m + a_{m-1}X_n^{m-1} + \dots + a_0,$$

où $m \geq 1$ et où, pour tout élément p de $[0, m-1]$, a_p appartient à l'idéal maximal \mathfrak{M} de l'anneau A . Le produit de deux polynômes distingués en est encore un.

1. Soient B un élément de $A[[X_n]]$ tel que $\bar{B} \neq 0$, et m la valuation réduite de B . Montrer qu'il existe un couple (C, P) et un seul constitué d'un élément inversible C de $A[[X_n]]$ et d'un polynôme distingué P de degré m tel que $B = CP$. Le polynôme distingué P est dit canoniquement associé à B .

(Pour démontrer l'unicité du couple (C, P) , on posera $P = X_n^m + R$, et on écrira la relation $B = CP$ sous la forme $X_n^m = C^{-1}B - R$; on appliquera alors le théorème préparatoire de Weierstrass. Pour démontrer l'existence du couple (C, P) , on prouvera que X_n^m peut s'écrire sous la forme

$$(1) \quad X_n^m = QB + \sum_{p=0}^{m-1} r_p X_n^p,$$

où $Q \in A[[X_n]]$ et où, pour tout élément p de $[0, m-1]$, $r_p \in A$. On prouvera alors que Q est inversible dans $A[[X_n]]$, et que le polynôme

$$P = X_n^m - \sum_{p=0}^{m-1} r_p X_n^p$$

est distingué, en considérant les séries réduites associées aux deux membres de la relation (1)).

2. Soient B et B' deux éléments de $A[[X_n]]$ tels que \bar{B} et \bar{B}' soient non nuls, m et m' leurs valuations réduites, P et P' les polynômes distingués canoniquement associés à B et B' . Montrer que la valuation réduite de BB' est égale à $m + m'$, et que le polynôme distingué canoniquement associé à BB' n'est autre que PP' .

3. Soit P un polynôme distingué. Prouver que P est irréductible dans l'anneau $A[X_n]$ si et seulement s'il est irréductible dans l'anneau $A[[X_n]]$.

55 A. Automorphismes de l'anneau des séries entières formelles.

Soit A un anneau intègre unitaire.

1. Soient B_1, B_2, \dots, B_n n éléments de $A[[X_1, X_2, \dots, X_n]]$ tels que, pour tout élément p de $[1, n]$,

$$B_i \equiv X_i \pmod{\mathfrak{J}_1} \quad (\text{mod. } \mathfrak{J}_1)$$

Soit φ l'application $C \mapsto C(B_1, B_2, \dots, B_n)$. Prouver que si $v(C) \geq p$, où $p \in \mathbb{N}$, alors

$$\varphi(C) - C \equiv 0 \pmod{\mathfrak{J}_p} \quad (\text{mod. } \mathfrak{J}_p).$$

En déduire que φ est un automorphisme de l'algèbre unitaire $A[[X_1, X_2, \dots, X_n]]$.

2. Soient, plus généralement, B'_1, B'_2, \dots, B'_n n éléments de $A[[X_1, X_2, \dots, X_n]]$ de valuation 1 et, pour tout couple (i, j) d'éléments de $[1, n]$, α_{ij} la valeur à l'origine de $D_j(B'_i)$. On suppose que la matrice (α_{ij}) est inversible dans l'anneau $M_n(A)$. Prouver que l'application $\varphi' : C \mapsto C(B'_1, B'_2, \dots, B'_n)$ est un automorphisme de l'algèbre unitaire $A[[X_1, X_2, \dots, X_n]]$ (On se ramènera au cas de la première question).

Montrer que, pour tout élément C de $A[[X_1, X_2, \dots, X_n]]$, $v[\varphi'(C)] = v(C)$.

3. Réciproquement, soit ψ un automorphisme de l'algèbre unitaire $A[[X_1, X_2, \dots, X_n]]$ satisfaisant à la condition suivante : pour toute suite (C_p) d'éléments de cette algèbre telle que $v(C_p)$ tende vers $+\infty$, alors $v[\psi(C_p)]$ tend vers $+\infty$. Pour tout élément i de $[1, n]$, on pose $B'_i = \psi(X_i)$. Prouver que $v(B'_i) \neq 0$. En déduire que, pour tout élément C de $A[[X_1, X_2, \dots, X_n]]$, $v[\psi(C)] \geq v(C)$. Prouver qu'il existe alors un automorphisme φ' tel que, pour tout élément i de $[1, n]$, $\varphi'(X_i)$ soit homogène de degré 1, et satisfaisant à la condition suivante : il existe un élément r de $[1, n]$ tel que

$$\begin{aligned} (\varphi' \circ \psi)(X_i) &\equiv X_i & (\text{mod. } \mathfrak{J}_1) & \quad \text{si } i \in [1, r] \\ (\varphi' \circ \psi)(X_i) &\equiv 0. & (\text{mod. } \mathfrak{J}_1) & \quad \text{si } i \notin [1, r] \end{aligned}$$

Prouver que r est nécessairement égal à n . En déduire que, pour tout élément i de $[1, n]$, $v(B'_i) = 1$, que l'application $\psi' : C \mapsto C(B'_1, B'_2, \dots, B'_n)$ est un automorphisme, et que $\psi = \psi'$.

56 A. Normalisation d'une série entière formelle.

On utilise les notations de l'exercice 54.

1. On suppose que le corps K est infini. Soient B un élément non nul de $K[[X_1, X_2, \dots, X_n]]$, de valuation q , et B_q la composante q -homogène de B dans l'algèbre $K[[X_1, X_2, \dots, X_n]]$. Prouver qu'il existe une suite $(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ d'éléments de K telle que $B_q(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, 1) \neq 0$.

Soit φ l'endomorphisme de l'algèbre unitaire $K[[X_1, X_2, \dots, X_n]]$ défini par les formules

$$\begin{aligned} \varphi(X_p) &= X_p + \alpha_p X_n & \text{si } p \in [1, n-1] \\ \varphi(X_n) &= X_n. \end{aligned}$$

Montrer que φ est un automorphisme, et que la série entière formelle réduite associée à $\varphi(B)$ est non nulle.

2. Soient A un anneau intègre unitaire, $B = \sum_{p,q} \alpha_{p,q} X^p Y^q$ un élément non nul de $A[[X, Y]]$ et \mathcal{E} l'ensemble des couples (p, q) tels que $\alpha_{p,q} \neq 0$. Soit (r, s) le plus petit élément de \mathcal{E} , $\mathbb{N} \times \mathbb{N}$ étant ordonné lexicographiquement. Prouver que, pour tout entier p strictement supérieur à s , $B(T^p, T)$ est non nul.

3. Soit B un élément non nul de $K[[X_1, X_2, \dots, X_n]]$. Prouver qu'il existe une suite $(r_1, r_2, \dots, r_{n-1})$ d'entiers naturels non nuls telle que $B(T^{r_1}, T^{r_2}, \dots, T^{r_{n-1}}, T) \neq 0$. (On commencera par considérer B comme élément de $A[[X_1, X_n]]$, où $A = K[[X_2, X_3, \dots, X_{n-1}]]$. A l'aide de la question 2, on prouvera qu'il existe un entier r_1 tel que $B_1 = B(T^{r_1}, X_2, \dots, X_{n-1}, T) \neq 0$. En répétant le même raisonnement pour B_1 , on en déduira le résultat par récurrence.)

Soit φ l'endomorphisme de l'algèbre unitaire $K[[X_1, X_2, \dots, X_n]]$ défini par les formules

$$\begin{aligned}\varphi(X_p) &= X_p + X_n^{r_p} & \text{si } p \in [1, n-1] \\ \varphi(X_n) &= X_n.\end{aligned}$$

A l'aide de l'exercice 55, montrer que φ est un automorphisme, et que la série entière formelle réduite associée à $\varphi(B)$ est non nulle.

4. En déduire le résultat suivant :

Pour toute suite (B_1, B_2, \dots, B_p) d'éléments non nuls de $K[[X_1, X_2, \dots, X_n]]$, il existe un automorphisme φ de cette algèbre unitaire tel que les séries entières formelles réduites associées à $\varphi(B_1), \varphi(B_2), \dots, \varphi(B_p)$ soient non nulles (normalisation des séries entières formelles).

(On se ramènera au cas d'une seule série entière formelle en considérant le produit $B_1 B_2 \dots B_p$.)

57 B. *Décomposition des séries entières formelles en facteurs irréductibles.*

On se propose de démontrer le résultat fondamental suivant :

L'anneau $K[[X_1, X_2, \dots, X_n]]$ des séries entières formelles à n indéterminées est factoriel.

On effectuera la démonstration par récurrence sur l'entier n , en supposant le résultat acquis pour l'anneau $A = K[[X_1, X_2, \dots, X_{n-1}]]$ et en prouvant que si B est un élément irréductible de $A[[X_n]]$ divisant le produit ST de deux éléments de $A[[X_n]]$, B divise l'un de ces éléments (cf. exercice 8). Pour cela, on pourra utiliser les étapes suivantes :

a) Grâce à l'exercice 56, on se ramènera au cas où les séries entières formelles réduites associées à B, S et T , sont non nulles.

b) Les séries entières formelles réduites associées à B, S et T étant supposées non nulles, on prouvera, grâce à l'exercice 54, que les polynômes distingués P, Q et R respectivement associés à B, S et T satisfont aux conditions suivantes : P est irréductible dans $A[X_n]$, et P divise QR dans $A[X_n]$.

c) En utilisant la factoriabilité de l'anneau $A[X_n]$ (cf. th. 2.9), on en déduira que P divise l'un des deux éléments Q et R et, enfin, que B divise l'un des deux éléments S et T .

CHAPITRE 3

ALGÈBRE MULTILINÉAIRE

INTRODUCTION

Dans ce chapitre, nous exposons quelques notions d'algèbre multilinéaire. Il est en effet devenu classique d'utiliser le langage et la théorie des formes multilinéaires alternées pour traiter des déterminants. D'autre part, la notion de forme multilinéaire alternée intervient de manière essentielle dans le calcul différentiel extérieur (cf. *Analyse* III). Enfin, la notion de forme multilinéaire symétrique permet de définir de manière intrinsèque les fonctions polynomiales sur un espace vectoriel.

C'est pourquoi nous avons consacré le § 1 à l'étude des formes p -linéaires, p -linéaires symétriques et p -linéaires alternées. Nous utilisons essentiellement les opérations de symétrisation et d'antisymétrisation d'une application p -linéaire. On construit ainsi des formes p -linéaires symétriques et alternées en symétrisant et en antisymétrisant les produits tensoriels de p formes linéaires. On détermine alors la structure de l'espace vectoriel des formes p -linéaires alternées. Celle de l'espace vectoriel des formes p -linéaires symétriques est rejetée en exercice.

Pour définir de manière intrinsèque la trace d'un endomorphisme, nous introduisons la notion d'endomorphisme élémentaire, ce qui fait l'objet du § 4. Les endomorphismes élémentaires interviennent d'ailleurs dans toutes les questions d'algèbre linéaire qui se ramènent à l'étude d'endomorphismes de rang 1.

En fait, les notions précédentes trouvent leur cadre naturel dans la théorie des algèbres tensorielle, symétrique et extérieure d'un espace vectoriel, qui dépasse le niveau de cet ouvrage. Le lecteur intéressé par cette question pourra se reporter à [2], [3] ou [8]. Néanmoins, en vue de calcul différentiel extérieur, nous rassemblons dans le § 5 quelques notions élémentaires sur le calcul tensoriel et sur le calcul extérieur.

Enfin, dans le § 6, nous étendons les principaux résultats de ce chapitre au cas des modules sur un anneau commutatif unitaire. On peut alors les appliquer en particulier à l'étude des équations diophantiennes, qui est esquissée en exercice, et à celle des entiers algébriques (cf. chapitre III.3).

Dans ce chapitre, K désigne un corps commutatif.

§ 1. APPLICATIONS p -LINÉAIRES

Au § 2.5, nous avons défini les fonctions symétriques et antisymétriques, et décrit les méthodes de symétrisation et d'antisymétrisation des fonctions de n variables à valeurs dans un corps. Dans ce paragraphe, nous étudions le cas des applications multilinéaires à valeurs dans un espace vectoriel F , non nécessairement égal à K .

1. APPLICATIONS p -LINÉAIRES

DÉFINITION 3.1. — Applications p -linéaires. — Soient E et F deux espaces vectoriels sur K , et p un entier strictement positif. On appelle application p -linéaire sur E à valeurs dans F une application multilinéaire de E^p dans F .

Les applications p -linéaires sur E à valeurs dans F constituent un sous-espace vectoriel de l'espace vectoriel $\mathcal{F}(E^p, F)$ de toutes les applications de E^p dans F . Ce sous-espace vectoriel est noté $\mathcal{M}_p(E, F)$. Lorsque $p = 1$, $\mathcal{M}_p(E, F)$ n'est autre que $\mathcal{L}(E, F)$.

DÉFINITION 3.2. — Applications p -linéaires alternées. — Soient E et F deux espaces vectoriels sur K , et p un entier strictement positif. On dit qu'une application p -linéaire S sur E à valeurs dans F est alternée si pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de vecteurs de E contenant deux vecteurs égaux \mathbf{x}_i et \mathbf{x}_j , où $i \neq j$,

$$S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_i, \dots, \mathbf{x}_j, \dots, \mathbf{x}_p) = \mathbf{0}.$$

Les applications p -linéaires alternées sur E à valeurs dans F constituent un sous-espace vectoriel de $\mathcal{M}_p(E, F)$, noté $\mathcal{A}_p(E, F)$.

DÉFINITION 3.3. — Applications p -linéaires symétriques et antisymétriques. — Soient E et F deux espaces vectoriels sur K , et p un entier strictement positif. On dit qu'une application p -linéaire S sur E à valeurs dans F est :

— *symétrique si pour toute permutation σ appartenant à \mathfrak{S}_p , et pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de vecteurs de E ,*

$$(1) \quad S(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \dots, \mathbf{x}_{\sigma(p)}) = S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p);$$

— *antisymétrique si, dans les mêmes conditions,*

$$(2) \quad S(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \dots, \mathbf{x}_{\sigma(p)}) = \varepsilon(\sigma) \cdot S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p).$$

où $\varepsilon(\sigma)$ désigne la signature de la permutation σ .

Les applications p -linéaires symétriques sur E à valeurs dans F constituent un sous-espace vectoriel de $\mathcal{M}_p(E, F)$, noté $\mathcal{S}_p(E, F)$.

REMARQUE 1. — Soient E, F et G trois espaces vectoriels sur K , et A une application linéaire de F dans G . Alors, pour toute application S p -linéaire (resp. p -linéaire alternée, p -linéaire symétrique, p -linéaire antisymétrique) sur E à valeurs dans F , $A \circ S$ est une application p -linéaire (resp. p -linéaire alternée, etc.) sur E à valeurs dans G .

REMARQUE 2. — Lorsque l'entier p est égal à 1, on notera que toute application p -linéaire est à la fois symétrique, antisymétrique et alternée.

PROPOSITION 3.1. — Caractérisation des applications p -linéaires symétriques et antisymétriques. — *Soit p un entier strictement supérieur à 1. Pour qu'une application p -linéaire S sur E à valeurs dans F soit symétrique (resp. antisymétrique), il faut et il suffit que, pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de p vecteurs de E , et pour tout entier $i \in [1, p - 1]$,*

$$S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{i+1}, \mathbf{x}_i, \dots, \mathbf{x}_p) = S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_i, \mathbf{x}_{i+1}, \dots, \mathbf{x}_p) \\ (\text{resp. } S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{i+1}, \mathbf{x}_i, \dots, \mathbf{x}_p) = -S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_i, \mathbf{x}_{i+1}, \dots, \mathbf{x}_p)).$$

Ces formules expriment que les relations (1) et (2) sont vérifiées lorsque la permutation σ est une transposition élémentaire. Les conditions énoncées sont donc nécessaires; elles sont suffisantes, puisque toute permutation est un produit de transpositions élémentaires, et que, pour tout couple (σ, σ') d'éléments de \mathfrak{S}_p ,

$$\varepsilon(\sigma\sigma') = \varepsilon(\sigma) \cdot \varepsilon(\sigma').$$

PROPOSITION 3.2. — Caractérisation et propriétés des applications p -linéaires alternées. — *Soient p un entier strictement supérieur à 1, et S une application p -linéaire sur E à valeurs dans F .*

1. *Pour que S soit alternée, il faut et il suffit que, pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de vecteurs de E contenant deux vecteurs consécutifs \mathbf{x}_i et \mathbf{x}_{i+1} égaux,*

$$S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_i, \mathbf{x}_{i+1}, \dots, \mathbf{x}_p) = 0.$$

2. *Si S est alternée, S est antisymétrique.*

3. *Si S est alternée, on ne change pas la valeur de S sur une suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de vecteurs de E en ajoutant à l'un de ces vecteurs une combinaison linéaire des autres vecteurs.*

En particulier, si l'un des vecteurs $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p$ est une combinaison linéaire des autres, alors $S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = 0$.

Assertions 1 et 2. — Soient i un élément de $[1, p - 1]$, et S une application p -linéaire sur E à valeurs dans F satisfaisant à la condition de l'assertion 1. Considérons une suite (x_1, x_2, \dots, x_p) de vecteurs de E , et écrivons que

$$S(x_1, \dots, x_i + x_{i+1}, x_i + x_{i+1}, \dots, x_p) = 0.$$

En développant, nous obtenons la relation suivante :

$$S(x_1, \dots, x_i, x_i, \dots, x_p) + S(x_1, \dots, x_i, x_{i+1}, \dots, x_p) \\ + S(x_1, \dots, x_{i+1}, x_i, \dots, x_p) + S(x_1, \dots, x_{i+1}, x_{i+1}, \dots, x_p) = 0.$$

Le premier et le quatrième termes sont nuls par hypothèse. L'application p -linéaire S est donc antisymétrique (cf. prop. 1); l'assertion 2 est ainsi prouvée.

Pour montrer que S est alternée, considérons une suite (x_1, x_2, \dots, x_p) de vecteurs de E comportant deux vecteurs égaux x_i et x_j , où, par exemple, $i < j$, et prouvons que

$$S(x_1, x_2, \dots, x_i, \dots, x_j, \dots, x_p) = 0.$$

Écartons le cas trivial où $j = i + 1$, et transposons j et $i + 1$.

Puisque S est antisymétrique,

$$S(x_1, \dots, x_i, x_{i+1}, \dots, x_j, \dots, x_p) = -S(x_1, \dots, x_i, x_j, \dots, x_{i+1}, \dots, x_p).$$

Or, par hypothèse, le second membre est nul; d'où l'assertion 1.

Assertion 3. — Ajoutons au vecteur x_i une combinaison linéaire $\sum_{j \neq i} \alpha_j x_j$ des autres vecteurs, et développons

$$S(x_1, \dots, x_{i-1}, x_i + \sum_{j \neq i} \alpha_j x_j, x_{i+1}, \dots, x_p)$$

en utilisant la multilinéarité de S ; puisque S est alternée, nous voyons que le seul terme non nul est $S(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_p)$.

REMARQUE 1. — *Réciproquement, si le corps K est de caractéristique différente de 2, toute application p -linéaire S antisymétrique est alternée.*

Soit en effet (x_1, x_2, \dots, x_p) une famille de vecteurs de E comportant deux vecteurs égaux x_i et x_j , où $i \neq j$. L'antisymétrie de S entraîne la relation $2S(x_1, x_2, \dots, x_p) = 0$, d'où la conclusion.

REMARQUE 2. — Il découle aussitôt de l'assertion 3 que si E est un espace vectoriel de dimension n sur K , alors, pour tout entier $p > n$, $\mathcal{A}_p(E) = \{0\}$.

PROPOSITION 3.3. — **Autre caractérisation des applications p -linéaires alternées.** — *Soient E un espace vectoriel de dimension finie sur K , muni d'une base $B = (e_1, e_2, \dots, e_n)$, et S une application p -linéaire sur E à valeurs dans un*

espace vectoriel F . Pour que S soit alternée, il faut et il suffit que S satisfasse aux deux conditions suivantes :

- a) $S(e_{i_1}, e_{i_2}, \dots, e_{i_p}) = 0$ lorsque deux indices i_j et i_k sont égaux, $j \neq k$;
- b) $S(e_{i_1}, e_{i_2}, \dots, e_{i_p})$ est changé en son opposé lorsqu'on transpose deux vecteurs e_{i_j} et e_{i_k} , où $j \neq k$.

La condition a) est évidemment nécessaire, et la condition b) l'est aussi, d'après l'assertion 2 de la proposition 3.2.

Réciproquement, soit S une application p -linéaire sur E à valeurs dans F satisfaisant aux conditions a) et b). Considérons une famille (x_1, x_2, \dots, x_p) de vecteurs de E comportant deux vecteurs égaux x_i et x_j , où $i \neq j$. Pour calculer $S(x_1, x_2, \dots, x_p)$, développons pour tout entier $k \in [1, p]$ le vecteur x_k dans la base B :

$$x_k = \sum_{h=1}^n \xi_{hk} e_h.$$

Calculons d'abord $S(e_{i_1}, \dots, x_{i_s}, \dots, x_j, \dots, e_{i_p})$, où i_1, \dots, i_p sont des entiers appartenant à l'intervalle $[1, n]$. D'après la multilinéarité de S , nous voyons que

$$S(e_{i_1}, \dots, x_{i_s}, \dots, x_j, \dots, e_{i_p}) = \sum_{l,m} \xi_{li} \cdot \xi_{mj} S(e_{i_1}, \dots, e_l, \dots, e_m, \dots, e_{i_p}).$$

Dans cette somme, distinguons deux sortes de termes : ceux tels que $l = m$ sont nuls d'après la condition a); ceux tels que $l \neq m$ sont deux à deux opposés, d'après la condition b). La somme considérée est donc nulle.

Par linéarité par rapport aux vecteurs d'indice différent de i et de j , nous en concluons que $S(x_1, \dots, x_{i_s}, \dots, x_j, \dots, x_p) = 0$.

PROPOSITION 3.4. — Extension d'une application linéaire. — Soient E , E' et F trois espaces vectoriels sur K , et U une application linéaire de E' dans E .

1. Pour toute application p -linéaire S sur E à valeurs dans F , l'application S_U de E'^p dans F définie par la formule

$$S_U(x_1, x_2, \dots, x_p) = S(U(x_1), U(x_2), \dots, U(x_p))$$

est une application p -linéaire sur E' à valeurs dans F .

2. L'application U_p qui à tout élément S de $\mathcal{M}_p(E, F)$ associe S_U est une application linéaire de $\mathcal{M}_p(E, F)$ dans $\mathcal{M}_p(E', F)$. L'image par U_p de $\mathcal{S}_p(E, F)$ est contenue dans $\mathcal{S}_p(E', F)$; autrement dit, si S est une application p -linéaire symétrique sur E à valeurs dans F , S_U est une application p -linéaire symétrique sur E' à valeurs dans F . De même, l'image par U_p de $\mathcal{A}_p(E, F)$ est contenue dans $\mathcal{A}_p(E', F)$; autrement dit, si S est une application p -linéaire alternée sur E à valeurs dans F , S_U est une application p -linéaire alternée sur E' à valeurs dans F .

3. Soient E'' un espace vectoriel sur K , et V une application linéaire de E'' dans E' . Alors, pour tout entier p strictement positif,

$$(U \circ V)_p = V_p \circ U_p.$$

4. Lorsque U est l'homothétie de rapport α dans l'espace vectoriel E , l'application linéaire U_p n'est autre que l'homothétie de rapport α^p dans l'espace vectoriel $\mathcal{M}_p(E, F)$.

Les assertions 1 et 2 sont immédiates; l'assertion 3 résulte aussitôt de la formule $S_{U \circ V} = (S_U)_V$. Enfin, l'assertion 4 découle de la formule suivante :

$$S_{\alpha U}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \alpha^p \cdot S_U(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p).$$

REMARQUE. — Lorsque $p = 1$ et $F = K$, l'application linéaire U_p de $\mathcal{M}_p(E, F) = E^*$ dans $\mathcal{M}_p(E', F) = E'^*$ n'est autre que l'application transposée tU de l'application linéaire U .

Voici maintenant une méthode générale de construction d'applications multilinéaires symétriques et d'applications multilinéaires alternées :

PROPOSITION 3.5. — Symétrisation et antisymétrisation d'une application p -linéaire. — Soient E et F deux espaces vectoriels sur K , p un entier strictement positif, \mathfrak{S}_p le groupe des permutations de $[1, p]$ et S une application p -linéaire sur E à valeurs dans F .

1. L'application $M(S)$ de E^p dans F définie par la formule

$$(1) \quad M(S)(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \sum_{\sigma \in \mathfrak{S}_p} S(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \dots, \mathbf{x}_{\sigma(p)})$$

est une application p -linéaire symétrique sur E à valeurs dans F .

De plus, l'application M qui à tout élément S de $\mathcal{M}_p(E, F)$ associe $M(S)$ est une application linéaire de $\mathcal{M}_p(E, F)$ dans $\mathfrak{S}_p(E, F)$ et, pour tout élément S de $\mathcal{M}_p(E, F)$,

$$M^2(S) = p! M(S).$$

L'application $M(S)$ s'appelle symétrisée de S , et l'application M opérateur de symétrisation. En particulier, lorsque K est de caractéristique zéro, l'application $\frac{1}{p!} M$ est un projecteur de $\mathcal{M}_p(E, F)$, dont l'image est $\mathfrak{S}_p(E, F)$.

2. L'application $A(S)$ de E^p dans F définie par la formule

$$(2) \quad A(S)(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) S(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \dots, \mathbf{x}_{\sigma(p)})$$

est une application p -linéaire alternée sur E à valeurs dans F .

De plus, l'application A qui à tout élément S de $\mathcal{M}_p(E, F)$ associe $A(S)$ est une application linéaire de $\mathcal{M}_p(E, F)$ dans $\mathcal{A}_p(E, F)$ et, pour tout élément S de $\mathcal{M}_p(E, F)$,

$$A^2(S) = p! A(S).$$

L'application $A(S)$ s'appelle antisymétrisée de S , et l'application A opérateur d'antisymétrisation. En particulier, lorsque K est de caractéristique zéro, l'application $\frac{1}{p!} A$ est un projecteur de $\mathcal{M}_p(E, F)$, dont l'image est $\mathcal{A}_p(E, F)$.

Assertion 1. — Soit σ_0 un élément de \mathfrak{S}_p . Alors

$$M(S)(\mathbf{x}_{\sigma_0(1)}, \mathbf{x}_{\sigma_0(2)}, \dots, \mathbf{x}_{\sigma_0(p)}) = \sum_{\sigma \in \mathfrak{S}_p} S(\mathbf{x}_{\sigma_0\sigma(1)}, \mathbf{x}_{\sigma_0\sigma(2)}, \dots, \mathbf{x}_{\sigma_0\sigma(p)}).$$

Comme l'application $\sigma \mapsto \sigma_0\sigma$ est une bijection de \mathfrak{S}_p sur lui-même, il en résulte que

$$M(S)(\mathbf{x}_{\sigma_0(1)}, \mathbf{x}_{\sigma_0(2)}, \dots, \mathbf{x}_{\sigma_0(p)}) = M(S)(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p),$$

ce qui prouve que $M(S)$ est symétrique.

Il est immédiat que l'application M est linéaire. Pour démontrer que $M^2(S) = p! M(S)$, il suffit de prouver que si T est une application p -linéaire symétrique sur E à valeurs dans F , alors $M(T) = p! T$, ce qui découle aussitôt de la formule (1).

Lorsque K est de caractéristique zéro, la formule $M(T) = p! T$ peut encore s'écrire $T = \frac{1}{p!} M(T)$, ce qui montre que $\frac{1}{p!} M$ est un projecteur.

Assertion 2. — Soit $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ une famille d'éléments de E comportant deux vecteurs égaux \mathbf{x}_i et \mathbf{x}_j , où $i \neq j$. Nous allons prouver que

$$A(S)(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = 0.$$

Désignons par σ_0 la transposition qui échange i et j , et par \mathfrak{A}_p le groupe alterné de degré p . Nous savons (cf. prop. I.2.31) que les classes à gauche \mathfrak{A}_p et $\sigma_0\mathfrak{A}_p$ constituent une partition de \mathfrak{S}_p . Donc

$$\begin{aligned} A(S)(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) \\ = \sum_{\sigma \in \mathfrak{A}_p} \varepsilon(\sigma) [S(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \dots, \mathbf{x}_{\sigma(p)}) - S(\mathbf{x}_{\sigma_0\sigma(1)}, \mathbf{x}_{\sigma_0\sigma(2)}, \dots, \mathbf{x}_{\sigma_0\sigma(p)})]. \end{aligned}$$

Tous les termes de cette somme sont nuls car, pour tout entier k appartenant à $[1, p]$, $\mathbf{x}_{\sigma_0\sigma(k)} = \mathbf{x}_{\sigma(k)}$. En effet,

- ou bien $\sigma(k) = i$, et $\mathbf{x}_{\sigma_0\sigma(k)} = \mathbf{x}_j = \mathbf{x}_i = \mathbf{x}_{\sigma(k)}$;
- ou bien $\sigma(k) = j$, et $\mathbf{x}_{\sigma_0\sigma(k)} = \mathbf{x}_i = \mathbf{x}_j = \mathbf{x}_{\sigma(k)}$;
- ou bien $\sigma(k)$ est différent de i et de j , et $\sigma_0\sigma(k) = \sigma(k)$.

Ainsi, l'application $A(S)$ est alternée.

La démonstration s'achève comme dans le cas des applications p -linéaires symétriques.

2. FORMES p -LINÉAIRES

Nous allons maintenant compléter les résultats précédents lorsque $F = K$.

DÉFINITION 3.4. — Formes p -linéaires. — Soient E un espace vectoriel sur K , et p un entier strictement positif. On appelle *forme p -linéaire* (resp. *p -linéaire alternée*, *p -linéaire symétrique*, *p -linéaire antisymétrique*) sur l'espace vecto-

riel E , une application p -linéaire (resp. p -linéaire alternée, p -linéaire symétrique, p -linéaire antisymétrique) sur E à valeurs dans K .

Dans toute la suite, nous noterons $\mathcal{M}_p(E)$ l'espace vectoriel des formes p -linéaires sur E , $\mathcal{S}_p(E)$ le sous-espace vectoriel de $\mathcal{M}_p(E)$ constitué des formes p -linéaires symétriques sur E , et $\mathcal{A}_p(E)$ le sous-espace vectoriel de $\mathcal{M}_p(E)$ constitué des formes p -linéaires alternées sur E .

Lorsque $p = 1$, $\mathcal{M}_p(E)$, $\mathcal{S}_p(E)$ et $\mathcal{A}_p(E)$ ne sont autres que l'espace dual E^* de E .

Voici un procédé fort important de construction de formes p -linéaires, de formes p -linéaires symétriques et de formes p -linéaires alternées :

DÉFINITION 3.5. — Produit tensoriel, produit symétrique et produit extérieur de formes p -linéaires. — Soient E un espace vectoriel sur K , p un entier strictement positif et $(y_1^*, y_2^*, \dots, y_p^*)$ une famille de p éléments de E^* .

1. L'application f de E^p dans K définie par la formule

$$f(x_1, x_2, \dots, x_p) = \langle y_1^*, x_1 \rangle \langle y_2^*, x_2 \rangle \dots \langle y_p^*, x_p \rangle \\ = (y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*)(x_1, x_2, \dots, x_p)$$

est une forme p -linéaire sur E , qu'on appelle produit tensoriel des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$, et qu'on note $y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$.

Ainsi, par définition :

$$(1) (y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*)(x_1, x_2, \dots, x_p) = \langle y_1^*, x_1 \rangle \langle y_2^*, x_2 \rangle \dots \langle y_p^*, x_p \rangle.$$

2. L'application $M(f)$ symétrisée de f est une forme p -linéaire symétrique sur E , qu'on appelle produit symétrique des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$ et qu'on note $y_1^* \cdot y_2^* \dots y_p^*$.

Ainsi, par définition,

$$(2) (y_1^* \cdot y_2^* \dots y_p^*)(x_1, x_2, \dots, x_p) = M(f)(x_1, \dots, x_p) \\ = \sum_{\sigma \in \mathfrak{S}_p} \langle y_1^*, x_{\sigma(1)} \rangle \langle y_2^*, x_{\sigma(2)} \rangle \dots \langle y_p^*, x_{\sigma(p)} \rangle.$$

Autrement dit,

$$(3) y_1^* \cdot y_2^* \dots y_p^* = M(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*).$$

3. L'application $A(f)$ antisymétrisée de f est une forme p -linéaire alternée sur E , qu'on appelle produit extérieur des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$, et qu'on note $y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*$.

Ainsi, par définition :

$$(4) (y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*)(x_1, x_2, \dots, x_p) = A(f)(x_1, \dots, x_p) \\ = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \langle y_1^*, x_{\sigma(1)} \rangle \langle y_2^*, x_{\sigma(2)} \rangle \dots \langle y_p^*, x_{\sigma(p)} \rangle.$$

Autrement dit,

$$(5) \quad y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* = A(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*).$$

On dit qu'une forme p -linéaire S est un élément *décomposable* de $\mathcal{M}_p(E)$ s'il existe une suite $(y_1^*, y_2^*, \dots, y_p^*)$ de formes linéaires telle que

$$S = y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*.$$

On définit de même les éléments décomposables de $\mathcal{P}_p(E)$ et de $\mathcal{A}_p(E)$.

PROPOSITION 3.6. — Propriétés des produits tensoriel, symétrique et extérieur. Soient E un espace vectoriel sur K , et p un entier strictement positif.

1. L'application qui à tout élément $(y_1^*, y_2^*, \dots, y_p^*)$ de $(E^*)^p$ associe le produit tensoriel $y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$ est une application p -linéaire sur E^* à valeurs dans $\mathcal{M}_p(E)$.

2. L'application qui à tout élément $(y_1^*, y_2^*, \dots, y_p^*)$ de $(E^*)^p$ associe le produit symétrique $y_1^* \cdot y_2^* \dots y_p^*$ est une application p -linéaire symétrique sur E^* à valeurs dans $\mathcal{P}_p(E)$.

Plus précisément, soient (x_1, x_2, \dots, x_p) une suite d'éléments de E , et S la forme p -linéaire sur E^* définie par la formule

$$S(y_1^*, y_2^*, \dots, y_p^*) = (y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*)(x_1, x_2, \dots, x_p).$$

Alors

$$(6) \quad M(S)(y_1^*, y_2^*, \dots, y_p^*) = (y_1^* \cdot y_2^* \dots y_p^*)(x_1, x_2, \dots, x_p).$$

3. L'application qui à tout élément $(y_1^*, y_2^*, \dots, y_p^*)$ de $(E^*)^p$ associe le produit extérieur $y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*$ est une application p -linéaire alternée sur E^* à valeurs dans $\mathcal{A}_p(E)$.

Plus précisément, soient (x_1, x_2, \dots, x_p) une suite d'éléments de E , et S la forme p -linéaire sur E^* définie par la formule

$$S(y_1^*, y_2^*, \dots, y_p^*) = (y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*)(x_1, x_2, \dots, x_p).$$

Alors

$$(7) \quad A(S)(y_1^*, y_2^*, \dots, y_p^*) = (y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*)(x_1, x_2, \dots, x_p).$$

L'assertion 1 découle aussitôt de la formule (1).

Assertion 2. — Notons d'abord que, d'après la proposition 3.5, $y_1^* \cdot y_2^* \dots y_p^*$ est un élément de $\mathcal{P}_p(E)$. De plus, l'application

$$(y_1^*, y_2^*, \dots, y_p^*) \mapsto y_1^* \cdot y_2^* \dots y_p^*$$

est p -linéaire, car elle est la composée de l'application p -linéaire

$$(y_1^*, y_2^*, \dots, y_p^*) \mapsto y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$$

et de l'application linéaire M .

Enfin, pour démontrer la formule (6), écrivons que

$$M(S)(y_1^*, y_2^*, \dots, y_p^*) = \sum_{\sigma \in \mathfrak{S}_p} \langle y_{\sigma(1)}^*, x_1 \rangle \langle y_{\sigma(2)}^*, x_2 \rangle \dots \langle y_{\sigma(p)}^*, x_p \rangle.$$

Pour tout élément σ de \mathfrak{S}_p ,

$$\prod_{i=1}^p \langle y_{\sigma(i)}^*, x_i \rangle = \prod_{j=1}^p \langle y_j^*, x_{\sigma^{-1}(j)} \rangle,$$

car σ est une bijection de $[1, p]$ sur lui-même. Comme l'application $\sigma \mapsto \sigma^{-1}$ est une bijection de \mathfrak{S}_p sur lui-même, la formule précédente s'écrit encore

$$M(S)(y_1^*, y_2^*, \dots, y_p^*) = \sum_{\tau \in \mathfrak{S}_p} \langle y_1^*, x_{\tau(1)} \rangle \langle y_2^*, x_{\tau(2)} \rangle \dots \langle y_p^*, x_{\tau(p)} \rangle,$$

donc

$$M(S)(y_1^*, y_2^*, \dots, y_p^*) = (y_1^* \cdot y_2^* \dots y_p^*)(x_1, x_2, \dots, x_p),$$

ce qu'il fallait prouver.

Assertion 3. — La démonstration est calquée sur celle de l'assertion 2, compte tenu du fait que, pour toute permutation σ , $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

COROLLAIRE. — **Cas des formes p -linéaires alternées.** — Soient E un espace vectoriel sur K , et p un entier strictement positif.

1. Pour toute famille $(y_1^*, \dots, y_{i-1}^*, y_{i+1}^*, \dots, y_p^*)$ d'éléments de E^* , pour tout couple $(y_i'^*, y_i''^*)$ d'éléments de E^* , et pour tout couple (α, β) d'éléments de K ,

$$\begin{aligned} (8) \quad y_1^* \wedge \dots \wedge y_{i-1}^* \wedge (\alpha y_i'^* + \beta y_i''^*) \wedge y_{i+1}^* \wedge \dots \wedge y_p^* \\ = \alpha (y_1^* \wedge \dots \wedge y_{i-1}^* \wedge y_i'^* \wedge y_{i+1}^* \wedge \dots \wedge y_p^*) \\ + \beta (y_1^* \wedge \dots \wedge y_{i-1}^* \wedge y_i''^* \wedge y_{i+1}^* \wedge \dots \wedge y_p^*). \end{aligned}$$

2. Soit $(y_1^*, y_2^*, \dots, y_p^*)$ une famille d'éléments de E^* . On ne change pas la valeur de $y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*$ en ajoutant à l'une de ces formes linéaires une combinaison linéaire des autres.

En particulier, si l'un de ces éléments de E^* est une combinaison linéaire des autres, alors :

$$y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* = 0.$$

3. Pour toute famille $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* , et pour toute permutation σ de $[1, p]$,

$$(9) \quad y_{\sigma(1)}^* \wedge y_{\sigma(2)}^* \wedge \dots \wedge y_{\sigma(p)}^* = \varepsilon(\sigma) \cdot (y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*).$$

PROPOSITION 3.7. — **Transposition.** — Soient E et F deux espaces vectoriels sur K , U une application linéaire de E dans F , tU sa transposée, et p un entier

strictement positif. Pour toute suite (x_1, x_2, \dots, x_p) d'éléments de E , et pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de F^* ,

$$(10) \quad [{}^tU(y_1^*) \otimes \dots \otimes {}^tU(y_p^*)](x_1, \dots, x_p) = (y_1^* \otimes \dots \otimes y_p^*)[U(x_1), \dots, U(x_p)]$$

$$(11) \quad [{}^tU(y_1^*) \dots {}^tU(y_p^*)](x_1, \dots, x_p) = (y_1^* \dots y_p^*)[U(x_1), \dots, U(x_p)]$$

$$(12) \quad [{}^tU(y_1^*) \wedge \dots \wedge {}^tU(y_p^*)](x_1, \dots, x_p) = (y_1^* \wedge \dots \wedge y_p^*)[U(x_1), \dots, U(x_p)].$$

Autrement dit, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de F^* ,

$$(10') \quad U_p(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = {}^tU(y_1^*) \otimes {}^tU(y_2^*) \otimes \dots \otimes {}^tU(y_p^*)$$

$$(11') \quad U_p(y_1^* \cdot y_2^* \dots y_p^*) = {}^tU(y_1^*) \cdot {}^tU(y_2^*) \dots {}^tU(y_p^*)$$

$$(12') \quad U_p(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*) = {}^tU(y_1^*) \wedge {}^tU(y_2^*) \wedge \dots \wedge {}^tU(y_p^*).$$

Les formules (10), (11) et (12) résultent aussitôt des formules (1), (2) et (4), et de l'identité fondamentale de la transposition.

3. DÉVELOPPEMENT DES APPLICATIONS p -LINÉAIRES

THÉORÈME 3.1. — Développement des applications p -linéaires. — Soient E un espace vectoriel de dimension finie non nulle n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , p un entier strictement positif, et \mathcal{F} l'ensemble des applications de $[1, p]$ dans $[1, n]$. Pour tout élément χ de \mathcal{F} , on désigne par e_χ l'élément de $\mathcal{M}_p(E)$ défini par la formule

$$(1) \quad e_\chi = e_{\chi(1)}^* \otimes e_{\chi(2)}^* \otimes \dots \otimes e_{\chi(p)}^*.$$

1. La forme multilinéaire e_χ satisfait à la condition suivante : pour tout élément ψ de \mathcal{F} ,

$$\begin{aligned} e_\chi(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)}) &= 1 && \text{si } \psi = \chi \\ &= 0 && \text{si } \psi \neq \chi. \end{aligned}$$

Si l'on considère une suite (x_1, x_2, \dots, x_p) de vecteurs de E , et que l'on évalue ces vecteurs dans la base B :

$$x_j = \sum_{i=1}^n \xi_{ij} e_i,$$

alors

$$(2) \quad e_\chi(x_1, x_2, \dots, x_p) = \xi_{\chi(1),1} \xi_{\chi(2),2} \dots \xi_{\chi(p),p}.$$

2. La forme p -linéaire e_χ est l'unique forme p -linéaire sur E prenant la valeur 1 sur $(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)})$ et la valeur 0 sur $(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)})$ pour tout élément ψ de \mathcal{F} différent de χ .

3. Soit S une application p -linéaire sur E à valeurs dans un espace vectoriel F sur K . Alors, pour tout élément $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ de E^p ,

$$(3) \quad S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \sum_{\chi \in \mathcal{F}} e_{\chi}(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) \cdot s_{\chi},$$

où s_{χ} est le vecteur de F défini par la formule :

$$s_{\chi} = S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)}).$$

L'assertion 1 résulte aussitôt de la définition de e_{χ} .

Assertions 2 et 3.

a) Soit S une application p -linéaire sur E à valeurs dans F ; alors :

$$(4) \quad S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} \dots \sum_{i_p=1}^{n_p} \xi_{i_1,1} \cdot \xi_{i_2,2} \dots \xi_{i_p,p} \cdot S(e_{i_1}, e_{i_2}, \dots, e_{i_p}).$$

Désignons par χ l'application de $[1, p]$ dans \mathbf{N} définie par la formule $\chi(j) = i_j$. La formule (4) s'écrit encore :

$$(5) \quad S(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \sum_{\chi \in \mathcal{F}} \xi_{\chi(1),1} \cdot \xi_{\chi(2),2} \dots \xi_{\chi(p),p} \cdot S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)}).$$

b) Cette dernière formule montre que e_{χ} est l'unique forme p -linéaire f sur E telle que

$$\begin{aligned} f(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)}) &= 1 && \text{si } \psi = \chi \\ &= 0 && \text{si } \psi \neq \chi. \end{aligned}$$

c) La formule (3) est une conséquence immédiate des formules (2) et (5).

Dans tous les corollaires, on conserve les mêmes notations.

COROLLAIRE 1. — Détermination d'une application p -linéaire. — Pour toute famille $(s_{\chi})_{\chi \in \mathcal{F}}$ d'éléments de F , il existe une application p -linéaire S et une seule sur E à valeurs dans F telle que, pour tout élément χ de \mathcal{F} ,

$$S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)}) = s_{\chi}.$$

On peut encore exprimer l'unicité de S de la manière suivante :

Pour que deux applications p -linéaires S et T sur E à valeurs dans F soient égales, il faut et il suffit que, pour tout élément $(\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_p)$ de B^p ,

$$S(\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_p) = T(\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_p).$$

L'unicité de S résulte aussitôt de la formule (3); l'existence de S résulte encore de la formule (3), jointe à l'assertion 1.

Appliquons maintenant les résultats précédents au cas des formes p -linéaires :

COROLLAIRE 2. — Produits tensoriels de bases. — Soit $B = (e_1, e_2, \dots, e_n)$ une base de l'espace vectoriel E . Alors les éléments $e_{\chi(1)}^* \otimes e_{\chi(2)}^* \otimes \dots \otimes e_{\chi(p)}^*$, où χ parcourt l'ensemble \mathcal{F} des applications de $[1, p]$ dans $[1, n]$, constituent une base de l'espace vectoriel $\mathcal{M}_p(E)$ des formes p -linéaires sur E , dite canoniquement associée à la base B de E . Lorsque $p = 1$, cette base n'est autre que la base duale de la base B .

La formule (3) montre aussitôt que la famille $(e_\chi)_{\chi \in \mathcal{F}}$ est une famille génératrice de $\mathcal{M}_p(E)$. Cette famille est libre, car l'assertion 1 du théorème précédent prouve que toute relation linéaire entre les vecteurs de cette famille est triviale.

COROLLAIRE 3. — Dimension de l'espace vectoriel $\mathcal{M}_p(E)$. — L'espace vectoriel $\mathcal{M}_p(E)$ des formes p -linéaires sur un espace vectoriel E de dimension n est de dimension n^p .

COROLLAIRE 4. — Formes p -linéaires décomposables. — Les formes p -linéaires décomposables constituent une partie génératrice de l'espace vectoriel $\mathcal{M}_p(E)$.

REMARQUE. — Ce corollaire est d'une grande importance, car il permet de ramener la plupart des problèmes concernant les formes multilinéaires à des problèmes concernant les produits tensoriels de formes linéaires.

COROLLAIRE 5. — Produits tensoriels de parties libres, ou génératrices. — Soit S une partie libre (resp. génératrice) de l'espace vectoriel E^* ; alors les formes p -linéaires sur E du type $y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$, où, pour tout $j \in [1, p]$, $y_j^* \in S$, constituent une partie libre (resp. génératrice) de l'espace vectoriel $\mathcal{M}_p(E)$.

En effet, si S est génératrice, nous pouvons extraire de S une base B' de E^* ; si S est libre, nous pouvons compléter S en une base B' de E^* . D'après le théorème I.3.9, il existe une base B de E et une seule dont B' soit la base duale. Le corollaire 5 est alors une conséquence immédiate du corollaire 2.

On trouvera la propriété universelle de l'espace vectoriel $\mathcal{M}_p(E)$ dans l'exercice 21.

4. DÉVELOPPEMENT DES APPLICATIONS p -LINÉAIRES ALTERNÉES

THÉORÈME 3.2. — Développement des applications p -linéaires alternées. — Soient E un espace vectoriel de dimension finie non nulle n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , p un entier strictement positif inférieur ou égal à n , \mathcal{E} l'ensemble des applications strictement croissantes de $[1, p]$ dans $[1, n]$, et \mathcal{I} l'ensemble des parties de l'intervalle $[1, n]$ ayant p éléments.

On sait que l'application de \mathcal{E} dans \mathcal{I} qui à tout élément φ de \mathcal{E} associe la

partie $\varphi([1, p])$ est une bijection de \mathcal{E} sur \mathcal{I} ; pour tout élément P de \mathcal{I} , on désigne par e_P l'élément de $\mathcal{A}_p(E)$ défini par la formule :

$$(1) \quad e_P = e_{\varphi(1)}^* \wedge e_{\varphi(2)}^* \wedge \dots \wedge e_{\varphi(p)}^*,$$

où φ désigne l'application strictement croissante de $[1, p]$ dans $[1, n]$ définie par P .

1. La forme p -linéaire alternée e_P satisfait à la condition suivante : pour toute application ψ strictement croissante de $[1, p]$ dans $[1, n]$, le scalaire $e_P(e_{\psi(1)}^*, e_{\psi(2)}^*, \dots, e_{\psi(p)}^*)$ est égal à 1 si $\psi = \varphi$, et à 0 si $\psi \neq \varphi$.

Si l'on considère une suite $(x_1, x_2, \dots, x_j, \dots, x_p)$ de vecteurs de E , et si l'on évalue les vecteurs x_j dans la base B :

$$x_j = \sum_{i=1}^n \xi_{ij} e_i,$$

alors

$$(2) \quad \begin{aligned} e_P(x_1, x_2, \dots, x_p) &= \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \langle e_{\varphi(1)}^*, x_{\sigma(1)} \rangle \langle e_{\varphi(2)}^*, x_{\sigma(2)} \rangle \dots \langle e_{\varphi(p)}^*, x_{\sigma(p)} \rangle \\ &= \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \xi_{\varphi(1), \sigma(1)} \xi_{\varphi(2), \sigma(2)} \dots \xi_{\varphi(p), \sigma(p)}. \end{aligned}$$

2. La forme p -linéaire alternée e_P est l'unique forme p -linéaire alternée sur E prenant la valeur 1 sur $(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)})$, et la valeur 0 sur $(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)})$ pour tout élément ψ de \mathcal{E} différent de φ .

La valeur de e_P sur (x_1, x_2, \dots, x_p) est encore donnée par la formule

$$(2') \quad e_P(x_1, x_2, \dots, x_p) = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \xi_{\varphi \circ \sigma(1), 1} \xi_{\varphi \circ \sigma(2), 2} \dots \xi_{\varphi \circ \sigma(p), p}.$$

3. Soit S une application p -linéaire alternée sur E à valeurs dans un espace vectoriel F sur K . Alors, pour tout élément (x_1, x_2, \dots, x_p) de E^p ,

$$(3) \quad S(x_1, x_2, \dots, x_p) = \sum_{P \in \mathcal{I}} e_P(x_1, x_2, \dots, x_p) \cdot s_P,$$

où s_P est le vecteur de F défini par la formule :

$$s_P = S(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)}),$$

φ désignant l'application strictement croissante de $[1, p]$ dans $[1, n]$ définie par la partie P .

Assertion 1. — La formule (1) résulte aussitôt de la définition du produit extérieur $e_P = e_{\varphi(1)}^* \wedge e_{\varphi(2)}^* \wedge \dots \wedge e_{\varphi(p)}^*$.

Soit maintenant ψ une application strictement croissante de $[1, p]$ dans $[1, n]$. Désignons par Q la partie $\psi([1, p])$; la formule (1) montre que

$$e_P(e_{\psi(1)}, \dots, e_{\psi(j)}, \dots, e_{\psi(p)}) = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \alpha_{\sigma},$$

où, pour tout $\sigma \in \mathfrak{S}_p$, le scalaire α_σ est donné par la formule :

$$\alpha_\sigma = \langle e_{\varphi(1)}^*, e_{\psi \circ \sigma(1)} \rangle \dots \langle e_{\varphi(j)}^*, e_{\psi \circ \sigma(j)} \rangle \dots \langle e_{\varphi(p)}^*, e_{\psi \circ \sigma(p)} \rangle.$$

— Ou bien $Q \neq P$; alors $\psi \circ \sigma([1, p]) = \psi([1, p]) = Q \neq P$. Il existe donc au moins un élément j de $[1, p]$ tel que $\varphi(j) \neq \psi \circ \sigma(j)$; par suite $\alpha_\sigma = 0$, pour tout élément σ de \mathfrak{S}_p . Finalement, il en découle que

$$e_P(e_{\psi(1)}, \dots, e_{\psi(j)}, \dots, e_{\psi(p)}) = 0, \quad \text{si } \psi \neq \varphi.$$

— Ou bien $Q = P$, c'est-à-dire $\psi = \varphi$; distinguons alors deux cas :

a) La permutation σ n'est pas l'identité. Il existe donc au moins un élément j de $[1, p]$ tel que $\sigma(j) \neq j$; par suite $\varphi(j) \neq \varphi \circ \sigma(j)$, et $\alpha_\sigma = 0$.

b) La permutation σ est l'identité. Il est alors évident que $\alpha_\sigma = 1$.

Finalement, il en découle que $e_P(e_{\varphi(1)}, \dots, e_{\varphi(j)}, \dots, e_{\varphi(p)}) = 1$.

Assertions 2 et 3.

a) Soit S une application p -linéaire alternée sur E à valeurs dans l'espace vectoriel F . Puisque S est une application p -linéaire sur E à valeurs dans F , nous pouvons écrire (cf. th. 3.1):

$$(4) \quad S(x_1, x_2, \dots, x_p) = \sum_{\chi \in \mathcal{F}} e_\chi(x_1, x_2, \dots, x_p) s_\chi,$$

où χ parcourt l'ensemble \mathcal{F} de toutes les applications de $[1, p]$ dans $[1, n]$, et où s_χ est le vecteur de F défini par la formule :

$$s_\chi = S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)}).$$

Du fait que l'application p -linéaire S est alternée, deux cas se présentent :

— Ou bien χ n'est pas injective; alors $s_\chi = S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)})$ est nul.

— Ou bien χ est injective; posons $P = \chi([1, p])$, et désignons par φ l'application strictement croissante de $[1, p]$ dans $[1, n]$ définie par P . Il existe alors un élément σ et un seul de \mathfrak{S}_p tel que $\chi = \varphi \circ \sigma$. Il en résulte que

$$S(e_{\chi(1)}, e_{\chi(2)}, \dots, e_{\chi(p)}) = \varepsilon(\sigma) S(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)}),$$

c'est-à-dire que

$$s_\chi = \varepsilon(\sigma) s_P.$$

La formule (4) peut donc encore s'écrire :

$$(5) \quad S(x_1, x_2, \dots, x_p) = \sum_{P \in \mathcal{P}} e'_P(x_1, x_2, \dots, x_p) \cdot s_P,$$

où e'_p est la forme p -linéaire sur E définie par la formule :

$$\begin{aligned} e'_p(x_1, x_2, \dots, x_p) &= \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) e_{\varphi \circ \sigma}(x_1, x_2, \dots, x_p) \\ &= \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \langle e_{\varphi \circ \sigma(1)}^*, x_1 \rangle \langle e_{\varphi \circ \sigma(2)}^*, x_2 \rangle \dots \langle e_{\varphi \circ \sigma(p)}^*, x_p \rangle \\ &= \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma) \xi_{\varphi \circ \sigma(1), 1} \xi_{\varphi \circ \sigma(2), 2} \dots \xi_{\varphi \circ \sigma(p), p}. \end{aligned}$$

b) La formule (5) prouve l'unicité d'une forme p -linéaire alternée f sur E telle que, étant donnée une partie P de $[1, n]$ ayant p éléments, $f(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)})$ soit égal à 1 si $\psi([1, p]) = P$, et à 0 si $\psi([1, p]) \neq P$: une telle forme f est nécessairement égale à e'_p . Or, nous savons qu'une telle forme existe, à savoir e_p (cf. assertion 1). L'assertion 2 en résulte, ainsi que la formule (2').

c) La formule (3) est maintenant une conséquence immédiate de la formule (5) et de l'égalité $e_p = e'_p$, valable pour toute partie P de $[1, n]$ ayant p éléments.

Dans tous les corollaires, on conserve les mêmes notations.

COROLLAIRE 1. — Détermination d'une application p -linéaire alternée. Pour toute famille $(s_P)_{P \in \mathfrak{F}}$ d'éléments de l'espace vectoriel F , il existe une application p -linéaire alternée S et une seule sur E à valeurs dans F telle que pour tout élément P de \mathfrak{F} ,

$$S(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)}) = s_P,$$

où φ désigne l'application strictement croissante de $[1, p]$ dans $[1, n]$ associée à la partie P .

L'unicité de S résulte aussitôt de la formule (3); l'existence de S résulte encore de la formule (3), jointe à l'assertion 1.

Appliquons maintenant les résultats précédents au cas des formes p -linéaires alternées :

COROLLAIRE 2. — Produits extérieurs de bases. — Soit $B = (e_1, e_2, \dots, e_n)$ une base de l'espace vectoriel E . Alors les éléments e_P , où P parcourt l'ensemble \mathfrak{F} des parties de $[1, n]$ ayant p éléments, constituent une base de l'espace vectoriel $\mathcal{A}_p(E)$ des formes p -linéaires alternées sur E , dite canoniquement associée à la base B de E .

La formule (3) montre aussitôt que la famille $(e_P)_{P \in \mathfrak{F}}$ est une famille génératrice de $\mathcal{A}_p(E)$. Cette famille est libre, car l'assertion 2 du théorème précédent prouve que toute relation linéaire entre les vecteurs de cette famille est triviale.

COROLLAIRE 3. — Dimension de l'espace vectoriel $\mathcal{A}_p(E)$. — Soient E un espace vectoriel de dimension n sur K , et p un entier strictement positif. Alors

l'espace vectoriel $\mathcal{A}_p(E)$ des formes p -linéaires alternées sur E est de dimension C_n^p lorsque $p \leq n$, et de dimension 0 lorsque $p > n$.

En effet, l'ensemble \mathcal{I} des parties de $[1, n]$ ayant p éléments est fini, et a pour cardinal C_n^p lorsque $p \leq n$ (cf. prop. I.1.48).

COROLLAIRE 4. — Formes p -linéaires alternées décomposables. — *Les formes p -linéaires alternées sur E décomposables constituent une partie génératrice de l'espace vectoriel $\mathcal{A}_p(E)$.*

En effet, soit B une base de E . Le corollaire 2 montre que les formes décomposables $e_p = e_{\varphi(1)}^* \wedge e_{\varphi(2)}^* \wedge \dots \wedge e_{\varphi(p)}^*$ constituent une base de $\mathcal{A}_p(E)$; d'où le corollaire.

On trouvera la propriété universelle de l'espace vectoriel $\mathcal{A}_p(E)$ dans l'exercice 23.

REMARQUE. — En calquant la méthode précédente on peut étudier les formes p -linéaires symétriques; cf. exercice 19.

Voici enfin deux critères d'indépendance qui sont des conséquences immédiates de la théorie précédente :

PROPOSITION 3.8. — Critère d'indépendance de p vecteurs dans un espace vectoriel de dimension n . — *Soient E un espace vectoriel de dimension n sur K , et (x_1, x_2, \dots, x_p) une suite de vecteurs de E . Pour que ces vecteurs soient linéairement indépendants, il faut et il suffit qu'il existe une forme p -linéaire alternée f sur E telle que $f(x_1, x_2, \dots, x_p) \neq 0$, ou encore qu'il existe une suite $(y_1^*, y_2^*, \dots, y_p^*)$ de formes linéaires sur E telle que*

$$(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*)(x_1, x_2, \dots, x_p) \neq 0.$$

Supposons d'abord que la famille (x_1, x_2, \dots, x_p) n'est pas libre; comme K est un corps, il en découle que l'un des vecteurs x_1, x_2, \dots, x_p est combinaison linéaire des autres (cf. prop. I.3.25). Il résulte alors de la proposition 2 que pour tout élément f de $\mathcal{A}_p(E)$, $f(x_1, x_2, \dots, x_p) = 0$.

Réciproquement, si la famille (x_1, x_2, \dots, x_p) est libre, nous pouvons la compléter en une base $(x_1, x_2, \dots, x_p, x_{p+1}, \dots, x_n)$ de E . Désignons par $(y_1^*, y_2^*, \dots, y_n^*)$ la base duale de la base précédente. Alors :

$$(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*)(x_1, x_2, \dots, x_p) = 1 \neq 0.$$

PROPOSITION 3.9. — Critère d'indépendance de p formes linéaires sur un espace vectoriel de dimension n . — *Soient E un espace vectoriel de dimension n sur K , et $(y_1^*, y_2^*, \dots, y_p^*)$ une suite de formes linéaires sur E . Pour que ces formes linéaires soient linéairement indépendantes, il faut et il suffit que*

$$y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* \neq 0.$$

Supposons d'abord que la famille $(y_1^*, y_2^*, \dots, y_p^*)$ n'est pas libre; comme K est un corps, il en découle que l'une des formes linéaires $y_1^*, y_2^*, \dots, y_p^*$ est combinaison linéaire des autres (cf. prop. I.3.25). Il résulte alors du corollaire de la proposition 3.6 que $y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* = 0$.

Réciproquement, si la famille $(y_1^*, y_2^*, \dots, y_p^*)$ est libre, nous pouvons la compléter en une base $(y_1^*, y_2^*, \dots, y_p^*, y_{p+1}^*, \dots, y_n^*)$ de E^* (cor. 2 du th. I.3.4). D'après le théorème I.3.9, il existe une base (e_1, e_2, \dots, e_n) et une seule de E dont $(y_1^*, y_2^*, \dots, y_n^*)$ soit la base duale. Alors

$$(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*)(e_1, e_2, \dots, e_p) = 1.$$

Donc $y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* \neq 0$.

§ 2. DÉTERMINANTS

1. DÉTERMINANT DE n VECTEURS

Appliquons les résultats du sous-paragraphe précédent au cas des formes n -linéaires alternées sur un espace vectoriel de dimension n .

DÉFINITION 3.6. — Déterminant de n vecteurs. — Soient E un espace vectoriel de dimension finie non nulle n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , et $(e_1^*, e_2^*, \dots, e_n^*)$ la base duale de B . La forme n -linéaire alternée $e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*$ s'appelle déterminant dans la base B , et se note Det_B . Ainsi, pour toute suite (x_1, x_2, \dots, x_n) de n vecteurs de E ,

$$(1) \quad \text{Det}_B(x_1, x_2, \dots, x_n) = (e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*)(x_1, x_2, \dots, x_n).$$

L'application Det_B a donc les propriétés suivantes :

— Pour toute suite (x_1, x_2, \dots, x_n) de n vecteurs de E et pour toute permutation σ de $[1, n]$,

$$\text{Det}_B(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) \cdot \text{Det}_B(x_1, x_2, \dots, x_n).$$

— Le déterminant de n vecteurs est inchangé lorsqu'on ajoute à l'un d'entre eux une combinaison linéaire des autres.

THÉORÈME 3.3. — Caractérisation du déterminant. — Soient E un espace vectoriel de dimension finie non nulle n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , et $(e_1^*, e_2^*, \dots, e_n^*)$ la base duale de B .

1. Soit $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$ une suite de n vecteurs de E , évalués dans la base B :

$$\mathbf{x}_j = \sum_{i=1}^n \xi_{ij} \mathbf{e}_i.$$

Alors

$$(2) \quad \text{Det}_B(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \xi_{1, \sigma(1)} \xi_{2, \sigma(2)} \dots \xi_{n, \sigma(n)}.$$

2. L'application $\text{Det}_B = \mathbf{e}_1^* \wedge \mathbf{e}_2^* \wedge \dots \wedge \mathbf{e}_n^*$ est l'unique forme n -linéaire alternée sur E prenant la valeur 1 sur $(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$. Sa valeur sur une suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$ de n vecteurs de E est encore donnée par la formule

$$(2') \quad \text{Det}_B(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \xi_{\sigma(1), 1} \xi_{\sigma(2), 2} \dots \xi_{\sigma(n), n}.$$

3. Soit f une forme n -linéaire alternée sur E . Pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n)$ de n vecteurs de E ,

$$(3) \quad f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = f(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n) \cdot \text{Det}_B(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n).$$

Ce théorème s'obtient en spécialisant le théorème de développement des applications p -linéaires alternées au cas où $p = n$. Alors \mathcal{T} est constitué d'un seul élément, à savoir $[1, n]$, et δ est réduit à un seul élément φ , à savoir l'application identique de $[1, n]$.

Dans ce cas particulier, la démonstration du théorème se réduit à la forme plus simple que voici :

L'assertion 1 résulte aussitôt de la définition du produit extérieur $\mathbf{e}_1^* \wedge \mathbf{e}_2^* \wedge \dots \wedge \mathbf{e}_n^*$.

Assertions 2 et 3.

a) Soit f une forme n -linéaire alternée sur E . Puisque f est multilinéaire, nous pouvons écrire

$$(4) \quad f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n \xi_{i_1, 1} \xi_{i_2, 2} \dots \xi_{i_n, n} f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_n}).$$

Considérons le terme de cette somme relatif aux indices i_1, i_2, \dots, i_n ; deux cas se présentent :

— ou bien deux indices i_q et i_r sont égaux, q étant différent de r ; alors $f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_n}) = 0$ puisque f est alternée;

— ou bien les indices i_1, i_2, \dots, i_n sont distincts deux à deux; il existe alors une permutation σ et une seule de $[1, n]$ telle que, pour tout entier $q \in [1, n]$, $\sigma(q) = i_q$. Comme f est alternée, nous avons la relation :

$$f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_n}) = f(\mathbf{e}_{\sigma(1)}, \mathbf{e}_{\sigma(2)}, \dots, \mathbf{e}_{\sigma(n)}) = \varepsilon(\sigma) \cdot f(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n).$$

La formule (4) s'écrit donc encore :

$$(5) \quad f(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) = f(e_1, e_2, \dots, e_n) \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \cdot \xi_{\sigma(1),1} \cdot \xi_{\sigma(2),2} \cdots \xi_{\sigma(n),n}.$$

b) Cette dernière formule prouve l'unicité d'une forme n -linéaire alternée g sur E telle que $g(e_1, e_2, \dots, e_n) = 1$. Or, nous savons qu'une telle forme existe, à savoir $e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*$. L'assertion 2 en résulte, ainsi que la formule (2).

c) La formule (3) est maintenant une conséquence immédiate des formules (2) et (5).

COROLLAIRE 1. — Bases de l'espace vectoriel $\mathcal{A}_n(E)$. — Soit E un espace vectoriel de dimension n sur K , muni d'une base $B = (e_1, e_2, \dots, e_n)$. Alors la forme n -linéaire alternée $\text{Det}_B = e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*$ constitue une base de l'espace vectoriel $\mathcal{A}_n(E)$.

COROLLAIRE 2. — Dimension de l'espace vectoriel $\mathcal{A}_n(E)$. — Soit E un espace vectoriel de dimension n sur K ; alors l'espace vectoriel $\mathcal{A}_n(E)$ est de dimension 1.

COROLLAIRE 3. — Critère de nullité pour un élément de $\mathcal{A}_n(E)$. — Soient E un espace vectoriel de dimension n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , et f une forme n -linéaire alternée sur E . Pour que f soit nulle, il faut et il suffit que $f(e_1, e_2, \dots, e_n) = 0$.

COROLLAIRE 4. — Calcul des valeurs d'une forme p -linéaire alternée. — Soient E un espace vectoriel de dimension finie non nulle n sur K , $B = (e_1, e_2, \dots, e_n)$ une base de E , p un entier strictement positif inférieur ou égal à n , et $(e_p)_{p \in \mathfrak{P}}$ la base de $\mathcal{A}_p(E)$ canoniquement associée à B . Alors, pour toute suite $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$ d'éléments de E et pour tout élément P de \mathfrak{P} ,

$$e_P(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p) = \text{Det}_{B_P}(\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_p),$$

où B_P désigne la famille $(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)})$, et $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_p$ les projections canoniques de $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p$ sur le sous-espace vectoriel E_P de E engendré par B_P .

REMARQUE. — Au n° 2, nous donnerons une interprétation intéressante de l'égalité des seconds membres [des formules (2) et (2')]. On peut d'ailleurs établir cette égalité par une méthode directe, en utilisant le fait que l'application $\sigma \mapsto \sigma^{-1}$ est une bijection de \mathfrak{S}_n sur lui-même.

La propriété la plus importante des déterminants est énoncée dans le

THÉORÈME 3.4. — Critère d'indépendance de n vecteurs d'un espace vectoriel de dimension n . — Soient E un espace vectoriel de dimension n sur K , muni

d'une base $B = (e_1, e_2, \dots, e_n)$, et (x_1, x_2, \dots, x_n) une suite de n vecteurs de E . Pour que ces vecteurs soient linéairement indépendants, il faut et il suffit que

$$\text{Det}_B(x_1, x_2, \dots, x_n) \neq 0.$$

Supposons d'abord que la famille (x_1, x_2, \dots, x_n) n'est pas libre; un des vecteurs x_1, x_2, \dots, x_n est donc combinaison linéaire des autres. Par suite, $\text{Det}_B(x_1, x_2, \dots, x_n) = 0$.

Réciproquement, si la famille (x_1, x_2, \dots, x_n) est libre, c'est une base de E . Puisque Det_B est une forme n -linéaire alternée non nulle, $\text{Det}_B(x_1, x_2, \dots, x_n) \neq 0$ (cf. cor. 3 du th. 3.3).

2. DÉTERMINANT D'UN ENDOMORPHISME

Nous avons vu que si l'espace vectoriel E est de dimension finie non nulle n sur K , l'espace vectoriel $\mathcal{A}_n(E)$ des formes n -linéaires alternées sur E est de dimension 1 (cf. cor. 3 du th. 3.1 ou cor. 2 du th. 3.3). Ce seul résultat permet de développer la théorie des déterminants des endomorphismes.

DÉFINITION 3.7. — Déterminant d'un endomorphisme. — Soit E un espace vectoriel de dimension finie non nulle n sur K . Pour tout endomorphisme U de E , l'extension U_n de U à l'espace vectoriel $\mathcal{M}_n(E)$ des formes n -linéaires sur E laisse stable le sous-espace vectoriel $\mathcal{A}_n(E)$ des formes n -linéaires alternées sur E (cf. prop. 3.4). Ce dernier étant de dimension 1, l'endomorphisme de $\mathcal{A}_n(E)$ coïncidant avec U_n est une homothétie (cf. cor. de la prop. I.3.36).

Le rapport de l'homothétie précédente s'appelle *déterminant* de l'endomorphisme U , et se note $\text{Det } U$.

Ainsi, le scalaire $\text{Det } U$ est défini par la formule fondamentale suivante : pour toute forme n -linéaire alternée f sur E , et pour toute suite (x_1, x_2, \dots, x_n) de n vecteurs de E ,

$$(1) \quad f[U(x_1), U(x_2), \dots, U(x_n)] = (\text{Det } U) \cdot f(x_1, x_2, \dots, x_n).$$

THÉORÈME 3.5. — Propriétés du déterminant d'un endomorphisme. — Soit E un espace vectoriel de dimension n sur K .

1. Si l'espace vectoriel E est muni d'une base B , alors, pour toute suite (x_1, x_2, \dots, x_n) de vecteurs de E , et pour tout endomorphisme U de E ,

$$(2) \quad \text{Det}_B [U(x_1), U(x_2), \dots, U(x_n)] = (\text{Det } U) \cdot \text{Det}_B (x_1, x_2, \dots, x_n).$$

En particulier, soit $B = (e_1, e_2, \dots, e_n)$ une base de E ; alors :

$$\text{Det } U = \text{Det}_B [U(e_1), U(e_2), \dots, U(e_n)].$$

2. Le déterminant de l'application identique de E est égal à 1; plus généralement, le déterminant de l'homothétie de rapport α est égal à α^n :

$$(3) \quad \text{Det } \alpha I_E = \alpha^n.$$

3. Le déterminant du composé de deux endomorphismes de E est égal au produit de leurs déterminants; autrement dit, pour tout couple (U, V) d'endomorphismes de E ,

$$(4) \quad \text{Det}(VU) = (\text{Det } V) \cdot (\text{Det } U).$$

4. Le déterminant du transposé tU d'un endomorphisme U de E est égal au déterminant de U :

$$(5) \quad \text{Det } {}^tU = \text{Det } U.$$

L'assertion 1 résulte aussitôt de la formule (1) : il suffit de prendre pour f la forme n -linéaire alternée Det_B .

L'assertion 2 est une conséquence immédiate de la formule $(\alpha I_E)_n = \alpha^n (I_E)_n$ (cf. prop. 3.4).

L'assertion 3 se déduit de même de la formule $(V \circ U)_n = U_n \circ V_n$ (cf. prop. 3.4).

Assertion 4. — Nous savons (cf. prop. 3.7) que, pour tout endomorphisme U de E , pour toute suite (x_1, x_2, \dots, x_n) d'éléments de E , et pour toute suite $(y_1^*, y_2^*, \dots, y_n^*)$ d'éléments de E^* ,

$$(6) \quad [{}^tU(y_1^*) \wedge \dots \wedge {}^tU(y_n^*)](x_1, \dots, x_n) \\ = (y_1^* \wedge \dots \wedge y_n^*)[U(x_1), \dots, U(x_n)].$$

a) Les éléments $y_1^*, y_2^*, \dots, y_n^*$ étant fixés, nous savons que $y_1^* \wedge y_2^* \wedge \dots \wedge y_n^*$ est une forme n -linéaire alternée sur E . En lui appliquant la formule (1), nous obtenons la relation suivante :

$$(7) \quad (y_1^* \wedge \dots \wedge y_n^*)[U(x_1), \dots, U(x_n)] \\ = (\text{Det } U) \cdot (y_1^* \wedge \dots \wedge y_n^*)(x_1, \dots, x_n).$$

b) Les éléments x_1, x_2, \dots, x_n étant fixés, l'application de $(E^*)^n$ dans K qui à toute suite $(y_1^*, y_2^*, \dots, y_n^*)$ d'éléments de E^* associe le scalaire

$$(y_1^* \wedge \dots \wedge y_n^*)(x_1, \dots, x_n)$$

est une forme n -linéaire alternée sur E^* (cf. prop. 3.6). Donc, par définition de $\text{Det } {}^tU$,

$$(8) \quad [{}^tU(y_1^*) \wedge \dots \wedge {}^tU(y_n^*)](x_1, \dots, x_n) \\ = (\text{Det } {}^tU) \cdot (y_1^* \wedge \dots \wedge y_n^*)(x_1, \dots, x_n).$$

En appliquant les formules (6), (7) et (8) au cas où (x_1, \dots, x_n) est une base de E , et où (y_1^*, \dots, y_n^*) est la base duale de celle-ci, nous obtenons la relation $\text{Det } {}^tU = \text{Det } U$.

COROLLAIRE 1. — Caractérisation des endomorphismes inversibles. — *Pour qu'un endomorphisme U de E soit inversible, il faut et il suffit que son déterminant soit non nul, et alors :*

$$\text{Det } U^{-1} = (\text{Det } U)^{-1}.$$

Supposons d'abord U inversible; il existe alors un endomorphisme V de E tel que $VU = UV = I_E$, d'où

$$(\text{Det } U) \cdot (\text{Det } V) = 1,$$

ce qui montre à la fois que $\text{Det } U$ est non nul, et que

$$\text{Det } U^{-1} = (\text{Det } U)^{-1}.$$

Réciproquement, supposons $\text{Det } U$ non nul; il en découle que, si $B = (e_1, e_2, \dots, e_n)$ est une base de E , le scalaire

$$\text{Det}_B[U(e_1), U(e_2), \dots, U(e_n)]$$

est non nul, et donc que les vecteurs $U(e_1), U(e_2), \dots, U(e_n)$ sont linéairement indépendants (cf. th. 3.4). Il s'ensuit que l'endomorphisme U est inversible.

COROLLAIRE 2. — Groupe spécial linéaire. — *Soit E un espace vectoriel de dimension finie sur K . Le groupe linéaire $\text{GL}(E)$ est constitué des endomorphismes de E dont le déterminant est non nul. De plus, l'application qui à tout élément U de $\text{GL}(E)$ associe le scalaire $\text{Det } U$ est un morphisme du groupe $\text{GL}(E)$ sur le groupe multiplicatif K^* . Le noyau de ce morphisme, constitué des endomorphismes de E dont le déterminant est égal à 1, est un sous-groupe distingué de $\text{GL}(E)$, appelé groupe spécial linéaire de E , et noté $\text{SL}(E)$.*

Ce groupe s'appelle aussi groupe unimodulaire, et ses éléments automorphismes unimodulaires.

Considérons un espace vectoriel E de dimension finie $n > 0$, muni d'une base $B = (e_1, e_2, \dots, e_n)$. Nous savons que, pour tout endomorphisme U de E ,

$$\text{Det } U = \text{Det}_B[U(e_1), U(e_2), \dots, U(e_n)].$$

Ainsi, le déterminant de U n'est autre que le déterminant dans la base B des vecteurs colonnes de la matrice $M_B(U)$ associée à U dans la base B . Ceci nous amène à poser la

DÉFINITION 3.8. — Déterminant d'une matrice carrée. — *Soit M une matrice carrée d'ordre n à éléments dans K . On appelle déterminant de M , et on note $\text{Det } M$, le déterminant de ses vecteurs colonnes dans la base canonique de K^n . C'est encore le déterminant dans la base canonique de K^n de l'endomorphisme de K^n canoniquement associé à M .*

Soit maintenant U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Alors, pour toute base B de E ,

$$\text{Det } [M_B(U)] = \text{Det } U.$$

Notation du déterminant d'une matrice carrée explicitée. — Soit M une matrice carrée d'ordre n :

$$M = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{i1} & \alpha_{i2} & \dots & \alpha_{ij} & \dots & \alpha_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{pmatrix} ;$$

son déterminant se note :

$$\text{Det } M = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{i1} & \alpha_{i2} & \dots & \alpha_{ij} & \dots & \alpha_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{vmatrix}.$$

Les propriétés des déterminants des matrices carrées se déduisent aussitôt du théorème 3.5, en utilisant l'isomorphisme canonique de l'algèbre unitaire $M_n(K)$ des matrices carrées d'ordre n à éléments dans K sur l'algèbre unitaire $\mathcal{L}(K^n)$ des endomorphismes de l'espace vectoriel K^n . Nous obtenons ainsi la

PROPOSITION 3.10. — Propriétés du déterminant d'une matrice carrée.

1. *Le déterminant de la matrice I_n est égal à 1 ; plus généralement, le déterminant de la matrice αI_n est égal à α^n :*

$$\text{Det } (\alpha I_n) = \alpha^n.$$

2. *Le déterminant du produit de deux matrices carrées d'ordre n est égal au produit de leurs déterminants ; autrement dit, pour tout couple (M, N) d'éléments de $M_n(K)$,*

$$\text{Det } NM = (\text{Det } N) \cdot (\text{Det } M).$$

3. *Le déterminant de la transposée tM d'une matrice carrée M d'ordre n est égal au déterminant de M :*

$$\text{Det } {}^tM = \text{Det } M.$$

Autrement dit : le déterminant des vecteurs lignes de M est égal au déterminant des vecteurs colonnes de M .

4. *On ne change pas la valeur du déterminant d'une matrice carrée M en ajoutant à un de ses vecteurs colonnes (resp. vecteurs lignes) une combinaison linéaire des autres vecteurs colonnes (resp. vecteurs lignes) de M .*

5. *Lorsqu'on échange deux colonnes, ou deux lignes, d'une matrice carrée M , le déterminant de M est transformé en son opposé.*

Les assertions 4 et 5 relatives aux vecteurs colonnes résultent des propriétés du déterminant de n vecteurs. Celles qui sont relatives aux vecteurs lignes en

découlent, puisque $\text{Det } {}^tM = \text{Det } M$, et que les vecteurs lignes de M ne sont autres que les vecteurs colonnes de tM .

REMARQUE. — La relation $\text{Det } {}^tM = \text{Det } M$ fournit une interprétation intéressante des formules (2) et (2') du théorème 3.3, donnant le développement du déterminant de n vecteurs.

Réciproquement, l'égalité des deuxièmes membres des formules (1) et (2) fournit une démonstration directe de la formule $\text{Det } {}^tM = \text{Det } M$. On peut en déduire une démonstration élémentaire de la formule $\text{Det } {}^tU = \text{Det } U$, où U est un endomorphisme d'un espace vectoriel E de dimension finie sur K : il suffit de choisir une base B de E , et d'écrire

$$\text{Det } {}^tU = \text{Det } [M_{B^*}({}^tU)] = \text{Det } [{}^tM_B(U)] = \text{Det } [M_B(U)] = \text{Det } U.$$

COROLLAIRE 1. — **Caractérisation des matrices carrées inversibles.** — *Pour qu'une matrice carrée M soit inversible, il faut et il suffit que son déterminant soit non nul, et alors :*

$$\text{Det } M^{-1} = (\text{Det } M)^{-1}.$$

COROLLAIRE 2. — **Groupe spécial linéaire de type n .** — *Le groupe multiplicatif $\text{GL}(n, K)$ des matrices carrées d'ordre n inversibles est constitué des matrices carrées d'ordre n dont le déterminant est non nul. Les matrices carrées d'ordre n dont le déterminant est égal à 1 constituent un sous-groupe distingué de $\text{GL}(n, K)$, qu'on note $\text{SL}(n, K)$ et qu'on appelle groupe spécial linéaire de type n .*

REMARQUE. — Il est immédiat que l'application $M \mapsto \text{Det } M$ est une application polynomiale de $M_n(K)$ dans K , qui induit un morphisme du groupe multiplicatif $\text{GL}_n(K)$ dans le groupe multiplicatif K^* . On trouvera dans l'exercice 4.46 une caractérisation des applications satisfaisant à ces conditions.

Voici enfin comment se transforme le déterminant de n vecteurs par changement de base :

PROPOSITION 3.11. — **Effet d'un changement de base sur le déterminant de n vecteurs.** — *Soient E un espace vectoriel de dimension n sur K , B et B' deux bases de E , et P la matrice de passage de B à B' . Alors, pour toute suite (x_1, x_2, \dots, x_n) de vecteurs de E ,*

$$\text{Det}_B(x_1, x_2, \dots, x_n) = (\text{Det } P) \cdot \text{Det}_{B'}(x_1, x_2, \dots, x_n).$$

En effet, l'application $(x_1, x_2, \dots, x_n) \mapsto \text{Det}_B(x_1, x_2, \dots, x_n)$ est une forme multilinéaire alternée sur E . Il résulte donc du théorème 3.3 que

$$\text{Det}_B(x_1, x_2, \dots, x_n) = \text{Det}_B(e'_1, e'_2, \dots, e'_n) \cdot \text{Det}_{B'}(x_1, x_2, \dots, x_n),$$

où e'_1, e'_2, \dots, e'_n désignent les éléments de la base B' . Enfin,

$$\text{Det } P = \text{Det}_B(e'_1, e'_2, \dots, e'_n),$$

puisque les vecteurs colonnes de P sont précisément les vecteurs e'_1, e'_2, \dots, e'_n .

Exercices conseillés : 13 à 15.

§ 3. CALCULS DE DÉTERMINANTS

1. DÉTERMINANTS DE MATRICES CARRÉES REMARQUABLES

On désigne par $B = (e_1, e_2, \dots, e_n)$ la base canonique de K^n .

EXEMPLE 1. — Déterminant d'une matrice de permutation. — Soient σ une permutation de $[1, n]$ et M_σ la matrice de permutation associée (cf. prop. I.3.57); alors:

$$\text{Det } M_\sigma = \varepsilon(\sigma),$$

où $\varepsilon(\sigma)$ désigne la signature de la permutation σ .

En effet,

$$\text{Det } M_\sigma = \text{Det}_B (e_{\sigma(1)}, e_{\sigma(2)}, \dots, e_{\sigma(n)}) = \varepsilon(\sigma).$$

EXEMPLE 2. — Déterminant d'une matrice diagonale. — Soit

$$D = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}$$

une matrice diagonale d'ordre n ; alors

$$\text{Det } D = \prod_{i=1}^n \alpha_i.$$

En effet,

$$\text{Det } D = \text{Det}_B (\alpha_1 e_1, \alpha_2 e_2, \dots, \alpha_n e_n) = \alpha_1 \alpha_2 \dots \alpha_n.$$

EXEMPLE 3. — Déterminant d'une matrice trigonale supérieure. — Soit

$$T = \begin{pmatrix} \alpha_1 & & * \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}$$

une matrice trigonale supérieure d'ordre n ; alors

$$(1) \quad \text{Det } T = \prod_{i=1}^n \alpha_i.$$

En particulier, le déterminant d'une matrice trigonale nilpotente est nul; le déterminant d'une matrice trigonale unipotente est égal à 1.

Désignons par f_1, f_2, \dots, f_n les transformés des vecteurs e_1, e_2, \dots, e_n par l'endomorphisme de K^n canoniquement associé à T . Alors

$$\text{Det } T = \text{Det}_B (f_1, f_2, \dots, f_n).$$

Or, pour tout $j \in [2, n]$, $f_j = \alpha_j e_j + g_j$, où g_j est une combinaison linéaire de e_1, e_2, \dots, e_{j-1} . Il s'ensuit que

$$\text{Det } T = \alpha_1 \alpha_2 \dots \alpha_n.$$

Les exemples 2 et 3 se généralisent en le

THÉOREME 3.6. — Déterminant d'une matrice trigonale de matrices. —
Soit

$$M = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1r} \\ 0 & A_{22} & \dots & A_{2r} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A_{rr} \end{pmatrix}$$

une matrice trigonale de matrices, les éléments diagonaux étant des matrices carrées. Alors

$$(1) \quad \text{Det } M = \prod_{i=1}^n \text{Det } A_{ii}.$$

En particulier, soit

$$M = \begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$$

une matrice diagonale de matrices carrées. Alors

$$\text{Det } M = \prod_{i=1}^r \text{Det } A_i.$$

La formule (1) résulte aussitôt du cas où $r = 2$ par récurrence sur r . Soit donc

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

une matrice décomposée en blocs, où $A \in \mathbf{M}_p(K)$, $B \in \mathbf{M}_{p,n-p}(K)$ et $D \in \mathbf{M}_{n-p}(K)$. Nous allons prouver que

$$\text{Det } M = (\text{Det } A) \cdot (\text{Det } D).$$

Soient en effet (e_1, e_2, \dots, e_n) la base canonique de K^n , F le sous-espace vectoriel de K^n engendré par e_1, e_2, \dots, e_p , G le sous-espace vectoriel engendré par $e_{p+1}, e_{p+2}, \dots, e_n$. Notons U l'endomorphisme de K^n canoniquement associé à M , V l'endomorphisme de F canoniquement associé à A et W l'endomorphisme de G canoniquement associé à D . Désignons enfin par f le déterminant dans la base canonique de K^n . Par définition de $\text{Det } M$,

$$(2) \quad \text{Det } M = f(U(e_1), U(e_2), \dots, U(e_n)).$$

Or, puisque M est décomposée en blocs triangulaires, pour tout $j \in [1, p]$, $U(e_j) = V(e_j)$. Nous sommes donc amené à étudier l'application g qui à tout élément (x_1, x_2, \dots, x_p) de F associe le scalaire

$$(3) \quad g(x_1, x_2, \dots, x_p) = f(x_1, x_2, \dots, x_p, U(e_{p+1}), \dots, U(e_n)).$$

Il est clair que g est une forme p -linéaire alternée sur F . Par définition même du déterminant de l'endomorphisme V , il en découle que

$$(4) \quad g(V(e_1), V(e_2), \dots, V(e_p)) = \text{Det } V \cdot g(e_1, e_2, \dots, e_p).$$

Des formules (2), (3) et (4) et de la relation $\text{Det } V = \text{Det } A$, nous déduisons que

$$(5) \quad \text{Det } M = \text{Det } A \cdot f(e_1, e_2, \dots, e_p, U(e_{p+1}), \dots, U(e_n)).$$

Or, pour tout $j \in [p+1, n]$, le vecteur $U(e_j) - W(e_j)$ appartient à F ; c'est donc une combinaison linéaire de e_1, e_2, \dots, e_p . Puisque f est multilinéaire alternée, il s'ensuit que

$$(6) \quad \begin{aligned} f(e_1, e_2, \dots, e_p, U(e_{p+1}), \dots, U(e_n)) \\ = f(e_1, e_2, \dots, e_p, W(e_{p+1}), \dots, W(e_n)). \end{aligned}$$

Nous sommes donc amené à étudier l'application h qui à tout élément (x_{p+1}, \dots, x_n) de G associe le scalaire

$$(7) \quad h(x_{p+1}, \dots, x_n) = f(e_1, e_2, \dots, e_p, x_{p+1}, \dots, x_n).$$

Un raisonnement analogue au précédent montre que

$$(8) \quad h(W(e_{p+1}), \dots, W(e_n)) = \text{Det } W \cdot h(e_{p+1}, \dots, e_n).$$

Des formules (5) à (8) et de la relation $\text{Det } W = \text{Det } D$, nous déduisons enfin que

$$(9) \quad \text{Det } M = (\text{Det } A) \cdot (\text{Det } D),$$

ce qu'il fallait prouver.

2. DÉVELOPPEMENT D'UN DÉTERMINANT SUIVANT UNE COLONNE, OU UNE LIGNE

DÉFINITION 3.9. — Matrices et déterminants mineurs d'une matrice carrée. Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$, $n > 1$. On appelle matrice mineure associée à l'élément α_{ij} , et on note A_{ij} , l'élément de $M_{n-1}(K)$ obtenu en supprimant la $i^{\text{ième}}$ ligne et la $j^{\text{ième}}$ colonne de M .

Le déterminant de la matrice A_{ij} s'appelle déterminant mineur associé à l'élément α_{ij} .

THÉORÈME 3.7. — Développement d'un déterminant suivant une colonne, ou une ligne. — Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$, $n > 1$.

1. Pour tout entier $j \in [1, n]$,

$$(1) \quad \text{Det } M = \sum_{i=1}^n (-1)^{i+j} \alpha_{ij} \text{Det } A_{ij}.$$

Le second membre de la formule (1) s'appelle développement du déterminant de la matrice M suivant la $j^{\text{ième}}$ colonne de M .

2. Pour tout entier $i \in [1, n]$,

$$(2) \quad \text{Det } M = \sum_{j=1}^n (-1)^{i+j} \alpha_{ij} \text{Det } A_{ij}.$$

Le second membre de la formule (2) s'appelle développement du déterminant de la matrice M suivant la $i^{\text{ième}}$ ligne de M .

Assertion 1. — Considérons l'espace vectoriel K^n , muni de sa base canonique $B = (e_1, e_2, \dots, e_i, \dots, e_n)$, et désignons par $a_1, a_2, \dots, a_j, \dots, a_n$ les vecteurs colonnes de la matrice M . Par définition,

$$\text{Det } M = \text{Det}_B(a_1, a_2, \dots, a_j, \dots, a_n).$$

Soit j un élément de $[1, n]$; la décomposition du vecteur a_j dans la base B s'écrit

$$a_j = \sum_{i=1}^n \alpha_{ij} e_i.$$

Comme l'application Det_B est multilinéaire alternée,

$$\begin{aligned} \text{Det } M &= (-1)^{j-1} \text{Det}_B(a_j, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \\ &= (-1)^{j-1} \sum_{i=1}^n \alpha_{ij} \text{Det}_B(e_i, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n). \end{aligned}$$

Donc

$$(3) \quad \text{Det } M = (-1)^{j-1} \sum_{i=1}^n \alpha_{ij} \text{Det } M_{ij},$$

où M_{ij} est la matrice ayant pour vecteurs colonnes

$$e_i, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n.$$

Soit M'_{ij} la matrice obtenue en échangeant successivement la $i^{\text{ième}}$ ligne de cette matrice avec les $i-1$ premières. Il est clair que

$$(4) \quad \text{Det } M_{ij} = (-1)^{i-1} \text{Det } M'_{ij}.$$

Or, M'_{ij} est de la forme

$$M'_{ij} = \begin{pmatrix} 1 & * \\ 0 & A_{ij} \end{pmatrix}.$$

D'après le théorème 3.6,

$$(5) \quad \text{Det } M'_{ij} = \text{Det } A_{ij}.$$

La formule (1) résulte alors des formules (3), (4) et (5).

L'assertion 2 se déduit aussitôt de l'assertion 1 par transposition.

EXEMPLE 1. — Calcul des déterminants d'ordre 2.

Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2. Alors :

$$\text{Det} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

EXEMPLE 2. — Calcul des déterminants d'ordre 3.

Soit $\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$ une matrice carrée d'ordre 3. Alors :

$$\begin{aligned} \text{Det} \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} &= a \cdot \begin{vmatrix} b' & c' \\ b'' & c'' \end{vmatrix} - b \cdot \begin{vmatrix} a' & c' \\ a'' & c'' \end{vmatrix} + c \cdot \begin{vmatrix} a' & b' \\ a'' & b'' \end{vmatrix} \\ &= ab'c'' - ac'b'' + bc'a'' - ba'c'' + ca'b'' - cb'a''. \end{aligned}$$

Voici un moyen mnémotechnique pour retrouver ce développement, connu sous le nom de *règle de Sarrus* :

— On écrit :

$$\begin{array}{ccccc} a & b & c & a & b \\ a' & b' & c' & a' & b' \\ a'' & b'' & c'' & a'' & b'' \end{array}$$

— On affecte les trois produits « parallèles à la diagonale principale » du signe +, et les trois produits « parallèles à la diagonale secondaire » du signe -.

— Le déterminant est égal à la somme de ces six termes.

EXEMPLE 3. — Calcul par récurrence de certains déterminants d'ordre n . — On se propose de calculer $D_n = \text{Det } M_n$, où $M_n = (\alpha_{ij})$ est la matrice carrée d'ordre n définie par les relations $\alpha_{ij} = 0$ si $i + j \neq n + 1$, $\alpha_{ij} = -1$ si $i + j = n + 1$; autrement dit, tous les éléments de M_n sont nuls sauf sur la diagonale secondaire, où ils valent -1 .

Le développement par rapport à la première ligne donne la formule de récurrence $D_n = (-1)^n D_{n-1}$, d'où $D_n = (-1)^{n+(n-1)+\dots+2} D_1$, où $D_1 = -1$. Finalement :

$$D_n = (-1)^{\frac{n(n+1)}{2}},$$

DÉFINITION 3.10. — Matrice des cofacteurs, matrice complémentaire. — Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$, $n > 1$. Pour tout couple (i, j) d'éléments de $[1, n]$, le scalaire $\alpha'_{ij} = (-1)^{i+j} \text{Det } A_{ij}$ s'appelle cofacteur de l'élément α_{ij} . La matrice $M' = (\alpha'_{ij})$ est un élément de $M_n(K)$, qu'on appelle matrice des cofacteurs de la matrice M . La matrice transposée de M' s'appelle matrice complémentaire de la matrice M , et se note \tilde{M} .

COROLLAIRE 1. — Soient M un élément de $M_n(K)$, $n > 1$, et \tilde{M} la matrice complémentaire de M . Alors :

$$\tilde{M} \cdot M = M \cdot \tilde{M} = (\text{Det } M) \cdot I_n.$$

Autrement dit :

— pour tout couple (h, j) d'éléments de $[1, n]$,

$$(1') \quad \sum_{i=1}^n (-1)^{i+h} \alpha_{ij} \text{Det } A_{ih} = \delta_{hj} \text{Det } M;$$

— pour tout couple (i, k) d'éléments de $[1, n]$,

$$(2') \quad \sum_{j=1}^n (-1)^{k+j} \alpha_{ij} \text{Det } A_{kj} = \delta_{ik} \text{Det } M.$$

Les formules (1') explicitent la relation $\tilde{M} \cdot M = (\text{Det } M) \cdot I_n$, tandis que les formules (2') explicitent la relation $M \cdot \tilde{M} = (\text{Det } M) \cdot I_n$.

Prouvons par exemple les formules (1'); distinguons deux cas :

a) $h = j$. La formule (1') n'est autre que la formule (1).

b) $h \neq j$. Désignons par a_1, a_2, \dots, a_n les vecteurs colonnes de la matrice M , et considérons la matrice $M_1 = (\gamma_{lm})$ obtenue en remplaçant dans la matrice M le vecteur a_h par le vecteur a_j . D'une part, le déterminant de M_1 est nul, puisque M_1 a deux colonnes égales. D'autre part, le développement de ce déterminant suivant la $h^{\text{ième}}$ colonne s'écrit

$$\text{Det } M_1 = \sum_{i=1}^n (-1)^{i+h} \gamma_{ih} \text{Det } A_{ih}.$$

puisque la matrice mineure de M_1 associée à l'élément γ_{ih} n'est autre que A_{ih} . La formule (1') résulte alors de la relation $\gamma_{ih} = \alpha_{ij}$, valable pour tout $i \in [1, n]$.

COROLLAIRE 2. — **Inverse d'une matrice carrée.** — Soit M une matrice carrée inversible d'ordre n à éléments dans K , $n > 1$. Alors :

$$M^{-1} = (\text{Det } M)^{-1} \cdot \tilde{M},$$

où \tilde{M} désigne la matrice complémentaire de M .

Exercices conseillés : 1 à 11.

3. APPLICATIONS DE LA THÉORIE DES POLYNÔMES

Considérons l'algèbre $M_n(K)$ des matrices carrées d'ordre n à éléments dans K . Introduisons n^2 indéterminées X_{ij} , où i et j parcourent $[1, n]$, et le corps $K(X_{ij})_{i,j \in [1, n]}$. La matrice $A = (X_{ij})$ est une matrice carrée d'ordre n

à éléments dans ce corps, et son déterminant est un élément de $K[X_{ij}]_{i,j \in [1,n]}$, que nous noterons $P(X_{ij})$: en effet,

$$P(X_{ij}) = \text{Det } A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) X_{\sigma(1),1} \cdots X_{\sigma(j),j} \cdots X_{\sigma(n),n}.$$

Soit maintenant $M = (\alpha_{ij})$ un élément de $M_n(K)$; le déterminant de M s'obtient évidemment en substituant dans le polynôme P les scalaires α_{ij} aux indéterminées X_{ij} .

Comme nous le verrons, cette remarque a de nombreuses applications. Voici deux exemples :

EXEMPLE 1. — Déterminants de Vandermonde. — Soient n un entier strictement supérieur à 1, et $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite de n éléments de K . On appelle *déterminant de Vandermonde associé à cette suite* le scalaire $D(\alpha_1, \alpha_2, \dots, \alpha_n)$ défini par la formule

$$D(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^j & \dots & \alpha_1^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_i & \dots & \alpha_i^j & \dots & \alpha_i^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^j & \dots & \alpha_n^{n-1} \end{vmatrix}.$$

Alors

$$(1) \quad D(\alpha_1, \alpha_2, \dots, \alpha_n) = V(\alpha_1, \alpha_2, \dots, \alpha_n),$$

où V désigne le polynôme de Vandermonde. Par suite,

$$(2) \quad D(\alpha_1, \alpha_2, \dots, \alpha_n) = \prod_{h>k} (\alpha_h - \alpha_k) = (-1)^{\frac{n(n-1)}{2}} \prod_{h<k} (\alpha_h - \alpha_k).$$

Introduisons n indéterminées X_1, X_2, \dots, X_n , et considérons le déterminant

$$D'(X_1, \dots, X_i, \dots, X_n) = \begin{vmatrix} 1 & X_1 & \dots & X_1^j & \dots & X_1^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & X_i & \dots & X_i^j & \dots & X_i^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & X_n^j & \dots & X_n^{n-1} \end{vmatrix}.$$

D'une part, D' est un polynôme antisymétrique, donc D' est divisible par le polynôme de Vandermonde V (cf. prop. 2.44). D'autre part, il est immédiat que D' est homogène de

degré $\sum_{j=1}^{n-1} j = \frac{n(n-1)}{2}$. Il existe donc un scalaire non nul β tel que $D' = \beta V$. Pour calculer β ,

notons que le coefficient de V relatif au monôme $X_2 X_3^2 \dots X_n^{n-1}$ est égal à 1; en considérant le développement du déterminant $D'(X_1, X_2, \dots, X_n)$, nous voyons que le coefficient de D' relatif à ce même monôme est aussi égal à 1. Finalement, $\beta = 1$ et $D' = V$.

La formule (1) s'obtient alors en substituant dans les polynômes D' et V les scalaires $\alpha_1, \alpha_2, \dots, \alpha_n$ aux indéterminées X_1, X_2, \dots, X_n .

EXEMPLE 2. — Déterminants de Vandermonde généralisés. — Soient n un entier strictement supérieur à 1 et $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite de n éléments de K . Pour tout entier j appartenant à $[1, n-1]$, on appelle déterminant de Vandermonde associé à j et à la suite $(\alpha_1, \alpha_2, \dots, \alpha_n)$ le scalaire $D_j(\alpha_1, \alpha_2, \dots, \alpha_n)$ défini par la formule

$$D_j(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{j-1} & \alpha_1^{j+1} & \dots & \alpha_1^n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_i & \dots & \alpha_i^{j-1} & \alpha_i^{j+1} & \dots & \alpha_i^n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^{j-1} & \alpha_n^{j+1} & \dots & \alpha_n^n \end{vmatrix}.$$

Alors

$$(2) \quad D_j(\alpha_1, \alpha_2, \dots, \alpha_n) = V(\alpha_1, \alpha_2, \dots, \alpha_n) S_{n-j}(\alpha_1, \alpha_2, \dots, \alpha_n),$$

où V désigne le polynôme de Vandermonde et où, pour tout entier p appartenant à $[1, n]$, S_p désigne le $p^{\text{ième}}$ polynôme symétrique élémentaire à n indéterminées.

Introduisons n indéterminées X_1, X_2, \dots, X_n , et considérons le déterminant

$$D'_j(X_1, \dots, X_i, \dots, X_n) = \begin{vmatrix} 1 & X_1 & \dots & X_1^{j-1} & X_1^{j+1} & \dots & X_1^n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & X_i & \dots & X_i^{j-1} & X_i^{j+1} & \dots & X_i^n \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & X_n^{j-1} & X_n^{j+1} & \dots & X_n^n \end{vmatrix}.$$

D'une part, D'_j est un polynôme antisymétrique, donc D'_j peut se mettre sous la forme $D'_j = VQ_j$, où Q_j est un polynôme symétrique (cf. prop. 2.44). D'autre part, il est immédiat que D'_j est homogène de degré $\frac{n(n+1)}{2} - j$, donc Q_j est de degré $n-j$. D'après le théorème 2.18, il en découle qu'il existe un élément A_j de $A[Y_1, Y_2, \dots, Y_n]$ et un seul tel que

$$Q_j = A_j(S_1, S_2, \dots, S_n).$$

où, pour tout $p \in [1, n]$, S_p désigne le $p^{\text{ième}}$ polynôme symétrique élémentaire des n indéterminées X_1, X_2, \dots, X_n .

Or, pour tout $i \in [1, n]$, $d_i^0(Q_j) \leq 1$; il en découle que A_j est de degré inférieur ou égal à 1 (cf. prop. 2.38). De plus, Q_j est homogène de degré $n-j$; il s'ensuit qu'il existe un scalaire $\beta_j \neq 0$ tel que $Q_j = \beta_j S_{n-j}$.

Il reste à calculer le scalaire β_j ; notons pour cela que le coefficient de VS_{n-j} relatif au monôme $X_2 X_3^2 \dots X_j^{j-1} X_{j+1}^{j+1} \dots X_n^n$ est égal à 1; en considérant le développement du déterminant D'_j , nous voyons que le coefficient de D'_j relatif à ce même monôme est, lui aussi, égal à 1. Finalement, $\beta_j = 1$, et $D'_j = VS_{n-j}$.

La formule (2) s'obtient alors en substituant dans les polynômes D'_j et VS_{n-j} les scalaires $\alpha_1, \alpha_2, \dots, \alpha_n$ aux indéterminées X_1, X_2, \dots, X_n .

Pour calculer certains déterminants, on peut utiliser la dérivation des polynômes et fractions rationnelles; cette méthode permet de mettre en évidence des facteurs multiples. On se sert alors de la

PROPOSITION 3.12. — Dérivation des déterminants. — Soient $K(X)$ le corps des fractions rationnelles à une indéterminée X à coefficients dans K , et $M = (\alpha_{ij})$ un élément de $M_n(K(X))$ (resp. de $M_n(K[X])$). Alors $\text{Det } M$ est une fraction rationnelle (resp. un polynôme) R , dont la dérivée est donnée par la formule :

$$D(\text{Det } M) = D(R) = \sum_{i=1}^n \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{i-1,1} & \dots & \alpha_{i-1,j} & \dots & \alpha_{i-1,n} \\ D\alpha_{i1} & \dots & D\alpha_{ij} & \dots & D\alpha_{in} \\ \alpha_{i+1,1} & \dots & \alpha_{i+1,j} & \dots & \alpha_{i+1,n} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{n1} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{vmatrix}.$$

Autrement dit, pour obtenir la dérivée de $\text{Det } M$, on ajoute les déterminants des n matrices M_i déduites de M en substituant à la $i^{\text{ème}}$ ligne

$$(\alpha_{i1}, \dots, \alpha_{ij}, \dots, \alpha_{in})$$

de M la ligne dérivée de celle-ci, c'est-à-dire

$$(D\alpha_{i1}, \dots, D\alpha_{ij}, \dots, D\alpha_{in}).$$

De même, pour obtenir la dérivée de $\text{Det } M$, on peut ajouter les déterminants des n matrices N_j déduites de M en substituant à la $j^{\text{ème}}$ colonne

$$(\alpha_{1j}, \dots, \alpha_{ij}, \dots, \alpha_{nj})$$

de M la colonne dérivée de celle-ci, c'est-à-dire

$$(D\alpha_{1j}, \dots, D\alpha_{ij}, \dots, D\alpha_{nj}).$$

En effet,

$$(1) \quad \text{Det } M = R = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \alpha_{1,\sigma(1)} \dots \alpha_{h,\sigma(h)} \dots \alpha_{n,\sigma(n)}.$$

Or, pour tout élément σ de \mathfrak{S}_n ,

$$(2) \quad D[\alpha_{1,\sigma(1)} \dots \alpha_{h,\sigma(h)} \dots \alpha_{n,\sigma(n)}] = \sum_{i=1}^n \alpha_{1,\sigma(1)} \dots \alpha_{i-1,\sigma(i-1)} D\alpha_{i,\sigma(i)} \alpha_{i+1,\sigma(i+1)} \dots \alpha_{n,\sigma(n)}.$$

Il découle de (1) et (2) que $D(R) = \sum_{i=1}^n R_i$, où

$$R_i = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \alpha_{1,\sigma(1)} \dots \alpha_{i-1,\sigma(i-1)} D\alpha_{i,\sigma(i)} \alpha_{i+1,\sigma(i+1)} \dots \alpha_{n,\sigma(n)}.$$

Le second membre de cette dernière formule n'est autre que le développement du déterminant de la matrice M_1 , d'où la proposition.

Exercices conseillés : 12, 17 et 18.

§ 4. TRACE D'UN ENDOMORPHISME

PROPOSITION 3.13. — **Applications linéaires élémentaires.** — Soient E et F deux espaces vectoriels sur K .

1. Pour tout élément (a^*, b) de $E^* \times F$, l'application $U_{a^*, b}$ qui à tout vecteur x de E associe le vecteur $\langle a^*, x \rangle b$ de F est une application linéaire de E dans F ; on l'appelle application linéaire élémentaire associée à (a^*, b) .

Si a^* et b ne sont pas nuls, l'image de $U_{a^*, b}$ est la droite Kb de F , et son noyau est l'hyperplan de E noyau de la forme linéaire a^* .

2. L'application $(a^*, b) \mapsto U_{a^*, b}$ est une application bilinéaire de $E^* \times F$ dans $\mathcal{L}(E, F)$.

3. Le sous-espace vectoriel de $\mathcal{L}(E, F)$ engendré par les applications linéaires élémentaires $U_{a^*, b}$, où a^* parcourt E^* et où b parcourt F , n'est autre que le sous-espace vectoriel $\mathcal{L}_f(E, F)$ constitué des applications linéaires de rang fini.

Les assertions 1 et 2 sont immédiates.

Assertion 3. — Il suffit de prouver que toute application linéaire U de rang fini est une combinaison linéaire des applications linéaires élémentaires. Désignons pour cela par n le rang de U , et par $B = (f_1, f_2, \dots, f_n)$ une base de $\text{Im}(U)$. Soit φ_i la forme linéaire sur $\text{Im}(U)$ qui à tout élément de $\text{Im}(U)$ associe sa $i^{\text{ème}}$ composante dans la base B . Il est clair que, pour tout $i \in [1, n]$, $y_i^* = \varphi_i \circ U$ est un élément de E^* , et que, pour tout vecteur x de E ,

$$U(x) = \sum_{i=1}^n \langle y_i^*, x \rangle f_i.$$

Cette dernière relation s'écrit encore

$$U = \sum_{i=1}^n U y_{i, f_i}^*,$$

ce qu'il fallait prouver.

EXEMPLE. — Supposons que les espaces vectoriels E et F sont de dimension finie sur K , et que E et F sont munis de bases $B = (e_1, \dots, e_j, \dots, e_p)$, $B' = (f_1, \dots, f_i, \dots, f_n)$. Désignons par $B^* = (e_1^*, \dots, e_j^*, \dots, e_p^*)$ la base duale de B . Alors les applications linéaires U_{ij} définies par les formules

$$U_{ij}(e_k) = \delta_{jk} f_i$$

(cf. prop. I.3.36) sont élémentaires; plus précisément :

$$U_{ij} = Ue_{j,f_i}^*.$$

Dans le cas particulier où $E = F$, on peut calculer le composé de deux endomorphismes élémentaires, de la manière suivante :

$$\begin{aligned} U_{a'^*,b'} U_{a^*,b}(x) &= U_{a'^*,b'}(\langle a^*, x \rangle \cdot b) = \langle a^*, x \rangle \cdot U_{a'^*,b'}(b) \\ &= \langle a^*, x \rangle \cdot \langle a'^*, b \rangle \cdot b'. \end{aligned}$$

D'où :

$$(1) \quad U_{a'^*,b'} U_{a^*,b} = \langle a'^*, b \rangle U_{a^*,b'}.$$

THÉORÈME 3.8. — Trace d'un endomorphisme. — Soit E un espace vectoriel de dimension finie sur K . Il existe une forme linéaire et une seule sur l'espace vectoriel $\mathfrak{L}(E)$, appelée trace et notée Tr , telle que pour tout endomorphisme élémentaire $U_{a^*,b}$ de E :

$$(2) \quad \text{Tr } U_{a^*,b} = \langle a^*, b \rangle.$$

Si E est muni d'une base $B = (e_1, e_2, \dots, e_n)$, et si l'on désigne par (α_{ij}) la matrice associée à un endomorphisme U de E dans la base B , alors :

$$(3) \quad \text{Tr } U = \sum_{i=1}^n \alpha_{ii}.$$

La trace de U est donc égale à la somme des éléments de la diagonale principale de la matrice associée à U dans la base B .

Prouvons d'abord l'unicité de la trace : elle résulte aussitôt du fait que la formule (2) la détermine sur les endomorphismes $U_{a^*,b}$, lesquels engendrent $\mathfrak{L}(E)$.

Supposons toujours l'existence de la trace acquise, et prenons une base B dans E : alors tout endomorphisme U de E s'écrit d'une manière et d'une seule sous la forme $U = \sum_{i,j} \alpha_{ij} U_{ij}$; d'où $\text{Tr } U = \sum_{i,j} \alpha_{ij} \text{Tr } U_{ij}$. Or,

$$\text{Tr } U_{ij} = \text{Tr } Ue_{j,e_i}^* = \langle e_j^*, e_i \rangle = \delta_{ij}.$$

Finalement :

$$\text{Tr } U = \sum_{i=1}^n \alpha_{ii}.$$

Pour montrer l'existence de la trace, nous sommes donc amené à la définir par la formule (3). Il est immédiat que l'application ainsi introduite est linéaire, et il reste à prouver qu'elle satisfait à la relation (2); soient pour cela a^* un élément de E^* et b un élément de E , que nous décomposons dans les bases B^* et B :

$$a^* = \sum_{j=1}^n \xi_j e_j^*, \quad b = \sum_{i=1}^n \eta_i e_i.$$

D'où :

$$U_{a^*, b} = \sum_{i,j} \xi_j \eta_i U e_{j, e_i}^* = \sum_{i,j} \xi_j \eta_i U_{ij},$$

et par conséquent

$$\text{Tr } U_{a^*, b} = \sum_{i=1}^n \xi_i \eta_i = \langle a^*, b \rangle.$$

Nous sommes amené à poser la

DÉFINITION 3.11. — Trace d'une matrice carrée. — Soit $M = (\alpha_{ij})$ une matrice carrée d'ordre n à éléments dans K . Le scalaire $\sum_{i=1}^n \alpha_{ii}$ s'appelle trace de M , et se note $\text{Tr } M$.

C'est encore la trace de l'endomorphisme de K^n canoniquement associé à M .

Soit maintenant U un endomorphisme d'un passage vectoriel E de dimension finie sur K . Alors, pour toute base B de E ,

$$\text{Tr } U = \text{Tr}[M_B(U)].$$

PROPOSITION 3.14. — Propriétés de la trace. — Soit E un espace vectoriel de dimension finie.

1. Pour tout couple (α, β) de scalaires, et tout couple (U, V) d'endomorphismes de E ,

$$(4) \quad \text{Tr } (\alpha U + \beta V) = \alpha \cdot \text{Tr } U + \beta \cdot \text{Tr } V.$$

2. La trace de l'endomorphisme identique I_E est égale à la dimension de E :

$$(5) \quad \text{Tr } I_E = \dim E.$$

3. Pour tout couple (U, V) d'endomorphismes de E ,

$$(6) \quad \text{Tr } UV = \text{Tr } VU.$$

4. Pour tout endomorphisme U de E ,

$$(7) \quad \text{Tr } {}^t U = \text{Tr } U,$$

où ${}^t U$ désigne l'application transposée de U .

Les assertions 1, 2 et 4 résultent aussitôt du théorème 3.8.

Assertion 3. — Vu la linéarité de la trace, et la bilinéarité du produit, il suffit de prouver la formule (6) lorsque U et V sont des endomorphismes élémentaires, car ces endomorphismes engendrent $\mathfrak{L}(E)$. Le produit de deux tels endomorphismes est alors donné par la formule (1) :

$$U_{a'^*, b'} U_{a^*, b} = \langle a'^*, b \rangle \cdot U_{a^*, b'},$$

d'où :

$$\text{Tr} (U_{a'^*, b'} U_{a^*, b}) = \langle a'^*, b \rangle \cdot \langle a^*, b' \rangle.$$

Le second membre étant invariant lorsqu'on échange (a'^*, b') et (a^*, b) , l'assertion en résulte.

COROLLAIRE 1. — Invariance de la trace par permutation circulaire. — Soient U_1, U_2, \dots, U_p des endomorphismes de E , et σ une permutation circulaire de l'intervalle $[1, p]$; alors :

$$\text{Tr} (U_{\sigma(1)} U_{\sigma(2)} \dots U_{\sigma(p)}) = \text{Tr} (U_1 U_2 \dots U_p).$$

Il suffit de le montrer lorsque σ est le cycle $[1, 2, \dots, p-1]$. Nous sommes ramené au cas de deux facteurs, en posant $U = U_1$, et $V = U_2 U_3 \dots U_p$.

REMARQUE. — Ce résultat peut tomber en défaut lorsque la permutation σ n'est pas circulaire : considérons par exemple un espace vectoriel E de dimension finie strictement supérieure à 1, $B = (e_i)_{1 \leq i \leq n}$ une base de E , et (U_{ij}) la base de $\mathcal{L}(E)$ canoniquement associée à B . Soient i, j, k trois éléments de $[1, n]$, j étant différent de k . Alors

$$\begin{aligned} U_{ij} U_{jk} U_{ki} &= U_{ii}, \\ U_{ij} U_{ki} U_{jk} &= 0. \end{aligned}$$

COROLLAIRE 2. — Invariance de la trace par automorphisme intérieur. — Soit A un automorphisme de l'espace vectoriel E ; alors, pour tout endomorphisme U de E ,

$$(8) \quad \text{Tr} (AUA^{-1}) = \text{Tr} U.$$

REMARQUE. — On peut caractériser la trace par les formules (4), (5) et (6), ou par les formules (4), (5) et (8) (cf. exercice 24).

COROLLAIRE 3. — Propriétés de la trace d'une matrice carrée.

1. Pour tout couple (α, β) de scalaires et tout couple (M, N) d'éléments de $M_n(K)$,

$$(4') \quad \text{Tr} (\alpha M + \beta N) = \alpha \cdot \text{Tr} M + \beta \cdot \text{Tr} N.$$

2. La trace de la matrice unité I_n est égale à n :

$$(5') \quad \text{Tr} I_n = n.$$

3. Pour tout couple (M, N) d'éléments de $M_n(K)$,

$$(6') \quad \text{Tr} MN = \text{Tr} NM.$$

4. Pour tout élément M de $M_n(K)$,

$$(7') \quad \text{Tr} {}^t M = \text{Tr} M.$$

5. Pour tout élément inversible P de $M_n(K)$ et pour tout élément M de $M_n(K)$,

$$(8') \quad \text{Tr}(PMP^{-1}) = \text{Tr } M.$$

Exercices conseillés : 31 à 35.

§ 5. NOTIONS SUR LE CALCUL TENSORIEL ET SUR LE CALCUL EXTÉRIEUR

1. ALGÈBRE DES FORMES MULTILINÉAIRES

DÉFINITION 3.12. — Produit tensoriel de deux formes multilinéaires. — Soient q et r deux entiers strictement positifs, E un espace vectoriel sur K , f une forme q -linéaire sur E et g une forme r -linéaire sur E . Alors l'application h de E^{q+r} dans K définie par la formule

$$(1) \quad h(u_1, u_2, \dots, u_q, v_1, v_2, \dots, v_r) = f(u_1, u_2, \dots, u_q) \cdot g(v_1, v_2, \dots, v_r)$$

est une forme $(q + r)$ -linéaire sur E , appelée produit tensoriel des formes multilinéaires f et g .

REMARQUE. — Lorsque $q = r = 1$, cette définition se réduit à celle du produit tensoriel de deux formes linéaires (cf. déf. 3.5).

Plus généralement, si f est de la forme $y_1^* \otimes y_2^* \otimes \dots \otimes y_q^*$ et si g est de la forme $z_1^* \otimes z_2^* \otimes \dots \otimes z_r^*$, alors

$$h = y_1^* \otimes y_2^* \otimes \dots \otimes y_q^* \otimes z_1^* \otimes z_2^* \otimes \dots \otimes z_r^*.$$

C'est pourquoi le produit tensoriel de f et de g peut être noté sans inconvénient $f \otimes g$. Avec cette nouvelle notation, la formule (1) prend la forme définitive suivante :

$$(2) \quad (f \otimes g)(u_1, u_2, \dots, u_q, v_1, v_2, \dots, v_r) = f(u_1, u_2, \dots, u_q) \cdot g(v_1, v_2, \dots, v_r).$$

PROPOSITION 3.15. — Caractérisation du produit tensoriel de deux formes multilinéaires. — Soient q et r deux entiers strictement positifs, et E un espace vectoriel sur K .

1. L'application $(f, g) \mapsto f \otimes g$ est une application bilinéaire de $\mathcal{M}_q(E) \times \mathcal{M}_r(E)$ dans l'espace vectoriel $\mathcal{M}_{q+r}(E)$.

2. Soient s un entier strictement positif, et h un élément de $\mathcal{M}_s(E)$. Alors

$$(f \otimes g) \otimes h = f \otimes (g \otimes h).$$

3. Si E est de dimension finie sur K , l'application $(f, g) \mapsto f \otimes g$ est l'unique application bilinéaire T de $\mathcal{M}_q(E) \times \mathcal{M}_r(E)$ dans $\mathcal{M}_{q+r}(E)$ telle que, pour tout élément $(y_1^*, y_2^*, \dots, y_q^*)$ de $(E^*)^q$ et pour tout élément $(z_1^*, z_2^*, \dots, z_r^*)$ de $(E^*)^r$,

$$T(y_1^* \otimes y_2^* \otimes \dots \otimes y_q^*, z_1^* \otimes z_2^* \otimes \dots \otimes z_r^*) = y_1^* \otimes y_2^* \otimes \dots \otimes y_q^* \otimes z_1^* \otimes z_2^* \otimes \dots \otimes z_r^*.$$

REMARQUE. — On notera que le produit tensoriel de deux formes multilinéaires n'est pas commutatif.

Dans la suite, nous conviendrons que $\mathcal{M}_0(E) = K$, et, pour tout scalaire α et pour tout élément f de $\mathcal{M}_p(E)$, où $p \in \mathbb{N}$, nous poserons

$$\alpha \otimes f = f \otimes \alpha = \alpha f.$$

Nous laissons au lecteur le soin de vérifier que la proposition 3.15 s'étend alors au cas où q, r , et s sont des entiers naturels.

DÉFINITION 3.13. — Formes multilinéaires sur un espace vectoriel. — Soient E un espace vectoriel sur K , et, pour tout $p \in \mathbb{N}$, $\mathcal{M}_p(E)$ l'espace vectoriel des formes p -linéaires sur E . On appelle forme multilinéaire sur E un élément $f = (f_p)_{p \in \mathbb{N}}$ de l'espace vectoriel $F = \bigoplus_{p \in \mathbb{N}} \mathcal{M}_p(E)$.

Ainsi, tout élément f de F s'écrit de manière unique sous la forme $f = \sum_{p=0}^{+\infty} f_p$, où pour tout $p \in \mathbb{N}$, $f_p \in \mathcal{M}_p(E)$, et où f_p est nul sauf pour un nombre fini d'entiers naturels p .

THÉORÈME 3.9. — Algèbre des formes multilinéaires. — Soient E un espace vectoriel sur K et F l'espace vectoriel $\bigoplus_{p \in \mathbb{N}} \mathcal{M}_p(E)$.

1. Il existe une application bilinéaire T et une seule de $F \times F$ dans F telle que pour tout couple (q, r) d'entiers naturels, et pour tout élément (f_q, g_r) de $\mathcal{M}_q(E) \times \mathcal{M}_r(E)$,

$$T(f_q, g_r) = f_q \otimes g_r.$$

Si $f = \sum_{q=0}^{+\infty} f_q$ et $g = \sum_{r=0}^{+\infty} g_r$ sont deux éléments de F , $T(f, g)$ est donné par la formule :

$$T(f, g) = \sum_{p=0}^{+\infty} h_p,$$

où, pour tout $p \in \mathbb{N}$,

$$h_p = \sum_{q+r=p} f_q \otimes g_r.$$

Désormais, la forme multilinéaire $T(f, g)$ sera appelée produit tensoriel des formes multilinéaires f et g , et notée $f \otimes g$.

Muni de l'application bilinéaire $(f, g) \mapsto f \otimes g$, l'espace vectoriel F s'appelle algèbre des formes multilinéaires sur E et se note $\mathcal{M}(E)$. Cette algèbre est associative et unitaire.

2. Lorsque l'espace vectoriel E est de dimension finie sur K , la sous-algèbre unitaire de $\mathcal{M}(E)$ engendrée par $E^* = \mathcal{M}_1(E)$ n'est autre que $\mathcal{M}(E)$.

Lorsque l'espace vectoriel E est muni d'une base $B = (e_1, e_2, \dots, e_n)$, on obtient une base de l'espace vectoriel $\mathcal{M}(E)$ en réunissant les bases B_p de $\mathcal{M}_p(E)$ canoniquement associées à B , où p parcourt \mathbb{N} .

REMARQUE 1. — Lorsque E est de dimension 1, pour tout $p \in \mathbb{N}$, l'espace vectoriel $\mathcal{M}_p(E)$ est isomorphe à l'espace vectoriel K , et le produit tensoriel d'une forme q -linéaire par une forme r -linéaire s'identifie au produit de deux scalaires dans K . Il en résulte que l'algèbre $\mathcal{M}(E)$ est isomorphe à l'algèbre $K[X]$ des polynômes à une indéterminée à coefficients dans K .

Lorsque E est de dimension strictement supérieure à 1, l'algèbre $\mathcal{M}(E)$ n'est pas commutative.

REMARQUE 2. — Lorsque l'espace vectoriel E n'est pas de dimension finie, E^* n'engendre pas l'algèbre unitaire $\mathcal{M}(E)$; cf. exercice 42.

On trouvera la propriété universelle de l'algèbre des formes multilinéaires dans l'exercice 37.

2. ALGÈBRE DES FORMES MULTILINÉAIRES ALTERNÉES

PROPOSITION 3.16. — Produit extérieur de deux formes multilinéaires alternées. — Soient q et r deux entiers strictement positifs, et E un espace vectoriel de dimension finie n sur K .

1. Il existe une application bilinéaire T de $\mathcal{A}_q(E) \times \mathcal{A}_r(E)$ dans $\mathcal{A}_{q+r}(E)$ et une seule telle que, pour tout élément $(y_1^*, y_2^*, \dots, y_q^*)$ de $(E^*)^q$ et pour tout élément $(z_1^*, z_2^*, \dots, z_r^*)$ de $(E^*)^r$,

$$T(y_1^* \wedge y_2^* \wedge \dots \wedge y_q^*, z_1^* \wedge z_2^* \wedge \dots \wedge z_r^*) = y_1^* \wedge y_2^* \wedge \dots \wedge y_q^* \wedge z_1^* \wedge z_2^* \wedge \dots \wedge z_r^*.$$

Pour tout élément (f, g) de $\mathcal{A}_q(E) \times \mathcal{A}_r(E)$, la forme $(q+r)$ -linéaire $T(f, g)$ s'appelle *produit extérieur des formes multilinéaires f et g* , et se note $f \wedge g$.

2. Soient s un entier strictement positif, et h un élément de $\mathcal{A}_s(E)$. Alors

$$(f \wedge g) \wedge h = f \wedge (g \wedge h).$$

3. Pour tout élément (f, g) de $\mathcal{A}_q(E) \times \mathcal{A}_r(E)$,

$$g \wedge f = (-1)^{qr} f \wedge g.$$

Écartons le cas trivial où $\sup(q, r) \geq n$: alors $T = 0$.

Assertion 1.

L'unicité de T est immédiate, puisque T est bilinéaire, et que les formes q -linéaires (resp. r -linéaires) alternées sur E décomposables constituent une partie génératrice de $\mathcal{A}_q(E)$ (resp. de $\mathcal{A}_r(E)$). En particulier, soit B une base de E ; nous savons (cf. cor. 2 du th. 3.2) que tout élément f de $\mathcal{A}_p(E)$ s'écrit d'une manière et d'une seule sous la forme $f = \sum_Q \alpha_Q e_Q$,

où Q parcourt l'ensemble des parties de $[1, n]$ ayant q éléments; de même, tout élément g de $\mathcal{A}_r(E)$ s'écrit d'une manière et d'une seule sous la forme $g = \sum_R \beta_R e_R$, où R parcourt l'en-

semble des parties de $[1, n]$ ayant r éléments. Il en découle que $T(f, g)$ est nécessairement donné par la relation suivante :

$$(1) \quad T(f, g) = \sum_{Q, R} \alpha_Q \beta_R e_Q \wedge e_R,$$

où $e_Q \wedge e_R$ est la forme $(q+r)$ -linéaire alternée sur E définie par la formule

$$e_Q \wedge e_R = e_{\varphi(1)}^* \wedge e_{\varphi(2)}^* \wedge \dots \wedge e_{\varphi(q)}^* \wedge e_{\psi(1)}^* \wedge e_{\psi(2)}^* \wedge \dots \wedge e_{\psi(r)}^*,$$

φ et ψ désignant les applications strictement croissantes de $[1, q]$ et de $[1, r]$ dans $[1, n]$ canoniquement associées aux parties Q et R .

Existence de T . Nous définissons T par la formule (1). Il est clair que T est une application bilinéaire. Il en résulte aussitôt qu'étant donnée une application strictement croissante ψ de $[1, r]$ dans $[1, n]$, l'application

$$(y_1^* \wedge y_2^* \wedge \dots \wedge y_q^*) \mapsto T(y_1^* \wedge y_2^* \wedge \dots \wedge y_q^*, e_{\psi(1)}^* \wedge e_{\psi(2)}^* \wedge \dots \wedge e_{\psi(r)}^*)$$

est une forme q -linéaire alternée sur E . Sur les éléments e_Q , cette forme prend la même valeur que la forme q -linéaire alternée

$$(y_1^*, y_2^*, \dots, y_q^*) \mapsto y_1^* \wedge y_2^* \wedge \dots \wedge y_q^* \wedge e_{\psi(1)}^* \wedge e_{\psi(2)}^* \wedge \dots \wedge e_{\psi(r)}^*.$$

Il découle du corollaire 1 du théorème 3.2 que ces deux formes q -linéaires sont égales.

Étant donné maintenant un élément $(y_1^*, y_2^*, \dots, y_q^*)$ de $(E^*)^q$, nous voyons par la même méthode que les deux formes r -linéaires alternées

$$\begin{aligned} (z_1^*, z_2^*, \dots, z_r^*) &\mapsto T(y_1^* \wedge y_2^* \wedge \dots \wedge y_q^*, z_1^* \wedge z_2^* \wedge \dots \wedge z_r^*) \\ (z_1^*, z_2^*, \dots, z_r^*) &\mapsto y_1^* \wedge y_2^* \wedge \dots \wedge y_q^* \wedge z_1^* \wedge z_2^* \wedge \dots \wedge z_r^* \end{aligned}$$

sont égales, ce qu'il fallait prouver.

Assertion 2. — Puisque les applications $(f, g, h) \mapsto (f \wedge g) \wedge h$ et $(f, g, h) \mapsto f \wedge (g \wedge h)$ sont trilineaires, et que les formes p -linéaires décomposables constituent une partie génératrice de l'espace vectoriel $\mathcal{A}_p(E)$ pour tout entier $p \in [1, n]$, il suffit de prouver la formule $(f \wedge g) \wedge h = f \wedge (g \wedge h)$ lorsque les trois formes f, g, h sont décomposables, ce qui est immédiat.

Assertion 3. — Comme pour l'assertion 2, nous nous ramenons aussitôt à prouver que pour tout élément $(y_1^*, y_2^*, \dots, y_q^*)$ de $(E^*)^q$, et pour tout élément $(z_1^*, z_2^*, \dots, z_r^*)$ de $(E^*)^r$, $z_1^* \wedge z_2^* \wedge \dots \wedge z_r^* \wedge y_1^* \wedge y_2^* \wedge \dots \wedge y_q^* = (-1)^{qr} y_1^* \wedge y_2^* \wedge \dots \wedge y_q^* \wedge z_1^* \wedge z_2^* \wedge \dots \wedge z_r^*$, ce qui résulte du corollaire de la proposition 3.6.

Dans la suite, nous conviendrons que $\mathcal{A}_0(E) = K$, et, pour tout scalaire α et pour tout élément f de $\mathcal{A}_p(E)$, où $p \in \mathbb{N}$, nous poserons

$$\alpha \wedge f = f \wedge \alpha = \alpha f.$$

Nous laissons au lecteur le soin de vérifier que la proposition 3.16 s'étend alors au cas où q, r et s sont des entiers naturels.

REMARQUE. — Soit f une forme p -linéaire alternée sur E , $p > 0$. Lorsque f est une forme p -linéaire alternée décomposable, $f \wedge f = 0$; lorsque K est de caractéristique différente de 2, et que p est impair, $f \wedge f = 0$, d'après l'assertion 3; lorsque $2p > n$, $f \wedge f = 0$. Mais il faut bien noter que si p est pair, et $2p \leq n$, en général $f \wedge f \neq 0$: prenons par exemple $n = 4$, $p = 2$, et considérons une base $B = (e_1, e_2, e_3, e_4)$ de E ; choisissons $f = e_1 \wedge e_2 + e_3 \wedge e_4$. Alors $f \wedge f = 2e_1 \wedge e_2 \wedge e_3 \wedge e_4 \neq 0$, si K est de caractéristique différente de 2.

DÉFINITION 3.14. — **Formes multilinéaires alternées sur un espace vectoriel.** — Soient E un espace vectoriel sur un corps K , et $\mathcal{M}(E)$ l'algèbre des formes multilinéaires sur E . On dit qu'un élément $f = \sum_{p=0}^{+\infty} f_p$ de $\mathcal{M}(E)$, où pour tout $p \in \mathbb{N}$, $f_p \in \mathcal{M}_p(E)$ est une forme multilinéaire alternée sur E si pour tout $p \in \mathbb{N}$, $f_p \in \mathcal{A}_p(E)$.

THÉORÈME 3.10. — **Algèbre des formes multilinéaires alternées sur E .** — Soit E un espace vectoriel de dimension finie n sur un corps K .

1. L'ensemble F des formes multilinéaires alternées sur E est un sous-espace vectoriel de l'espace vectoriel $\mathcal{M}(E)$ des formes multilinéaires sur E . De plus, F est somme directe de la famille des sous-espaces vectoriels $\mathcal{A}_p(E)$, où p parcourt $[0, n]$.

Autrement dit, tout élément f de F s'écrit de manière unique sous la forme $f = \sum_{p=0}^n f_p$, où pour tout $p \in [0, n]$, $f_p \in \mathcal{A}_p(E)$.

2. Il existe une application bilinéaire T et une seule de $F \times F$ dans F telle que pour tout couple (q, r) d'entiers naturels, et pour tout élément (f_q, g_r) de $\mathcal{A}_q(E) \times \mathcal{A}_r(E)$,

$$T(f_q, g_r) = f_q \wedge g_r.$$

Si $f = \sum_{q=0}^n f_q$, et si $g = \sum_{r=0}^n g_r$ sont deux éléments de F , $T(f, g)$ est donné par la formule

$$T(f, g) = \sum_{p=0}^n h_p,$$

où, pour tout $p \in [0, n]$,

$$h_p = \sum_{q+r=p} f_q \wedge g_r.$$

Désormais, la forme multilinéaire alternée $T(f, g)$ sera appelée *produit extérieur des formes multilinéaires alternées* f et g , et notée $f \wedge g$.

Muni de l'application bilinéaire $(f, g) \mapsto f \wedge g$, l'espace vectoriel F s'appelle *algèbre des formes multilinéaires alternées sur E* , et se note $\mathcal{A}(E)$. Cette algèbre est associative et unitaire; elle est de dimension finie sur K , égale à 2^n .

3. La sous-algèbre unitaire de $\mathcal{A}(E)$ engendrée par $E^* = \mathcal{A}_1(E)$ n'est autre que $\mathcal{A}(E)$.

Ce théorème est une conséquence immédiate du sous-paragraphe 1, mis à part le calcul de la dimension de l'espace vectoriel $\mathcal{A}(E)$, que voici :

$$\dim \mathcal{A}(E) = \sum_{p=0}^n \dim \mathcal{A}_p(E) = \sum_{p=0}^n C_n^p = 2^n$$

(cf. prop. I.1.49).

REMARQUE 1. — Lorsque E est de dimension strictement supérieure à 1, l'algèbre $\mathcal{A}(E)$ n'est pas commutative, en général : en effet, nous savons que pour tout élément (f, g) de $\mathcal{A}_q(E) \times \mathcal{A}_r(E)$,

$$g \wedge f = (-1)^{qr} f \wedge g.$$

REMARQUE 2. — L'étude du cas où l'espace vectoriel E n'est pas de dimension finie est esquissée dans les exercices 41 et 42.

On trouvera la propriété universelle de l'algèbre des formes multilinéaires alternées dans l'exercice 39.

REMARQUE 3. — En calquant les méthodes précédentes, on peut définir l'algèbre des formes multilinéaires symétriques; cf. exercice 36.

§ 6. ALGÈBRE MULTILINÉAIRE SUR UN MODULE

Dans ce paragraphe, A désigne un anneau commutatif unitaire.

Nous allons examiner rapidement comment les théories exposées dans les paragraphes précédents s'étendent au cas des A -modules.

1. APPLICATIONS p -LINÉAIRES, FORMES p -LINÉAIRES

DÉFINITION 3.1 bis. — **Applications p -linéaires.** — Soient E et F deux A -modules, et p un entier strictement positif. On appelle *application p -linéaire sur E à valeurs dans F* une application multilinéaire de E^p dans F .

Les applications p -linéaires sur E à valeurs dans F constituent un A -module, noté $\mathcal{M}_p(E, F)$.

La définition et les propriétés des applications p -linéaires alternées, symétriques et anti-symétriques (cf. déf. 3.2 et 3.3, prop. 3.1, 3.2, 3.4 et 3.5) se généralisent aussitôt, ainsi que la proposition 3.3, à condition de supposer que E est un A -module libre de type fini.

Lorsque $F = A$, la notion d'application p -linéaire se spécialise en celle de forme p -linéaire. On note $\mathcal{M}_p(E)$ le A -module des formes p -linéaires sur E , $\mathcal{S}_p(E)$ et $\mathcal{A}_p(E)$ les sous-modules des formes p -linéaires symétriques et des formes p -linéaires alternées sur E .

La définition et les propriétés des produits tensoriels, symétriques et extérieurs de formes linéaires (cf. déf. 3.5 et prop. 3.6 et 3.7) subsistent dans ce nouveau cadre. En revanche, les propositions 3.8 et 3.9 ne s'étendent pas; on pourra consulter à ce sujet l'exercice 24.

2. DÉTERMINANTS

DÉFINITION 3.6 bis. — Déterminant de n vecteurs. — Soient E un A -module libre ayant une base finie $B = (e_1, e_2, \dots, e_n)$, et $(e_1^*, e_2^*, \dots, e_n^*)$ la base duale de B . La forme n -linéaire alternée $e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*$ s'appelle *déterminant dans la base B* , et se note Det_B .

Le théorème 3.3 s'étend alors sans aucun changement dans la démonstration.

En particulier, $\text{Det}_B = e_1^* \wedge e_2^* \wedge \dots \wedge e_n^*$ est la seule forme n -linéaire alternée sur E prenant la valeur 1 sur (e_1, e_2, \dots, e_n) , et elle constitue une base du A -module $\mathcal{A}_n(E)$ des formes n -linéaires alternées sur E .

La différence essentielle avec le cas des espaces vectoriels apparaît lors du théorème de caractérisation des bases à l'aide du déterminant (cf. th. 3.4), lequel doit être modifié (cf. *infra*).

DÉFINITION 3.7 bis. — Déterminant d'un endomorphisme. — Soit E un A -module libre de dimension finie non nulle n (i. e. ayant une base finie à n éléments). Pour tout endomorphisme U de E , l'extension U_n de U au A -module $\mathcal{M}_n(E)$ laisse stable le sous-module $\mathcal{A}_n(E)$. Ce dernier étant de dimension 1, l'endomorphisme de $\mathcal{A}_n(E)$ coïncidant avec U_n est une homothétie. Le rapport de cette homothétie s'appelle *déterminant de U* , et se note $\text{Det } U$.

Ainsi, pour tout élément f de $\mathcal{A}_n(E)$ et pour toute suite (x_1, x_2, \dots, x_n) de n vecteurs de E ,

$$f[U(x_1), U(x_2), \dots, U(x_n)] = (\text{Det } U) \cdot f(x_1, x_2, \dots, x_n).$$

Les propriétés du déterminant d'un endomorphisme (cf. th. 3.5) se généralisent immédiatement, mais le corollaire du théorème 3.5 relatif à la caractérisation des endomorphismes inversibles doit être modifié (cf. *infra*).

La définition du déterminant d'une matrice carrée d'ordre n à éléments dans A est calquée sur la définition 3.8. La proposition 3.10 concernant les propriétés du déterminant d'une matrice carrée subsiste; il n'en est pas de même de ses corollaires, traitant de l'inversibilité des matrices carrées (cf. *infra*).

3. CALCULS DE DÉTERMINANTS

On suppose que E est un A -module libre ayant une base à n éléments, $n > 0$.

Les calculs de déterminants de matrices carrées remarquables (matrices de permutation, matrices diagonales, matrices triangulaires, matrices triangulaires de matrices) subsistent sans aucun changement.

La définition des matrices mineures et des déterminants mineurs d'une matrice carrée (cf. déf. 3.9), ainsi que la formule de développement d'un déterminant suivant une colonne ou une ligne (cf. th. 3.7) s'étendent, sans aucun changement dans les démonstrations.

Exactement comme dans le cas des corps, on définit la matrice M' des cofacteurs d'une matrice carrée M d'ordre n à éléments dans A , ainsi que sa matrice complémentaire \tilde{M} . Les propriétés de la matrice complémentaire (cf. cor. 1 du th. 3.7) se généralisent aussitôt.

En particulier, pour tout élément M de $M_n(A)$,

$$(1) \quad \tilde{M} \cdot M = M \cdot \tilde{M} = (\text{Det } M) \cdot I_n.$$

Cette formule a plusieurs conséquences très importantes :

a) Caractérisation des matrices carrées inversibles. — Pour qu'un élément M de $M_n(A)$ soit inversible dans l'anneau $M_n(A)$, il faut et il suffit que $\text{Det } M$ soit inversible dans l'anneau A . Alors

$$M^{-1} = (\text{Det } M)^{-1} \tilde{M}.$$

Supposons d'abord que M admette un inverse N . De la relation $NM = MN = I_n$ il résulte que

$$(\text{Det } M) \cdot (\text{Det } N) = 1,$$

ce qui prouve que $\text{Det } M$ est inversible dans A .

Réciproquement, si $\text{Det } M$ est inversible dans A , la relation (1) montre que $(\text{Det } M)^{-1} \tilde{M}$ est inverse de M .

b) Caractérisation des endomorphismes inversibles. — Soit E un A -module libre de dimension finie non nulle n . Pour qu'un endomorphisme U de E soit inversible dans l'anneau $\mathcal{L}(E)$, il faut et il suffit que $\text{Det } U$ soit inversible dans l'anneau A .

Soit $B = (e_1, e_2, \dots, e_n)$ une base de E . Nous savons que l'application $U \mapsto M_B(U)$ est un isomorphisme de l'algèbre unitaire $\mathcal{L}(E)$ sur l'algèbre unitaire $M_n(A)$. L'inversibilité de U équivaut donc à celle de $M_B(U)$; le résultat annoncé découle alors du a), puisque $\text{Det } U = \text{Det } M_B(U)$.

c) Caractérisation des bases. — Soit E un A -module libre de dimension finie non nulle n , muni d'une base $B = (e_1, e_2, \dots, e_n)$. Pour qu'une suite (x_1, x_2, \dots, x_n) de n vecteurs de E soit une base de E , il faut et il suffit que $\text{Det}_B(x_1, x_2, \dots, x_n)$ soit inversible dans l'anneau A .

Les résultats qui précèdent interviennent de manière essentielle dans l'étude des entiers algébriques (cf. *Algèbre* III). Ils servent aussi à fournir des critères pour qu'une suite de n éléments de A^n soit une base de ce A -module.

EXEMPLE. — Bases de Z^n . — Pour qu'une suite (x_1, x_2, \dots, x_n) de n éléments de Z^n soit une base du Z -module Z^n , il faut et il suffit que $\text{Det}(x_1, x_2, \dots, x_n) = \pm 1$.

On laisse au lecteur le soin d'établir un résultat analogue pour les sous-groupes discrets de R^n (cf. ex. I.6.48).

Exercices conseillés : 24 à 27.

4. TRACE D'UN ENDOMORPHISME

On suppose que les A -modules E et F sont libres de dimension finie.

La définition et les propriétés des applications linéaires élémentaires (cf. prop. 3.13)

subsistent sans aucun changement, ainsi que le théorème d'existence et de caractérisation de la trace d'un endomorphisme (cf. th. 3.8).

De même, les propriétés de la trace d'une matrice carrée (cf. prop. 3.14 et ses cor.) s'étendent aussitôt.

5. CALCUL TENSORIEL ET CALCUL EXTÉRIEUR

Tous les résultats du § 5 s'étendent sans aucun changement lorsqu'on suppose que E est un A -module libre de dimension finie.

EXERCICES

CALCULS DE DÉTERMINANTS

1. Soient α , β et γ des nombres réels. Calculer les déterminants suivants :

$$\begin{vmatrix} 1 & \cos \gamma & \cos \beta \\ \cos \gamma & 1 & \cos \alpha \\ \cos \beta & \cos \alpha & 1 \end{vmatrix} \quad \begin{vmatrix} 1 & \cos \alpha & \sin \alpha \\ 1 & \cos \beta & \sin \beta \\ 1 & \cos \gamma & \sin \gamma \end{vmatrix} \quad \begin{vmatrix} 1 & \cos \alpha & \sin 2\alpha \\ 1 & \cos \beta & \sin 2\beta \\ 1 & \cos \gamma & \sin 2\gamma \end{vmatrix}$$

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \cos \gamma & \cos \beta \\ 1 & \cos \gamma & 1 & \cos \alpha \\ 1 & \cos \beta & \cos \alpha & 1 \end{vmatrix}.$$

2. Soient α , β et γ des scalaires. Calculer le déterminant suivant :

$$\begin{vmatrix} \alpha & \gamma & \gamma & \beta \\ \gamma & \alpha & \beta & \gamma \\ \gamma & \beta & \alpha & \gamma \\ \beta & \gamma & \gamma & \alpha \end{vmatrix}.$$

3. Soient n un entier naturel non nul, β un scalaire et $(\alpha_0, \alpha_1, \dots, \alpha_n)$ une suite de $n + 1$ scalaires. Calculer le déterminant suivant :

$$\begin{vmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \alpha_n \\ -1 & \beta & 0 & \dots & 0 & 0 \\ 0 & -1 & \beta & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \beta & 0 \\ 0 & 0 & 0 & \dots & -1 & \beta \end{vmatrix}.$$

4. 1. Soient m et p deux entiers strictement positifs, $m \geq p$. Calculer

$$\begin{vmatrix} 1 & C_m^1 & C_m^2 & \dots & C_m^{p-1} & C_m^p \\ 1 & C_{m+1}^1 & C_{m+1}^2 & \dots & C_{m+1}^{p-1} & C_{m+1}^p \\ 1 & C_{m+2}^1 & C_{m+2}^2 & \dots & C_{m+2}^{p-1} & C_{m+2}^p \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & C_{m+p}^1 & C_{m+p}^2 & \dots & C_{m+p}^{p-1} & C_{m+p}^p \end{vmatrix}.$$

2. Soit n un entier naturel. Calculer le déterminant

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & C_2^1 & C_3^1 & \dots & C_{n-1}^1 & C_n^1 \\ 1 & C_3^2 & C_4^2 & \dots & C_n^2 & C_{n+1}^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & C_n^{n-1} & C_{n+1}^{n-1} & \dots & C_{2n-3}^{n-1} & C_{2n-2}^{n-1} \end{vmatrix}.$$

3. Soient n et p deux entiers naturels. Montrer que le déterminant

$$\begin{vmatrix} C_{n+1}^1 & 1 & 0 & 0 & \dots & 0 \\ C_{n+2}^2 & C_{n+2}^1 & 1 & 0 & \dots & 0 \\ C_{n+3}^3 & C_{n+3}^2 & C_{n+3}^1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ C_{n+p}^p & C_{n+p}^{p-1} & C_{n+p}^{p-2} & C_{n+p}^{p-3} & \dots & C_{n+p}^1 \end{vmatrix}$$

est égal à C_{n+p}^p .

4. Soient K un corps de caractéristique nulle, et α un scalaire. Calculer le déterminant

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & C_1^1 & 0 & \dots & 0 & \alpha \\ 1 & C_2^1 & C_2^2 & \dots & 0 & \alpha^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & C_n^1 & C_n^2 & \dots & C_n^{n-1} & \alpha^n \end{vmatrix}$$

5. Soit n un entier strictement positif. Calculer le déterminant

$$\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ n+1 & n+2 & n+3 & \dots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \dots & 3n \\ \dots & \dots & \dots & \dots & \dots \\ n^2-n+1 & n^2-n+2 & n^2-n+3 & \dots & n^2 \end{vmatrix}.$$

6. Soient α et β deux scalaires. Calculer le déterminant

$$\begin{vmatrix} \alpha + \beta & 2\alpha & 2\alpha & \dots & 2\alpha \\ 2\beta & \alpha + \beta & 2\alpha & \dots & 2\alpha \\ 2\beta & 2\beta & \alpha + \beta & \dots & 2\alpha \\ \dots & \dots & \dots & \dots & \dots \\ 2\beta & 2\beta & 2\beta & \dots & \alpha + \beta \end{vmatrix}.$$

7. Soient n un entier strictement positif, $(\alpha_i)_{1 \leq i \leq n}$ et $(\beta_j)_{1 \leq j \leq n}$ deux suites de scalaires. Calculer le déterminant

$$\begin{vmatrix} \alpha_1 + \beta_1 & \beta_1 & \beta_1 & \dots & \beta_1 \\ \beta_2 & \alpha_2 + \beta_2 & \beta_2 & \dots & \beta_2 \\ \beta_3 & \beta_3 & \alpha_3 + \beta_3 & \dots & \beta_3 \\ \dots & \dots & \dots & \dots & \dots \\ \beta_n & \beta_n & \beta_n & \dots & \alpha_n + \beta_n \end{vmatrix}.$$

8. Soient n un entier strictement positif, $\alpha_1, \alpha_2, \dots, \alpha_n$ des scalaires. Calculer le déterminant

$$\begin{vmatrix} -\alpha_1 & \alpha_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -\alpha_2 & \alpha_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & -\alpha_3 & \alpha_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & -\alpha_n & \alpha_n \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{vmatrix}.$$

9. Soient n un entier naturel, $\alpha_0, \alpha_1, \dots, \alpha_n$ des nombres réels. Calculer les déterminants

$$\begin{vmatrix} 1 & \cos \alpha_0 & \cos 2\alpha_0 & \dots & \cos n\alpha_0 \\ 1 & \cos \alpha_1 & \cos 2\alpha_1 & \dots & \cos n\alpha_1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \cos \alpha_n & \cos 2\alpha_n & \dots & \cos n\alpha_n \end{vmatrix} \quad \begin{vmatrix} \sin \alpha_0 & \sin 2\alpha_0 & \dots & \sin (n+1)\alpha_0 \\ \sin \alpha_1 & \sin 2\alpha_1 & \dots & \sin (n+1)\alpha_1 \\ \dots & \dots & \dots & \dots \\ \sin \alpha_n & \sin 2\alpha_n & \dots & \sin (n+1)\alpha_n \end{vmatrix}.$$

10. Soient n un entier supérieur ou égal à 2, $\alpha_0, \alpha_1, \dots, \alpha_n$ et β des nombres réels. Montrer que

$$\begin{vmatrix} \cos \alpha_0 & \cos (\alpha_0 + \beta) & \dots & \cos (\alpha_0 + n\beta) \\ \cos \alpha_1 & \cos (\alpha_1 + \beta) & \dots & \cos (\alpha_1 + n\beta) \\ \dots & \dots & \dots & \dots \\ \cos \alpha_n & \cos (\alpha_n + \beta) & \dots & \cos (\alpha_n + n\beta) \end{vmatrix} = 0.$$

11. Soient K un corps commutatif, n un entier naturel, $(\lambda_j)_{1 \leq j \leq n}$ une suite de n scalaires, et $M = (\alpha_{ij})$ un élément de $M_{n+1}(K)$ tel que

$$\alpha_{ij} = \lambda_j \alpha_{i,j+1} \quad \text{si } i \geq j+1,$$

Montrer que

$$\text{Det } (\alpha_{ij}) = (\alpha_{11} - \lambda_1 \alpha_{12})(\alpha_{22} - \lambda_2 \alpha_{23}) \dots (\alpha_n - \lambda_n \alpha_{n,n+1}) \alpha_{n+1,n+1}.$$

Applications.

1. Soient $(\alpha_i)_{1 \leq i \leq n}$ et $(\beta_j)_{1 \leq j \leq n}$ deux suites de scalaires. Calculer

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \beta_1 & \alpha_1 & \alpha_1 & \dots & \alpha_1 \\ \beta_1 & \beta_2 & \alpha_2 & \dots & \alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ \beta_1 & \beta_2 & \beta_3 & \dots & \alpha_n \end{vmatrix}.$$

2. Soient $\xi, \alpha_1, \alpha_2, \dots, \alpha_n$ des scalaires. Calculer

$$\begin{vmatrix} \xi & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & 1 \\ \alpha_1 & \xi & \alpha_2 & \dots & \alpha_{n-1} & 1 \\ \alpha_1 & \alpha_2 & \xi & \dots & \alpha_{n-1} & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n & 1 \end{vmatrix} \quad \begin{vmatrix} \xi & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1 & \xi & \alpha_2 & \dots & \alpha_n \\ \alpha_1 & \alpha_2 & \xi & \dots & \alpha_n \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \xi \end{vmatrix}.$$

12. Soient K un corps commutatif, n et p deux entiers strictement positifs, $(\alpha_1, \dots, \alpha_j, \dots, \alpha_p)$ une suite de p scalaires, et $(Q_1, \dots, Q_i, \dots, Q_p)$ une suite d'éléments de $K[X]$ de degré

inférieur ou égal à n . On considère la matrice carrée $M = (\gamma_{ij})$ où, pour tout couple (i, j) d'indices appartenant à l'intervalle $[1, p]$, $\gamma_{ij} = Q_i(\alpha_j)$.

1. Prouver que si $p > n + 1$, $\text{Det } M = 0$.

2. On suppose que $p = n + 1$. Pour tout $i \in [1, p]$, on écrit Q_i sous la forme

$$Q_i = \sum_{j=1}^p \beta_{ij} X^{j-1}, \text{ et on note } N \text{ la matrice carrée } (\beta_{ij}). \text{ Prouver que}$$

$$\text{Det } M = (\text{Det } N) \cdot V(\alpha_1, \alpha_2, \dots, \alpha_p).$$

En déduire une condition nécessaire et suffisante pour que $\text{Det } M$ soit différent de 0.

3. Soit $(\beta_1, \dots, \beta_i, \dots, \beta_p)$ une suite de p scalaires. On considère la matrice $N = (\gamma_{ij})$, où $\gamma_{ij} = (\beta_i + \alpha_j)^n$. Prouver que si $p > n + 1$, $\text{Det } N = 0$. Calculer $\text{Det } N$ lorsque $p = n + 1$.

Retrouver la valeur de ce déterminant à l'aide de la théorie des polynômes à plusieurs indéterminées.

Application. — Soient n et p deux entiers strictement positifs tels que $n < p$. Calculer le déterminant

$$\begin{vmatrix} 1^n & 2^n & 3^n & \dots & p^n \\ 2^n & 3^n & 4^n & \dots & (p+1)^n \\ 3^n & 4^n & 5^n & \dots & (p+2)^n \\ \dots & \dots & \dots & \dots & \dots \\ p^n & (p+1)^n & (p+2)^n & \dots & (2p-1)^n \end{vmatrix}.$$

THÉORIE DES DÉTERMINANTS

13. Déterminant de la transposée d'une matrice carrée.

Soient $B = (e_1, e_2, \dots, e_n)$ la base canonique de K^n et B^* la base duale de B . Pour tout élément M de $M_n(K)$, on note x_1, x_2, \dots, x_n les vecteurs colonnes de M , et $y_1^*, y_2^*, \dots, y_n^*$ les vecteurs lignes de M .

1. Prouver que l'application f qui à toute suite (x_1, x_2, \dots, x_n) de n éléments de K^n associe le scalaire $\text{Det}_{B^*}(y_1^*, y_2^*, \dots, y_n^*)$ est n -linéaire. (On pourra utiliser la formule du développement de ce déterminant.)

2. Prouver que f est alternée. (On pourra comparer le rang des formes linéaires $y_1^*, y_2^*, \dots, y_n^*$ à celui des vecteurs x_1, x_2, \dots, x_n .)

3. Calculer $f(e_1, e_2, \dots, e_n)$.

4. Déduire de ce qui précède que

$$f(x_1, x_2, \dots, x_n) = \text{Det}_B(x_1, x_2, \dots, x_n).$$

14 A. Soient E un ensemble non vide, n un entier naturel non nul, et (f_1, f_2, \dots, f_n) une suite de n éléments de $\mathcal{F}(E, K)$. Montrer qu'il est équivalent de dire :

1. Les fonctions f_1, f_2, \dots, f_n sont linéairement indépendantes dans $\mathcal{F}(E, K)$.

2. Il existe une suite (y_1, y_2, \dots, y_n) de points distincts de E telle que

$$\text{Det}(f_i(y_j)) \neq 0.$$

(Pour démontrer que $1 \Rightarrow 2$, on pourra raisonner par récurrence sur n .)

15 A. Soient G un groupe et f un élément de $\mathcal{F}(G, K)$. Montrer qu'il est équivalent de dire :

1. Le sous-espace vectoriel E_f (resp. ${}_fE$) de $\mathcal{F}(G, K)$ engendré par les translatées à droite (resp. à gauche) de f , c'est-à-dire les fonctions de la forme

$$f_x : y \mapsto f(yx) \quad (\text{resp. } {}_xf : y \mapsto f(xy))$$

est de dimension finie.

2. Il existe deux suites (g_1, g_2, \dots, g_n) et (h_1, h_2, \dots, h_n) d'éléments de $\mathcal{F}(G, K)$ telles que, pour tout couple (x, y) d'éléments de G ,

$$f(xy) = \sum_{i=1}^n g_i(x)h_i(y).$$

Dans ces conditions, prouver qu'on peut choisir les fonctions g_i dans l'espace vectoriel E_f et les fonctions h_i dans l'espace vectoriel ${}_fE$. (On pourra prendre pour la suite (h_1, h_2, \dots, h_n) une base $(a_1f, a_2f, \dots, a_nf)$ de ${}_fE$ et décomposer ${}_xf$ dans cette base sous la forme

$${}_xf = \sum_{i=1}^n g_i(x)f_{a_i}.$$

On montrera alors que g_i appartient à E_f , en utilisant l'exercice précédent.)

16 B. Développement de Laplace d'un déterminant.

Soient A un anneau commutatif unitaire, $B = (e_1, e_2, \dots, e_n)$ la base canonique de A^n , p un entier tel que $0 < p < n$, et \mathcal{T} l'ensemble des parties de $[1, n]$ à p éléments. Pour toute partie P de $[1, n]$, on désigne par P' le complémentaire de P dans $[1, n]$, et on pose

$$\varepsilon_P = (-1)^{\text{card } C(P)},$$

où $C(P)$ désigne l'ensemble des éléments (i, i') de $P \times P'$ tels que $i > i'$.

Pour tout élément $M = (\alpha_{ij})$ de $M_n(A)$ et pour tout couple (P, Q) de parties non vides de $[1, n]$ on note $M_{P,Q}$ la matrice (α_{ij}) où i parcourt P et où j parcourt Q .

1. Prouver que, pour tout élément M de $M_n(A)$,

$$\text{Det } M = \sum_{P \in \mathcal{T}} \text{Det } M_{P,[1,p]} \cdot \text{Det}_B(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)}, x_{p+1}, \dots, x_n),$$

où, pour tout $j \in [p+1, n]$, x_j désigne le $j^{\text{ième}}$ vecteur colonne de M , et où φ désigne l'application strictement croissante de $[1, p]$ dans $[1, n]$ définie par P . (On pourra étudier la forme p -linéaire alternée f qui à tout élément (y_1, y_2, \dots, y_p) de A^p associe $\text{Det}_B(y_1, y_2, \dots, y_p, x_{p+1}, \dots, x_n)$.)

En déduire que

$$\text{Det } M = \sum_{P \in \mathcal{J}} \varepsilon_P \text{Det } M_{P, [1, p]} \cdot \text{Det } M_{P', [p+1, n]}.$$

Examiner le cas particulier où M est de la forme

$$\begin{pmatrix} M_1 & N \\ 0 & M_2 \end{pmatrix},$$

où $M_1 \in M_p(A)$, $M_2 \in M_{n-p}(A)$ et $N \in M_{p, n-p}(A)$.

2. Soit H un élément de \mathcal{J} . Prouver que

$$\text{Det } M = \varepsilon_H \sum_{P \in \mathcal{J}} \varepsilon_P \text{Det } M_{P, H} \cdot \text{Det } M_{P', H'}$$

(formule de développement de Laplace du déterminant de M suivant les p colonnes relatives à H).

En déduire que pour tout élément I de \mathcal{J} distinct de H ,

$$\sum_{P \in \mathcal{J}} \varepsilon_P \text{Det } M_{P, H} \cdot \text{Det } M_{P', I'} = 0.$$

3. Établir de même une formule de développement de Laplace de M suivant les p lignes relatives à un élément H de \mathcal{J} .

4. *Applications.*

a) Soient a, b, c et d quatre éléments de K . Calculer le déterminant

$$\begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ a & b & c & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & a & b & c & d \\ 0 & a^2 & b^2 & c^2 & d^2 \end{vmatrix}.$$

b) Soient p et q deux éléments de K . Pour tout élément (x, y, z, t) de K^4 , on pose

$$M_{x, y, z, t} = \begin{pmatrix} x & py & qz & -pqt \\ y & x & qt & -qz \\ z & -pt & x & py \\ t & -z & y & x \end{pmatrix}.$$

Prouver que

$$\text{Det } M_{x, y, z, t} = [(x^2 - py^2) - q(z^2 - pt^2)]^2.$$

17 A. Déterminants des matrices antisymétriques.

Soit n un entier naturel non nul. On rappelle (cf. exercice I.3.67) qu'un élément M de $M_n(K)$ est dit antisymétrique si ${}^t M = -M$.

1. On suppose que la caractéristique de K est différente de 2. Prouver que si $n = 2p + 1$, où $p \in \mathbb{N}$, le déterminant d'une matrice antisymétrique d'ordre n est nul.

2. On suppose que $n = 2p$, où $p \in \mathbb{N}^*$. Soit $A = K[X_{ij}]_{1 \leq i < j \leq n}$ l'algèbre des poly-

nômes à $\frac{n(n-1)}{2}$ indéterminées à coefficients dans K . Soit $T = (T_{ij})$ l'élément de $M_n(A)$ défini par les relations

$$T_{ij} = X_{ij} \text{ si } i < j, \quad T_{ij} = 0 \text{ si } i = j \quad \text{et} \quad T_{ij} = -X_{ji} \text{ si } i > j.$$

On note U la matrice mineure de T associée à la première ligne et à la première colonne, et V la matrice mineure de T associée aux deux premières lignes et aux deux premières colonnes. Enfin, pour tout élément j de $[2, n]$, on note U_j la matrice mineure de U associée à T_{2j} .

Prouver que pour tout élément k de $[2, n]$,

$$\sum_{j=2}^n (-1)^{j+1} T_{kj} \text{Det } U_j = 0.$$

En multipliant la deuxième colonne de T par $\text{Det } V$, et en lui ajoutant chacune des $n-2$ dernières colonnes multipliées respectivement par $(-1)^{j+1} \text{Det } U_j$, prouver qu'il existe un élément W de $M_{n-1}(A)$ tel que

$$\text{Det } T \cdot \text{Det } V = (\text{Det } W) \cdot \left(\sum_{j=2}^n (-1)^{j+1} T_{1j} \text{Det } U_j \right).$$

En développant $\text{Det } W$ suivant la première colonne de W , prouver que

$$\text{Det } T \cdot \text{Det } V = \left(\sum_{j=2}^n (-1)^{j+1} T_{1j} \text{Det } U_j \right)^2.$$

En déduire, par récurrence sur l'entier p , qu'il existe un élément P de $K[X_{ij}]_{1 \leq i < j \leq n}$ tel que $\text{Det } T = P^2$. (On utilisera la factorialité de l'anneau A .)

Prouver finalement le résultat suivant :

Pour tout entier naturel non nul p , il existe un élément P_p de $K[X_{ij}]_{1 \leq i < j \leq 2p}$ tel que, pour tout élément antisymétrique $M = (\alpha_{ij})$ de $M_{2p}(K)$,

$$\text{Det } M = [P_p(\alpha_{ij})]^2.$$

(On trouvera une autre démonstration de ce résultat au chapitre III.1, utilisant la réduction des formes bilinéaires alternées.)

18 A. Déterminants des matrices centrosymétriques.

Soient n un entier naturel non nul et $A = K[X_{ij}]$ l'anneau des polynômes à n^2 indéterminées à coefficients dans K .

1. On suppose que $n = 2p$, où $p \in \mathbb{N}^*$. On considère les matrices $T = (T_{ij})$ et $U = (U_{ij})$ définies par les relations

$$\begin{aligned} T_{ij} &= U_{ij} = X_{ij} & \text{si } j \leq p \\ T_{ij} &= -U_{ij} = X_{n+1-i, n+1-j} & \text{si } j > p. \end{aligned}$$

A l'aide de l'exercice I.3.66, montrer qu'il existe deux couples (T', T'') et (U', U'') d'éléments de $M_p(A)$ tels que

$$\text{Det } T = \text{Det } T' \cdot \text{Det } T'' \quad \text{et} \quad \text{Det } U = \text{Det } U' \cdot \text{Det } U''.$$

2. On suppose que $n = 2p + 1$, où $p \in \mathbb{N}^*$. On considère les matrices $T = (T_{ij})$ et $U = (U_{ij})$ définies par les relations

$$\begin{aligned} T_{ij} &= U_{ij} = X_{ij} && \text{si } j \leq p \text{ ou si } j = p \text{ et } i \leq p + 1 \\ T_{ij} &= -U_{ij} = X_{n+1-i, n+1-j} && \text{dans les autres cas.} \end{aligned}$$

Montrer qu'il existe un élément T' de $M_p(A)$ et un élément T'' de $M_{p+1}(A)$ tels que

$$\text{Det } T = \text{Det } T' \cdot \text{Det } T'',$$

et que si K est de caractéristique différente de 2, $\text{Det } U = 0$.

3. Appliquer les résultats précédents aux matrices centrosymétriques à éléments dans K .

FORMES MULTILINÉAIRES

19 A. Développement des applications p -linéaires symétriques.

Soient E un espace vectoriel de dimension finie non nulle n sur K , p un entier naturel non nul et \mathcal{S} l'ensemble des applications s de $[1, n]$ dans \mathbb{N} telles que $\sum_{j=1}^n s(j) = p$.

1. Soit $B = (e_1, e_2, \dots, e_n)$ une base de E . Pour tout élément s de \mathcal{S} , on désigne par e_s l'élément de $\mathcal{S}_p(E)$ défini par la formule

$$e_s = \prod_{j=1}^n (e_j^*)^{s(j)} = e_{\varphi(1)}^* \cdot e_{\varphi(2)}^* \cdots e_{\varphi(p)}^*,$$

où φ désigne l'unique application croissante de $[1, p]$ dans $[1, n]$ telle que, pour tout élément j de $[1, n]$, $s(j) = \text{card } \varphi^{-1}(j)$.

a) Soient ψ une application de $[1, p]$ dans $[1, n]$ et t l'élément de \mathcal{S} défini par la formule $t(j) = \text{card } \psi^{-1}(j)$. Prouver que

$$\begin{aligned} e_s(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)}) &= s! && \text{si } t = s \\ &= 0 && \text{si } t \neq s, \end{aligned}$$

où l'on pose $s! = \prod_{j=1}^n s(j)!$

b) En déduire que si K est de caractéristique 0, $\frac{1}{s!} e_s$ est l'unique forme p -linéaire symétrique sur E prenant la valeur 1 sur $(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)})$ et la valeur 0 sur $(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)})$ si $t \neq s$.

c) On suppose que K est de caractéristique 0. Soit S une application p -linéaire symétrique sur E à valeurs dans un espace vectoriel F sur K . Prouver que, pour toute suite (x_1, x_2, \dots, x_p) d'éléments de E ,

$$S(x_1, x_2, \dots, x_p) = \sum_{s \in \mathcal{S}} \frac{1}{s!} e_s(x_1, x_2, \dots, x_p) b_s,$$

où $b = S(e_{\varphi(1)}, e_{\varphi(2)}, \dots, e_{\varphi(p)})$.

En déduire que les éléments e_s , où s parcourt \mathcal{S} , constituent une base de l'espace vectoriel $\mathcal{S}_p(E)$ des formes p -linéaires symétriques sur E .

2. Prouver que si K est de caractéristique 0, l'espace vectoriel $\mathcal{S}_p(E)$ est de dimension C_{n+p-1}^p , et que les formes p -linéaires symétriques décomposables constituent une famille génératrice de cet espace vectoriel.

3. Montrer que les résultats précédents peuvent tomber en défaut si K n'est pas de caractéristique 0. (On pourra considérer l'espace vectoriel $\mathcal{S}_2(E)$ des formes bilinéaires symétriques sur E , le corps K étant de caractéristique 2. On montrera que pour tout élément j de $[1, n]$, $e_j^* \cdot e_j^* = 0$, et que la forme bilinéaire symétrique $e_j^* \otimes e_j^*$ n'appartient pas au sous-espace vectoriel engendré par la famille $(e_s)_{s \in \mathcal{S}}$.)

20. Symétrisation et antisymétrisation réduite.

On conserve les notations de l'exercice 19.

1. Soit f une forme p -linéaire sur un espace vectoriel E . On appelle symétrisée réduite de f la forme p -linéaire $S'(f)$ définie par la formule

$$S'(f)(x_1, x_2, \dots, x_p) = \sum_{\sigma \in \mathfrak{S}_p/G} f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(p)}),$$

où G désigne le stabilisateur de f dans \mathfrak{S}_p . Prouver que $S'(f)$ est une forme p -linéaire symétrique.

2. On suppose que l'espace vectoriel E est de dimension finie non nulle n . Soit $B = (e_1, e_2, \dots, e_n)$ une base de E . Pour tout élément s de \mathcal{S} , on pose

$$e'_s = S'(e_{\varphi(1)}^* \otimes e_{\varphi(2)}^* \otimes \dots \otimes e_{\varphi(p)}^*).$$

Prouver que, pour toute application ψ de $[1, p]$ dans $[1, n]$,

$$\begin{aligned} e'_s(e_{\psi(1)}, e_{\psi(2)}, \dots, e_{\psi(p)}) &= 1 && \text{si } t = s \\ &= 0 && \text{si } t \neq s. \end{aligned}$$

En déduire que les éléments e'_s , où s parcourt \mathcal{S} , constituent une base de l'espace vectoriel $\mathcal{S}_p(E)$ des formes p -linéaires symétriques sur E .

Prouver enfin que pour tout élément s de \mathcal{S} , $e_s = s! e'_s$.

3. Définir de manière analogue l'antisymétrisée réduite $A'(f)$ d'une forme p -linéaire f . Pour toute partie P de E ayant p éléments, on pose

$$e'_P = A'(e_{\varphi(1)}^* \otimes e_{\varphi(2)}^* \otimes \dots \otimes e_{\varphi(p)}^*),$$

où φ est l'application strictement croissante de $[1, p]$ dans $[1, n]$ canoniquement associée à P . Comparer e'_P et e_P .

21 A. Propriété universelle de l'espace vectoriel $\mathcal{M}_p(E)$.

Soient E un espace vectoriel de dimension finie sur K et p un entier naturel non nul. Prouver que, pour tout couple (F, T) constitué d'un espace vectoriel F sur K et d'une application p -linéaire T de $(E^*)^p$ dans F , il existe une application linéaire \tilde{T} et une seule de $\mathcal{M}_p(E)$ dans F telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$\tilde{T}(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = T(y_1^*, y_2^*, \dots, y_p^*).$$

(Pour établir l'existence de \tilde{T} , on pourra considérer une base de E .)

22 B. Propriété universelle de l'espace vectoriel $\mathcal{S}_p(E)$.

Soient E un espace vectoriel de dimension finie sur K et p un entier naturel non nul.

1. On suppose que K est de caractéristique 0. Prouver que, pour tout couple (F, T) constitué d'un espace vectoriel F sur K et d'une application p -linéaire symétrique T de $(E^*)^p$ dans F , il existe une application linéaire \tilde{T} et une seule de $\mathcal{S}_p(E)$ dans F telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$\tilde{T}(y_1^* \cdot y_2^* \dots y_p^*) = T(y_1^*, y_2^*, \dots, y_p^*).$$

En déduire qu'il existe une application linéaire S et une seule de $\mathcal{M}_p(E)$ dans $\mathcal{S}_p(E)$ telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$,

$$S(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = y_1^* \cdot y_2^* \dots y_p^*.$$

Prouver que S coïncide avec l'endomorphisme de symétrisation de $\mathcal{M}_p(E)$.

Montrer que S est surjective, et que le noyau de S n'est autre que le sous-espace vectoriel H de $\mathcal{M}_p(E)$ engendré par les éléments de la forme

$$y_{\tau(1)}^* \otimes y_{\tau(2)}^* \otimes \dots \otimes y_{\tau(p)}^* - y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*,$$

où τ parcourt l'ensemble des transpositions élémentaires de $[1, p]$ et où, pour tout élément j de $[1, p]$, y_j^* appartient à E^* .

2. Dans le cas où la caractéristique de K est quelconque, on considère encore le sous-espace vectoriel H de $\mathcal{M}_p(E)$ défini comme dans la question 1, et l'application canonique φ de $\mathcal{M}_p(E)$ sur $\mathcal{M}_p(E)/H$. Prouver que le couple $(\mathcal{M}_p(E)/H, \varphi)$ satisfait à la propriété universelle énoncée dans la question 1. (On pourra utiliser l'exercice 21.) Montrer qu'il existe une application linéaire j et une seule de $\mathcal{M}_p(E)/H$ dans $\mathcal{S}_p(E)$ telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$(j \circ \varphi)(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = y_1^* \cdot y_2^* \dots y_p^*.$$

Montrer que si K est de caractéristique 0, j est un isomorphisme d'espaces vectoriels. En déduire que H est égal au noyau de S .

3. Prouver enfin que si K est de caractéristique 0, $\mathcal{M}_p(E) = \text{Ker}(S) \oplus \text{Im}(S)$. (On pourra utiliser la relation $S^2 = p! S$.)

23 A. Propriété universelle de l'espace vectoriel $\mathcal{A}_p(E)$.

Soient E un espace vectoriel de dimension finie sur K et p un entier naturel non nul.

1. Prouver que, pour tout couple (F, T) constitué d'un espace vectoriel F sur K et d'une application p -linéaire alternée T de $(E^*)^p$ dans F , il existe une application linéaire \tilde{T} et une seule de $\mathcal{A}_p(E)$ dans F telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$\tilde{T}(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*) = T(y_1^*, y_2^*, \dots, y_p^*).$$

En déduire qu'il existe une application linéaire A et une seule de $\mathcal{M}_p(E)$ dans $\mathcal{A}_p(E)$ telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$,

$$A(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*.$$

Prouver que A coïncide avec l'endomorphisme d'antisymétrisation de $\mathcal{M}_p(E)$.

Montrer que A est surjective, et que le noyau de A contient le sous-espace vectoriel H de $\mathcal{M}_p(E)$ engendré par les éléments de la forme $y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*$, où, pour tout élément j de $[1, p]$, y_j^* appartient à E^* et où il existe deux éléments distincts j et k de $[1, p]$ tels que $y_j^* = y_k^*$.

2. Prouver que l'espace vectoriel quotient $\mathcal{M}_p(E)/H$ et l'application canonique φ de $\mathcal{M}_p(E)$ sur $\mathcal{M}_p(E)/H$ satisfont à la propriété universelle de l'espace vectoriel $\mathcal{A}_p(E)$. (On pourra utiliser l'exercice 21.) Montrer qu'il existe une application linéaire j et une seule de $\mathcal{M}_p(E)/H$ dans $\mathcal{A}_p(E)$ telle que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$(j \circ \varphi)(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*,$$

et que j est un isomorphisme d'espaces vectoriels. En déduire que H est égal au noyau de A .

3. Prouver enfin que si K est de caractéristique 0, $\mathcal{A}_p(E) = \text{Ker}(A) \oplus \text{Im}(A)$. (On pourra utiliser la relation $A^2 = p! A$.)

24 B. Identité fondamentale des formes p -linéaires alternées.

Soient A un anneau commutatif unitaire et E un A -module.

1. Soient p un entier naturel non nul, g une forme p -linéaire alternée sur E et h l'application de E^{p+1} dans E qui à tout élément $(x_1, x_2, \dots, x_{p+1})$ associe le vecteur

$$h(x_1, x_2, \dots, x_{p+1}) = \sum_{i=1}^{p+1} (-1)^i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{p+1}) \cdot x_i.$$

Prouver que l'application h est p -linéaire alternée.

2. Dans toute la suite, on suppose que E est un A -module libre de type fini, admettant une base $B = (e_1, e_2, \dots, e_p)$. Soient p un entier naturel non nul, et $(x_1, x_2, \dots, x_{p+1})$ une suite de $p+1$ éléments de E telle que, pour tout élément f de $\mathcal{A}_{p+1}(E)$,

$$f(x_1, x_2, \dots, x_{p+1}) = 0.$$

Prouver que, pour toute application multilinéaire alternée h de E^{p+1} dans E ,

$$h(x_1, x_2, \dots, x_{p+1}) = 0.$$

En déduire que, pour tout élément g de $\mathcal{A}_p(E)$,

$$\sum_{i=1}^{p+1} (-1)^i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{p+1}) \cdot x_i = 0$$

(identité fondamentale des formes p -linéaires alternées).

3. Soit (x_1, x_2, \dots, x_p) une suite de p éléments de E . Prouver qu'il est équivalent de dire :

- a) La famille (x_1, x_2, \dots, x_p) n'est pas libre.
- b) Il existe un élément non nul λ de A tel que, pour tout élément f de $\mathcal{A}_p(E)$,

$$\lambda f(x_1, x_2, \dots, x_p) = 0.$$

(Pour démontrer que $b) \Rightarrow a)$, on étudiera d'abord le cas où $p = 1$, en décomposant le vecteur x_1 dans la base B , et on raisonnera ensuite par récurrence sur l'entier p . Plus précisément, l'assertion étant démontrée à l'ordre p , on considérera une famille $(x_1, x_2, \dots, x_{p+1})$ satisfaisant à la condition $b)$, et on distinguera deux cas suivant que, pour tout élément g de $\mathcal{A}_p(E)$, $\lambda g(x_1, x_2, \dots, x_p) = 0$, ou non. Dans le second cas, on utilisera l'identité fondamentale des formes p -linéaires alternées.)

4. Prouver que si l'anneau A est intègre, il est équivalent de dire :

a) La famille (x_1, x_2, \dots, x_p) n'est pas libre.

b) Il existe un élément f de $\mathcal{A}_p(E)$ tel que $f(x_1, x_2, \dots, x_p) \neq 0$.

25 A. Caractérisation des bases des modules libres de type fini.

Dans cet exercice, on se propose de donner une autre démonstration du théorème de caractérisation des bases des modules libres de type fini (cf. § 3.6).

Soient A un anneau commutatif unitaire et E un A -module libre de type fini, ayant une base $B = (e_1, e_2, \dots, e_n)$. Soit (x_1, x_2, \dots, x_n) une suite de n éléments de E . Montrer qu'il est équivalent de dire :

a) La suite (x_1, x_2, \dots, x_n) est une base de E .

b) L'élément $\text{Det}_B(x_1, x_2, \dots, x_n)$ est inversible dans A .

(Pour démontrer que $b) \Rightarrow a)$, on prouvera d'abord qu'il existe un élément g de $\mathcal{A}_p(E)$ tel que $g(x_1, x_2, \dots, x_n) = 1$. On appliquera alors l'identité fondamentale des formes p -linéaires alternées (cf. exercice 24) à la suite $(x_1, x_2, \dots, x_n, x)$. On en déduira que (x_1, x_2, \dots, x_n) est génératrice. On prouvera enfin que cette famille est libre, en utilisant le critère d'indépendance linéaire obtenu dans l'exercice 24.)

26 A. Familles libres et familles génératrices des modules libres de type fini.

Soient A un anneau commutatif unitaire et E un A -module libre de type fini, ayant une base $B = (e_1, e_2, \dots, e_n)$.

1. Montrer que toute famille génératrice d'éléments de E a au moins n éléments. (On pourra raisonner par l'absurde, en supposant qu'il existe une famille génératrice (f_1, f_2, \dots, f_p) , où $p < n$. On en déduira que, pour tout entier $q > p$, $\mathcal{A}_q(E) = \{0\}$.)

En conclure que toute base de E est finie, et admet n éléments. (On retrouve ainsi le résultat de l'exercice I.3.88.)

2. Montrer que toute famille libre d'éléments de E a au plus n éléments. (On appliquera le critère d'indépendance linéaire obtenu dans l'exercice 24.)

3. Montrer que toute famille génératrice d'éléments de E ayant n éléments est une base de E . (On supposera par l'absurde qu'elle n'est pas libre, et on utilisera le critère d'indépendance précité.) En revanche, toute famille libre d'éléments de E ayant n éléments n'est pas nécessairement une base de E (même si $A = \mathbb{Z}$ et $E = \mathbb{Z}$).

27 A. Produits tensoriels de familles libres d'un module libre de type fini.

Soit A un anneau commutatif unitaire.

1. Soient E et F deux A -modules libres de type fini, ayant pour bases $B = (e_1, e_2, \dots, e_n)$ et $B' = (f_1, f_2, \dots, f_p)$. Étant donné un élément (x^*, y^*) de $E^* \times F^*$, on note $x^* \otimes y^*$ la forme bilinéaire sur $E \times F$ définie par la formule

$$(x^* \otimes y^*)(u, v) = \langle x^*, u \rangle \cdot \langle y^*, v \rangle.$$

Prouver que toute forme bilinéaire S sur $E \times F$ peut s'écrire d'une manière et d'une

seule sous la forme $S = \sum_{j=1}^p z_j^* \otimes f_j^*$, où, pour tout élément j de $[1, p]$, $z_j^* \in E^*$.

En déduire que, pour toute famille libre $(x_1^*, x_2^*, \dots, x_r^*)$ d'éléments de E^* et pour toute famille libre $(y_1^*, y_2^*, \dots, y_s^*)$ d'éléments de F^* , la famille $(x_i^* \otimes y_j^*)$, où (i, j) parcourt $[1, r] \times [1, s]$, est libre dans $\mathcal{B}(E \times F)$. (On pourra décomposer y_j^* dans la base duale de B' .)

2. Soit E un A -module libre de type fini, ayant pour base $B = (e_1, e_2, \dots, e_n)$. Montrer que si L est une partie libre de E^* , alors, pour tout entier naturel non nul q , les éléments de $\mathcal{M}_q(E)$ de la forme $y_1^* \otimes y_2^* \otimes \dots \otimes y_q^*$, où, pour tout élément j de $[1, q]$, y_j^* appartient à L , constituent une partie libre de $\mathcal{M}_q(E)$.

28 A. Caractérisation des formes multilinéaires proportionnelles.

Soit (E_1, E_2, \dots, E_n) une suite de n espaces vectoriels sur un corps infini K .

1. Prouver, par récurrence sur n , que si f est une forme multilinéaire non nulle sur $E_1 \times E_2 \times \dots \times E_n$, l'ensemble des éléments (x_1, x_2, \dots, x_n) de $E_1 \times E_2 \times \dots \times E_n$ tels que $f(x_1, x_2, \dots, x_n) \neq 0$ engendre l'espace vectoriel produit $E_1 \times E_2 \times \dots \times E_n$.

Montrer que ce résultat ne s'étend pas au cas des corps finis. (On pourra considérer le cas où $n = 2$, $E_1 = E_2 = K = \mathbb{Z}/2\mathbb{Z}$ et où $f(x_1, x_2) = x_1 x_2$.)

2. Soient f et g deux formes multilinéaires sur $E_1 \times E_2 \times \dots \times E_n$. On suppose que, pour tout élément (x_1, x_2, \dots, x_n) de $E_1 \times E_2 \times \dots \times E_n$ tel que $f(x_1, x_2, \dots, x_n) = 0$, alors $g(x_1, x_2, \dots, x_n) = 0$. Montrer qu'il existe un scalaire α tel que $g = \alpha f$.

(On écartera le cas trivial où $f = 0$, et on considérera alors un élément (e_1, e_2, \dots, e_n) de $E_1 \times E_2 \times \dots \times E_n$ tel que $f(e_1, e_2, \dots, e_n) = 1$; on posera $\alpha = g(e_1, e_2, \dots, e_n)$. On prouvera par récurrence sur l'entier p , $1 \leq p \leq n$, que, pour tout élément (x_1, x_2, \dots, x_p) de $E_1 \times E_2 \times \dots \times E_p$,

$$g(x_1, x_2, \dots, x_p, e_{p+1}, \dots, e_n) = \alpha f(x_1, x_2, \dots, x_p, e_{p+1}, \dots, e_n).$$

Pour passer de l'entier p à l'entier $p + 1$, on supposera d'abord que

$$f(x_1, x_2, \dots, x_p, e_{p+1}, \dots, e_n) \neq 0,$$

et on passera au cas général grâce à la question 1.)

Montrer que, dans le cas des formes bilinéaires, le résultat de la question 2 reste valable lorsque K est quelconque. (On pourra procéder comme dans la question précédente, en traitant d'abord les cas où $f(x_1, e_2) \neq 0$ et où $f(e_1, x_2) \neq 0$. On traitera ensuite le cas où $f(x_1, e_2) = f(e_1, x_2) = 0$ en introduisant le couple $(x_1 + e_1, x_2 - \beta e_2)$, où $\beta = f(x_1, x_2)$.)

TRACE D'UN ENDOMORPHISME

29 A. Trace d'un endomorphisme de rang fini.

1. Soient E et F deux espaces vectoriels sur K , et $(f_i)_{i \in I}$ une famille de vecteurs de F . Prouver que si $(f_i)_{i \in I}$ est une famille génératrice, les applications linéaires élémentaires U_{a^*, f_i} , où a^* parcourt E^* et où i parcourt I , engendrent l'espace vectoriel $\mathcal{L}(E, F)$.

On suppose que $(f_i)_{i \in I}$ est libre, et on considère une famille à support fini $(a_i^*)_{i \in I}$ d'éléments de E^* . Prouver que si cette famille satisfait à la relation $\sum_{i \in I} U a_{i, f_i}^* = 0$, alors $a_i^* = 0^*$ pour tout $i \in I$.

En déduire que si $(f_i)_{i \in I}$ est une base de F , tout élément U de $\mathcal{L}_f(E, F)$ peut s'écrire d'une manière et d'une seule sous la forme

$$U = \sum_{i \in I} U y_{i, f_i}^*,$$

où $(y_i^*)_{i \in I}$ est une famille à support fini d'éléments de E^* .

2. En déduire le résultat suivant :

Soit E un espace vectoriel sur K . Il existe une forme linéaire et une seule sur l'espace vectoriel $\mathcal{L}_f(E)$ des endomorphismes de E de rang fini, appelée trace et notée Tr , telle que, pour tout endomorphisme élémentaire $U_{a^, b}$ de E ,*

$$(1) \quad \text{Tr } U_{a^*, b} = \langle a^*, b \rangle.$$

Généraliser à ce cas les propriétés de la trace (proposition 3.14 et ses corollaires 1 et 2).

30 B. Caractérisations de la trace.

Soient E un espace vectoriel sur K , $\mathcal{L}_f(E)$ l'espace vectoriel des endomorphismes de E de rang fini, et g une forme linéaire sur $\mathcal{L}_f(E)$.

1. On suppose que, pour tout couple (U, V) d'éléments de $\mathcal{L}_f(E)$,

$$(1) \quad g(UV) = g(VU).$$

Montrer qu'il existe un scalaire α tel que, pour tout élément U de $\mathcal{L}_f(E)$,

$$g(U) = \alpha \cdot \text{Tr } (U).$$

(On pourra expliciter la relation (1) lorsque U et V sont des endomorphismes élémentaires.)

2. On suppose que, pour tout élément (a^*, b) de $E^* \times E$ tel que $\langle a^*, b \rangle = 0$, $g(U_{a^*, b}) = 0$. Montrer qu'il existe alors un scalaire α tel que, pour tout élément U de $\mathcal{L}_f(E)$,

$$g(U) = \alpha \cdot \text{Tr } (U).$$

(On pourra utiliser l'exercice 28.)

3. Montrer que si (a^*, b) est un élément de $E^* \times E$ tel que $\langle a^*, b \rangle \neq -1$, alors

$$A_{a^*, b} = I_E + U_{a^*, b}$$

est un automorphisme de E , dont on explicitera l'automorphisme inverse. Examiner le cas où $\langle a^*, b \rangle = -1$.

On suppose que pour tout élément (a^*, b) de $E^* \times E$ tel que $\langle a^*, b \rangle = 0$ et pour tout élément U de $\mathcal{L}_f(E)$,

$$g(A_{a^*, b} U A_{a^*, b}^{-1}) = g(U).$$

Montrer qu'il existe alors un scalaire α tel que, pour tout élément U de $\mathcal{L}_f(E)$,

$$g(U) = \alpha \cdot \text{Tr}(U).$$

(On se ramènera à la question 2, en appliquant la relation (2) au cas où $U = U_{a^*, x}$, où $x \in E$.)

En particulier, toute forme linéaire sur $\mathcal{L}_f(E)$ invariante par automorphisme intérieur est proportionnelle à la trace.

Retrouver aussi le résultat de la question 1.

- 31 B.** Soit E un espace vectoriel de dimension finie sur K . Pour tout endomorphisme A de E , on note $\text{Ad}(A)$ l'application de $\mathcal{L}(E)$ dans lui-même définie par la formule

$$\text{Ad}(A)(U) = AU - UA.$$

1. Prouver que $\text{Ad}(A)$ est un endomorphisme de l'espace vectoriel $F = \mathcal{L}(E)$, et que l'application $\text{Ad} : A \mapsto \text{Ad}(A)$ est une application linéaire de $\mathcal{L}(E)$ dans $\mathcal{L}(F)$. En utilisant l'exercice I.3.55, déterminer le noyau de Ad .

2. Déterminer le noyau de ${}^t[\text{Ad}(A)]$, et, grâce à l'exercice 30, prouver que l'intersection des noyaux des endomorphismes ${}^t[\text{Ad}(A)]$, où A parcourt $\mathcal{L}(E)$, n'est autre que la droite engendrée par la trace.

- 32 A.** Soit E un espace vectoriel de dimension finie sur K . Pour tout endomorphisme A de E , on désigne par f_A l'application de $\mathcal{L}(E)$ dans K définie par la formule

$$f_A(U) = \text{Tr}(AU).$$

Montrer que f_A est une forme linéaire sur $\mathcal{L}(E)$, et que l'application $A \mapsto f_A$ est un isomorphisme de $\mathcal{L}(E)$ sur $\mathcal{L}(E)^*$. Expliciter l'isomorphisme réciproque en calculant $f_A(U_{a^*, b})$, où $(a^*, b) \in E^* \times E$, et en choisissant une base de E .

- 33 B.** *Réduction des endomorphismes de trace nulle.*

On suppose que la caractéristique de K est nulle. Soient E un espace vectoriel de dimension finie sur K et U un endomorphisme de E .

1. Prouver que si U n'est pas une homothétie, il existe un vecteur x de E tel que x et $U(x)$ soient linéairement indépendants. (On pourra montrer que si, pour tout élément x de E , x et $U(x)$ sont colinéaires, tout plan P est stable par U , et que U induit une homothétie sur P .)

2. On suppose que U n'est pas nul et que $\text{Tr}(U) = 0$. Prouver que U n'est pas une homothétie.

Soient x un vecteur de E tel que x et $U(x)$ soient linéairement indépendants, et F un sous-espace vectoriel supplémentaire de la droite Kx , contenant $U(x)$. Prouver que l'endomorphisme V de F qui à tout élément y associe $P_F[U(y)]$ est de trace nulle. (On pourra choisir une base de E contenant x et $U(x)$.)

3. En déduire, par récurrence sur la dimension de E , le résultat suivant :

Pour tout endomorphisme U de E de trace nulle, il existe une base B de E telle que tous les éléments diagonaux de $M_B(U)$ soient nuls.

4. Montrer que ce résultat tombe en défaut lorsque la caractéristique p de K n'est pas nulle, en considérant l'application identique de K^p .

34 B. *Caractérisation des endomorphismes de trace nulle.*

Soient D une matrice diagonale d'ordre n , et $\alpha_1, \alpha_2, \dots, \alpha_n$ ses éléments diagonaux.

1. Déterminer le noyau de l'endomorphisme $\text{Ad}(D) : M \mapsto DM - MD$ de $M_n(K)$. Montrer que ce noyau est réduit à l'ensemble $D_n(K)$ des matrices diagonales si et seulement si les scalaires α_i sont distincts deux à deux. Prouver alors que l'image de $\text{Ad}(D)$ est constituée des matrices dont tous les éléments diagonaux sont nuls.

2. A l'aide de l'exercice 33, en déduire le résultat suivant :

Soient E un espace vectoriel de dimension finie sur un corps de caractéristique nulle, et U un endomorphisme de E . Pour que la trace de U soit nulle, il faut et il suffit qu'il existe deux endomorphismes A et B de E tels que $U = AB - BA$.

35 A. *Automorphismes de l'algèbre des endomorphismes.*

I. — Soit E un espace vectoriel de dimension finie $n > 0$ sur K .

On appelle *système d'unités matricielles* de $\mathcal{L}(E)$ toute famille (U_{ij}) d'endomorphismes non nuls de E , où i et j parcourent $[1, n]$, telle que

$$U_{ij} \cdot U_{kl} = \delta_{jk} U_{il},$$

quels que soient $i, j, k, l \in [1, n]$.

1. Prouver que pour toute base B de E , la base (U_{ij}) de $\mathcal{L}(E)$ canoniquement associée à B constitue un système d'unités matricielles de $\mathcal{L}(E)$. Prouver que pour tout système d'unités matricielles (V_{ij}) de $\mathcal{L}(E)$, il existe un endomorphisme f de l'espace vectoriel $\mathcal{L}(E)$ et un seul transformant (U_{ij}) en (V_{ij}) . Prouver que f est un automorphisme de l'algèbre unitaire $\mathcal{L}(E)$.

(On pourra utiliser l'exercice I.3.52.)

2. Prouver que pour tout système d'unités matricielles (V_{ij}) de $\mathcal{L}(E)$, il existe une base B' de E telle que (V_{ij}) soit la base de $\mathcal{L}(E)$ canoniquement associée à B' .

3. Montrer que, pour tout couple $((U_{ij}), (V_{ij}))$ de systèmes d'unités matricielles de $\mathcal{L}(E)$, il existe un automorphisme A de E tel que pour tout couple (i, j) d'éléments de $[1, n]$,

$$V_{ij} = A^{-1}U_{ij}A.$$

4. Soit g un automorphisme de l'algèbre unitaire $\mathcal{L}(E)$. Montrer que g transforme un système d'unités matricielles de $\mathcal{L}(E)$ en un système d'unités matricielles de $\mathcal{L}(E)$.

En déduire le résultat suivant :

L'application qui à tout élément A de $\text{GL}(E)$ associe l'automorphisme intérieur σ_A défini par A est un morphisme surjectif du groupe $\text{GL}(E)$ sur le groupe $\text{Aut}(\mathcal{L}(E))$ des automorphismes de l'algèbre unitaire $\mathcal{L}(E)$; son noyau est constitué des homothéties non nulles de E .

5. Appliquer ces résultats à l'étude des automorphismes de l'algèbre unitaire $M_n(K)$.

II. — Soit E un espace vectoriel sur K .

On considère l'ensemble \mathcal{M} des projecteurs minimaux de $\mathcal{L}(E)$, c'est-à-dire des éléments minimaux de l'ensemble des projecteurs non nuls de E , ordonné par la relation définie par les couples (P, Q) tels que $P = PQ = QP$.

1. Prouver que les éléments de \mathcal{M} ne sont autres que les projecteurs de rang 1, c'est-à-dire les endomorphismes élémentaires $U_{a^*, b}$ où $\langle a^*, b \rangle = 1$.

2. Soient P et Q deux éléments de \mathcal{M} . Prouver qu'il existe un automorphisme A de E tel que $Q = A^{-1}PA$.

3. Soit f un automorphisme de l'algèbre unitaire $\mathfrak{L}(E)$. Prouver que f transforme les projecteurs minimaux en des projecteurs minimaux. En déduire que f transforme les endomorphismes de rang 1 en des opérateurs de rang 1, et les endomorphismes de rang fini en des endomorphismes de rang fini.

4. Soient a^* un élément de E^* et b un élément de E tels que $\langle a^*, b \rangle = 1$ et $P_0 = U_{a^*, b}$ le projecteur minimal déterminé par $U_{a^*, b}$. Soit enfin f un automorphisme de $\mathfrak{L}(E)$. Prouver qu'il existe un automorphisme A de E tel que l'automorphisme g de $\mathfrak{L}(E)$ défini par la formule $g(U) = A f(U) A^{-1}$ laisse fixe P_0 .

Prouver qu'il existe un endomorphisme B de E et un seul tel que pour tout $x \in E$,

$$g(U_{a^*, x}) = U_{a^*, B(x)}.$$

Montrer que B est un automorphisme de E , que $B(b) = b$, que ${}^t B(a^*) = a^*$, et que l'automorphisme h de $\mathfrak{L}(E)$ défini par la formule $h(U) = B^{-1} g(U) B$ laisse fixes tous les endomorphismes de E .

En déduire que tout automorphisme de l'algèbre unitaire $\mathfrak{L}(E)$ est intérieur.

ALGÈBRE DES FORMES MULTILINÉAIRES

36 A. Algèbre des formes multilinéaires symétriques.

Dans cet exercice, on s'inspire des méthodes utilisées dans le paragraphe 3.5.

Soit E un espace vectoriel de dimension finie sur un corps K de caractéristique 0.

1. Soient q et r deux entiers naturels non nuls. Prouver qu'il existe une application bilinéaire $T_{q,r}$ et une seule de $\mathcal{Y}_q(E) \times \mathcal{Y}_r(E)$ dans $\mathcal{Y}_{q+r}(E)$ telle que, pour tout élément $(y_1^*, y_2^*, \dots, y_q^*)$ de $(E^*)^q$ et pour tout élément $(z_1^*, z_2^*, \dots, z_r^*)$ de $(E^*)^r$,

$$T_{q,r}(y_1^* \cdot y_2^* \cdots y_q^*, z_1^* \cdot z_2^* \cdots z_r^*) = y_1^* \cdot y_2^* \cdots y_q^* \cdot z_1^* \cdot z_2^* \cdots z_r^*.$$

(On pourra utiliser l'exercice 19.)

Pour tout élément (f, g) de $\mathcal{Y}_q(E) \times \mathcal{Y}_r(E)$, $T_{q,r}(f, g)$ s'appelle produit (symétrique) des formes multilinéaires symétriques f et g , et se note $f \cdot g$.

Montrer que $g \cdot f = f \cdot g$, et que, pour tout entier naturel non nul s et pour tout élément h de $\mathcal{Y}_s(E)$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

2. Dans la suite, on convient que $\mathcal{Y}_0(E) = K$, et on définit le produit d'un scalaire α et d'un élément f de $\mathcal{Y}_p(E)$ par la formule $\alpha \cdot f = \alpha f$.

Étendre les résultats de la question 1 au cas où q , r et s sont des entiers naturels.

Montrer que la somme F des sous-espaces vectoriels $\mathcal{Y}_p(E)$ de l'espace vectoriel $\mathcal{M}(E)$, où p parcourt \mathbb{N} , est directe, et qu'il existe une application bilinéaire T et une seule de $F \times F$ dans F prolongeant les applications $T_{q,r}$. Prouver que T définit sur F une structure d'algèbre associative, commutative et unitaire. Cette algèbre s'appelle algèbre des formes multilinéaires symétriques sur E , et se note $\mathcal{Y}(E)$; pour tout couple (f, g) d'éléments de $\mathcal{Y}(E)$, $T(f, g)$ s'appelle produit (symétrique) des formes multilinéaires symétriques f et g , et se note $f \cdot g$.

Montrer enfin que la sous-algèbre unitaire de $\mathcal{Y}(E)$ engendrée par $E^* = \mathcal{Y}_1(E)$ n'est autre que $\mathcal{Y}(E)$.

37 A. Propriété universelle de l'algèbre des formes multilinéaires.

1. Soit E un espace vectoriel de dimension finie sur K . Prouver que, pour tout couple (C, f) constitué d'une K -algèbre associative unitaire C et d'une application

linéaire f de E^* dans C , il existe un morphisme \tilde{f} et un seul de l'algèbre unitaire $\mathcal{M}(E)$ dans C qui prolonge f ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$\tilde{f}(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = f(y_1^*) \cdot f(y_2^*) \dots f(y_p^*).$$

(On pourra utiliser l'exercice 21.)

2. Soient E et F deux espaces vectoriels de dimension finie sur K . Montrer que, pour toute application linéaire U de E^* dans F^* , il existe un morphisme $T(U)$ et un seul de l'algèbre unitaire $\mathcal{M}(E)$ dans l'algèbre unitaire $\mathcal{M}(F)$ qui prolonge U ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$T(U)(y_1^* \otimes y_2^* \otimes \dots \otimes y_p^*) = U(y_1^*) \otimes U(y_2^*) \otimes \dots \otimes U(y_p^*).$$

Soient G un espace vectoriel de dimension finie sur K et V une application linéaire de F^* dans G^* . Prouver que $T(V \circ U) = T(V) \circ T(U)$.

Prouver que si U est injective, ou surjective, il en est de même de $T(U)$.

Prouver enfin que l'image de $T(U)$ est la sous-algèbre unitaire de $\mathcal{M}(F)$ engendrée par $\text{Im}(U)$, et que le noyau de $T(U)$ est l'idéal bilatère de $\mathcal{M}(E)$ engendré par $\text{Ker}(U)$. (Pour cette dernière assertion, on pourra considérer une base de $\text{Ker}(U)$, et la compléter en une base de E^* .)

38. A. Propriété universelle de l'algèbre des formes multilinéaires symétriques.

On utilise les résultats de l'exercice 36. On suppose que K est de caractéristique 0.

1. Soit E un espace vectoriel de dimension finie sur K . Prouver que, pour tout couple (C, f) constitué d'une K -algèbre associative unitaire C et d'une application linéaire f de E^* dans C telle que, pour tout couple (y^*, z^*) d'éléments de E^* , $f(y^*) \cdot f(z^*) = f(z^*) \cdot f(y^*)$, il existe un morphisme \tilde{f} et un seul de l'algèbre unitaire $\mathcal{S}(E)$ dans C qui prolonge f ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$f(y_1^* \cdot y_2^* \dots y_p^*) = f(y_1^*) \cdot f(y_2^*) \dots f(y_p^*).$$

(On pourra utiliser l'exercice 22.)

2. Soient E et F deux espaces vectoriels de dimension finie sur K . Montrer que, pour toute application linéaire U de E^* dans F^* , il existe un morphisme $S(U)$ et un seul de l'algèbre unitaire $\mathcal{S}(E)$ dans l'algèbre unitaire $\mathcal{S}(F)$ qui prolonge U ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$S(U)(y_1^* \cdot y_2^* \dots y_p^*) = U(y_1^*) \cdot U(y_2^*) \dots U(y_p^*).$$

Soient G un espace vectoriel de dimension finie sur K et V une application linéaire de F^* dans G^* . Prouver que $S(V \circ U) = S(V) \circ S(U)$.

Prouver que si U est injective, ou surjective, il en est de même de $S(U)$.

Prouver enfin que l'image de $T(U)$ est la sous-algèbre unitaire de $\mathcal{S}(F)$ engendrée par $\text{Im}(U)$, et que le noyau de $S(U)$ est l'idéal de $\mathcal{S}(E)$ engendré par $\text{Ker}(U)$.

39 A. Propriété universelle de l'algèbre des formes multilinéaires alternées.

1. Soit E un espace vectoriel de dimension finie sur K . Prouver que, pour tout couple (C, f) constitué d'une K -algèbre associative unitaire C et d'une application linéaire f de E^* dans C telle que, pour tout élément y^* de E^* , $[f(y^*)]^2 = 0$, il existe un mor-

phisme \tilde{f} et un seul de l'algèbre unitaire $\mathcal{A}(E)$ dans C qui prolonge f ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$\tilde{f}(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*) = f(y_1^*) \cdot f(y_2^*) \dots f(y_p^*).$$

(On pourra utiliser l'exercice 23.)

2. Soient E et F deux espaces vectoriels de dimension finie sur K . Montrer que, pour toute application linéaire U de E^* dans F^* , il existe un morphisme $A(U)$ et un seul de l'algèbre unitaire $\mathcal{A}(E)$ dans l'algèbre unitaire $\mathcal{A}(F)$ qui prolonge U ; montrer que, pour toute suite $(y_1^*, y_2^*, \dots, y_p^*)$ d'éléments de E^* ,

$$A(U)(y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*) = U(y_1^*) \wedge U(y_2^*) \wedge \dots \wedge U(y_p^*).$$

Soient G un espace vectoriel de dimension finie sur K et V une application linéaire de F^* dans G^* . Prouver que $A(V \circ U) = A(V) \circ A(U)$.

Prouver que si U est injective, ou surjective, il en est de même de $A(U)$.

Prouver enfin que l'image de $A(U)$ est la sous-algèbre unitaire de $\mathcal{A}(F)$ engendrée par $\text{Im}(U)$, et que le noyau de $A(U)$ est l'idéal bilatère de $\mathcal{A}(E)$ engendré par $\text{Ker}(U)$.

40 A. Produit de deux formes multilinéaires symétriques.

Soit E un espace vectoriel sur K . Pour tout entier naturel non nul p , on considère l'opération de \mathfrak{S}_p sur $\mathcal{M}_p(E)$ définie par la formule

$$(\sigma f)(x_1, x_2, \dots, x_p) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(p)}).$$

1. Soient p et q deux entiers naturels non nuls, f un élément de $\mathcal{P}_p(E)$ et g un élément de $\mathcal{P}_q(E)$. Prouver que la forme $(p+q)$ -linéaire $f \otimes g$ est invariante par le sous-groupe H de $G = \mathfrak{S}_{p+q}$ constitué des permutations σ de $[1, p+q]$ laissant stables les deux intervalles $[1, p]$ et $[p+1, p+q]$. Montrer que l'ensemble P des permutations σ de $[1, p+q]$ telles que

$$\sigma(1) < \sigma(2) < \dots < \sigma(p) \quad \text{et} \quad \sigma(p+1) < \sigma(p+2) < \dots < \sigma(p+q)$$

est un système de représentants dans G de G/H . En déduire que l'application qui à tout élément $(x_1, \dots, x_p, x_{p+1}, \dots, x_{p+q})$ de E^{p+q} associe le scalaire

$$\sum_{\sigma \in P} f(x_{\sigma(1)}, \dots, x_{\sigma(p)}) \cdot g(x_{\sigma(p+1)}, \dots, x_{\sigma(p+q)})$$

est une forme $(p+q)$ -linéaire symétrique sur E ; on l'appelle produit symétrique, ou plus simplement produit, de f et de g , et on la note $f \cdot g$. Ainsi,

$$f \cdot g = I_{G,H}(f \otimes g).$$

Montrer que l'application $(f, g) \mapsto f \cdot g$ de $\mathcal{P}_p(E) \times \mathcal{P}_q(E)$ dans $\mathcal{P}_{p+q}(E)$ est bilinéaire. Prouver que la symétrisée de $f \otimes g$ est donnée par la relation

$$S(f \otimes g) = p! q! f \cdot g.$$

2. Dans la suite, on convient que $\mathcal{P}_0(E) = K$, et on définit le produit d'un scalaire α et d'un élément f de $\mathcal{P}_p(E)$ par la formule $\alpha \cdot f = \alpha f$.

Montrer que, pour tout couple (p, q) d'entiers naturels, pour tout élément f de $\mathcal{P}_p(E)$

et pour tout élément g de $\mathcal{Y}_q(E)$, $g \cdot f = f \cdot g$, et que, pour tout entier naturel r et pour tout élément h de $\mathcal{Y}_r(E)$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$. (On pourra démontrer que les deux membres sont égaux à $I_{G, H'}(f \otimes g \otimes h)$, où G désigne le groupe \mathfrak{S}_{p+q+r} et H' le sous-groupe de G constitué des permutations laissant stables les intervalles $[1, p]$, $[p+1, p+q]$ et $[p+q+1, p+q+r]$.)

3. On considère sur l'espace vectoriel $\mathcal{Y}(E) = \sum_{r=0}^{+\infty} \mathcal{Y}_r(E)$ la structure de K -algèbre définie par l'application bilinéaire T qui à tout couple (f, g) d'éléments de $\mathcal{Y}(E)$ associe

$$T(f, g) = \sum_{r=0}^{+\infty} \left(\sum_{p+q=r} f_p \cdot g_q \right),$$

où $f = \sum_{p=0}^{+\infty} f_p$ et $g = \sum_{q=0}^{+\infty} g_q$. Montrer que cette algèbre est associative, commutative et unitaire.

4. Soient $(y_1^*, y_2^*, \dots, y_p^*)$ et $(z_1^*, z_2^*, \dots, z_q^*)$ deux suites d'éléments de E^* ; on pose $f = y_1^* \cdot y_2^* \dots y_p^*$ et $g = z_1^* \cdot z_2^* \dots z_q^*$. Prouver que

$$f \cdot g = y_1^* \cdot y_2^* \dots y_p^* \cdot z_1^* \cdot z_2^* \dots z_q^*.$$

En déduire que si E est de dimension finie, et K de caractéristique 0, le produit $f \cdot g$ coïncide avec celui qui a été défini dans l'exercice 36.

41 A. Produit de deux formes multilinéaires alternées.

Soit E un espace vectoriel sur K . Pour tout entier naturel non nul p , on considère l'opération de \mathfrak{S}_p sur $\mathfrak{M}_p(E)$ définie par la formule

$$(\sigma f)(x_1, x_2, \dots, x_p) = \varepsilon(\sigma) f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(p)}).$$

1. Soient p et q deux entiers naturels non nuls, f un élément de $\mathcal{A}_p(E)$ et g un élément de $\mathcal{A}_q(E)$. Prouver que la forme $(p+q)$ -linéaire $f \otimes g$ est invariante par le sous-groupe H de $G = \mathfrak{S}_{p+q}$ constitué des permutations σ de $[1, p+q]$ laissant stables les deux intervalles $[1, p]$ et $[p+1, p+q]$. Montrer que l'ensemble P des permutations σ de $[1, p+q]$ telles que

$$\sigma(1) < \sigma(2) < \dots < \sigma(p) \quad \text{et} \quad \sigma(p+1) < \sigma(p+2) < \dots < \sigma(p+q)$$

est un système de représentants dans G de G/H . En déduire que l'application qui à tout élément $(x_1, \dots, x_p, x_{p+1}, \dots, x_{p+q})$ associe le scalaire

$$\sum_{\sigma \in P} \varepsilon(\sigma) f(x_{\sigma(1)}, \dots, x_{\sigma(p)}) \cdot g(x_{\sigma(p+1)}, \dots, x_{\sigma(p+q)})$$

est une forme $(p+q)$ -linéaire alternée sur E ; on l'appelle produit extérieur de f et de g , et on la note $f \wedge g$. Ainsi,

$$f \wedge g = I_{G, H}(f \otimes g).$$

Montrer que l'application $(f, g) \mapsto f \wedge g$ de $\mathcal{A}_p(E) \times \mathcal{A}_q(E)$ dans $\mathcal{A}_{p+q}(E)$ est bilinéaire. Prouver que l'antisymétrisée de $f \otimes g$ est donnée par la relation

$$A(f \otimes g) = p! q! f \wedge g.$$

2. Dans la suite, on convient que $\mathcal{A}_0(E) = K$, et on définit le produit d'un scalaire α et d'un élément f de $\mathcal{A}_p(E)$ par la formule $\alpha \wedge f = \alpha f$.

Montrer que, pour tout couple (p, q) d'entiers naturels, pour tout élément f de $\mathcal{A}_q(E)$ et pour tout élément g de $\mathcal{A}_p(E)$,

$$(1) \quad g \wedge f = (-1)^{pq} f \wedge g,$$

et que, pour tout entier naturel r et pour tout élément h de $\mathcal{A}_r(E)$,

$$(f \wedge g) \wedge h = f \wedge (g \wedge h).$$

(On pourra démontrer que les deux membres sont égaux à $I_{G,H'}(f \otimes g \otimes h)$, où G désigne le groupe \mathfrak{S}_{p+q+r} et H' le sous-groupe de G constitué des permutations laissant stables les intervalles $[1, p]$, $[p+1, p+q]$ et $[p+q+1, p+q+r]$.)

3. On considère sur l'espace vectoriel $\mathcal{A}(E) = \sum_{r=0}^{+\infty} \mathcal{A}_r(E)$ la structure de K -algèbre définie par l'application bilinéaire T qui à tout couple (f, g) d'éléments de $\mathcal{A}(E)$ associe

$$T(f, g) = \sum_{r=0}^{+\infty} \left(\sum_{p+q=r} f_p \wedge g_q \right),$$

où $f = \sum_{p=0}^{+\infty} f_p$ et $g = \sum_{q=0}^{+\infty} g_q$. Montrer que cette algèbre est associative et unitaire. On traduit la relation (1) en disant que cette algèbre est anticommutative.

4. Soient $(y_1^*, y_2^*, \dots, y_p^*)$ et $(z_1^*, z_2^*, \dots, z_q^*)$ deux suites d'éléments de E^* ; on pose $f = y_1^* \wedge y_2^* \wedge \dots \wedge y_p^*$ et $g = z_1^* \wedge z_2^* \wedge \dots \wedge z_q^*$. Prouver que

$$f \wedge g = y_1^* \wedge y_2^* \wedge \dots \wedge y_p^* \wedge z_1^* \wedge z_2^* \wedge \dots \wedge z_q^*.$$

En déduire que si E est de dimension finie, le produit extérieur $f \wedge g$ coïncide avec celui qui a été défini dans le théorème 3.10.

42 A. Algèbre des formes multilinéaires sur un espace vectoriel de dimension infinie.

Soient E un espace vectoriel de dimension infinie et $(e_i)_{i \in I}$ une base de E . On considère la forme bilinéaire S qui à tout couple (x, y) de vecteurs de E associe $\sum_{i \in I} \xi_i \eta_i$, où

$$x = \sum_{i \in I} \xi_i e_i \text{ et } y = \sum_{i \in I} \eta_i e_i.$$

1. Prouver que S n'appartient pas au sous-espace vectoriel de $\mathcal{M}_2(E)$ engendré par les formes bilinéaires $e_i^* \otimes e_j^*$, où i et j parcourent I .

2. En déduire que S n'appartient pas au sous-espace vectoriel de $\mathcal{M}_2(E)$ engendré par les formes bilinéaires décomposables.

3. Prouver enfin que S n'appartient pas à la sous-algèbre unitaire de $\mathcal{M}(E)$ engendrée par E^* .

CHAPITRE 4

ÉQUATIONS LINÉAIRES

INTRODUCTION

Dans le premier paragraphe de ce chapitre, nous étudions la notion de rang d'une matrice, en liaison avec la théorie des matrices équivalentes. Nous introduisons à ce propos la notion d'opération élémentaire, dont l'importance est capitale pour le traitement numérique des matrices (calcul de déterminants, inversion des matrices, résolution de systèmes linéaires), pour la géométrie du groupe unimodulaire et pour la réduction des matrices (calcul des diviseurs élémentaires). Le lecteur intéressé par cette dernière théorie pourra se reporter à [3] ou [5].

Au § 2, nous exposons les résultats généraux concernant les équations linéaires, indépendamment de la notion de dimension. Ces résultats peuvent en effet s'appliquer à l'étude des équations différentielles et des équations aux dérivées partielles, et à celle des problèmes linéaires portant sur les polynômes. Le § 3 est consacré à deux cas particuliers importants : polynôme d'interpolation de Lagrange, polynômes de Hilbert.

Enfin, dans les §§ 4 et 5, nous exposons les résultats classiques concernant les systèmes linéaires, et nous examinons les divers aspects pratiques du problème de l'inversion des matrices carrées.

Dans tout ce chapitre, K désigne un corps commutatif.

§ 1. RANG D'UNE MATRICE

1. RANG D'UNE MATRICE

DÉFINITION 4.1. — Rang d'une matrice. — Soient n et p deux entiers naturels non nuls, et M un élément de $M_{n,p}(K)$. On appelle rang de M , et on note $\text{rang}(M)$, le rang de l'application linéaire de K^p dans K^n canoniquement associée à M .

PROPOSITION 4.1. — Propriétés du rang.

1. Soient E et F deux espaces vectoriels de dimension finie sur K non réduits à $\{0\}$, B une base de E , et B' une base de F . Alors, pour toute application linéaire U de E dans F ,

$$(1) \quad \text{rang}(U) = \text{rang}[M_{B,B'}(U)].$$

2. Pour tout élément M de $M_{n,p}(K)$,

$$(2) \quad \text{rang}({}^t M) = \text{rang}(M).$$

3. Pour tout élément M de $M_{n,p}(K)$, le rang de M est égal au rang de ses vecteurs colonnes, ou encore au rang de ses vecteurs lignes.

L'assertion 1 est évidente.

Assertion 2. — Soit U l'application linéaire de K^p dans K^n canoniquement associée à M ; la relation

$$\text{rang}({}^t U) = \text{rang}(U)$$

entraîne aussitôt la relation (2).

Assertion 3. — Par définition, le rang de M est égal au rang de ses vecteurs colonnes; il est encore égal au rang de ses vecteurs lignes, d'après l'assertion 2.

COROLLAIRE. — Caractérisation des matrices carrées inversibles. — Soient n un entier naturel non nul, et M un élément de l'algèbre unitaire $M_n(K)$. Il est équivalent de dire :

1. La matrice M est inversible.
2. La matrice M est inversible à gauche.
3. La matrice M est inversible à droite.
4. La matrice tM est inversible.
5. Le rang de M est égal à n .
6. Le rang des vecteurs colonnes de M est égal à n .
7. Le rang des vecteurs lignes de M est égal à n .
8. Le déterminant de M est non nul.

Voyons maintenant comment varie le rang d'une matrice lorsqu'on enlève une colonne :

PROPOSITION 4.2. — Calcul du rang à l'aide des vecteurs colonnes. — Soient M un élément non nul de $M_{n,p}(K)$, où $p > 1$, et x_1, x_2, \dots, x_p ses vecteurs colonnes ; soit M' l'élément de $M_{n,p-1}(K)$ ayant pour vecteurs colonnes x_1, x_2, \dots, x_{p-1} .

Si le vecteur x_p est combinaison linéaire des vecteurs x_1, x_2, \dots, x_{p-1} , alors

$$\text{rang}(M') = \text{rang}(M).$$

Si le vecteur x_p n'est pas combinaison linéaire des vecteurs x_1, x_2, \dots, x_{p-1} , alors

$$\text{rang}(M') = \text{rang}(M) - 1.$$

L'énoncé est analogue dans le cas des vecteurs lignes.

Cela résulte aussitôt des propriétés du rang d'un système de vecteurs (cf. prop. I.3.35).

2. MATRICES PRINCIPALES

Nous allons maintenant développer une autre méthode du calcul du rang d'une matrice.

DÉFINITION 4.2. — Matrices extraites. — Soit M un élément de $M_{n,p}(K)$. On appelle matrice extraite de la matrice M toute matrice M' de la forme $(\alpha_{ij})_{i \in I, j \in J}$, où I est une partie non vide $[1, n]$ et où J est une partie non vide de $[1, p]$.

Étant donnée une matrice $M' = (\alpha_{ij})_{i \in I, j \in J}$ extraite de la matrice M , nous noterons M_1 la matrice $(\alpha_{ij})_{i \in [1, n], j \in J}$; les vecteurs colonnes de M_1 sont donc les vecteurs colonnes x_j de M dont l'indice j appartient à J . La matrice M' est aussi une matrice extraite de M_1 , obtenue en enlevant les lignes de M_1 dont l'indice i n'appartient pas à I .

PROPOSITION 4.3. — Calcul du rang à l'aide des matrices extraites. — Soit M un élément non nul de $M_{n,p}(K)$, de rang r .

1. Le rang de toute matrice M' extraite de M est inférieur ou égal à r .

2. Toute matrice carrée inversible extraite de M est d'ordre inférieur ou égal à r .

3. Il existe une matrice carrée inversible extraite de M et d'ordre r .

Assertion 1. — Considérons la matrice M_1 précédemment définie; le rang de M_1 est le rang de ses vecteurs colonnes, et est donc inférieur ou égal au rang de M ; le rang de M' est le rang de ses vecteurs lignes, et est donc inférieur ou égal au rang de M_1 , d'où l'inégalité :

$$\text{rang}(M') \leq \text{rang}(M).$$

L'assertion 2 en découle aussitôt, puisque le rang d'une matrice carrée inversible est égal à son ordre.

Assertion 3. — La famille des vecteurs colonnes de M ayant pour rang r , nous pouvons en extraire une famille libre $(x_j)_{j \in J}$ où J a r éléments. Soit M_1 la matrice extraite de M admettant ces r vecteurs pour vecteurs colonnes; le rang de M_1 est égal à r . La famille des vecteurs lignes $y_1'^*, y_2'^*, \dots, y_n'^*$ de M_1 a encore pour rang r ; nous pouvons en extraire une famille libre $(y_i'^*)_{i \in I}$ où I a r éléments. La matrice M' ayant pour vecteurs lignes ces r vecteurs est une matrice carrée d'ordre r , inversible puisque $\text{rang}(M') = r$.

DÉFINITION 4.3. — Matrices principales. — Soit M un élément non nul de $\mathbf{M}_{n,p}(K)$, de rang r . Une matrice carrée inversible extraite de M et d'ordre r s'appelle matrice principale extraite de M .

Étant donnée une matrice principale P extraite de M , les lignes de M relatives à P s'appellent lignes principales; les colonnes de M relatives à P s'appellent colonnes principales.

DÉFINITION 4.4. — Matrices bordantes. — Soient $M = (\alpha_{ij})$ un élément de $\mathbf{M}_{n,p}(K)$, et $P = (\alpha_{ij})_{i \in I, j \in J}$ une matrice carrée extraite de M . On appelle matrice bordante associée à P toute matrice extraite de M obtenue en prenant un entier i_0 n'appartenant pas à I et un entier j_0 n'appartenant pas à J , et en ajoutant à la matrice P la ligne constituée par les éléments $\alpha_{i_0,j}$, $j \in J$, et la colonne constituée par les éléments α_{i,j_0} , $i \in I \cup \{i_0\}$.

PROPOSITION 4.4. — Caractérisation des matrices principales. — Soient M un élément non nul de $\mathbf{M}_{n,p}(K)$, et P une matrice carrée inversible extraite de M . Pour que la matrice P soit principale, il faut et il suffit qu'il n'existe pas de matrice bordante inversible associée à P .

Soient en effet r le rang de la matrice M , et q l'ordre de la matrice inversible P .

Si la matrice P est principale, alors $q = r$; toutes les matrices carrées inversibles extraites de M sont d'ordre inférieur ou égal à q . Il n'existe donc pas de matrice bordante inversible associée à P .

Réciproquement, supposons que la matrice P ne soit pas principale, c'est-à-dire que $q < r$. Soient $(\mathbf{x}_j)_{j \in J}$ les q vecteurs colonnes de M relatifs à P , et M_1 la matrice ayant ces vecteurs pour vecteurs colonnes. La matrice P est une matrice inversible extraite de M_1 ; le rang de M_1 est donc supérieur ou égal à q . La matrice M_1 ayant q colonnes, son rang est égal à q , ce qui prouve que la famille $(\mathbf{x}_j)_{j \in J}$ est libre. Puisque l'entier q est strictement inférieur au rang r de la famille $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_p)$, il existe un entier j_0 n'appartenant pas à J tel que le vecteur \mathbf{x}_{j_0} n'appartienne pas au sous-espace engendré par la famille $(\mathbf{x}_j)_{j \in J}$. Par conséquent, la famille $(\mathbf{x}_j)_{j \in J \cup \{j_0\}}$ est encore libre, et le rang de la matrice M_2 admettant ces vecteurs pour vecteurs colonnes est égal à $q + 1$. Puisque la matrice P est inversible, les q vecteurs lignes $(\mathbf{y}_i^*)_{i \in I}$ de M_2 relatifs à P sont linéairement indépendants. Il existe donc un entier i_0 n'appartenant pas à I tel que le vecteur $\mathbf{y}_{i_0}^*$ n'appartienne pas au sous-espace engendré par ces vecteurs. La matrice carrée d'ordre $q + 1$ admettant pour vecteurs lignes les vecteurs $(\mathbf{y}_i^*)_{i \in I \cup \{i_0\}}$ est inversible, et c'est une matrice bordante associée à P .

3. MATRICES ÉQUIVALENTES

Interprétons maintenant les résultats du § I.3.16 : soient E et F deux espaces vectoriels non réduits à $\{\mathbf{0}\}$ de dimensions respectives p et n sur K , B_1 et B_2 deux bases de E , B'_1 et B'_2 deux bases de F , P la matrice de passage de B_1 à B_2 , et Q la matrice de passage de B'_1 à B'_2 . Soient d'autre part U une application linéaire de E dans F , $M_1(U)$ la matrice associée à U dans les bases B_1 et B'_1 , et $M_2(U)$ la matrice associée à U dans les bases B_2 et B'_2 . Nous savons (cf. § I.3.16) que $M_1(U)$ et $M_2(U)$ sont liées par la relation

$$M_2(U) = Q^{-1}M_1(U)P.$$

Ceci nous conduit à introduire dans l'ensemble $M_{n,p}(K)$ des matrices à n lignes et p colonnes à éléments dans K la relation binaire définie par les couples (M, M') tels qu'il existe un élément inversible S de $M_p(K)$ et un élément inversible T de $M_n(K)$ tels que

$$M' = TMS.$$

Il est immédiat que cette relation binaire est une relation d'équivalence.

DÉFINITION 4.5. — Matrices équivalentes. — Deux matrices à n lignes et p colonnes sont dites équivalentes si elles sont liées par la relation précédente.

REMARQUE. — Pour que deux matrices M et M' soient équivalentes, il faut et il suffit que leurs transposées tM et ${}^tM'$ le soient.

En effet, pour qu'une matrice carrée soit inversible, il faut et il suffit que sa transposée le soit.

PROPOSITION 4.5. — Interprétation vectorielle de l'équivalence des matrices.
 — Soient M_1 et M_2 deux matrices à n lignes et p colonnes, supposées équivalentes. On désigne par B_1 et B'_1 les bases canoniques de K^p et de K^n , et par U l'application linéaire de K^p dans K^n canoniquement associée à M_1 . (La matrice M_1 n'est autre que la matrice associée à U dans les bases B_1 et B'_1 .) Il existe alors une base B_2 de K^p et une base B'_2 de K^n telles que M_2 soit la matrice associée à U dans les bases B_2 et B'_2 .

Les matrices M_1 et M_2 ont donc le même rang.

Supposons en effet que les matrices M_1 et M_2 soient liées par la relation $M_2 = TM_1S$, où S est un élément inversible de $M_p(K)$, et où T est un élément inversible de $M_n(K)$. Il existe une base B_2 et une seule de K^p telle que S soit la matrice de passage de B_1 à B_2 , et il existe une base B'_2 et une seule de K^n telle que T^{-1} soit la matrice de passage de B'_1 à B'_2 . La matrice associée à U dans les bases B_2 et B'_2 n'est autre que $(T^{-1})^{-1}M_1S = TM_1S = M_2$, ce qu'il fallait prouver.

THÉORÈME 4.1. — Caractérisation des applications linéaires de rang donné.
 — Soient E et F deux espaces vectoriels non réduits à $\{0\}$ de dimensions respectives p et n sur K , r un entier naturel, et U une application linéaire de E dans F . Pour que le rang de U soit égal à r , il faut et il suffit qu'il existe une base B de E et une base B' de F telles que $M_{B,B'}(U) = J_r$, où, pour tout entier naturel $r \leq \inf(n, p)$, J_r est l'élément de $M_{n,p}(K)$ défini par les relations suivantes: $\alpha_{ii} = 1$ si $i \in [1, r]$ et $\alpha_{ij} = 0$ dans les autres cas. Autrement dit,

$$J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Cette condition est suffisante, puisque le rang de la matrice J_r est égal à r , et que

$$\text{rang}(U) = \text{rang}(M_{B,B'}(U)).$$

Montrons maintenant que cette condition est nécessaire. Nous savons que si U est de rang r , le noyau de U est de dimension $p - r$ (cf. th. I.3.7). Considérons un sous-espace E' supplémentaire de $\text{Ker}(U)$ dans E ; la dimension de E' est donc égale à r . Choisissons une base (e_1, e_2, \dots, e_r) de E' , et une base (e_{r+1}, \dots, e_p) de $\text{Ker}(U)$. Il s'ensuit que $B = (e_1, e_2, \dots, e_r, e_{r+1}, \dots, e_p)$ est une base de E , et que la famille $(U(e_1), U(e_2), \dots, U(e_r))$ est une base de $\text{Im}(U)$ (cf. prop. I.3.28). Pour tout $i \in [1, r]$, posons $f_i = U(e_i)$, et complétons la famille libre (f_1, f_2, \dots, f_r) en une base $B' = (f_1, f_2, \dots, f_r, f_{r+1}, \dots, f_n)$ de F . Il est immédiat que la matrice associée à U dans les bases B et B' n'est autre que J_r .

REMARQUE. — La démonstration précédente fournit un procédé pratique d'obtention des bases B et B' .

COROLLAIRE 1. — Caractérisation des matrices de rang donné. — Soient n et p deux entiers strictement positifs, et r un entier naturel. Pour qu'une matrice M à n lignes et p colonnes à éléments dans K soit de rang r , il faut et il suffit que M soit équivalente à J_r .

Supposons que M et J_r soient équivalentes; d'après la proposition 4.5, ces matrices ont même rang. Donc

$$\text{rang}(M) = \text{rang}(J_r) = r.$$

Réciproquement, soit M une matrice de rang r . Considérons l'application linéaire U de K^p dans K^n canoniquement associée à M . En appliquant à U le théorème précédent, nous voyons que les matrices M et J_r sont équivalentes.

COROLLAIRE 2. — Caractérisation des matrices équivalentes. — Pour que deux éléments de $M_{n,p}(K)$ soient équivalents, il faut et il suffit qu'ils aient même rang.

4. OPÉRATIONS ÉLÉMENTAIRES

PROPOSITION 4.6. — Affinités, transvections. — Soient E un espace vectoriel de dimension finie $n > 0$ sur K , H un hyperplan de E , U un endomorphisme de E laissant invariant tout élément de H , et V l'endomorphisme de la droite E/H déduit de U par passage au quotient. L'endomorphisme V est donc une homothétie; soit α son rapport.

1. Lorsque $\alpha \neq 1$, il existe une droite D supplémentaire de H et une seule stable par U . On dit alors que U est l'affinité d'axe D , de rapport α , relative à l'hyperplan H .

2. Lorsque $\alpha = 1$, pour toute forme linéaire f sur E dont le noyau est égal à H , il existe un vecteur e et un seul de H tel que, pour tout vecteur x de E ,

$$(1) \quad U(x) = x + f(x) \cdot e.$$

On dit alors que U est une transvection relative à l'hyperplan H .

Soit φ l'application linéaire canonique de E sur E/H .

Assertion 1. — Unicité. — Soient D une droite supplémentaire de H stable par U , et e un élément non nul de D . Il existe donc un scalaire β tel que $U(e) = \beta e$. Il en découle que $V[\varphi(e)] = \beta\varphi(e)$; par suite, $\beta = \alpha \neq 1$. Soit maintenant x un vecteur de E n'appartenant pas à H ; il existe donc un scalaire λ non nul et un élément h de H tels que

$$(2) \quad x = \lambda e + h.$$

Il s'ensuit que

$$(3) \quad U(x) = \lambda\alpha e + h.$$

Puisque $\lambda \neq 0$ et $\alpha \neq 1$, $U(\mathbf{x})$ est colinéaire à \mathbf{x} si et seulement si $\mathbf{h} = \mathbf{0}$. Donc tout vecteur \mathbf{x} de E n'appartenant pas à H tel que $U(\mathbf{x})$ soit colinéaire à \mathbf{x} appartient à D , ce qu'il fallait prouver.

Les relations (2) et (3) montrent enfin que le vecteur \mathbf{e} est nécessairement colinéaire au vecteur $U(\mathbf{x}) - \mathbf{x}$.

Existence. — Puisque $\alpha \neq 1$, il existe un vecteur \mathbf{x}_0 de E tel que $V[\varphi(\mathbf{x}_0)] \neq \varphi(\mathbf{x}_0)$. Comme $V \circ \varphi = \varphi \circ U$, cela signifie que le vecteur $\mathbf{e} = U(\mathbf{x}_0) - \mathbf{x}_0$ n'appartient pas à H . La droite $D = K\mathbf{e}$ est donc un sous-espace vectoriel supplémentaire de H dans E , d'après la proposition I.3.34. Il reste à voir que D est stable par U ; notons pour cela que \mathbf{x}_0 n'appartient pas à H , et que, par suite, $E = K\mathbf{x}_0 \oplus H$. En particulier, il existe un scalaire γ et un élément \mathbf{y} de H tels que $\mathbf{e} = \gamma\mathbf{x}_0 + \mathbf{y}$. Il en découle que

$$U(\mathbf{e}) = \gamma U(\mathbf{x}_0) + \mathbf{y} = (\gamma + 1)\mathbf{e},$$

ce qu'il fallait prouver.

Assertion 2. — L'unicité de \mathbf{e} est immédiate, puisque la forme linéaire f n'est pas nulle. La relation (1) montre encore que si $f(\mathbf{x}) \neq 0$, le vecteur \mathbf{e} est nécessairement égal au vecteur $[f(\mathbf{x})]^{-1}[U(\mathbf{x}) - \mathbf{x}]$.

Existence. — Soit \mathbf{x}_0 un vecteur de E n'appartenant pas à H ; considérons le vecteur $\mathbf{e} = [f(\mathbf{x}_0)]^{-1}[U(\mathbf{x}_0) - \mathbf{x}_0]$. Le vecteur \mathbf{e} appartient à H , puisque

$$(\varphi \circ U)(\mathbf{x}_0) - \varphi(\mathbf{x}_0) = (V \circ \varphi)(\mathbf{x}_0) - \varphi(\mathbf{x}_0) = \mathbf{0}.$$

Les deux applications linéaires $\mathbf{x} \mapsto U(\mathbf{x})$ et $\mathbf{x} \mapsto \mathbf{x} + f(\mathbf{x}) \cdot \mathbf{e}$ sont égales, puisqu'elles prennent la même valeur sur \mathbf{x}_0 , et sur H .

COROLLAIRE. — **Matrices d'affinité, matrices de transvection.**

1. Lorsque $\alpha \neq 1$, pour tout $i \in [1, n]$, il existe une base $B = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ de E telle que la matrice $M_B(U)$ associée à U dans cette base soit la matrice diagonale définie par les relations

$$\alpha_{ii} = \alpha \quad \text{et} \quad \alpha_{jj} = 1 \quad \text{si} \quad j \neq i.$$

Une telle matrice s'appelle matrice d'affinité.

2. Lorsque $\alpha = 1$, pour tout couple (i, j) d'éléments distincts de $[1, n]$, il existe une base $B = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ de E telle que la matrice $M_B(U)$ associée à U dans cette base soit de la forme

$$M_B(U) = I_n + \lambda M_{ij},$$

où $\lambda \in K$, et où (M_{ij}) désigne la base canonique de $M_n(K)$. Une telle matrice s'appelle matrice de transvection.

Les notions d'affinité et de transvection vont nous permettre de donner des exemples importants de matrices équivalentes :

DÉFINITION 4.6. — Opérations élémentaires. — *On appelle opération élémentaire une application $M \mapsto M'$ de $\mathbf{M}_{n,p}(K)$ dans lui-même de l'un des types suivants :*

- a) *La matrice M' se déduit de la matrice M par permutation de deux colonnes (resp. de deux lignes) ;*
- b) *la matrice M' se déduit de la matrice M par multiplication d'une colonne (resp. d'une ligne) par un scalaire non nul ;*
- c) *la matrice M' se déduit de la matrice M par addition à un vecteur colonne (resp. à un vecteur ligne) du produit d'un autre vecteur colonne (resp. d'un autre vecteur ligne) par un scalaire.*

Dans tous les cas, M' est équivalente à M , puisque le rang des vecteurs colonnes (resp. des vecteurs lignes) de M est inchangé.

Plus précisément :

Soient M et M' deux éléments de $\mathbf{M}_{n,p}(K)$, U et U' les applications linéaires de K^p dans K^n canoniquement associées à M et M' , $\mathbf{a}_1, \dots, \mathbf{a}_j, \dots, \mathbf{a}_p$ les vecteurs colonnes de M , et $\mathbf{a}'_1, \dots, \mathbf{a}'_j, \dots, \mathbf{a}'_p$ les vecteurs colonnes de M' .

a₁) *Cas où M' se déduit de M par permutation de deux colonnes.* Plus précisément, supposons que, pour tout entier $j \in [1, p]$, $\mathbf{a}'_j = \mathbf{a}_{\sigma(j)}$, où σ est une transposition. Il est immédiat que $U' = U \cdot U_\sigma$, où U_σ désigne l'endomorphisme de K^p associé à la permutation σ . Par suite, $M' = M \cdot M_\sigma$; l'opération élémentaire envisagée correspond donc à une multiplication à droite par une matrice de permutation.

a₂) *Cas où M' se déduit de M par permutation de deux lignes.* Si les vecteurs lignes de M' se déduisent des vecteurs lignes de M par une transposition τ , alors $M' = M_\tau \cdot M$.

b₁) *Cas où M' se déduit de M par multiplication du $j^{\text{ième}}$ vecteur colonne par un scalaire λ non nul.* Il est clair que $U' = U \cdot A_j^\lambda$, où A_j^λ désigne l'affinité de K^p d'axe Ke_j , de rapport λ , relative à l'hyperplan $\langle e_j^*, \mathbf{x} \rangle = 0$. Par suite, $M' = M \cdot M_j^\lambda$, où M_j^λ est la matrice associée à A_j^λ ; l'opération élémentaire envisagée correspond donc à une multiplication à droite par une matrice d'affinité.

b₂) *Cas où M' se déduit de M par multiplication du $i^{\text{ième}}$ vecteur ligne par un scalaire μ non nul.* Alors, $U' = A_i^\mu \cdot U$; donc $M' = M_i^\mu \cdot M$.

c₁) *Cas où M' se déduit de M par addition au $j^{\text{ième}}$ vecteur colonne du produit par un scalaire λ du $k^{\text{ième}}$ vecteur colonne, où $k \neq j$.* Il est immédiat que $U' = U \cdot U_{jk}^\lambda$, où U_{jk}^λ désigne la transvection de K^p d'axe Ke_k , de rapport λ , relative à l'hyperplan

$$\langle e_j^*, \mathbf{x} \rangle = 0.$$

Par suite, $M' = M(I_p + \lambda M_{kj})$; l'opération élémentaire envisagée correspond donc à une multiplication à droite par une matrice de transvection.

c₂) Cas où M' se déduit de M par addition au $i^{\text{ème}}$ vecteur ligne du produit par un scalaire μ du $h^{\text{ème}}$ vecteur ligne, où $h \neq i$. Alors $U' = U_{ih}^\mu \cdot U$; donc

$$M' = (I_n + \mu M_{hi})M.$$

REMARQUE 1. — De ce qui précède, il résulte que si un élément M' de $M_{n,p}(K)$ se déduit d'un élément M de $M_{n,p}(K)$ par une suite finie d'opérations élémentaires, les matrices M et M' sont équivalentes.

La réciproque de cette assertion fait l'objet de l'exercice 39. On trouvera, en outre, dans cet exercice, un algorithme permettant, étant donné un élément M de $M_{n,p}(K)$ de calculer son rang r , et de déterminer un élément inversible P de $M_p(K)$ et un élément inversible Q de $M_n(K)$ tels que $M = QJ_rP$.

REMARQUE 2. — La théorie des opérations élémentaires et celle des matrices équivalentes peuvent se généraliser au cas des matrices dont les éléments appartiennent à un anneau principal A ; les cas les plus intéressants sont ceux où $A = \mathbb{Z}$ et où $A = K[X]$. On pourra consulter à ce sujet les exercices 51 à 53.

Exercices conseillés : 39 à 46.

§ 2. ÉQUATIONS LINÉAIRES

Soient E et F deux espaces vectoriels sur K , U une application de E dans F , et b un élément de F . On appelle équation définie par U et b l'équation

$$(1) \quad U(x) = b.$$

Conformément au § I.1.3, on appelle solution de l'équation (1) tout élément x_0 de E tel que $U(x_0) = b$.

DÉFINITION 4.7. — **Équations linéaires.** — On dit que l'équation (1) est linéaire si U est une application linéaire de E dans F . Le vecteur b s'appelle second membre de l'équation (1).

Lorsque $b = 0$, on dit que l'équation (1) est homogène, ou, par abus de langage, sans second membre.

L'équation

$$(2) \quad U(x) = 0$$

s'appelle équation linéaire homogène associée à l'équation (1).

EXEMPLES.

1. Soient E un espace vectoriel sur K , α^* une forme linéaire sur E , et β un scalaire. L'équation

$$(3) \quad \alpha^*(x) = \langle \alpha^*, x \rangle = \beta$$

est linéaire.

Si $E = K^p$, notons $\alpha_1, \alpha_2, \dots, \alpha_p$ les composantes de la forme linéaire α^* dans la base canonique de $(K^p)^*$, et $\xi_1, \xi_2, \dots, \xi_p$ les composantes du vecteur x dans la base canonique de K^p . L'équation (1) s'écrit alors

$$(4) \quad \alpha_1 \xi_1 + \alpha_2 \xi_2 + \dots + \alpha_p \xi_p = \beta.$$

Les scalaires $\alpha_1, \alpha_2, \dots, \alpha_p$ s'appellent coefficients, les scalaires $\xi_1, \xi_2, \dots, \xi_p$ inconnues de l'équation (4). On dit que l'équation (4) est une équation linéaire à p inconnues.

*2. On prend pour E l'espace vectoriel des fonctions à valeurs complexes, définies et continûment dérivables sur un intervalle I de \mathbf{R} , et pour F l'espace vectoriel des fonctions à valeurs complexes, définies et continues sur I . Soient a, b, c trois éléments de F . On considère l'application D de E dans F qui à tout élément g de E associe sa dérivée $D(g)$. L'équation

$$a \cdot D(f) + b \cdot f = c$$

est une équation linéaire, à savoir l'équation linéaire associée au couple (U, c) , où U est l'équation linéaire de E dans F définie par la formule

$$U(g) = a \cdot D(g) + b \cdot g.$$

Une telle équation s'appelle équation différentielle linéaire du premier ordre, avec second membre (cf. Analyse III).*

*3. On prend pour E l'espace vectoriel des fonctions à valeurs réelles, définies et deux fois continûment différentiables sur \mathbf{R}^2 , et pour F l'espace vectoriel des fonctions à valeurs réelles, définies et continues sur \mathbf{R}^2 . Soit Δ l'application linéaire de E dans F qui à tout élément h de E associe

$$\Delta h = \frac{\partial^2 h}{\partial x^2} + \frac{\partial^2 h}{\partial y^2}.$$

Pour tout élément g de F , l'équation $\Delta f = g$ est une équation linéaire.*

*4. On prend pour E l'espace vectoriel des fonctions à valeurs réelles, définies et une fois continûment différentiables sur \mathbf{R}^3 , et pour F l'espace vectoriel des fonctions définies et continues sur \mathbf{R}^3 à valeurs dans \mathbf{R}^3 . Soit b un élément de F ; alors l'équation

$$\text{grad } f = b$$

est linéaire.*

Plus généralement, soient E un espace vectoriel sur K , et $(F_i)_{i \in I}$ une famille d'espaces vectoriels sur K . Pour tout $i \in I$, on considère une application U_i de E dans F_i , et un élément b_i de F_i . On appelle système d'équations associé aux familles $(U_i)_{i \in I}$ et $(b_i)_{i \in I}$, et on note (S) , la famille d'équations

$$U_i(x) = b_i, \quad i \in I.$$

On appelle solution du système (S) tout élément \mathbf{x}_0 de E tel que, pour tout élément i de I ,

$$U_i(\mathbf{x}_0) = \mathbf{b}_i.$$

La recherche de l'ensemble $\mathfrak{S}(S)$ des solutions de (S) s'appelle résolution du système (S) .

Étant donnés deux systèmes (S) et (T) ,

$$\begin{array}{ll} (S) & U_i(\mathbf{x}) = \mathbf{b}_i, \quad i \in I, \\ (T) & V_j(\mathbf{x}) = \mathbf{c}_j, \quad j \in J, \end{array}$$

on dit que (S) implique (T) si toute solution de (S) est solution de (T) , c'est-à-dire si $\mathfrak{S}(S) \subset \mathfrak{S}(T)$. On dit que les systèmes (S) et (T) sont équivalents si les solutions de (S) et de (T) sont les mêmes, c'est-à-dire si $\mathfrak{S}(S) = \mathfrak{S}(T)$.

DÉFINITION 4.8. — Systèmes linéaires. — On dit que le système (S) est linéaire si, pour tout élément i de I , U_i est une application linéaire de E dans F_i . La famille $(\mathbf{b}_i)_{i \in I}$ s'appelle second membre du système (S) .

Si, pour tout $i \in I$, $\mathbf{b}_i = \mathbf{0}$, on dit que le système (S) est homogène, ou, par abus de langage, sans second membre.

Le système linéaire

$$U_i(\mathbf{x}) = \mathbf{0}, \quad i \in I,$$

s'appelle système linéaire homogène associé au système linéaire (S) .

REMARQUE. — La notion de système d'équations linéaires paraît plus générale que celle d'équation linéaire. En fait, il n'en est rien : soient en effet E un espace vectoriel sur K , $(F_i)_{i \in I}$ une famille d'espaces vectoriels sur K , $(U_i)_{i \in I}$ un élément de l'ensemble produit $\prod_{i \in I} \mathcal{L}(E, F_i)$, et $(\mathbf{b}_i)_{i \in I}$ un élément de l'ensemble

produit $\prod_{i \in I} F_i$. Considérons le système

$$(S) \quad U_i(\mathbf{x}) = \mathbf{b}_i, \quad i \in I.$$

Introduisons l'espace vectoriel F produit de la famille des espaces vectoriels F_i , où i parcourt I , notons \mathbf{b} l'élément $(\mathbf{b}_i)_{i \in I}$ de F , et désignons par U l'application de E dans F qui à tout élément \mathbf{x} de E associe l'élément $(U_i(\mathbf{x}))_{i \in I}$ de F . Il est immédiat que U est une application linéaire de E dans F , et que le système (S) est équivalent à l'unique équation linéaire suivante :

$$U(\mathbf{x}) = \mathbf{b}.$$

On notera que si le système (S) est homogène, l'équation linéaire précédente l'est aussi.

Cette remarque nous permettra, dans la suite, de déduire les résultats relatifs aux systèmes linéaires des résultats relatifs à une seule équation linéaire.

PROPOSITION 4.7. — Propriétés de l'ensemble des solutions d'une équation linéaire. — Soient E et F deux espaces vectoriels sur K , U une application linéaire de E dans F , et b un élément de F . On considère l'équation linéaire

$$(1) \quad U(x) = b.$$

1. Si l'équation (1) est homogène, ses solutions forment un sous-espace vectoriel de E , à savoir le noyau de U . En particulier, une équation homogène admet toujours la solution 0 , dite triviale.

2. Si l'équation (1) admet une solution x_0 , on obtient toutes les solutions de cette équation en ajoutant à x_0 une solution quelconque de l'équation homogène associée.

3. On suppose données une famille $(f_i)_{i \in I}$ de vecteurs de F et, pour tout $i \in I$, une solution x_i de l'équation $U(x) = f_i$. On suppose, en outre, que le vecteur b puisse s'écrire sous la forme $b = \sum_{i \in I} \beta_i f_i$; alors le vecteur $x_0 = \sum_{i \in I} \beta_i x_i$ est une solution de l'équation (1).

REMARQUE. — Cette proposition est très utile en pratique, lorsque U est surjective. Pour résoudre l'équation linéaire (1), il suffit en effet de résoudre l'équation homogène associée et les équations $U(x) = f_i$, où $(f_i)_{i \in I}$ est une base de l'espace vectoriel F , choisie de façon à simplifier la résolution de ces équations. Très fréquemment, on procède de la façon suivante :

- a) On détermine le noyau de l'application linéaire U .
 - b) On choisit convenablement un supplémentaire E' de ce noyau dans E . Alors la restriction V de l'application linéaire surjective U à E' est un isomorphisme de E' sur F (cf. prop. I.3.28).
 - c) On choisit une base convenable $(f_i)_{i \in I}$ de F , et on calcule, pour tout $i \in I$, l'unique solution x_i de l'équation $V(x) = f_i$.
 - d) Soit b un élément de F ; on l'écrit sous la forme $b = \sum_{i \in I} \beta_i f_i$. Le vecteur $x_0 = \sum_{i \in I} \beta_i x_i$ est alors le seul vecteur de E' solution de l'équation $V(x) = b$.
 - e) La solution générale de l'équation $U(x) = b$ s'obtient en ajoutant au vecteur x_0 un élément quelconque du noyau de U .
- On trouvera des exemples dans le paragraphe suivant.

THÉORÈME 4.2. — Unicité des solutions d'une équation linéaire quel que soit le second membre. — Soient E et F deux espaces vectoriels sur K , et U une application linéaire de E dans F . Il est équivalent de dire :

- 1. Pour tout vecteur b de F , l'équation $U(x) = b$ admet au plus une solution.
- 2. L'équation linéaire homogène $U(x) = 0$ admet pour seule solution la solution triviale; autrement dit, l'application linéaire U est injective.

Si E et F sont de dimension finie, ces conditions sont aussi équivalentes aux suivantes.

- 3. L'application tU transposée de U est surjective.
- 4. L'ensemble des vecteurs de E orthogonaux à l'image de tU est réduit au vecteur nul.

L'équivalence des conditions 1 et 2 est immédiate.

Montrons maintenant l'équivalence des conditions 2, 3 et 4, dans le cas de la dimension finie. Le théorème I.3.12 montre que

$$(1) \quad \text{Im} ({}^tU) = [\text{Ker} (U)]^\perp.$$

Il en résulte que $2 \Rightarrow 3$. Prouvons maintenant que $3 \Rightarrow 4$: supposons que tU soit surjective, et considérons un vecteur \mathfrak{x} de E orthogonal à l'image de tU , c'est-à-dire à E^* . Un tel vecteur est nul, d'après le corollaire 2 de la proposition I.3.42.

Il reste à montrer que $4 \Rightarrow 2$: soit \mathfrak{x} un élément du noyau de U ; alors, pour tout élément y^* de F^* ,

$$\langle {}^tU(y^*), \mathfrak{x} \rangle = \langle y^*, U(\mathfrak{x}) \rangle = 0.$$

Ainsi, \mathfrak{x} est orthogonal à l'image de tU , donc est nul.

REMARQUE. — En fait, les conditions 1, 2, 3 et 4 sont toujours équivalentes, même lorsque E et F ne sont pas de dimension finie : la même démonstration s'applique, à condition de tenir compte des remarques suivant le théorème I.3.12 et la proposition I.3.42.

THÉORÈME 4.3. — Existence des solutions d'une équation linéaire quel que soit le second membre. — Soient E et F deux espaces vectoriels sur K , et U une application linéaire de E dans F . Il est équivalent de dire :

1. Pour tout vecteur b de F , l'équation $U(\mathfrak{x}) = b$ admet au moins une solution.

2. L'application linéaire U est surjective.

Si E et F sont de dimension finie, ces conditions sont encore équivalentes aux suivantes :

3. L'application tU transposée de U est injective.

4. L'ensemble des éléments de F^* orthogonaux à l'image de U est réduit à la forme linéaire nulle.

L'équivalence des conditions 1 et 2 est évidente.

Montrons maintenant l'équivalence des conditions 2, 3 et 4 dans le cas de la dimension finie. Le théorème I.3.12 montre que

$$(2) \quad \text{Ker} ({}^tU) = [\text{Im} (U)]^\perp.$$

Ainsi, tU est injective si et seulement si $[\text{Im} (U)]^\perp = \{0^*\}$, ce qui prouve l'équivalence des conditions 3 et 4.

Il est évident que $2 \Rightarrow 4$; enfin, $4 \Rightarrow 2$, puisque, d'après le théorème I.3.10 la relation $[\text{Im} (U)]^\perp = \{0^*\}$, entraîne la relation $\text{Im} (U) = F$.

REMARQUE. — En fait, les conditions 1, 2, 3 et 4 sont toujours équivalentes, même lorsque E et F ne sont pas de dimension finie : la même démonstration s'applique, à condition de tenir compte de l'exercice I.3.40 au lieu du théorème I.3.10.

Voici maintenant un critère d'existence et d'unicité :

PROPOSITION 4.8. — Existence et unicité des solutions d'une équation linéaire, quel que soit le second membre. — Soient E et F deux espaces vectoriels sur K , et U une application linéaire de E dans F . Il est équivalent de dire :

1. Pour tout vecteur \mathbf{b} de F , l'équation $U(\mathbf{x}) = \mathbf{b}$ admet une solution et une seule.
2. L'application linéaire U est bijective.

De plus, si ces conditions équivalentes sont satisfaites, l'unique solution de l'équation $U(\mathbf{x}) = \mathbf{b}$ n'est autre que $U^{-1}(\mathbf{b})$; l'application de F dans E qui à tout vecteur \mathbf{b} associe cette solution est donc linéaire. On dit aussi que la solution dépend linéairement du second membre.

Si E et F sont de dimension finie, les conditions 1 et 2 sont encore équivalentes à la suivante :

3. L'application tU transposée de U est bijective.

REMARQUE. — En tenant compte des remarques suivant les théorèmes 4.2 et 4.3, on voit que les conditions 1, 2 et 3 sont équivalentes même lorsque les espaces vectoriels E et F ne sont pas de dimension finie.

Voici enfin un critère d'existence d'une solution d'une équation linéaire de second membre donné :

THÉORÈME 4.4. — Existence d'une solution d'une équation linéaire dont le second membre est donné. — Soient E et F deux espaces vectoriels sur K , U une application linéaire de E dans F , et \mathbf{b} un élément de F . Il est équivalent de dire :

1. L'équation linéaire $U(\mathbf{x}) = \mathbf{b}$ admet au moins une solution.
2. Le vecteur \mathbf{b} appartient à l'image de U .

Si E et F sont de dimension finie, ces conditions sont aussi équivalentes aux suivantes :

3. Le vecteur \mathbf{b} est orthogonal au noyau de l'application tU transposée de U .
4. Toute forme linéaire sur F orthogonale à l'image de U est orthogonale à \mathbf{b} .

L'équivalence des conditions 1 et 2 est immédiate.

Montrons maintenant l'équivalence des conditions 2, 3 et 4, dans le cas de la dimension finie. Le théorème I.3.12 montre que

$$(2) \quad \text{Ker} ({}^tU) = [\text{Im} (U)]^\perp.$$

Ainsi, la condition 3 s'énonce encore : \mathbf{b} appartient à $([\text{Im} (U)]^\perp)'$. Or, le théorème I.3.10 montre que $([\text{Im} (U)]^\perp)' = \text{Im} (U)$, ce qui prouve l'équivalence des conditions 2 et 3.

Il est immédiat que la condition 3 est équivalente à la suivante : le sous-espace vectoriel $\text{Ker } ({}^tU)$ est orthogonal à \mathbf{b} ; d'après la relation (2), cela signifie que $[\text{Im } (U)]^\perp$ est orthogonal à \mathbf{b} , d'où l'équivalence des conditions 3 et 4.

REMARQUE. — Ici encore, les conditions 1, 2, 3 et 4 sont toujours équivalentes, même lorsque E et F ne sont pas de dimension finie. Le théorème I.3.10 doit alors être remplacé par les résultats de l'exercice I.3.40.

§ 3. EXEMPLES D'ÉQUATIONS LINÉAIRES

Appliquons maintenant les résultats du § 2 à deux exemples classiques.

THÉORÈME 4.5. — Polynôme d'interpolation de Lagrange. — *Soient K un corps commutatif, n un entier strictement positif, et $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite de scalaires distincts deux à deux.*

1. *Pour tout élément $\mathbf{b} = (\beta_1, \beta_2, \dots, \beta_n)$ de K^n , il existe un élément $P_{\mathbf{b}}$ de $K[X]$ et un seul de degré strictement inférieur à n , et tel que, pour tout $i \in [1, n]$,*

$$P_{\mathbf{b}}(\alpha_i) = \beta_i.$$

Ce polynôme est appelé polynôme d'interpolation de Lagrange associé à la suite $(\beta_1, \beta_2, \dots, \beta_n)$.

2. *L'application qui à tout élément \mathbf{b} de K^n associe le polynôme $P_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel K^n sur l'espace vectoriel des polynômes à coefficients dans K de degré strictement inférieur à n .*

3. *Pour tout élément \mathbf{b} de K^n , les éléments P de $K[X]$ tels que, pour tout $i \in [1, n]$,*

$$P(\alpha_i) = \beta_i,$$

sont les polynômes de la forme

$$P = P_{\mathbf{b}} + Q \prod_{i=1}^n (X - \alpha_i),$$

où Q parcourt $K[X]$.

4. *Le polynôme d'interpolation de Lagrange associé au vecteur \mathbf{e}_i , où $(\mathbf{e}_i)_{1 \leq i \leq n}$ désigne la base canonique de K^n , est donné par la formule*

$$(1) \quad P_i = \frac{\prod_{j \neq i} (X - \alpha_j)}{\prod_{j \neq i} (\alpha_i - \alpha_j)}.$$

Pour tout élément b de K^n , le polynôme P_b est donné par la formule suivante, dite formule d'interpolation de Lagrange :

$$(2) \quad P_b = \sum_{i=1}^n \beta_i P_i.$$

Notons d'abord que, pour tout $i \in [1, n]$, l'application δ_{α_i} qui à tout élément P de $K[X]$ associe $P(\alpha_i)$ est une forme linéaire sur l'espace vectoriel $K[X]$. Le système d'équations

$$(S) \quad P(\alpha_i) = \beta_i, \quad i \in [1, n],$$

est donc linéaire.

Considérons alors l'application U de $K[X]$ dans K^n qui à tout polynôme P associe le vecteur $(P(\alpha_i))_{1 \leq i \leq n}$. Il est immédiat que U est une application linéaire, et que le système (S) est équivalent à l'unique équation linéaire

$$U(P) = b.$$

a) **Résolution de l'équation homogène $U(P) = 0$.** — Les éléments du noyau de U sont les polynômes P tels que, pour tout $i \in [1, n]$, $P(\alpha_i) = 0$. Ces polynômes ne sont autres que

les multiples du polynôme $\prod_{i=1}^n (X - \alpha_i)$.

b) **Choix d'un supplémentaire du noyau de U .** — L'espace vectoriel E' des polynômes de degré strictement inférieur à n est un sous-espace vectoriel supplémentaire du noyau de U dans $K[X]$. Soit V la restriction de U à E' ; d'après la proposition I.3.28, V est injective. Comme $\dim E' = n$, V est un isomorphisme de E' sur K^n . Il en découle que, pour tout élément b de K^n , il existe un élément P_b de E' et un seul tel que, pour tout $i \in [1, n]$, $P_b(\alpha_i) = \beta_i$. Il en résulte aussi que l'application $b \mapsto P_b$ est un isomorphisme de K^n sur E' .

Les assertions 1, 2 et 3 sont alors évidentes.

c) **Résolution de l'équation $V(P) = e_i$.** — Soit P_i l'unique solution de cette équation. Pour tout entier $j \in [1, n]$, $j \neq i$, $P_i(\alpha_j) = 0$; le polynôme P_i est donc divisible par le polynôme $R_i = \prod_{j \neq i} (X - \alpha_j)$. Comme $\deg(R_i) = n - 1$, et $\deg(P_i) \leq n - 1$, il existe un scalaire γ_i tel que $P_i = \gamma_i R_i$. En substituant à X le scalaire α_i , nous voyons que

$$\gamma_i = \frac{1}{\prod_{j \neq i} (\alpha_i - \alpha_j)}.$$

L'assertion 4 s'en déduit aussitôt.

THÉORÈME 4.6. — Polynôme d'interpolation de Lagrange-Sylvester. — Soient K un corps commutatif de caractéristique zéro, D la dérivation canonique de l'algèbre $K[X]$, r un entier strictement positif, $(\alpha_1, \alpha_2, \dots, \alpha_r)$ une suite de scalaires distincts deux à deux, et (n_1, n_2, \dots, n_r) une suite d'entiers strictement positifs. On désigne par I la partie de $[1, r] \times \mathbb{N}$ constituée des couples (i, h) tels que h appartienne à l'intervalle $[0, n_i - 1]$. On sait que I est un ensemble fini, et que son cardinal est égal à $n = \sum_{i=1}^r n_i$.

1. Pour tout élément $\mathbf{b} = (\beta_{i,h})_{(i,h) \in I}$ de K^I , il existe un élément $P_{\mathbf{b}}$ de $K[X]$ et un seul, de degré strictement inférieur à n , et tel que, pour tout élément (i, h) de I ,

$$(D^h P_{\mathbf{b}})(\alpha_i) = \beta_{i,h}.$$

Ce polynôme est appelé *polynôme d'interpolation de Lagrange-Sylvester associé à la famille de scalaires $(\beta_{i,h})$* .

2. L'application qui à tout élément \mathbf{b} de K^I associe le polynôme $P_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel K^I sur l'espace vectoriel des polynômes à coefficients dans K de degré strictement inférieur à n .

3. Pour tout élément \mathbf{b} de K^I , les éléments P de $K[X]$ tels que, pour tout élément (i, h) de I ,

$$(D^h P)(\alpha_i) = \beta_{i,h},$$

sont les polynômes de la forme

$$P = P_{\mathbf{b}} + Q \prod_{i=1}^r (X - \alpha_i)^{n_i},$$

où Q parcourt $K[X]$.

Notons d'abord que pour tout élément (i, h) de $[1, r] \times \mathbf{N}$, l'application $\delta_{\alpha_i, h}$ qui à tout élément P de $K[X]$ associe le scalaire $(D^h P)(\alpha_i)$ est une forme linéaire sur l'espace vectoriel $K[X]$. Le système d'équations

$$(S) \quad (D^h P)(\alpha_i) = \beta_{i,h}, \quad (i, h) \in I,$$

est donc linéaire.

Considérons alors l'application U de $K[X]$ dans K^I qui à tout polynôme P associe le vecteur dont les composantes sont les scalaires $(D^h P)(\alpha_i)$. Il est immédiat que U est une application linéaire, et que le système (S) est équivalent à l'unique équation linéaire suivante :

$$U(P) = \mathbf{b}.$$

Pour résoudre cette équation, procédons comme dans le théorème 4.5 :

a) Résolution de l'équation homogène $U(P) = \mathbf{0}$. — Les éléments du noyau de U sont les polynômes P tels que, pour tout élément (i, h) de I , $(D^h P)(\alpha_i) = 0$. D'après le corollaire 2 du théorème 1.9, cela revient à dire que, pour tout $i \in [1, r]$, le scalaire α_i est une racine d'ordre supérieur ou égal à n_i . Il résulte alors du théorème 1.2 que ces polynômes ne sont autres que

les multiples du polynôme $\prod_{i=1}^r (X - \alpha_i)^{n_i}$.

b) Recherche d'un supplémentaire du noyau de U . — L'espace vectoriel E des polynômes de degré strictement inférieur à n est un sous-espace supplémentaire du noyau de U dans $K[X]$. Comme au théorème 4.5, on démontrera l'existence et l'unicité de $P_{\mathbf{b}}$, et on verra que l'application $\mathbf{b} \mapsto P_{\mathbf{b}}$ est un isomorphisme de K^I sur E .

Les assertions 1, 2 et 3 sont alors évidentes.

REMARQUE 1. — **Détermination explicite du polynôme d'interpolation de Lagrange-Sylvester.** — Contrairement au cas, examiné dans le théorème 4.5, où tous les entiers n_i sont égaux à 1, on ne peut pas donner une formule simple explicitant le polynôme $P_{\mathbf{b}}$. Essayons en effet de calculer l'unique solution $P_{i,h}$ de l'équation $V(P) = e_{i,h}$, où $(e_{i,h})_{(i,h) \in I}$ désigne la base canonique de K^I . Pour tout entier $j \in [1, r]$, $j \neq i$, $(D^k P_{i,h})(\alpha_j) = 0$ pour tout $k \in [0, n_j - 1]$; d'autre part, $(D^k P_{i,h})(\alpha_i) = 0$ pour tout $k \in [0, h - 1]$. D'après le corollaire 2 du théorème 1.9, et le théorème 1.2, le polynôme $P_{i,h}$ est donc divisible par le polynôme

$$R_{i,h} = (X - \alpha_i)^h \cdot \prod_{j \neq i} (X - \alpha_j)^{n_j}.$$

Lorsque l'entier h est égal à $n_i - 1$, il en résulte qu'il existe un scalaire γ_i tel que $P_{i,h} = \gamma_i R_{i,h}$. En substituant à X le scalaire α_i dans les polynômes $D^h P_{i,h}$ et $D^h R_{i,h}$, nous voyons que

$$\gamma_i = \frac{1}{(n_i - 1)!} \cdot \frac{1}{\prod_{j \neq i} (\alpha_i - \alpha_j)^{n_j}}.$$

Introduisons donc, pour tout élément (i, h) de I , le polynôme $S_{i,h}$ défini par la formule suivante :

$$(1) \quad S_{i,h} = \frac{(X - \alpha_i)^h}{h!} \cdot \frac{\prod_{j \neq i} (X - \alpha_j)^{n_j}}{\prod_{j \neq i} (\alpha_i - \alpha_j)^{n_j}}.$$

Alors la famille $(S_{i,h})$, où (i, h) parcourt I , est une base de l'espace vectoriel des polynômes de degré strictement inférieur à n . En particulier, pour tout élément $\mathbf{b} = (\beta_{j,k})$ de K^I , le polynôme $P_{\mathbf{b}}$ est donné par la formule suivante, dite formule d'interpolation de Lagrange-Sylvester :

$$(2) \quad P_{\mathbf{b}} = \sum_{(i,h) \in I} \gamma_{i,h} \cdot S_{i,h},$$

où, étant donné un élément j de $[1, r]$, les scalaires $\gamma_{j,0}, \dots, \gamma_{j,k}, \dots, \gamma_{j,n_j-1}$ se calculent par récurrence sur k à l'aide des relations suivantes :

$$(3) \quad \beta_{j,k} = \gamma_{j,0} \cdot (D^k S_{j,0})(\alpha_j) + \gamma_{j,1} \cdot (D^k S_{j,1})(\alpha_j) + \dots + \gamma_{j,k}.$$

Puisque les polynômes $S_{i,h}$ constituent une famille de n éléments de E , et que la dimension de E est égale à n , il suffit de prouver que cette famille est libre. Considérons donc une relation linéaire $\sum_{(i,h) \in I} \lambda_{i,h} \cdot S_{i,h} = 0$ entre ses éléments, et supposons par l'absurde qu'il existe un élément (j, k) de I tel que $\lambda_{j,k} \neq 0$. Il en résulte aussitôt que la valuation au point α_j du polynôme $\sum_{(i,h) \in I} \lambda_{i,h} \cdot S_{i,h}$ est inférieure ou égale à k ; d'où la contradiction cherchée.

Pour calculer les scalaires $\gamma_{i,h}$, considérons un élément (j, k) de I , et substituons à X le scalaire α_j dans les dérivées $k^{\text{ièmes}}$ des deux membres de la relation (2) :

$$(4) \quad \beta_{j,k} = \sum_{(i,h) \in I} \gamma_{i,h} \cdot (D^k S_{i,h})(\alpha_j).$$

La relation (3) s'en déduit, car $(D^k S_{i,h})(\alpha_j)$ est nul si $i \neq j$, ou si $i = j$ et $h > k$, et est égal à 1 si $i = j$ et $h = k$.

REMARQUE 2. — L'énoncé et la démonstration du théorème 4.6 sont encore valables lorsque la caractéristique de K est supérieure au plus grand des entiers n_i . Par suite, le théorème 4.6 joint à la remarque 1, se spécialise en théorème 4.5 lorsque tous les entiers n_i sont égaux à 1; dans ce cas le polynôme de Lagrange-Sylvester n'est autre que le polynôme de Lagrange.

REMARQUE 3. — Lorsque l'entier r est égal à 1, la formule d'interpolation de Lagrange-Sylvester se spécialise en la formule de Taylor.

THÉORÈME 4.7. — Polynômes de Hilbert. — Soient K un corps de caractéristique zéro, et Δ l'application de l'algèbre $K[X]$ dans elle-même qui à tout polynôme P associe le polynôme ΔP défini par la formule

$$(1) \quad (\Delta P)(X) = P(X + 1) - P(X).$$

1. L'application Δ est un endomorphisme de l'espace vectoriel $K[X]$. Cet endomorphisme est surjectif, et son noyau est K . De plus, si P est non constant, $d^0(\Delta P) = d^0(P) - 1$.

Soit E le sous-espace vectoriel de $K[X]$ constitué des polynômes P tels que $P(0) = 0$; alors la restriction de Δ à E est un isomorphisme de l'espace vectoriel E sur l'espace vectoriel $K[X]$.

En particulier, étant donné un élément Q de $K[X]$, il existe un élément P de $K[X]$ et un seul tel que

$$(2) \quad P(X + 1) - P(X) = Q(X), \quad \text{et} \quad P(0) = 0.$$

2. Il existe une suite $(H_0, H_1, \dots, H_n, \dots)$ et une seule d'éléments de $K[X]$ telle que $H_0 = 1$, et que, pour tout $n \in \mathbb{N}^*$, $\Delta H_n = H_{n-1}$ et $H_n(0) = 0$. Pour tout entier $n > 0$, le polynôme H_n est donné par la formule suivante :

$$(3) \quad H_n = \frac{X(X-1) \dots (X-n+1)}{n!}.$$

Les polynômes H_n sont appelés polynômes de Hilbert; ils forment une base de l'espace vectoriel $K[X]$.

3. Soit Q un élément de $K[X]$; alors la décomposition du polynôme Q dans la base des polynômes de Hilbert s'écrit :

$$(4) \quad Q = \sum_{n=0}^{+\infty} (\Delta^n Q)(0) \cdot H_n.$$

4. Soit Q un élément de $K[X]$, écrit sous la forme $Q = \sum_{n=0}^{+\infty} \alpha_n H_n$; alors l'unique polynôme P tel que $P(X + 1) - P(X) = Q(X)$ et que $P(0) = 0$ est donné par la formule suivante :

$$(5) \quad P = \sum_{n=0}^{+\infty} \alpha_n H_{n+1}.$$

Assertion 1. — Il est clair que l'application Δ est linéaire. Déterminons d'abord son noyau : soit P un polynôme appartenant au noyau de Δ , c'est-à-dire tel que $P(X+1) = P(X)$. Il en résulte aussitôt que le polynôme $P(X) - P(0)$ admet pour racines tous les entiers rationnels (le corps K étant de caractéristique zéro, nous identifions le corps \mathbb{Q} à un sous-corps de K ; cf. prop. I.2.42). Il découle du théorème 1.3 que le polynôme $P(X) - P(0)$ est nul, donc que P est constant. Réciproquement, il est évident que tout polynôme constant appartient au noyau de Δ .

Il résulte facilement de la formule du binôme que si P n'est pas constant, $d^\circ(\Delta P) = d^\circ(P) - 1$.

Considérons maintenant le sous-espace vectoriel E de $K[X]$. Comme E est un sous-espace supplémentaire de K dans $K[X]$, la restriction U de Δ à E est une application linéaire injective de E dans $K[X]$ (cf. prop. I.3.28). Pour achever la preuve de l'assertion 1, il nous reste à montrer que U est surjective.

A cet effet, introduisons, pour tout entier p strictement positif, l'espace vectoriel E_p constitué des éléments de E de degré inférieur ou égal à p , et l'espace vectoriel F_p constitué des éléments de $K[X]$ dont le degré est strictement inférieur à p . Il est immédiat que si R est un élément de E_p , alors $U(R)$ est un élément de F_p . La restriction U_p de U à E_p définit donc une application linéaire de E_p dans F_p , injective puisque U l'est. Comme $\dim E_p = \dim F_p = p$, U_p est un isomorphisme de E_p sur F_p (cf. th. I.3.7).

Soit maintenant Q un élément de $K[X]$, de degré n ; puisque U_{n+1} est un isomorphisme de E_{n+1} sur F_{n+1} , il existe un élément P de E_{n+1} et un seul tel que $U_{n+1}(P) = Q$, c'est-à-dire tel que $U(P) = Q$. L'application U est donc surjective.

Assertion 2. — On montre aussitôt, par récurrence sur n , qu'il existe une suite $(H_0, H_1, \dots, H_p, \dots, H_n)$ d'éléments de $K[X]$ et une seule telle que $H_0 = 1$, et que, pour tout $p \in [1, n]$, $H_p \in E$ et $\Delta H_p = H_{p-1}$. Il est d'autre part immédiat que les polynômes définis par la formule (3) conviennent.

Assertion 3. — Soit Q un élément de $K[X]$, écrit sous la forme :

$$(6) \quad Q = \sum_{n=0}^{+\infty} \alpha_n H_n.$$

Pour calculer α_0 , il suffit de substituer à X le scalaire 0 dans les deux membres de la relation (6); nous obtenons $Q(0) = \alpha_0$. Plus généralement, pour calculer α_p , appliquons l'opérateur Δ^p aux deux membres de la relation (6) :

$$(7) \quad \Delta^p Q = \sum_{n=p}^{+\infty} \alpha_n H_{n-p}.$$

Il suffit alors de substituer à X le scalaire 0 dans les deux membres de la relation (7); nous obtenons $(\Delta^p Q)(0) = \alpha_p$.

L'assertion 4 est maintenant évidente.

REMARQUE. — Le théorème 4.7 se généralise aussitôt au cas où on remplace Δ par un opérateur de composition d'ordre 1. La formule de Taylor, qui présente une analogie frappante avec la formule (4), rentre dans ce cadre plus général.

COROLLAIRE 1. — **Calcul de la somme des valeurs d'un polynôme sur les entiers inférieurs à un entier donné.** — Soient Q un polynôme à coefficients dans K , et P l'unique polynôme tel que $P(X+1) - P(X) = Q(X)$ et $P(0) = 0$. Alors, pour tout entier naturel n , la somme $S_n = \sum_{m=0}^n Q(m)$ est égale à $P(n+1)$.

EXEMPLE 1. — Somme des puissances $p^{\text{ièmes}}$ des entiers inférieurs à un entier donné. — Soient p un entier naturel, et P_p l'unique polynôme tel que

$$P_p(X+1) - P_p(X) = X^p, \quad \text{et} \quad P_p(0) = 0.$$

Alors la somme $S_n^p = \sum_{m=0}^n m^p$ est égale à $P_p(n+1)$.

Pour expliciter S_n^p , il suffit de calculer le polynôme P_p ; la méthode la plus simple consiste à développer X^p dans la base des polynômes de Hilbert par la formule (4).

Lorsque $p = 0$, $X^0 = H_0$; donc $P_0 = H_1 = X$, et

$$S_n^0 = \sum_{m=0}^n 1 = n+1.$$

Lorsque $p = 1$, $X^1 = H_1$; donc $P_1 = H_2 = \frac{X(X-1)}{2}$, et

$$S_n^1 = \sum_{m=0}^n m = \frac{(n+1)n}{2}.$$

Lorsque $p = 2$, $X^2 = H_1 + 2H_2$; donc $P_2 = H_2 + 2H_3 = \frac{X(X-1)(2X-1)}{6}$, et

$$S_n^2 = \sum_{m=0}^n m^2 = \frac{(n+1)n(2n+1)}{6}.$$

Lorsque $p = 3$, $X^3 = H_1 + 6H_2 + 6H_3$, donc $P_3 = H_2 + 6H_3 + 6H_4 = \frac{X^2(X-1)^2}{4}$ et

$$S_n^3 = \sum_{m=0}^n m^3 = \frac{(n+1)^2 n^2}{4}.$$

EXEMPLE 2. — Somme des premiers termes d'une progression arithmétique. — Soit A un anneau commutatif de caractéristique zéro. Étant donnés deux éléments a et x de A , on appelle *progression arithmétique* de premier terme a et de raison x la suite $(a + nx)_{n \in \mathbb{N}}$. Alors

la somme $S_n = \sum_{m=0}^n (a + mx)$ est donnée par la formule $S_n = (n+1)a + \frac{(n+1)n}{2}x$.

COROLLAIRE 2. — Polynômes qui, pour des valeurs entières de la variable, prennent des valeurs entières. — Soient K un corps de caractéristique zéro, et P un polynôme à coefficients dans K . Pour que $P(n)$ soit un entier rationnel pour tout entier rationnel n , il faut et il suffit que P soit une combinaison linéaire à coefficients entiers rationnels des polynômes de Hilbert.

Considérons l'ensemble M des éléments P de $K[X]$ tels que $P(n) \in \mathbb{Z}$, pour tout $n \in \mathbb{Z}$. Il est immédiat que toute combinaison linéaire à coefficients entiers rationnels d'éléments de M est encore un élément de M . D'autre part, pour tout élément P de M , $\Delta P = P(X+1) - P(X)$ appartient encore à M . Réciproquement, pour tout élément Q de M , l'unique polynôme P tel que $\Delta P = Q$ et que $P(0) = 0$ appartient lui aussi à M , car, pour tout entier naturel n ,

$$P(n) = \sum_{m=1}^{n-1} Q(m), \quad \text{et pour tout entier } n < 0, P(n) = - \sum_{m=-1}^n Q(m). \quad \text{Comme } H_0 = 1 \text{ appartient}$$

3. Interprétation vectorielle. — On cherche les familles $(\xi_1, \dots, \xi_j, \dots, \xi_p)$ de scalaires telles que

$$\xi_1 \mathbf{a}_1 + \xi_2 \mathbf{a}_2 + \dots + \xi_j \mathbf{a}_j + \dots + \xi_p \mathbf{a}_p = \mathbf{b}.$$

4. Interprétation duale. — On cherche les vecteurs \mathbf{x} de K^p tels que

$$\left\{ \begin{array}{l} \langle \mathbf{a}'_1, \mathbf{x} \rangle = \beta_1 \\ \langle \mathbf{a}'_2, \mathbf{x} \rangle = \beta_2 \\ \dots\dots\dots \\ \langle \mathbf{a}'_i, \mathbf{x} \rangle = \beta_i \\ \dots\dots\dots \\ \langle \mathbf{a}'_n, \mathbf{x} \rangle = \beta_n \end{array} \right.$$

c'est-à-dire les vecteurs \mathbf{x} sur lesquels les n formes linéaires \mathbf{a}'_i prennent des valeurs données β_i .

On appelle *rang* d'un système (S') de n équations linéaires à p inconnues le rang de la matrice M , c'est-à-dire le rang de l'application linéaire U .

Étant donné un système linéaire (S') , on note (S) le système linéaire homogène associé à (S') .

Enfin, étant donné un système linéaire homogène (S) de matrice associée M , on appelle *système transposé*, ou parfois *système dual*, le système linéaire homogène de matrice associée ${}^t M$.

Nous allons maintenant appliquer les résultats du § 2 aux systèmes linéaires de n équations à p inconnues, en utilisant leur interprétation opératorielle.

La proposition 4.7, jointe à la théorie du rang, fournit la

PROPOSITION 4.9. — Propriétés de l'ensemble des solutions d'un système linéaire.

1. Soit (S) un système linéaire homogène de n équations à p inconnues, de rang r . Alors l'espace vectoriel des solutions de (S) est de dimension $p - r$.

2. Toute solution d'un système linéaire (S') s'obtient en ajoutant à une solution particulière de (S') une solution du système homogène (S) associé à (S') .

3. Pour trouver une solution d'un système linéaire (S') , il suffit de trouver une solution pour chacun des n systèmes linéaires suivants :

$$(S'_i) \qquad U(\mathbf{x}) = \mathbf{e}_i,$$

où $(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_i, \dots, \mathbf{e}_n)$ désigne la base canonique de K^n .

Appliquons maintenant le théorème 4.2 :

PROPOSITION 4.10. — Unicité des solutions d'un système linéaire quel que soit le second membre. — Soit (S) un système linéaire homogène de n équations à p inconnues. Il est équivalent de dire :

1. Tout système linéaire (S') ayant (S) pour système homogène associé admet au plus une solution.

2. Le système linéaire homogène (S) admet pour seule solution la solution triviale.

2'. Les vecteurs colonnes $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_p$ sont linéairement indépendants dans K^n .

3. Les vecteurs lignes $\mathbf{a}'_1, \mathbf{a}'_2, \dots, \mathbf{a}'_n$ engendrent $(K^p)^*$.

4. L'ensemble des vecteurs de K^p orthogonaux à tous les vecteurs lignes est réduit au vecteur nul.

5. Le rang r du système linéaire (S) est égal à p .

Il suffit de tenir compte des propriétés suivantes :

a) Pour que le vecteur $(\lambda_1, \dots, \lambda_j, \dots, \lambda_p)$ de K^p appartienne au noyau de U , il faut et il suffit que

$$\sum_{j=1}^p \lambda_j \mathbf{a}_j = \mathbf{0}.$$

b) Les vecteurs lignes $\mathbf{a}'_1, \mathbf{a}'_2, \dots, \mathbf{a}'_n$ engendrent l'image de tU .

De même, le théorème 4.3 permet d'énoncer la

PROPOSITION 4.11. — Existence des solutions d'un système linéaire quel que soit le second membre. — Soit (S) un système linéaire homogène de n équations à p inconnues. Il est équivalent de dire :

1. Tout système linéaire (S') ayant (S) pour système homogène associé admet au moins une solution.

1'. Pour toute suite $(\beta_1, \dots, \beta_i, \dots, \beta_n)$ de scalaires, il existe un élément \mathbf{x} de K^p tel que, pour tout $i \in [1, n]$, $\langle \mathbf{a}'_i, \mathbf{x} \rangle = \beta_i$.

(On dit parfois que les n formes linéaires $\mathbf{a}'_1, \dots, \mathbf{a}'_i, \dots, \mathbf{a}'_n$ peuvent prendre des valeurs arbitraires.)

2. Les vecteurs colonnes $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_p$ engendrent K^n .

3. Le système transposé de (S) admet pour seule solution la solution triviale.

3'. Les vecteurs lignes $\mathbf{a}'_1, \mathbf{a}'_2, \dots, \mathbf{a}'_n$ sont linéairement indépendants dans $(K^p)^*$.

4. L'ensemble des éléments de $(K^n)^*$ s'annulant sur tous les vecteurs colonnes est réduit à la forme linéaire nulle.

5. Le rang r du système linéaire (S) est égal à n .

De la proposition 4.8, et des caractérisations des applications linéaires bijectives, nous déduisons la

PROPOSITION 4.12. — Existence et unicité des solutions d'un système linéaire, quel que soit le second membre. — Soit (S) un système linéaire homogène de n équations à p inconnues. Il est équivalent de dire :

1. Tout système linéaire (S') ayant (S) pour système homogène associé admet une solution et une seule.

2. Les entiers p et n sont égaux, et la matrice M associée au système linéaire (S) est inversible.
3. Les entiers p et n sont égaux, et la matrice tM est inversible.
4. Le rang du système linéaire (S) est égal à n et à p .
5. Les entiers p et n sont égaux, et le déterminant de la matrice M associée à (S) est non nul.

De plus, si ces conditions équivalentes sont vérifiées, l'unique solution de l'équation $U(\mathbf{x}) = \mathbf{b}$ n'est autre que $U^{-1}(\mathbf{b})$. L'application de K^n dans lui-même qui à tout vecteur \mathbf{b} de K^n associe cette solution est donc linéaire. On dit aussi que la solution dépend linéairement du second membre.

DÉFINITION 4.9. — Systèmes de Cramer. — Un système linéaire (S') dont le système homogène associé (S) satisfait aux conditions équivalentes du théorème précédent s'appelle système de Cramer.

Appliquons enfin le théorème 4.4 et la théorie du rang, pour obtenir un théorème d'existence pour un système linéaire dont le second membre est donné :

THÉORÈME 4.8. — Existence d'une solution d'un système linéaire dont le second membre est donné. — Soient (S') un système linéaire de n équations à p inconnues, et \mathbf{b} le second membre de (S') . Il est équivalent de dire :

1. Le système linéaire (S') a au moins une solution.
2. Le second membre \mathbf{b} appartient à l'image de l'application linéaire U .
- 2'. Le second membre \mathbf{b} appartient au sous-espace vectoriel de K^n engendré par les vecteurs colonnes $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_p$.
3. Le vecteur \mathbf{b} est orthogonal au noyau de l'application tU transposée de U .
- 3'. Toute relation linéaire $\sum_{i=1}^n \lambda_i \mathbf{a}_i^* = \mathbf{0}^*$ vérifiée par les vecteurs lignes l'est aussi par les scalaires β_i constituant le second membre, c'est-à-dire que

$$\sum_{i=1}^n \lambda_i \beta_i = 0.$$

4. Toute forme linéaire sur K^n orthogonale à l'image de U est orthogonale à \mathbf{b} .
- 4'. Toute forme linéaire sur K^n orthogonale aux vecteurs colonnes $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_p$ est orthogonale à \mathbf{b} .

L'équivalence des conditions 1, 2, 3 et 4 a été vue au théorème 4.4.

$2 \Leftrightarrow 2'$, puisque les vecteurs colonnes $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_p$ engendrent l'image de U . De même, $4 \Leftrightarrow 4'$.

$3 \Leftrightarrow 3'$. Introduisons l'élément \mathbf{y}^* de $(K^n)^*$ ayant pour coordonnées les scalaires λ_i , et désignons par $(\mathbf{f}_1, \dots, \mathbf{f}_i, \dots, \mathbf{f}_n)$ la base canonique de K^n . Alors :

$$\sum_{i=1}^n \lambda_i \mathbf{a}_i^* = \sum_{i=1}^n \lambda_i {}^tU(\mathbf{f}_i^*) = {}^tU\left(\sum_{i=1}^n \lambda_i \mathbf{f}_i^*\right) = {}^tU(\mathbf{y}^*),$$

et :

$$\sum_{i=1}^n \lambda_i \beta_i = \langle y^*, b \rangle.$$

Ainsi, la condition 3' signifie que, pour tout élément y^* de $(K^n)^*$ tel que ${}^tU(y^*) = 0^*$, le scalaire $\langle y^*, b \rangle$ est nul, ou encore que tout élément y^* du noyau de tU est orthogonal à b . D'où l'équivalence de 3 et 3'.

En résumé :

THÉORÈME 4.9. — Théorème de Fontené-Rouché. — Soit (S') un système de n équations linéaires à p inconnues, de rang r . (On sait que $r \leq \inf(n, p)$.) Alors :

1. Si $r = n = p$, il y a existence et unicité de la solution.
2. Si $r = n < p$, il y a existence de la solution ; les solutions du système homogène associé (S) forment un espace vectoriel de dimension $p - r$.
3. Si $r < n$, il y a existence d'une solution sous les conditions équivalentes du théorème 4.8. Lorsqu'il y a existence :

- a) si $r = p$, il y a unicité de la solution ;
- b) si $r < p$, les solutions de (S) forment un espace vectoriel de dimension $p - r$.

En pratique, on peut ramener la résolution des systèmes linéaires de n équations à p inconnues au cas particulier où le rang du système est égal à n :

PROPOSITION 4.13. — Équations redondantes. — Soient (S') un système linéaire, et $P = (\alpha_{ij})_{i \in I, j \in J}$ une matrice principale extraite de M . On suppose que le système (S') a au moins une solution. Alors le système (S'_1) constitué des équations principales de (S') est équivalent au système (S') .

Autrement dit, le système (S'_1) obtenu en ôtant de (S') les équations non principales a les mêmes solutions que le système (S') . C'est pourquoi les équations non principales sont dites redondantes.

Nous pouvons nous ramener au cas où $I = [1, r]$. Soient donc $a_1'^*, a_2'^*, \dots, a_r'^*$ les vecteurs lignes de M relatifs à P ; le système (S'_1) s'écrit alors :

$$(S'_1) \quad \langle a_i'^*, x \rangle = \beta_i, \quad i \in [1, r].$$

Il est clair que toute solution de (S') est solution de (S'_1) . Réciproquement, soit x_1 une solution de (S'_1) ; par hypothèse, nous savons qu'il existe une solution x_0 du système (S') . Le vecteur x_0 est *a fortiori* une solution de (S'_1) ; le vecteur $x_1 - x_0$ est donc orthogonal aux formes linéaires $a_1'^*, a_2'^*, \dots, a_r'^*$. Or, les formes linéaires $a_{r+1}'^*, \dots, a_n'^*$ sont combinaisons linéaires des précédentes. Il en découle que $x_1 - x_0$ est solution du système homogène (S) associé à (S') . Par suite, x_1 est solution de (S') .

Le déterminant de la matrice M du système homogène associé à (S') est égal au déterminant de Vandermonde $V(\alpha_1, \dots, \alpha_j, \dots, \alpha_n)$ (cf. § 3.3). Ce déterminant étant non nul, (S') est un système de Cramer; donc, pour tout $j \in [1, n]$,

$$\xi_j = \frac{V(\alpha_1, \dots, \alpha_{j-1}, \beta, \alpha_{j+1}, \dots, \alpha_n)}{V(\alpha_1, \dots, \alpha_{j-1}, \alpha_j, \alpha_{j+1}, \dots, \alpha_n)}.$$

En utilisant la valeur des déterminants de Vandermonde, nous obtenons la formule suivante :

$$\xi_j = \frac{\prod_{k \neq j} (\beta - \alpha_k)}{\prod_{k \neq j} (\alpha_j - \alpha_k)}.$$

Exercices conseillés : 11, 12, 18, 19, 26 et 30.

2. EMPLOI DES DÉTERMINANTS, DANS LE CAS GÉNÉRAL

Nous nous proposons d'abord de donner un critère d'existence de solutions d'un système linéaire à l'aide de la notion de matrice principale. Nous conservons les notations du paragraphe 4.

DÉFINITION 4.10. — Matrices caractéristiques d'un système linéaire. — Soient (S') un système linéaire de n équations à p inconnues, $M = (\alpha_{ij})$ la matrice du système homogène associé (S) , et \mathbf{b} le second membre de (S') . On considère la matrice M' obtenue en ajoutant à M un $(p + 1)^{\text{ième}}$ vecteur colonne égal à \mathbf{b} .

Soit P une matrice principale extraite de M ; on appelle matrice caractéristique associée à P toute matrice bordante de P dans M' , où la colonne bordante est extraite de \mathbf{b} . Il y a donc $n - r$ matrices caractéristiques, où $r = \text{rang}(M)$. Les déterminants de ces matrices sont appelés déterminants caractéristiques.

Si $P = (\alpha_{ij})_{i \in I, j \in J}$, les équations d'indice i appartenant à I s'appellent équations principales, les inconnues d'indice j appartenant à J s'appellent inconnues principales.

Le théorème d'existence d'une solution d'un système linéaire dont le second membre est donné (th. 4.8) peut maintenant être complété de la manière suivante :

THÉORÈME 4.11. — Critère d'existence à l'aide des déterminants caractéristiques. — Soient (S') un système linéaire de n équations à p inconnues, M la matrice du système homogène associé (S) , et M' la matrice obtenue en ajoutant à M un $(p + 1)^{\text{ième}}$ vecteur colonne égal au second membre \mathbf{b} de (S') .

Si M est non nulle, il est équivalent de dire :

1. Le système linéaire (S') a au moins une solution.
5. Le rang de la matrice M' est égal au rang de la matrice M .

6. Il existe une matrice principale P extraite de M telle que tous les déterminants caractéristiques associés à P soient nuls.

7. Pour toute matrice principale P extraite de M , tous les déterminants caractéristiques associés à P sont nuls.

Montrons d'abord que $1 \Leftrightarrow 5$. La condition 5 signifie que le vecteur b est une combinaison linéaire des vecteurs colonnes de la matrice M , c'est-à-dire des vecteurs a_1, a_2, \dots, a_p . Ainsi, $5 \Leftrightarrow 2'$, donc $5 \Leftrightarrow 1$.

Nous allons maintenant prouver que $5 \Rightarrow 7 \Rightarrow 6 \Rightarrow 5$.

$5 \Rightarrow 7$: soit P une matrice principale extraite de M . Comme le rang de M' est égal à celui de M , P est aussi une matrice principale extraite de M' . Il résulte alors de la proposition 4.4 que toute matrice bordante de P dans M' est non inversible, ce qui s'applique en particulier à toute matrice caractéristique associée à P .

$7 \Rightarrow 6$ est évident, puisque la matrice M est non nulle.

$6 \Rightarrow 5$: soit P une matrice principale extraite de M telle que tous les déterminants caractéristiques associés à P soient nuls. Ses matrices bordantes dans M' sont de deux sortes :

a) La colonne additionnelle est extraite de b . La matrice bordante est une matrice caractéristique, non inversible par hypothèse.

b) La colonne additionnelle est extraite d'un des vecteurs colonnes de M . La matrice bordante est donc extraite de M , et non inversible, puisque P est une matrice principale extraite de M .

Toutes les matrices bordantes de P dans M' étant non inversibles, la matrice P est une matrice principale extraite de M' (cf. prop. 4.4). La matrice M' a donc le même rang que M .

COROLLAIRE. — **Systèmes linéaires de $n + 1$ équations à n inconnues, de rang n .** — Soient n un entier strictement positif, et (S') le système linéaire de $n + 1$ équations à n inconnues suivant :

$$\alpha_{i1}\xi_1 + \dots + \alpha_{ij}\xi_j + \dots + \alpha_{in}\xi_n = \beta_i, \quad i \in [1, n + 1].$$

On suppose que le rang du système (S') est égal à n , c'est-à-dire que le rang de la matrice (α_{ij}) est égal à n . Alors, pour que le système (S') admette au moins une solution, il faut et il suffit que

$$\begin{vmatrix} \alpha_{11} & \dots & \alpha_{1j} & \dots & \alpha_{1n} & \beta_1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{i1} & \dots & \alpha_{ij} & \dots & \alpha_{in} & \beta_i \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{n1} & \dots & \alpha_{nj} & \dots & \alpha_{nn} & \beta_n \\ \alpha_{n+1,1} & \dots & \alpha_{n+1,j} & \dots & \alpha_{n+1,n} & \beta_{n+1} \end{vmatrix} = 0.$$

En effet, le rang de M' est supérieur ou égal à celui de M , donc est égal soit à n , soit à $n + 1$. Pour que (S') admette au moins une solution, il faut et il suffit donc que la matrice carrée M' ne soit pas de rang $n + 1$, c'est-à-dire que $\text{Det } M' = 0$.

On peut déduire du théorème 4.11 un procédé pratique de résolution d'un système linéaire (S') de n équations à p inconnues, de rang $r > 0$:

— On choisit une matrice principale P extraite de la matrice M du système homogène associé à (S') .

— On calcule les $n - r$ déterminants caractéristiques associés à P :

a) ou bien l'un de ces déterminants est non nul; alors le système linéaire (S') n'admet pas de solution;

b) ou bien tous ces déterminants sont nuls; alors le système linéaire (S') admet au moins une solution.

— Dans ce dernier cas, on sait (cf. prop. 4.13) que le système (S') est équivalent au système (S'_1) constitué des équations principales. Deux éventualités se présentent :

1. Le rang r est égal au nombre p d'inconnues; le système linéaire (S'_1) est alors un système de Cramer, qu'on peut résoudre à l'aide des formules de Cramer.

2. Le rang r est strictement inférieur au nombre d'inconnues p . On peut alors faire passer les $p - r$ inconnues non principales dans le second membre, et leur donner des valeurs arbitraires λ_j . On calcule enfin les r inconnues principales à l'aide des formules de Cramer.

Voici un exemple illustrant ces méthodes :

PROPOSITION 4.14. — **Systèmes homogènes de $n + 1$ équations à $n + 1$ inconnues, de rang n .** — Soient n un entier strictement positif, et (S) le système linéaire homogène de $n + 1$ équations à $n + 1$ inconnues suivant :

$$\alpha_{i1}\xi_1 + \dots + \alpha_{ij}\xi_j + \dots + \alpha_{i,n+1}\xi_{n+1} = 0, \quad i \in [1, n + 1].$$

On suppose que le rang du système (S) est égal à n , et que, par exemple, les n premières équations sont principales. Soient alors $\Delta_1, \dots, \Delta_j, \dots, \Delta_{n+1}$ les cofacteurs des éléments $\alpha_{n+1,1}, \dots, \alpha_{n+1,j}, \dots, \alpha_{n+1,n+1}$. L'un au moins de ces cofacteurs est non nul, et l'espace vectoriel des solutions du système linéaire homogène (S) n'est autre que la droite engendrée par le vecteur de composantes $\Delta_1, \dots, \Delta_j, \dots, \Delta_{n+1}$.

Considérons la matrice M_1 du système (S_1) constitué des n premières équations. Cette matrice M_1 étant de rang n , l'un au moins des cofacteurs Δ_j est non nul. Il résulte alors du corollaire 1 du théorème 3.7 que le vecteur $(\Delta_1, \dots, \Delta_j, \dots, \Delta_{n+1})$ est une solution non nulle du système (S_1) . D'après la proposition 4.13, ce vecteur est aussi une solution de (S) ; la proposition en découle, puisque l'espace vectoriel des solutions de (S) est de dimension 1 (cf. prop. 4.9).

REMARQUE 1. — On pourra s'exercer à retrouver ce résultat en cherchant les solutions du système (S_1) à l'aide du procédé pratique exposé ci-dessus.

2. Si les n vecteurs lignes de M sont linéairement indépendants (ce qui impose $n \leq p$), le système (S') a au moins une solution quel que soit le second membre. Les solutions du système linéaire homogène (S) associé à (S') constituent alors un sous-espace vectoriel de E^p isomorphe à E^{p-n} .

3. Si les p vecteurs colonnes de M sont linéairement indépendants, le système (S') a au plus une solution quel que soit le second membre.

Assertion 1. — Supposons d'abord qu'il existe une solution $(x_1, \dots, x_j, \dots, x_n)$; nous voyons aussitôt que, pour tout $j \in [1, n]$, x_j est nécessairement donné par la formule (1) : il suffit pour cela de multiplier pour tout $i \in [1, n]$ les deux membres de la $i^{\text{ème}}$ équation par le scalaire α'_{ij} et d'ajouter toutes les relations ainsi obtenues, en tenant compte de la relation

$$\sum_{i=1}^n \alpha_{ik} \alpha'_{ij} = \delta_{jk} \text{Det}(M).$$

Pour montrer l'existence d'une solution, on définit pour tout $j \in [1, n]$ le vecteur x_j par la relation (1), et on vérifie que, pour tout $i \in [1, n]$, $\sum_{k=1}^n \alpha_{ik} x_k = b_i$. Le reste de l'assertion est alors immédiat.

L'assertion 2 se ramène aussitôt à la précédente, en considérant une matrice principale P extraite de M , et en faisant passer les $p-n$ inconnues non principales au second membre. Supposons par exemple que x_1, \dots, x_n sont les inconnues principales; l'application qui à tout élément (y_{n+1}, \dots, y_p) de E^{p-n} associe l'unique élément $(x_1, \dots, x_n, y_{n+1}, \dots, y_p)$ de E^p tel que, pour tout $i \in [1, n]$,

$$\sum_{j=1}^n \alpha_{ij} x_j = - \sum_{j=n+1}^p \alpha_{ij} y_j,$$

est un isomorphisme de l'espace vectoriel E^{p-n} sur le sous-espace vectoriel de E^p constitué des solutions du système homogène (S) associé à (S') .

Assertion 3. — Il suffit de prouver que le système homogène associé à (S') admet pour seule solution la solution triviale. Pour cela, on se ramène à l'assertion 1 en considérant une matrice principale P extraite de M .

EXEMPLE. — Il existe un triplet (x, y, z) et un seul de vecteurs d'un espace vectoriel E sur C tel que

$$\begin{cases} x + y + z = 0 \\ x + jy + j^2z = 0 \\ x + j^2y + jz = 0 \end{cases}$$

à savoir le triplet $(0, 0, 0)$.

En effet, la matrice

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & j & j^2 \\ 1 & j^2 & j \end{pmatrix}$$

est inversible.

— Ou bien le système (S') comporte au moins deux équations, et (S') est alors équivalent à la réunion de (S'_1) et du système (S'_1) constitué des $n - 1$ dernières équations de (T'_0) .

b) Quels que soient i et j , $\alpha_{ij} = 0$.

— S'il existe un élément i de $[1, n]$ tel que $\beta_i \neq 0$, le système (S') n'admet aucune solution.

— Si, pour tout $i \in [1, n]$, $\beta_i = 0$, alors tout élément $(\xi_1, \dots, \xi_j, \dots, \xi_p)$ de K^p est solution de (S') .

2) Lorsque (S') est équivalent à (S_1'') et (S_1') , on applique à (S_1') les raisonnements précédents. En itérant ce procédé, au bout d'un nombre fini r de pas, on arrive à l'un des deux cas suivants, pour le système linéaire (S_r') :

a) Le système (S'_r) ne comporte qu'une seule équation, la matrice M_r du système homogène associé au système (S'_r) n'étant pas nulle. Le système linéaire (S') est alors équivalent au système (S'') constitué des équations

$$\begin{array}{ll} (S_1'') & \xi_1 = \alpha'_{12}\xi_2 + \alpha'_{13}\xi_3 + \dots + \alpha'_{1p}\xi_p + \beta'_1 \\ (S_2'') & \xi_2 = \alpha'_{23}\xi_3 + \dots + \alpha'_{2p}\xi_p + \beta'_2 \\ \dots & \dots \\ (S_r'') & \xi_r = \alpha'_{r,r+1}\xi_{r+1} + \dots + \alpha'_{rp}\xi_p + \beta'_r \end{array}$$

On peut donc donner aux $p-r$ inconnues ξ_{r+1}, \dots, ξ_p des valeurs arbitraires $\lambda_{r+1}, \dots, \lambda_p$, et les équations $(S_1''), (S_2''), \dots, (S_r'')$ déterminent de manière unique les inconnues $\xi_1, \xi_2, \dots, \xi_r$.

b) La matrice M_r du système homogène associé au système (S'_r) est nulle.

— Si le second membre du système linéaire (S'_r) n'est pas nul, le système (S') n'admet aucune solution.

— Si le second membre du système linéaire (S'_r) est nul, les équations $(S''_1), \dots, (S''_{r-1})$ déterminent de manière unique les inconnues $\xi_1, \xi_2, \dots, \xi_{r-1}$ quand on a donné aux inconnues ξ_r, \dots, ξ_n des valeurs arbitraires.

REMARQUE. — Cette méthode est assez éloignée de la théorie exposée plus haut; elle s'apparente à la méthode de Gauss d'inversion des matrices (cf. *infra*). On notera qu'elle s'étend sans aucun changement au cas des corps non commutatifs.

5. MÉTHODE D'ADDITION

On simplifie le système linéaire (S') par des combinaisons linéaires convenables d'équations. Deux cas se présentent :

— Ou bien l'on a déjà prouvé l'existence et l'unicité de la solution par une autre méthode; il suffit alors d'aboutir par conditions nécessaires successives à des formules donnant les valeurs des inconnues ξ_j .

REMARQUE 1. — Une variante de la méthode d'addition consiste à introduire des équations et des inconnues auxiliaires; cf. exercice 24.

REMARQUE 2. — **Comparaison des différentes méthodes de résolution.** — La méthode des déterminants est commode pour les systèmes d'ordre faible, surtout quand les coefficients dépendent de paramètres.

La méthode d'addition, très élégante, sera employée chaque fois qu'on le pourra.

Enfin, la méthode de substitution est employée dans les exemples numériques, surtout quand le nombre des équations et des inconnues est élevé.

Lorsqu'on a à résoudre un système de Cramer dont le premier membre est fixe pour diverses valeurs du second membre, il pourra être commode d'inverser la matrice M du système homogène associé (cf. *infra*).

Le nombre d'opérations nécessitées par ces diverses méthodes est fort différent; cf. exercice 48.

Exercices conseillés : 22 à 30.

6. RECHERCHE DE L'INVERSE D'UNE MATRICE CARRÉE

1. **Méthode de Cramer.** — Soit \tilde{M} la matrice complémentaire de la matrice M . Nous savons (cf. cor. 2 du th. 3.7) que

$$M^{-1} = (\text{Det } M)^{-1} \cdot \tilde{M}.$$

Sauf exception, cette méthode n'est praticable que pour les matrices d'ordre 2 et 3.

2. **Interprétation géométrique.** — Soient U l'endomorphisme de K^n canoniquement associé à M , et (e_1, e_2, \dots, e_n) la base canonique de K^n .

Il est facile d'inverser l'endomorphisme U lorsque U est un endomorphisme de permutation, ou un endomorphisme orthogonal, ou encore un endomorphisme unitaire (cf. chap. III.1).

On peut aussi calculer, pour tout $i \in [1, n]$, l'unique vecteur x_i de K^n tel que $U(x_i) = e_i$. La matrice M^{-1} admet alors pour vecteurs colonnes les vecteurs x_i .

Cette méthode est favorable lorsqu'on peut résoudre le système linéaire $U(x) = y$ par addition.

3. **Méthode des polynômes.** — Soit $P = \alpha_p X^p + \dots + \alpha_0$ un élément de $K[X]$ tel que $\alpha_0 \neq 0$. Si $P(M) = 0$, M est inversible, et

$$M^{-1} = -\alpha_0^{-1}(\alpha_p M^{p-1} + \dots + \alpha_1 I_n).$$

La recherche de tels polynômes P sera abordée au chapitre 5.

4. Méthode de réduction. — Elle consiste à se ramener à l'inversion des matrices remarquables.

a) Lorsqu'on peut diagonaliser M , c'est-à-dire l'écrire sous la forme $M = PDP^{-1}$, où D est une matrice diagonale, l'inversion de M se ramène à celle de D , qui est immédiate. (Il peut arriver que le calcul de P et de P^{-1} soit nettement plus facile que le calcul direct de M^{-1} .)

b) Lorsque M est trigonale unipotente, l'inversion de M a déjà été traitée (cf. prop. I.3.63).

c) Lorsqu'on peut trigonaliser M , c'est-à-dire l'écrire sous la forme $M = PTP^{-1}$, où T est une matrice trigonale, l'inversion de M se ramène à celle de T . Or, l'inversion d'une telle matrice T est facile : il suffit de résoudre les systèmes linéaires $U(x) = e_i$ par la méthode de substitution.

5. Méthode de Gauss (dite parfois méthode du pivot). — Elle s'appuie sur le résultat fondamental suivant :

Pour qu'un élément M de $GL_n(K)$ puisse s'écrire sous la forme $M = VT$, où V est trigonale unipotente inférieure, et T trigonale supérieure, il faut et il suffit que tous les mineurs principaux de M soient non nuls.

La démonstration de ce théorème est esquissée dans l'exercice 48, où l'on trouvera un algorithme permettant de déterminer V et T . Lorsque M est mise sous la forme $M = VT$, l'inversion de M se ramène à celles de V et de T , lesquelles sont faciles ; c'est pourquoi cette méthode est une des plus employées en calcul numérique.

Enfin, on verra dans les exercices 49 et 50 comment le problème de l'inversion des éléments quelconques de $GL_n(K)$ se ramène au cas précédent.

***6. Méthode de Schmidt.** — Elle consiste à orthonormaliser la famille des vecteurs colonnes de M (cf. chap. III.1). On obtient ainsi un algorithme permettant d'écrire M sous la forme $M = TU$, où T est trigonale, et U orthogonale. L'inversion de M s'en déduit aussitôt.

7. Méthode de Gauss dans le cas des matrices hermitiennes. — Elle s'appuie sur le résultat suivant : toute matrice carrée hermitienne M d'ordre n dont les mineurs principaux sont non nuls peut s'écrire sous la forme $M = VDV^*$, où V est trigonale supérieure et D diagonale à éléments réels. La démonstration de ce théorème figure au chapitre III.1, où l'on trouvera un algorithme permettant de déterminer V et D .

8. Méthode de Cholesky, pour les matrices hermitiennes strictement positives. — Elle s'appuie sur le résultat suivant (cf. chap. III.1) : toute matrice carrée hermitienne strictement positive M d'ordre n peut s'écrire sous la forme $M = T^*T$, où T est une matrice trigonale supérieure dont les éléments diagonaux sont réels strictement positifs.*

EXERCICES

MATRICES INVERSIBLES

1. Soient α, β, γ trois nombres réels. Calculer le déterminant de la matrice

$$M = \begin{pmatrix} 1 & \cos^2 \alpha & \cot \alpha \\ 1 & \cos^2 \beta & \cot \beta \\ 1 & \cos^2 \gamma & \cot \gamma \end{pmatrix}.$$

Calculer l'inverse de la matrice M , lorsqu'il existe.

2. Soient α, β, γ trois nombres complexes. Calculer le déterminant de la matrice

$$M = \begin{pmatrix} \alpha - \beta - \gamma & 2\alpha & 2\alpha \\ 2\beta & \beta - \gamma - \alpha & 2\beta \\ 2\gamma & 2\gamma & \gamma - \alpha - \beta \end{pmatrix}.$$

Calculer l'inverse de la matrice M , lorsqu'il existe.

3. Soient n un entier strictement supérieur à 1, et $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite de n éléments de K distincts deux à deux. Calculer l'inverse de l'élément suivant de $M_n(K)$:

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^j & \dots & \alpha_1^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_i & \dots & \alpha_i^j & \dots & \alpha_i^{n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^j & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

4. Soient n un entier strictement positif, $(\alpha_i)_{1 \leq i \leq n}$ et $(\beta_j)_{1 \leq j \leq n}$ deux suites de n éléments de K telles que, pour tout couple (i, j) d'indices, $\alpha_i + \beta_j \neq 0$.

Montrer que le déterminant de la matrice $M = (\gamma_{ij})$, où

$$\gamma_{ij} = \frac{1}{\alpha_i + \beta_j},$$

est égal à

$$\frac{\prod_{i < j} (\alpha_j - \alpha_i)(\beta_j - \beta_i)}{\prod_{i,j} (\alpha_i + \beta_j)}.$$

Calculer l'inverse de M , lorsqu'il existe.

5. Soient n un entier strictement positif, $\alpha_1, \alpha_2, \dots, \alpha_n$ et β des scalaires. Calculer le déterminant de la matrice

$$M = \begin{pmatrix} \beta + \alpha_1 & \beta & \dots & \beta \\ \beta & \beta + \alpha_2 & \dots & \beta \\ \dots & \dots & \dots & \dots \\ \beta & \beta & \dots & \beta + \alpha_n \end{pmatrix}.$$

Calculer l'inverse de M , lorsqu'il existe.

6. Soient $\alpha_1, \alpha_2, \dots, \alpha_n$ des scalaires. Calculer le déterminant de la matrice

$$M = \begin{pmatrix} \alpha_1 + \alpha_2 & -\alpha_2 & 0 & 0 & \dots & 0 & 0 & 0 \\ -\alpha_2 & \alpha_2 + \alpha_3 & -\alpha_3 & 0 & \dots & 0 & 0 & 0 \\ 0 & -\alpha_3 & \alpha_3 + \alpha_4 & -\alpha_4 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & -\alpha_{n-1} & \alpha_{n-1} + \alpha_n & -\alpha_n \\ 0 & 0 & 0 & 0 & \dots & 0 & -\alpha_n & \alpha_n \end{pmatrix}.$$

Calculer l'inverse de M , lorsqu'il existe.

7. Soit β un scalaire. Calculer l'inverse de l'élément (α_{ij}) de $M_n(K)$, où

$$\begin{aligned} \alpha_{ij} &= 1 & \text{si} & \quad i = j \\ \alpha_{ij} &= \beta & \text{si} & \quad i = j - 1 \\ \alpha_{ij} &= 0 & \text{si} & \quad i \neq j \quad \text{et} \quad i \neq j - 1. \end{aligned}$$

8. Soient n un entier naturel non nul, $\alpha_1, \alpha_2, \dots, \alpha_n$ et ξ des scalaires, et U l'endomorphisme de K^{n+1} canoniquement associé à la matrice

$$M = \begin{pmatrix} \xi & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \alpha_n \\ \alpha_1 & \xi & \alpha_2 & \dots & \alpha_{n-1} & \alpha_n \\ \alpha_1 & \alpha_2 & \xi & \dots & \alpha_{n-1} & \alpha_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n & \xi \end{pmatrix}.$$

Lorsque U est inversible, résoudre les équations $U(\mathbf{x}) = \mathbf{e}_j$, où $(\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{n+1})$ désigne la base canonique de K^{n+1} .

En déduire la matrice inverse de M , lorsqu'elle existe.

ÉQUATIONS LINÉAIRES

9. On considère les systèmes linéaires suivants, sur le corps des nombres complexes :

$$(S) \quad \begin{cases} x - y + z = 1 \\ x + y + z = 0 \\ x + y - z = -1 \end{cases}$$

$$(S') \quad \begin{cases} x - y + z - 1 + j(x + y + z) + j^2(x + y - z + 1) = 0 \\ j(x - y + z - 1) + j^2(x + y + z) + x + y - z + 1 = 0 \\ x - y + z - 1 - 2(x + y + z) + x + y - z + 1 = 0. \end{cases}$$

Les systèmes linéaires (S) et (S') sont-ils équivalents ?

Résoudre le système (S') .

10. Résoudre et discuter les systèmes linéaires suivants, les coefficients étant des nombres complexes :

$$\begin{cases} x + y + z = a + b + c \\ bx + cy + az = a^2 + b^2 + c^2 \\ cx + ay + bz = a^2 + b^2 + c^2 \end{cases}$$

$$\begin{cases} ax + by + z = 1 \\ x + aby + z = b \\ x + by + az = 1 \end{cases}$$

$$\begin{cases} x + ay + a^2z = 0 \\ \bar{a}x + y + az = 0 \\ \bar{a}^2x + \bar{a}y + z = 0 \end{cases}$$

$$\begin{cases} x + ay + a^2z = a^4 \\ x + by + b^2z = b^4 \\ x + cy + c^2z = c^4 \end{cases}$$

$$\begin{cases} (b + c)x + (bc - 1)y + (1 + b^2)(1 + c^2)z = a \\ (c + a)x + (ca - 1)y + (1 + c^2)(1 + a^2)z = b \\ (a + b)x + (ab - 1)y + (1 + a^2)(1 + b^2)z = c. \end{cases}$$

11. Soit α un nombre complexe. Résoudre et discuter le système linéaire

$$\begin{cases} \xi_1 + \alpha \xi_2 + \alpha^2 \xi_3 + \alpha^3 \xi_4 = \alpha \\ \alpha \xi_1 + \alpha^2 \xi_2 + \alpha^3 \xi_3 + \xi_4 = \alpha^2 \\ \alpha^2 \xi_1 + \alpha^3 \xi_2 + \xi_3 + \alpha \xi_4 = \alpha^3 \\ \alpha^3 \xi_1 + \xi_2 + \alpha \xi_3 + \alpha^2 \xi_4 = \alpha^4 \\ \xi_1 - \xi_2 + \xi_3 - \xi_4 = 2. \end{cases}$$

12. Soient $\alpha_1, \alpha_2, \alpha_3$ et α_4 des nombres complexes. Résoudre et discuter les systèmes linéaires suivants :

$$\left\{ \begin{array}{l} \xi_1 + \alpha_1 \xi_2 + \alpha_1^3 \xi_3 + \alpha_1^4 \xi_4 = \alpha_1^2 \\ \xi_1 + \alpha_2 \xi_2 + \alpha_2^3 \xi_3 + \alpha_2^4 \xi_4 = \alpha_2^2 \\ \xi_1 + \alpha_3 \xi_2 + \alpha_3^3 \xi_3 + \alpha_3^4 \xi_4 = \alpha_3^2 \\ \xi_1 + \alpha_4 \xi_2 + \alpha_4^3 \xi_3 + \alpha_4^4 \xi_4 = \alpha_4^2 \end{array} \right.$$

$$\left\{ \begin{array}{l} \xi_1 + \alpha_1 \xi_2 + \alpha_1^2 \xi_3 + \alpha_1^4 \xi_4 = \alpha_1^3 \\ \xi_1 + \alpha_2 \xi_2 + \alpha_2^2 \xi_3 + \alpha_2^4 \xi_4 = \alpha_2^3 \\ \xi_1 + \alpha_3 \xi_2 + \alpha_3^2 \xi_3 + \alpha_3^4 \xi_4 = \alpha_3^3 \\ \xi_1 + \alpha_4 \xi_2 + \alpha_4^2 \xi_3 + \alpha_4^4 \xi_4 = \alpha_4^3 \end{array} \right.$$

13. Résoudre et discuter les systèmes suivants :

$$\left\{ \begin{array}{l} x^2 - yz = a \\ y^2 - zx = b \\ z^2 - xy = c \end{array} \right. \quad a, b, c, x, y, z \in \mathbf{R};$$

$$\left\{ \begin{array}{l} x^2 + y^2 + z^2 = \alpha \\ ax + by + cz = \beta \\ dx + ey + fz = \gamma \end{array} \right. \quad a, b, c, d, e, f, \alpha, \beta, \gamma, x, y, z \in \mathbf{R};$$

$$\left\{ \begin{array}{l} \operatorname{tg} x \cdot \operatorname{tg} (y - z) = a \\ \operatorname{tg} y \cdot \operatorname{tg} (z - x) = b \\ \operatorname{tg} z \cdot \operatorname{tg} (x - y) = c \end{array} \right. \quad a, b, c, x, y, z \in \mathbf{R}.$$

14 A. *Polynômes de Hilbert-Samuel.*

1. Soit P un élément de $\mathbf{Q}[X]$ satisfaisant à la condition suivante : il existe un entier rationnel p_0 tel que, pour tout entier rationnel $p \geq p_0$, $P(p)$ appartienne à \mathbf{Z} . Montrer que toutes les composantes de P dans la base de $\mathbf{Q}[X]$ constituée des polynômes de Hilbert H_r sont des entiers rationnels.

2. Prouver que les polynômes $H_s = H_{s(1)}(X_1)H_{s(2)}(X_2) \dots H_{s(n)}(X_n)$, où s parcourt l'ensemble des applications de $[1, n]$ dans \mathbf{N} , constituent une base de l'espace vectoriel $\mathbf{Q}[X_1, X_2, \dots, X_n]$. Montrer que ces polynômes constituent une base du sous-module du \mathbf{Z} -module $\mathbf{Q}[X_1, X_2, \dots, X_n]$ constitué des polynômes P tels que, pour tout élément a de \mathbf{Z}^n , $P(a)$ appartienne à \mathbf{Z} . Généraliser à ce cas le résultat de la question 1.

15. *Calculs de sommes à l'aide des polynômes de Hilbert.*

Soient p un entier naturel et n un entier naturel non nul.

1. A l'aide de la formule donnant $D^p(X^m)$, calculer le polynôme

$$H_{p,n} = \sum_{m=0}^n m(m-1) \dots (m-p+1) X^m.$$

2. Soit P un polynôme à coefficients complexes. En utilisant la théorie des polynômes de Hilbert, donner une méthode de calcul du polynôme

$$Q = P(0) + P(1)X + P(2)X^2 + \dots + P(n)X^n.$$

Appliquer cette méthode au cas où $P = Y^p$. Expliciter les calculs pour $p = 0, 1, 2$ et 3 .

3. En utilisant des méthodes analogues, calculer les polynômes suivants :

$$\begin{aligned} 1 + 2X^2 + 4X^4 + \dots + 3nX^{2n} \\ 1 + 3X^3 + 6X^6 + \dots + 3nX^{3n} \\ 1 + 3X^3 + 12X^6 + \dots + 3n^2X^{3n}. \end{aligned}$$

4. Soit α un nombre réel. Calculer

$$e^{i\alpha} + 2^p e^{2i\alpha} + \dots + n^p e^{ni\alpha}.$$

16 A. Inégalités de Cauchy pour une fonction polynomiale.

On désigne par z_0, z_1, \dots, z_{n-1} les racines $n^{\text{ièmes}}$ de l'unité dans le corps des nombres complexes.

1. Soit

$$P = \alpha_0 + \alpha_1 X + \dots + \alpha_{n-1} X^{n-1}$$

un élément de $C[X]$ de degré inférieur ou égal à $n - 1$. Pour tout $r \in [1, n]$, on pose

$$\beta_r = z_0^{n-r} P(z_0) + z_1^{n-r} P(z_1) + \dots + z_{n-1}^{n-r} P(z_{n-1}).$$

Calculer β_r en fonction des scalaires $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$. Calculer $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ en fonction des scalaires $P(z_0), P(z_1), \dots, P(z_{n-1})$.

2. En déduire que, pour tout entier $p \in [0, n - 1]$,

$$|\alpha_p| \leq \sup_{j \in [0, n-1]} |P(z_j)|.$$

Soit p_0 un élément de $[0, n - 1]$. Déterminer un polynôme P tel que

$$|\alpha_{p_0}| = \sup_{j \in [0, n-1]} |P(z_j)|.$$

3. Pour tout nombre réel $\rho \geq 0$, et pour tout élément P de $C[X]$, on pose

$$M_P(\rho) = \sup_{|z|=\rho} |P(z)|.$$

Prouver que, pour tout $\rho > 0$, et pour tout entier naturel p , le coefficient α_p de X^p dans P satisfait à la relation

$$|\alpha_p| \leq \frac{M_P(\rho)}{\rho^p}.$$

17. Soient n un entier supérieur ou égal à 3, α, β et γ trois nombres complexes.

1. On considère l'élément suivant de $M_n(C)$:

$$M_{\alpha, \beta, \gamma} = \begin{pmatrix} \alpha & \beta & 0 & \dots & 0 & 0 \\ \gamma & \alpha & \beta & \dots & 0 & 0 \\ 0 & \gamma & \alpha & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \gamma & \alpha \end{pmatrix}.$$

Calculer le déterminant de $M_{\alpha, \beta, \gamma}$.

- $$\left\{ \begin{array}{l} \xi_i + \alpha_i \xi_{n+1} = \beta_i \quad i \in [1, n], \\ \sum_{i=1}^n \alpha_i \xi_i + \xi_{n+1} = \beta_{n+1}. \end{array} \right.$$

$$\begin{cases} \xi_i + \alpha_i \xi_{n+1} = \beta_i & i \in [1, n], \\ \sum_{i=1}^n \alpha_i \xi_i + \xi_{n+1} = \beta_{n+1}. \end{cases}$$

- $$\left\{ \begin{array}{l} \alpha\xi_1 + \xi_2 + \dots + \xi_n = 1 \\ \xi_1 + \alpha\xi_2 + \dots + \xi_n = \beta \\ \dots\dots\dots \\ \xi_1 + \xi_2 + \dots + \alpha\xi_n = \beta^{n-1}. \end{array} \right.$$

- $$(\beta_i - \alpha)\xi_1 + (\beta_i^2 - \alpha^2)\xi_2 + \dots + (\beta_i^n - \alpha^n)\xi_n = 1, \quad i \in [1, n].$$

$$\left(\text{On pourra introduire l'inconnue auxiliaire } \eta = \sum_{i=1}^n \alpha^i \xi_i. \right)$$

- $$(1) \quad \forall i \in [2, n-1], \quad \forall j \in [2, n-1], \quad \alpha_{ij} = \frac{1}{4} (\alpha_{i-1,j} + \alpha_{i+1,j} + \alpha_{i,j-1} + \alpha_{i,j+1}).$$

1. Établir la relation

$$\forall (i, j) \in J, \quad \alpha_{ij} \leq \sup (\alpha_{i-1,j}, \alpha_{i+1,j}, \alpha_{i,j-1}, \alpha_{i,j+1}).$$

2. Soit $\beta = \sup_{(i,j) \in I} \alpha_{ij}$. Montrer que s'il existe un élément (i, j) de J tel que $\alpha_{ij} = \beta$, alors, pour tout élément (i', j') de I , $\alpha_{i'j'} = \beta$.

3. Montrer qu'étant donnés les scalaires α_{ij} pour tout élément (i, j) de $I - J$, il existe une famille $(\alpha_{ij})_{(i, j) \in J}$ et une seule de scalaires satisfaisant à la relation (1).

$$D_X^{2m}(P) + D_Y^{2m}(P) = 0.$$

Montrer que les scalaires α_{ij} définis par la relation $\alpha_{ij} = P(i, j)$ satisfont à la relation (1).

26. *Algèbre des matrices circulantes.*

On considère l'espace vectoriel K^n muni de sa base canonique (e_1, e_2, \dots, e_n) , et l'application φ de K^n dans $M_n(K)$ qui à tout vecteur $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ associe la matrice

$$M_a = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_n & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_n & \alpha_1 & \dots & \alpha_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_2 & \alpha_3 & \alpha_4 & \dots & \alpha_1 \end{pmatrix}.$$

Soit enfin F l'image de K^n par φ .

1. Montrer que F est un espace vectoriel sur K . Trouver une base de F . Montrer que φ définit un isomorphisme de K^n sur F .

2. Soit $J = M_{e_n}$; montrer que F n'est autre que la sous-algèbre unitaire de $M_n(K)$ engendrée par J .

Lorsque $K = \mathbb{C}$, calculer $\text{Det } M_a$.

Lorsque $K = \mathbb{R}$, et lorsque $K = \mathbb{C}$, déterminer les éléments inversibles et les diviseurs de zéro de F .

3. Pour tout couple (x, y) d'éléments de K^n , on considère l'unique élément z de K^n tel que $M_z = M_x M_y$. Montrer que, muni de la loi de composition interne $(x, y) \mapsto z$, K^n est une algèbre commutative unitaire.

4. Résoudre et discuter le système linéaire

$$M_a(x) = b,$$

où b est un élément donné de K^n .

Expliciter les résultats précédents lorsque, pour tout $p \in [1, n]$, $\alpha_p = \alpha + (p-1)\beta$, où $\alpha, \beta \in \mathbb{C}$. Étudier de même le cas où $\alpha_p = \alpha\beta^{p-1}$.

27. *Matrices circulantes.*

Soit n un entier naturel non nul. On désigne par z_1 le nombre complexe $e^{\frac{2i\pi}{n}}$.

I. 1. Soit $A = (\alpha_{pq})$ l'élément de $M_n(\mathbb{C})$ défini par la formule

$$\alpha_{pq} = z_1^{(p-1)(q-1)}.$$

Expliciter les matrices $A^2, \overline{A}^2, A\overline{A}$ et $\overline{A}A$. Montrer que A est inversible, et calculer A^r , où $r \in \mathbb{Z}$.

Calculer le produit des déterminants de A et \overline{A} , ainsi que les carrés des déterminants de A et de \overline{A} .

2. Calculer le produit des carrés des différences deux à deux des racines de l'équation

$$(1) \quad z^n - 1 = 0.$$

On précisera le signe de ce produit suivant les valeurs de n .

3. Soit M l'élément suivant de $M_n(\mathbb{C})$:

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_0 \\ \dots & \dots & \dots & \dots \\ a_{n-1} & a_0 & \dots & a_{n-2} \end{pmatrix},$$

où a_0, a_1, \dots, a_{n-1} sont n nombres complexes, et où chaque ligne se déduit de la précédente par la permutation circulaire $\tau = [a_0, a_1, \dots, a_{n-1}]$.

Expliciter les matrices $AM, MA, \overline{AM}, \overline{MA}, AMA, \overline{AMA}$ et $AM\overline{A}$. On introduira, pour tout $p \in [0, n-1]$, les nombres complexes

$$\begin{aligned} \sigma_p &= a_0 + a_1 z_1^p + \dots + a_{n-1} z_1^{(n-1)p}, \\ \sigma'_p &= a_0 + a_1 \overline{z_1}^p + \dots + a_{n-1} \overline{z_1}^{(n-1)p}. \end{aligned}$$

4. Prouver que $AM\overline{A}$ est de la forme DM_σ , où D est une matrice diagonale et M_σ une matrice de permutation, que l'on explicitera. Calculer le déterminant de M , et l'inverse de M , lorsqu'il existe.

II. Soit m un entier appartenant à $[1, n-1]$. On note A_m l'élément (α_{pq}) de $M_n(\mathbb{C})$ défini par la formule

$$\alpha_{pq} = z_1^{m(p-1)(q-1)}.$$

1. Calculer $A_m \overline{A_m}$, et en déduire que A_m est inversible si et seulement si m est premier avec n . Calculer alors l'inverse de A_m .

2. Soit M_m l'élément de $M_n(\mathbb{C})$ dont la première ligne est

$$\alpha_0 \quad \alpha_1 \quad \dots \quad \alpha_{n-1},$$

et dont chaque ligne se déduit de la précédente par la permutation circulaire τ^m . Prouver que si m n'est pas premier avec n , M_m n'est pas inversible.

On suppose désormais que m est premier avec n . Prouver alors que $A_m M_m \overline{A_m}$ est de la forme DM_σ , où D est une matrice diagonale et M_σ une matrice de permutation, que l'on explicitera. Calculer le déterminant de M_m , et l'inverse de M_m , lorsqu'il existe.

(Le cas où $m = n-1$ a déjà fait l'objet de l'exercice 26.)

28. Matrices circulantes de matrices.

Soient r et n deux entiers naturels non nuls, et z_1 le nombre complexe $e^{\frac{2i\pi}{n}}$.

1. Soit $A = (A_{pq})$ l'élément de $M_{rn}(\mathbb{C})$ décomposé en les blocs

$$A_{pq} = z_1^{(p-1)(q-1)} I_r.$$

Calculer $A\overline{A}$. En déduire que A est inversible, et calculer A^{-1} .

2. Soit M l'élément suivant de $M_{rn}(\mathbb{C})$:

$$\begin{pmatrix} M_0 & M_1 & \dots & M_{n-1} \\ M_1 & M_2 & \dots & M_0 \\ \dots & \dots & \dots & \dots \\ M_{n-1} & M_0 & \dots & M_{n-2} \end{pmatrix},$$

où M_0, M_1, \dots, M_{n-1} sont des éléments de $M_r(\mathbb{C})$. Calculer $AM\overline{A}$, et évaluer $\text{Det } M$ en fonction des déterminants des matrices

$$S_p = M_0 + z_1^p M_1 + \dots + z_1^{(n-1)p} M_{n-1}.$$

3. Généraliser les résultats de la deuxième partie de l'exercice 27.

29. Soient r un entier naturel non nul, et (A, B) un couple d'éléments de $M_r(\mathbb{C})$. On pose

$$M = \begin{pmatrix} A & B \\ -B & A \end{pmatrix}.$$

Prouver que

$$\text{Det } M = \text{Det } (A + iB) \cdot \text{Det } (A - iB).$$

En déduire que si A et B appartiennent à $M_r(\mathbb{R})$, $\text{Det } M$ est positif, et que M est inversible si et seulement si

$$\text{Ker } (A) \cap \text{Ker } (B) = \{ \mathbf{0} \}.$$

30. Soient n un entier naturel, et E l'ensemble des éléments de $M_{n+1}(\mathbb{C})$ de la forme

$$M_{\alpha, \beta} = \begin{pmatrix} \alpha & \beta & \beta & \dots & \beta \\ \beta & \alpha & \beta & \dots & \beta \\ \beta & \beta & \alpha & \dots & \beta \\ \dots & \dots & \dots & \dots & \dots \\ \beta & \beta & \beta & \dots & \alpha \end{pmatrix},$$

où α et β parcourent \mathbb{C} .

1. Calculer le déterminant de $M_{\alpha, \beta}$.

2. Montrer que E est une sous-algèbre commutative unitaire de $M_{n+1}(\mathbb{C})$. Trouver sa dimension; déterminer les éléments inversibles et les diviseurs de zéro.

Calculer l'inverse de $M_{\alpha, \beta}$, lorsqu'il existe.

31 A. *Interpolation de Lagrange pour les polynômes à coefficients vectoriels.*

On utilise les notations et les résultats de l'exercice 2.27.

1. Soient E un espace vectoriel sur K , n un entier naturel non nul, et $(\alpha_1, \alpha_2, \dots, \alpha_n)$ une suite de scalaires distincts deux à deux. Montrer que, pour tout élément $\mathbf{b} = (b_1, b_2, \dots, b_n)$ de E^n , il existe un élément $P_{\mathbf{b}}$ et un seul de $E[X]$ de degré strictement inférieur à n tel que, pour tout élément i de $[1, n]$, $P_{\mathbf{b}}(\alpha_i) = b_i$, et que l'application $\mathbf{b} \rightarrow P_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel E^n sur l'espace vectoriel des polynômes à coefficients dans E de degré strictement inférieur à n (interpolation de Lagrange).

2. Étendre de même le théorème d'interpolation de Lagrange-Sylvester au cas des polynômes à coefficients vectoriels.

32. *Systèmes linéaires vectoriels.*

Soient E un espace vectoriel sur K , n et p deux entiers naturels non nuls, et (S') un système linéaire de n équations à p inconnues dans E , ayant pour matrice $M = (\alpha_{ij})$.

1. Prouver que (S') admet une solution si et seulement si toute relation linéaire vérifiée par les vecteurs lignes de M l'est aussi par les vecteurs $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ constituant le second membre de (S') .

2. Soient r le rang de M et $P = (\alpha_{ij})_{i \in I, j \in J}$ une matrice principale extraite de M . On suppose que $I = J = [1, r]$. Montrer que (S') admet une solution si et seulement si, pour tout élément h de $[r + 1, n]$,

$$\sum_{i=0}^n (-1)^{i-1} (\text{Det } M_{ih}) b_i + (-1)^r (\text{Det } P) b_h = 0,$$

où M_{ih} désigne la matrice (α_{kj}) , où k parcourt $(I \cup \{h\}) - \{i\}$ et j parcourt J .

33. Différences successives d'un polynôme.

Soit Δ l'endomorphisme de $K[X]$ défini par la relation

$$\Delta(P) = P(X + 1) - P(X).$$

Pour tout entier naturel non nul p , déterminer le noyau et l'image de Δ^p .

Montrer que, pour tout élément Q de $K[X]$, il existe un polynôme P et un seul tel que $\Delta^p(P) = Q$, $P(0) = P(1) = \dots = P(p-1) = 0$; expliciter P en développant Q dans la base des polynômes de Hilbert. Plus généralement, montrer que, pour toute suite $(\alpha_0, \alpha_1, \dots, \alpha_{p-1})$ d'éléments de K , il existe un polynôme P et un seul tel que $\Delta^p(P) = Q$ et que, pour tout élément j de $[0, p-1]$, $P(j) = \alpha_j$; expliciter P .

APPLICATIONS DE LA THÉORIE DES GRAPHS

34 A. Graphes.

On appelle *graphe* attaché à un ensemble non vide X tout couple constitué de X et d'une partie G de $X \times X$. Dans la suite, on identifiera le graphe (X, G) à G .

On dit qu'un graphe est fini si l'ensemble X est fini.

On dit qu'un graphe G est réflexif, symétrique, antisymétrique, transitif, si la relation binaire définie par G est réflexive, symétrique, antisymétrique, transitive. On définit de même les graphes d'ordre et d'équivalence.

1. L'intersection des graphes symétriques et réflexifs contenant G est le plus petit graphe symétrique et réflexif contenant G ; on l'appelle graphe symétrique et réflexif engendré par G , et on le note \bar{G} . Montrer que \bar{G} est constitué des couples (x, x) , où $x \in X$, et des couples (x, y) tels que (x, y) ou (y, x) appartienne à G .

2. On appelle *chaîne* d'un graphe G joignant deux éléments x et y de X une suite (z_0, z_1, \dots, z_p) d'éléments de X telle que $z_0 = x$, $z_p = y$ et que, pour tout $j \in [0, p-1]$, $(z_j, z_{j+1}) \in G$. L'entier p s'appelle longueur de cette chaîne.

L'intersection de tous les graphes d'équivalence contenant G est le plus petit graphe d'équivalence contenant G ; on l'appelle graphe d'équivalence engendré par G , et on le note \tilde{G} . Montrer que \tilde{G} est constitué des couples (x, y) d'éléments de X qui peuvent être joints par une chaîne de G . Les classes d'équivalence associées à la relation d'équivalence définie par \tilde{G} s'appellent composantes connexes du graphe G ; elles constituent une partition de X . Ainsi, la composante connexe d'un point x de X est l'ensemble des points y de X qui peuvent être joints à x par une chaîne de G .

On dit que G est connexe si G n'admet qu'une seule composante connexe.

On appelle alors écart de deux éléments x et y de X la plus petite des longueurs des chaînes de G joignant x et y , notée $d_G(x, y)$. Montrer que l'application $(x, y) \mapsto d_G(x, y)$ est une distance sur X .

Enfin, on appelle chaîne orientée d'un graphe G joignant un élément x à un élément y une suite (z_0, z_1, \dots, z_p) d'éléments de X telle que $z_0 = x$, $z_p = y$ et que, pour tout $j \in [0, p-1]$, $(z_j, z_{j+1}) \in G$. On dit que G est fortement connexe si, pour tout couple (x, y) de points de X , il existe une chaîne orientée de G joignant x à y . Un graphe fortement connexe est connexe, la réciproque pouvant tomber en défaut.

35 A. Matrice associée à un graphe.

Soit G un graphe attaché à un ensemble fini X ayant n éléments. On appelle matrice associée à G l'élément $M = (n_{xy})$ de $M_X(Q)$ défini par les relations

$$\begin{aligned} n_{xy} &= 1 && \text{si } (x, y) \in G \\ n_{xy} &= 0 && \text{si } (x, y) \notin G. \end{aligned}$$

Réciproquement, tout élément M de $M_X(Q)$ dont les éléments sont égaux à 0 ou à 1 définit un graphe attaché à X . On note alors U l'endomorphisme de Q^X canoniquement associé à M .

1. Caractériser les graphes réflexifs, symétriques et antisymétriques à l'aide des matrices associées.

2. Prouver que G est connexe si et seulement si M est indécomposable (c'est-à-dire qu'il n'existe pas de partition de X en deux parties Y et Z telles que les sous-espaces vectoriels engendrés par $(e_i)_{i \in Y}$ et $(e_j)_{j \in Z}$ soient stables par U).

Plus généralement, soient X_1, X_2, \dots, X_r les composantes connexes de G . Montrer que M peut s'écrire sous la forme $M = M_\sigma^{-1} M' M_\sigma$, où σ est une permutation de X , et

$$M' = \begin{pmatrix} M_1 & & 0 \\ & M_2 & \\ & & \ddots \\ 0 & & & M_r \end{pmatrix}.$$

où, pour tout $j \in [1, r]$, $M_j \in M_{X_j}(Q)$, et où M_j est indécomposable.

3. Prouver que G est fortement connexe si et seulement si M est irréductible (c'est-à-dire qu'il n'existe pas de partie Y de X non vide et distincte de X telle que le sous-espace vectoriel engendré par $(e_i)_{i \in Y}$ soit stable par U). Plus précisément, montrer que s'il existe un élément x de X tel que la partie Y de X constituée des éléments y pouvant être joints à x par une chaîne orientée de G soit non vide et distincte de X , alors M peut s'écrire sous la forme $M = M_\sigma^{-1} M' M_\sigma$, où σ est une permutation de X , et

$$M' = \begin{pmatrix} M_1 & * \\ 0 & M_2 \end{pmatrix},$$

où $M_2 \in M_Y(Q)$ et $M_1 \in M_{X-Y}(Q)$.

36 A. Graphe attaché à une matrice.

Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$. On appelle graphe attaché à M l'ensemble des couples (i, j) de $[1, n]$ tels que $\alpha_{ij} \neq 0$. A l'aide de l'exercice précédent, démontrer les résultats suivants :

1. Pour que le graphe attaché à M ne soit pas connexe, il faut et il suffit qu'il existe une permutation σ de $[1, n]$ telle que $M' = M_\sigma M M_\sigma^{-1}$ s'écrive sous la forme

$$M' = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix},$$

où $M_1 \in M_p(K)$, $M_2 \in M_{n-p}(K)$.

2. Pour que le graphe attaché à M ne soit pas fortement connexe, il faut et il suffit qu'il existe une permutation σ de $[1, n]$ telle que $M' = M_\sigma M M_\sigma^{-1}$ s'écrive sous la forme

$$M' = \begin{pmatrix} M_1 & * \\ 0 & M_2 \end{pmatrix},$$

où $M_1 \in \mathbf{M}_p(K)$, $M_2 \in \mathbf{M}_{n-p}(K)$.

37 A. Théorème d'Hadamard-Frobenius.

Soient $M = (\alpha_{ij})$ un élément de $\mathbf{M}_n(\mathbb{C})$, et U l'endomorphisme de \mathbb{C}^n canoniquement associé à M .

1. Montrer que si, pour tout élément i de $[1, n]$,

$$|\alpha_{ii}| > \sum_{j \neq i} |\alpha_{ij}|,$$

la matrice M est inversible (théorème d'Hadamard).

(On supposera par l'absurde qu'il existe un vecteur non nul $x = (\xi_1, \xi_2, \dots, \xi_n)$ de \mathbb{C}^n appartenant au noyau de U . On considérera un élément i de $[1, n]$ tel que, pour tout élément k de $[1, n]$, $|\xi_k| \leq |\xi_i|$, et on arrivera à une contradiction en calculant la $i^{\text{ème}}$ composante du vecteur $U(x)$.)

2. On suppose que, pour tout élément i de $[1, n]$,

$$(1) \quad |\alpha_{ii}| \geq \sum_{j \neq i} |\alpha_{ij}|,$$

l'inégalité étant stricte pour au moins une valeur de i , et que, pour tout couple (i, h) d'éléments de $[1, n]$, il existe une suite finie (k_1, k_2, \dots, k_m) d'éléments de $[1, n]$ telle que les éléments $\alpha_{i,k_1}, \alpha_{k_1,k_2}, \dots, \alpha_{k_m,h}$ soient non nuls (c'est-à-dire que le graphe attaché à M est fortement connexe; cf. exercice 36). Montrer que la matrice M est inversible (théorème d'Hadamard-Frobenius).

(On montrera d'abord que, pour tout élément i de $[1, n]$, $\alpha_{ii} \neq 0$. On notera h un élément de $[1, n]$ tel que l'inégalité (1) soit stricte. On procédera comme dans la première question, et on montrera que $|\xi_{k_1}| = |\xi_i|$, et, de proche en proche, que $|\xi_h| = |\xi_i|$. On arrivera à une contradiction.)

38 B. Théorème de Thévenin.

On utilise la théorie des graphes (cf. exercices 3.34 à 3.36).

Soient n un entier naturel non nul $(\beta_1, \beta_2, \dots, \beta_{n+1})$ une suite de nombres réels et $M = (\alpha_{ij})$ un élément de $\mathbf{M}_{n+1}(\mathbb{R})$ satisfaisant aux conditions suivantes :

a) La matrice M est symétrique.

b) Les éléments de la diagonale principale de M sont nuls, les autres éléments positifs ou nuls, et chaque ligne contient au moins deux éléments non nuls.

c) Pour tout couple (i, j) d'éléments de $[1, n+1]$, il existe une suite (k_1, k_2, \dots, k_m) d'éléments de $[1, n+1]$ telle que les éléments $\alpha_{i,k_1}, \alpha_{k_1,k_2}, \dots, \alpha_{k_m,j}$ soient non nuls.

On considère le système (S) de $n+1$ équations linéaires à $n+1$ inconnues suivant :

$$\left(\sum_{j=1}^{n+1} \alpha_{ij} \right) \xi_i - \sum_{j=1}^{n+1} \alpha_{ij} \xi_j = \beta_i.$$

1. Prouver que le rang du système homogène (S) associé à (S') est inférieur ou égal à n .
2. Prouver que le graphe G associé à la matrice M du système (S) est connexe.
3. Soit (i, j) un couple d'éléments de $[1, n + 1]$ tel que

$$d_G(i, j) = \sup_{k, l} d_G(k, l).$$

Montrer que le graphe G_i obtenu en supprimant i est encore connexe. (On supposera par l'absurde qu'il ne l'est pas; on considérera un élément k d'une composante connexe de G_i ne contenant pas j . On prouvera que $d_G(j, k) > d_G(i, j)$.)

4. En déduire que la matrice M_i obtenue en supprimant la $i^{\text{ième}}$ ligne et la $i^{\text{ième}}$ colonne de M est inversible. (On pourra utiliser le théorème d'Hadamard-Frobenius; cf. exercice 37.)

5. Prouver que M est de rang n , et déterminer les solutions de (S) .

6. Montrer que (S') admet une solution si et seulement si $\sum_{i=1}^{n+1} \beta_i = 0$.

Appliquer les résultats précédents au cas où, pour tout élément i de $[1, n + 1]$, $\beta_i = \sum_{j=1}^{n+1} \gamma_{ij}$, la matrice carrée (γ_{ij}) étant antisymétrique.

(Ce cas particulier est connu en électricité sous le nom de théorème de Thévenin : dans un réseau électrique comportant des résistances, des f. é. m. et des f. c. é. m., les tensions existent et sont déterminées à une constante additive près.)

CALCUL DU RANG D'UNE MATRICE

39 A. Calcul du rang à l'aide des opérations élémentaires.

On désigne par (M_{ij}) la base canonique de l'espace vectoriel $M_n(K)$. Pour tout scalaire λ , et pour tout couple (i, j) d'éléments distincts de $[1, n]$, on pose $U_{ij}(\lambda) = I_n + \lambda M_{ij}$. On désigne enfin par G_n l'ensemble des éléments P de $M_n(K)$ qui peuvent s'écrire sous forme de produits de telles matrices.

1. On considère sur l'ensemble $M_{n,p}(K)$ la relation binaire \mathcal{R} définie par les couples (M, M') satisfaisant à la condition suivante : il existe un élément P de G_n et un élément Q de G_p tels que

$$M' = PMQ.$$

Prouver que \mathcal{R} est une relation d'équivalence.

2. Soit $M = (\alpha_{ij})$ un élément non nul de $M_{n,p}(K)$. Transformer M en un élément $M' = (\alpha'_{ij})$ tel que $M' \mathcal{R} M$ et que $\alpha'_{11} = 1$.

3. Soit $M' = (\alpha'_{ij})$ un élément de $M_{n,p}(K)$ tel que $\alpha'_{11} = 1$. Transformer M' en un élément $M'' = (\alpha''_{ij})$ tel que $M'' \mathcal{R} M'$, que $\alpha''_{11} = 1$, que, pour tout $i \in [2, n]$, $\alpha''_{i1} = 0$, et que, pour tout $j \in [2, p]$, $\alpha''_{1j} = 0$.

4. On suppose $n \neq p$. Soit M un élément de $M_{n,p}(K)$, de rang r . Montrer que $M \mathcal{R} J_r$, où

$$J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

En déduire que la relation $M\mathcal{R}M'$ a lieu si et seulement si les matrices M et M' sont équivalentes (au sens du § 4.1).

5. On suppose que $n = p$. Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$, de rang r . Montrer que, si $r \neq n$, la relation $M\mathcal{R}J_r$ est encore valable, et que, si $r = n$, c'est-à-dire si $M \in \text{GL}_n(K)$, il existe un scalaire α et un seul tel que $M\mathcal{R}D_\alpha$, où

$$D_\alpha = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \alpha \end{pmatrix},$$

à savoir $\alpha = \text{Det } M$.

En déduire une méthode pratique de calcul du déterminant d'une matrice carrée.

Applications.

a) Montrer que si M et M' sont deux éléments équivalents de $M_n(K)$ (au sens du § 4.1), on peut transformer M en M' par une suite finie d'opérations élémentaires.

b) Prouver que le groupe $\text{GL}_n(K)$ est engendré par les éléments $U_{ij}(\lambda)$, où $i \neq j$ et $\lambda \in K$, et par les éléments D_α , où $\alpha \in K^*$.

c) Prouver que le groupe $\text{SL}_n(K)$ est engendré par les éléments $U_{ij}(\lambda)$, où $i \neq j$ et $\lambda \in K$.

40 B. Sous-groupes des commutateurs de $\text{GL}(E)$ et $\text{SL}(E)$.

Soit E un espace vectoriel de dimension finie n sur K , $n \geq 2$.

1. Soit H un hyperplan de E et x et y deux vecteurs de E non colinéaires et n'appartenant pas à H . Montrer qu'il existe une transvection U de E relative à H telle que $U(x) = y$ si et seulement si $a = y - x$ appartient à H .

En déduire que, pour tout couple (x, y) de vecteurs non colinéaires de E , il existe une transvection U telle que $U(x) = y$.

Prouver que si x et y sont deux vecteurs de E , colinéaires, non nuls, et distincts, il n'existe pas de transvection U de E telle que $U(x) = y$, mais qu'il existe deux transvections U_1 et U_2 de E telles que $U_2[U_1(x)] = y$.

2. Soient H et H' deux hyperplans distincts de E , x un élément de H n'appartenant pas à H' , et x' un élément de H' n'appartenant pas à H . On pose $b = x' - x$. Prouver qu'il existe une transvection U de E telle que $U(H) = H'$, que $U(x) = x'$, et que $U(b) = b$.

3. Soient U et U' deux transvections de E distinctes de I_E , relatives à des hyperplans H et H' . Soient φ et φ' deux éléments de E^* , a et a' deux éléments de H et H' tels que pour tout vecteur x de E , $U(x) = x + \varphi(x)a$ et $U'(x) = x + \varphi'(x)a'$.

Prouver que s'il existe un élément V de $\text{GL}(E)$ tel que $U' = VUV^{-1}$, alors $V(H) = H'$ et il existe un scalaire λ non nul tel que $V(a) = \lambda a'$ et $\varphi' = \lambda \varphi \circ V^{-1}$. Réciproquement, prouver qu'il existe un automorphisme V de E tel que $V(H) = H'$, $V(a) = a'$ et $\varphi' = \varphi \circ V^{-1}$.

4. En déduire les résultats suivants :

Deux transvections de E distinctes de I_E sont conjuguées dans $\text{GL}(E)$. Le sous-groupe D des commutateurs de $\text{GL}(E)$ est égal à $\text{SL}(E)$, sauf si K est le corps à 2 éléments et si $n = 2$.

(Pour la seconde assertion on prouvera que deux éléments de $\text{SL}(E)$ conjugués dans $\text{GL}(E)$ ont même image dans $\text{GL}(E)/D$. On appliquera alors la première assertion, et le résultat de l'exercice 39.)

5. On suppose que $n \geq 3$. Prouver que deux transvections de E distinctes de I_E sont conjuguées dans $\text{SL}(E)$.

(On pourra se ramener au cas où ces transvections sont relatives à un même hyperplan H , en utilisant la question 2; on appliquera alors la question 1.)

Prouver enfin le résultat suivant :

Le groupe $SL(E)$ est égal à son groupe des commutateurs sauf si $\text{card } K = 2$ et $n = 2$, ou si $\text{card } K = 3$ et $n = 2$.

(Lorsque $\dim E = 2$, on procédera par un calcul direct.)

41. Calculer le rang de l'élément suivant de $M_{6,5}(\mathbb{R})$:

$$\begin{pmatrix} 2 & -1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 1 & -2 \\ 2 & -3 & 1 & 2 & -2 \\ 1 & 0 & 1 & -2 & -6 \\ 4 & -1 & 3 & -1 & -8 \\ 1 & 2 & 1 & -1 & 0 \end{pmatrix}.$$

42. Soit α un nombre réel. Déterminer le rang de la matrice

$$\begin{pmatrix} 1 & \cos \alpha & \cos 2\alpha & \cos 3\alpha \\ \cos \alpha & \cos 2\alpha & \cos 3\alpha & \cos 4\alpha \\ \cos 2\alpha & \cos 3\alpha & \cos 4\alpha & \cos 5\alpha \\ \cos 3\alpha & \cos 4\alpha & \cos 5\alpha & \cos 6\alpha \end{pmatrix}.$$

43. 1. Soit $M = (\alpha_{ij})$ un élément de $M_4(K)$ tel qu'aucun déterminant extrait d'ordre 2 ne soit nul.

Montrer que si les déterminants des matrices mineures A_{11} , A_{12} , A_{33} et A_{44} sont nuls, tous les déterminants mineurs de M sont nuls.

2. Soit plus généralement M un élément de $M_n(K)$ tel qu'aucun déterminant extrait d'ordre $n - 2$ ne soit nul. On suppose en outre

— qu'il existe un élément i_0 de $[1, n]$ et deux éléments distincts j_1 et j_2 de $[1, n]$ tels que

$$\text{Det } A_{i_0 j_1} = 0 \quad \text{et} \quad \text{Det } A_{i_0 j_2} = 0 ;$$

— que, pour tout élément j de $[1, n]$, il existe un élément i de $[1, n]$ différent de i_0 tel que $\text{Det } A_{ij} = 0$.

Montrer que tous les déterminants mineurs de M sont nuls.

44. *Matrice complémentaire.*

Soient $M = (\alpha_{ij})$ un élément de $M_n(K)$, et $\tilde{M} = (\beta_{ij})$ la matrice complémentaire de M .

1. Montrer que

— si M est de rang n , il en est de même de \tilde{M} ;

— si M est de rang $n - 1$, \tilde{M} est de rang 1;

— si M est de rang inférieur ou égal à $n - 2$, \tilde{M} est nulle.

2. Soient $\xi_1, \xi_2, \dots, \xi_n, \eta_1, \eta_2, \dots, \eta_n$ des scalaires, et

$$N = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} & \xi_1 \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} & \xi_2 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} & \xi_n \\ \eta_1 & \eta_2 & \dots & \eta_n & 0 \end{pmatrix}.$$

Montrer que

$$\text{Det } N = - \sum_{i,j} \beta_{ji} \xi_i \eta_j.$$

3. Si $\text{Det } M = 0$, montrer que l'application qui, au couple (x, y) de vecteurs de K^n , où $x = (\xi_1, \xi_2, \dots, \xi_n)$ et $y = (\eta_1, \eta_2, \dots, \eta_n)$ associe le scalaire $\text{Det } N$, est le produit de deux formes linéaires sur K^n (On pourra utiliser l'exercice I.3.61).

45 A. Centralisateurs, normalisateurs.

Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} une partie de $\text{GL}(E)$. On appelle centraliseur (resp. normalisateur) de \mathcal{A} , et on note $C(\mathcal{A})$ (resp. $N(\mathcal{A})$) l'ensemble des éléments P de $\text{GL}(E)$ tels que, pour tout élément A de \mathcal{A} , $PAP^{-1} = A$ (resp. tels que $P\mathcal{A}P^{-1} = \mathcal{A}$).

1. Déterminer les éléments de $\text{GL}(E)$ commutant à une transvection donnée.
2. Déterminer le centralisateur et le normalisateur du sous-groupe $\text{GL}_H(E)$ des transvections d'hyperplan H . En déduire le centre de $\text{GL}(E)$.
3. Déterminer le centralisateur et le normalisateur du sous-groupe de $\text{GL}_n(K)$ constitué des matrices diagonales inversibles.
4. Déterminer le centralisateur et le normalisateur du sous-groupe de $\text{GL}_n(K)$ constitué des matrices trigonales supérieures inversibles.
5. Déterminer le centralisateur et le normalisateur du sous-groupe de $\text{GL}_n(K)$ constitué des matrices trigonales supérieures unipotentes.

46 B. Caractérisation du déterminant.

On utilise les notations de l'exercice 39.

1. Prouver que, pour tout entier rationnel p , l'application $f_p : M \mapsto (\text{Det } M)^p$ est une application rationnelle de $\text{GL}_n(K)$ dans K^* , polynomiale si $p \geq 0$, et que f_p est un morphisme du groupe multiplicatif $\text{GL}_n(K)$ dans le groupe multiplicatif K^* .

2. Prouver que, pour tout couple (i, j) d'éléments distincts de $[1, n]$, l'application $\lambda \mapsto U_{ij}(\lambda) = I_n + \lambda M_{ij}$ est une application polynomiale de K dans $M_n(K)$, qui définit un morphisme du groupe additif K sur un sous-groupe, noté G_{ij} , du groupe multiplicatif $\text{GL}_n(K)$.

3. Prouver que l'application $\alpha \mapsto D_\alpha$, où

$$D_\alpha = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \alpha \end{pmatrix},$$

est une application polynomiale de K dans $M_n(K)$, qui définit un morphisme du groupe multiplicatif K^* sur un sous-groupe, noté G , du groupe multiplicatif $\text{GL}_n(K)$.

4. Soit f une application rationnelle de $\text{GL}_n(K)$ dans K . On suppose que f est un morphisme du groupe multiplicatif $\text{GL}_n(K)$ dans le groupe multiplicatif K^* . Prouver, à l'aide de l'exercice 2.13, que, pour tout élément M de G_{ij} , $f(M) = 1$. Prouver de même, à l'aide de l'exercice 2.16, qu'il existe un entier rationnel p tel que, pour tout élément D_α de G , $f(D_\alpha) = \alpha^p$. Montrer que si f est polynomiale, p est positif.

A l'aide de l'exercice 39, en déduire le résultat suivant :

Les applications $M \mapsto (\text{Det } M)^p$, où p appartient à \mathbb{Z} , sont les seuls morphismes rationnels du groupe multiplicatif $\text{GL}_n(K)$ dans le groupe multiplicatif K^ ; les applications*

$M \mapsto (\text{Det } M)^n$, où n appartient à \mathbb{N} , sont les seuls morphismes polynomiaux de $\text{GL}_n(K)$ dans K^* . En particulier, l'application $M \mapsto \text{Det } M$ est la seule application polynomiale f homogène de degré n de $\text{M}_n(K)$ dans K telle que, pour tout couple (M, N) d'éléments de $\text{GL}_n(K)$,

$$f(MN) = f(M)f(N).$$

Prouver de même que la fonction constante et égale à 1 est le seul morphisme rationnel du groupe multiplicatif $\text{SL}_n(K)$ dans le groupe multiplicatif K^* .

DÉCOMPOSITION D'UNE MATRICE CARRÉE

47 A. Structure du groupe des matrices trigonales supérieures unipotentes.

On désigne par (M_{ij}) la base canonique de l'espace vectoriel $\text{M}_n(K)$, et par $\text{U}_+(n, K)$ (resp. $\text{U}_-(n, K)$) le sous-groupe de $\text{GL}(n, K)$ constitué des matrices trigonales supérieures (resp. trigonales inférieures) unipotentes.

Pour tout scalaire λ et pour tout couple (i, j) d'éléments distincts de $[1, n]$, on pose

$$U_{ij}(\lambda) = I_n + \lambda M_{ij}.$$

Ainsi, lorsque $i < j$, $U_{ij}(\lambda)$ est un élément de $\text{U}_+(n, K)$, et lorsque $i > j$, $U_{ij}(\lambda)$ est un élément de $\text{U}_-(n, K)$.

1. Soit $M = (\alpha_{ij})$ un élément de $\text{U}_+(n, K)$. Calculer la matrice

$$M' = M \cdot U_{12}(-\alpha_{12}) \cdot U_{13}(-\alpha_{13}) \cdots U_{1n}(-\alpha_{1n}).$$

2. On désigne par I l'ensemble des couples (i, j) d'éléments de $[1, n]$ tels que $i < j$ et par φ l'application qui à tout élément (α_{ij}) de K^I associe la matrice

$$M = M_{n-1} M_{n-2} \cdots M_1,$$

où, pour tout $i \in [1, n-1]$,

$$M_i = U_{in}(\alpha_{in}) \cdot U_{i,n-1}(\alpha_{i,n-1}) \cdots U_{i,i+1}(\alpha_{i,i+1}).$$

Prouver que φ est une bijection de K^I sur $\text{U}_+(n, K)$, et que φ est une application polynomiale, ainsi que son application réciproque.

En particulier, le groupe multiplicatif $\text{U}_+(n, K)$ est engendré par les éléments $U_{ij}(\lambda)$, où (i, j) parcourt I , et λ parcourt K .

3. Pour tout entier naturel $m > 0$, on désigne par $\text{U}_m(n, K)$ l'ensemble des matrices trigonales supérieures unipotentes (α_{ij}) telles que $\alpha_{ij} = 0$ pour tout couple (i, j) tel que $0 < j - i < m$. On notera que si $m \geq n$, $\text{U}_m(n, K)$ est réduit à $\{I_n\}$.

Soient (i, j) et (i', j') deux éléments de I , et (λ, λ') un couple de scalaires. Calculer le commutateur

$$C = U_{ij}(\lambda) \cdot U_{i'j'}(\lambda') \cdot U_{ij}(-\lambda) \cdot U_{i'j'}(-\lambda').$$

Prouver que si $U_{ij}(\lambda)$ appartient à $\text{U}_m(n, K)$ et si $U_{i'j'}(\lambda')$ appartient à $\text{U}_m(n, K)$, alors C appartient à $\text{U}_{m+m}(n, K)$.

En déduire que, pour toute relation d'ordre total sur l'ensemble I , tout élément M de $U_+(n, K)$ peut s'écrire sous la forme

$$M = \prod_{(i,j) \in I} U_{ij}(\beta_{ij}).$$

(On partira du cas particulier de la question 1, et on montrera qu'en permutant un élément de la forme $U_{ij}(\lambda)$ avec d'autres, on introduit des commutateurs appartenant à $U_{j-i+1}(n, K)$).

4. Traiter de même le cas des matrices triangulaires inférieures unipotentes.

48 B. Décomposition de Gauss d'une matrice carrée.

On désigne par (M_{ij}) la base canonique de l'espace vectoriel $M_n(K)$, par $U_+(n, K)$ (resp. $U_-(n, K)$) le sous-groupe de $GL(n, K)$ constitué des matrices triangulaires supérieures (resp. triangulaires inférieures) unipotentes, par $T_+^*(n, K)$ le sous-groupe de $GL(n, K)$ constitué des matrices triangulaires supérieures inversibles, et par $D^*(n, K)$ le sous-groupe de $GL(n, K)$ constitué des matrices diagonales inversibles.

Soit M un élément de $M_n(K)$. Pour tout $i \in [1, n]$, on désigne par $\Delta_i(M)$ le $i^{\text{ème}}$ mineur principal de M , c'est-à-dire le mineur de M associé aux parties $[1, i]$ et $[1, i]$ de $[1, n]$. L'ensemble $C(n, K)$ des éléments M de $M_n(K)$ tels que, pour tout $i \in [1, n]$, $\Delta_i(M)$ soit non nul s'appelle *cellule* de $M_n(K)$. On notera que $C(n, K)$ contient $T_+^*(n, K)$.

1. En utilisant l'exercice 47, prouver que, pour tout élément M de $M_n(K)$, pour tout élément U de $U_-(n, K)$ et pour tout élément V de $U_+(n, K)$, les mineurs principaux de la matrice VMU sont égaux aux mineurs principaux de la matrice M . Autrement dit, pour tout $h \in [1, n]$,

$$\Delta_h(VMU) = \Delta_h(M).$$

En particulier, si M est un élément de $C(n, K)$, il en est de même de VMU .

2. Soit $M = (\alpha_{ij})$ un élément de $M_n(K)$ tel que $\Delta_1(M) = \alpha_{11}$ soit non nul. Déterminer un élément V de $U_-(n, K)$ tel que le premier vecteur colonne de VM ait pour composantes : $\alpha_{11}, 0, 0, \dots, 0$.

3. En déduire le résultat fondamental suivant :

L'application $(V, T) \mapsto VT$ est une bijection de $U_-(n, K) \times T_+^(n, K)$ sur la cellule $C(n, K)$; c'est une application polynomiale, dont l'application réciproque est rationnelle.*

On obtient en particulier l'énoncé suivant, dû à Gauss :

Pour tout élément M de la cellule $C(n, K)$ il existe un couple (V, T) et un seul, où $V \in U_-(n, K)$ et $T \in T_+^(n, K)$, tel que $M = VT$.*

Les éléments diagonaux $\lambda_1, \lambda_2, \dots, \lambda_n$ de T sont liés aux mineurs principaux de M par les relations

$$\lambda_1 = \Delta_1(M), \quad \text{et, pour tout } i \in [2, n], \quad \lambda_i = \frac{\Delta_i(M)}{\Delta_{i-1}(M)}.$$

4. Prouver que l'application $(V, D, U) \mapsto VDU$ est une bijection de l'ensemble $U_-(n, K) \times D^*(n, K) \times U_+(n, K)$ sur la cellule $C(n, K)$, qu'elle est polynomiale, et que son application réciproque est rationnelle.

En particulier, pour tout élément M de la cellule $C(n, K)$, il existe un triplet (V, D, U) et un seul, où $V \in U_-(n, K)$, $D \in D^*(n, K)$ et $U \in U_+(n, K)$, tel que $M = VDU$.

5. Soit $C_0(n, K)$ l'ensemble des éléments M de $M_n(K)$ dont tous les mineurs principaux sont égaux à 1. Prouver que l'application $(V, U) \mapsto VU$ est une bijection de $U_-(n, K) \times U_+(n, K)$ sur $C_0(n, K)$ polynomiale, ainsi que son application réciproque.

6. Dédurre de la question 2 le résultat suivant :

Soit M un élément de $M_n(K)$ de rang r , et tel que, pour tout $h \in [1, r]$, $\Delta_h(M) \neq 0$. Il existe un triplet (V, D, U) et un seul, où $V \in U_-(n, K)$, $D \in D(n, K)$ et $U \in U_+(n, K)$ tel que $M = VDU$. De plus, les éléments diagonaux $\lambda_1, \lambda_2, \dots, \lambda_n$ de D satisfont aux relations suivantes :

$$\lambda_1 = \Delta_1(M); \text{ pour tout } i \in [2, r], \lambda_i = \frac{\Delta_i M}{\Delta_{i-1}(M)}; \text{ pour tout } i \in [r+1, n], \lambda_i = 0.$$

7. Généraliser les résultats précédents au cas des matrices à éléments dans un anneau commutatif unitaire.

8. Dédurre de la question 3 une méthode pratique de résolution des systèmes de Cramer, et d'inversion des matrices carrées, en se ramenant au cas où la matrice considérée est trigonale supérieure. Évaluer les nombres d'opérations (additions, multiplications et divisions) nécessitées par cette méthode, et par celle de Cramer.

49 B. Drapeaux d'un espace vectoriel.

Soit E un espace vectoriel de dimension finie $n > 0$ sur K . On appelle *drapeau* de E une suite croissante $\mathcal{F} = (F_0, F_1, \dots, F_n)$ de sous-espaces vectoriels de E telle que, pour tout $i \in [0, n]$, $\dim F_i = i$. Dans toute la suite, on suppose que E est muni d'une base $B = (e_1, e_2, \dots, e_n)$; on désigne par \mathcal{F}_0 le drapeau de E associé à B , c'est-à-dire le drapeau défini par les relations $F_i = \bigoplus_{j \leq i} K e_j$. Soit enfin \mathcal{U} le sous-groupe de $\text{GL}(E)$ constitué des automorphismes U de E tels que la matrice $M_B(U)$ soit trigonale supérieure unipotente.

1. Déterminer les automorphismes de E laissant stable le drapeau \mathcal{F}_0 . Soient \mathcal{F} et \mathcal{F}' deux drapeaux de E . Prouver qu'il existe un automorphisme de E transformant \mathcal{F} en \mathcal{F}' .

2. Pour toute permutation σ de $[1, n]$, on désigne par U_σ l'automorphisme de E défini par les relations $U_\sigma(e_j) = e_{\sigma(j)}$.

Soient σ une permutation de $[1, n]$, (α_{ij}) une matrice trigonale supérieure unipotente, et U l'élément de \mathcal{U} tel que $M_B(U) = (\alpha_{ij})$. On désigne par $\mathcal{F} = (F_0, F_1, \dots, F_n)$ le drapeau transformé du drapeau \mathcal{F}_0 par l'automorphisme UU_σ . Prouver que, pour tout $i \in [1, n]$, $\sigma(i)$ n'est autre que le plus grand des entiers j tels que F_i contienne un vecteur dont les composantes dans la base B d'indices $\sigma(1), \sigma(2), \dots, \sigma(i-1)$ soient nulles et dont la $j^{\text{ième}}$ composante dans cette base soit non nulle. Prouver que, pour tout $k \in [1, n]$,

$$(UU_\sigma)(e_k) = e_{\sigma(k)} + \sum_{i < \sigma(k)} \alpha_{i, \sigma(k)} e_i.$$

3. Réciproquement, soit $\mathcal{F} = (F_0, F_1, \dots, F_n)$ un drapeau de E . On considère la permutation σ de $[0, n]$ définie par la condition suivante : pour tout $i \in [1, n]$, $\sigma(i)$ est le plus grand des entiers j tels que F_i contienne un vecteur dont les composantes dans la base B d'indices $\sigma(1), \sigma(2), \dots, \sigma(i-1)$ soient nulles et dont la $j^{\text{ième}}$ composante dans cette base soit non nulle. Prouver qu'il existe une base (f_1, f_2, \dots, f_n) de E telle que, pour tout $k \in [1, n]$, $F_k = \bigoplus_{j \leq k} K f_j$ et que f_k soit de la forme

$$f_k = e_{\sigma(k)} + \sum_{i < \sigma(k)} \beta_{i, \sigma(k)} e_i.$$

En déduire le résultat fondamental suivant :

Pour tout drapeau \mathcal{F} de E , il existe une permutation σ et une seule de $[1, n]$ et un élément U de \mathcal{U} tels que UU_σ transforme \mathcal{F}_0 en \mathcal{F} .

50 C. Décomposition de Bruhat de $\mathrm{GL}(n, K)$.

Soit n un entier strictement positif. On désigne par $U_+(n, K)$ (resp. $U_-(n, K)$) le sous-groupe de $\mathrm{GL}(n, K)$ constitué des matrices trigonales supérieures (resp. inférieures) unipotentes, par $T_+^*(n, K)$ le sous-groupe de $\mathrm{GL}(n, K)$ constitué des matrices trigonales supérieures inversibles, et par $D^*(n, K)$ le sous-groupe de $\mathrm{GL}(n, K)$ constitué des matrices diagonales inversibles. Enfin, pour toute permutation σ de $[1, n]$, on désigne par U_σ l'élément de $\mathrm{GL}(n, K)$ associé à σ , et on note G_σ l'ensemble des éléments de M de $\mathrm{GL}(n, K)$ de la forme $M = UU_\sigma T$, où $U \in U_+(n, K)$ et $T \in T_+^*(n, K)$.

1. On désigne par \mathcal{F}_0 le drapeau canonique de K^n , c'est-à-dire le drapeau de K^n associé à la base canonique de K^n . Soient M un élément de $\mathrm{GL}(n, K)$, et A l'automorphisme de K^n canoniquement associé à M . En appliquant les résultats de l'exercice précédent au drapeau \mathcal{F} de K^n transformé de \mathcal{F}_0 par A , démontrer que tout élément M de $\mathrm{GL}(n, K)$ appartient à un ensemble G_σ et un seul.

2. Pour toute permutation σ de $[1, n]$, on désigne par $U_\sigma(n, K)$ l'ensemble des éléments M de $\mathrm{GL}(n, K)$ de la forme $M = U_\sigma^{-1}UU_\sigma$, où $U \in U_+(n, K)$. Montrer que, pour tout couple (i, j) d'éléments distincts de $[1, n]$ et pour tout scalaire λ ,

$$U_\sigma^{-1}U_{ij}(\lambda)U_\sigma = U_{\sigma^{-1}(i), \sigma^{-1}(j)}(\lambda).$$

A l'aide de l'exercice 47, en déduire que tout élément M de $U_\sigma(n, K)$ peut s'écrire sous la forme

$$M = M_-M_+, \text{ où } M_- \in U_\sigma(n, K) \cap U_-(n, K) \text{ et où } M_+ \in U_\sigma(n, K) \cap U_+(n, K).$$

Prouver que cette décomposition est unique.

3. On note $U'_\sigma(n, K)$ l'ensemble des éléments U de $U_+(n, K)$ tels que $U_\sigma^{-1}UU_\sigma$ appartienne à $U_-(n, K)$. Soit M un élément de G_σ , de la forme

$$M = UU_\sigma T, \text{ où } U \in U_+(n, K) \text{ et } T \in T_+^*(n, K).$$

En introduisant l'élément $U_\sigma^{-1}UU_\sigma$, montrer que M peut s'écrire sous la forme $M = U'U_\sigma T'$, où $U' \in U'_\sigma(n, K)$ et où $T' \in T_+^*(n, K)$. Prouver que $U_\sigma^{-1}M$ appartient à la cellule $C(n, K)$ de $M_n(K)$ (cf. exercice 48). En déduire que la décomposition $M = U'U_\sigma T'$ est unique.

On obtient finalement le résultat suivant (décomposition de Bruhat) :

a) Les ensembles G_σ , où σ parcourt le groupe symétrique \mathfrak{S}_n , constituent une partition de $\mathrm{GL}(n, K)$.

b) Pour toute permutation σ de $[1, n]$, l'application $(U', D, U'') \mapsto U'U_\sigma D U''$ est une bijection de $U'_\sigma(n, K) \times D^*(n, K) \times U_+(n, K)$ sur G_σ ; c'est une application polynomiale dont l'application réciproque est rationnelle.

4. Soit σ_0 la permutation de $[1, n]$ définie par les relations $\sigma_0(i) = n + 1 - i$. Prouver que l'application $M \mapsto U_{\sigma_0}^{-1}M$ est une bijection de G_{σ_0} sur la cellule $C(n, K)$.

MATRICES À ÉLÉMENTS DANS UN ANNEAU PRINCIPAL

51 B. Facteurs invariants d'une matrice à éléments dans un anneau euclidien.

1. Soit A un anneau commutatif unitaire.

a) Soit n un entier naturel strictement supérieur à 1. Montrer que, pour tout élément α de A et pour tout couple (i, j) d'éléments distincts de $[1, n]$, la matrice

$$U_{ij}(\alpha) = I_n + \alpha M_{ij}$$

est inversible dans $M_n(A)$, et calculer son inverse.

Montrer que, pour tout élément inversible α de A et pour tout élément h de $[1, n]$ la matrice $A_h(\alpha) = I_n + (\alpha - 1)M_{hh}$ est inversible dans $M_n(A)$, et calculer son inverse.

On note G_n le sous-groupe de $GL_n(A)$ engendré par les matrices $U_{ij}(\alpha)$ et les matrices $A_h(\alpha)$. Prouver que toute matrice de permutation M_σ appartient à G_n . (On examinera d'abord le cas où σ est une transposition.) On convient que G_1 est réduit à l'élément neutre.

b) Soient n et p deux entiers naturels non nuls. Prouver que, dans l'ensemble $M_{n,p}(A)$, la relation binaire \mathcal{R} définie par les couples (M, M') tels qu'il existe un élément T de G_n et un élément S de G_p satisfaisant à la relation $M' = TMS$ est une relation d'équivalence. Prouver que si $M' \mathcal{R} M$, les matrices M et M' sont équivalentes.

2. Soit (A, d) un anneau euclidien (cf. exercice I.2.44). Pour tout élément M de $M_{n,p}(A)$, on désigne par r le rang de M considérée comme matrice à éléments dans le corps des fractions de A ; pour tout élément j de $[1, r]$, on note γ_j un générateur de l'idéal de A engendré par les mineurs de M d'ordre j . Les idéaux $A\gamma_j$ s'appellent *invariants fondamentaux* de M . Enfin, on dit qu'un élément D de $M_{n,p}(A)$ est *réduit* si $D = 0$ ou si

$$D = \begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix},$$

où D' est une matrice diagonale de la forme suivante :

$$D' = \begin{pmatrix} \delta_1 & & 0 \\ & \delta_2 & \\ & \cdot & \cdot \\ 0 & & \delta_r \end{pmatrix},$$

$\delta_1, \delta_2, \dots, \delta_r$ étant des éléments non nuls de A tels que, pour tout élément j de $[1, r-1]$, δ_j divise δ_{j+1} . Déterminer les invariants fondamentaux de D .

Prouver le résultat fondamental suivant :

Tout élément $M = (\alpha_{ij})$ de $M_{n,p}(A)$ peut s'écrire sous la forme $M = TDS$, où D est un élément réduit de $M_{n,p}(A)$, où $T \in G_n$ et $S \in G_p$. Montrer que le rang de D est égal à celui de M , et que, pour tout élément j de $[1, r]$,

$$A\gamma_j = A\delta_1\delta_2 \dots \delta_j.$$

Les idéaux $A\delta_j$ de la matrice réduite D sont donc définis de manière unique; on les appelle *facteurs invariants* de M .

(Pour démontrer l'existence du triplet (T, D, S) , on écartera le cas trivial où l'un des deux entiers n et p est égal à 1; on se ramènera au cas où $\alpha_{11} \neq 0$ et où $d(\alpha_{11}) \leq d(\alpha_{ij})$

pour tout élément (i, j) de $[1, n] \times [1, p]$, et on prouvera alors l'existence d'un élément M' de $\mathbf{M}_{n,p}(A)$ tel que $M'RM$ de la forme suivante :

$$M' = \begin{pmatrix} \alpha'_{11} & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & & & \\ \vdots & & & & \\ 0 & & & & \alpha'_{11}M'_1 \end{pmatrix},$$

où $\alpha'_{11} \in A$ et où $M'_1 \in \mathbf{M}_{n-1,p-1}(A)$.

Pour étudier l'unicité de D , on montrera que deux éléments M et M' de $\mathbf{M}_{n,p}(A)$ satisfaisant à la relation $M'RM$ ont les mêmes invariants fondamentaux.)

3. En déduire les résultats suivants :

Soit A un anneau euclidien. Pour qu'un élément M de $\mathbf{M}_n(A)$ appartienne à $\mathrm{GL}_n(A)$, il faut et il suffit que A appartienne à \mathbf{G}_n , ou encore que tous les facteurs invariants de M soient inversibles dans A . Pour que deux éléments M et M' de $\mathbf{M}_{n,p}(A)$ soient équivalents, il faut et il suffit que $M'RM$, ou encore que M et M' aient les mêmes facteurs invariants.

4. Appliquer les résultats précédents aux cas où $A = \mathbb{Z}$ et où $A = K[X]$.

Calculer les facteurs invariants de la matrice de l'exercice 41, des matrices

$$\begin{pmatrix} 2 & -3 & -4 \\ 3 & 1 & 5 \\ -1 & 0 & -1 \\ 0 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 7 & 5 & 3 & -2 \\ 0 & 4 & 2 & 2 & 0 \\ 2 & -2 & 4 & 0 & 2 \\ 3 & -1 & 7 & 1 & 3 \end{pmatrix}.$$

et des matrices à éléments dans $\mathbb{C}[X]$ suivantes :

$$\begin{pmatrix} X^3 + X^2 + X & 2X^3 + X^2 + X - 1 \\ 3X^3 + 2X^2 + 2X - 1 & 6X^3 + 2X^2 + 2X - 4 \\ X^3 - X^2 - X - 2 & 2X^3 - X^2 - X - 3 \end{pmatrix}$$

$$\begin{pmatrix} X & 1 & 1 & \dots & 1 \\ 0 & X & 1 & \dots & 1 \\ 0 & 0 & X & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & X \end{pmatrix}$$

$$\begin{pmatrix} 1 & X + \alpha_1 & (X + \alpha_1)^2 & \dots & (X + \alpha_1)^{n-1} \\ 1 & X + \alpha_2 & (X + \alpha_2)^2 & \dots & (X + \alpha_2)^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X + \alpha_n & (X + \alpha_n)^2 & \dots & (X + \alpha_n)^{n-1} \end{pmatrix},$$

où les scalaires α_i sont distincts deux à deux.

52 B. Systèmes linéaires à coefficients dans un anneau euclidien.

On utilise les résultats de l'exercice précédent.

Soit A un anneau euclidien.

1. Soient U une application linéaire de A^p dans A^n , et r son rang.

Montrer qu'il existe une base $B = (e_1, e_2, \dots, e_p)$ de A^p et une base $B' = (f_1, f_2, \dots, f_n)$ de A^n telles que, pour tout élément i de $[1, r]$, $U(e_i) = \alpha_i f_i$, et que, pour tout élément i de

$[r + 1, p]$, $U(e_i) = 0$, les scalaires α_i étant des éléments non nuls de A dont chacun divise le suivant.

2. Soit b un élément de A^n . Appliquer les résultats de la question 1 à la résolution de l'équation $U(x) = b$.

53 B. *Facteurs invariants d'une matrice à éléments dans un anneau principal.*

Soit A un anneau principal.

1. Montrer que le résultat de la question 1 de l'exercice précédent reste valable lorsque l'anneau A est principal.

(On démontrera grâce aux exercices I.3.100 et I.3.102 que le noyau de U admet un sous-module supplémentaire E dans A^p . On considérera les facteurs invariants $A\alpha_1, A\alpha_2, \dots, A\alpha_r$ du sous-module $\text{Im}(U)$ de A^n , et une base (f_1, f_2, \dots, f_n) de A^n telle que $(\alpha_1 f_1, \alpha_2 f_2, \dots, \alpha_r f_r)$ soit une base de $\text{Im}(U)$. On introduira une base (e_1, e_2, \dots, e_r) de E telle que, pour tout élément j de $[1, r]$, $U(e_j) = \alpha_j f_j$, et on complètera cette base de E en une base (e_1, e_2, \dots, e_p) de A^p à l'aide d'une base de $\text{Ker}(U)$.)

Les idéaux $A\alpha_1, A\alpha_2, \dots, A\alpha_r$ s'appellent *facteurs invariants* de U .

2. En déduire le résultat suivant :

Pour que deux éléments M et M' de $M_{n,p}(A)$ soient équivalents, il faut et il suffit qu'ils aient les mêmes facteurs invariants.

CHAPITRE 5

RÉDUCTION DES ENDOMORPHISMES

INTRODUCTION

Dans bien des questions, tant en algèbre qu'en analyse, on est amené à calculer des fonctions d'un endomorphisme U d'un espace vectoriel E de dimension finie n sur un corps K (puissances, exponentielle, etc.). A cet effet, il est utile de chercher les droites de E stables par U , et de déterminer si E est somme directe de telles droites. Ces considérations conduisent aux notions de valeur propre et de vecteur propre d'un endomorphisme. Malheureusement, il peut arriver qu'il n'existe aucune valeur propre, ce qui amène à supposer dans un premier temps que le corps K est algébriquement clos. Même dans ce cas, il peut arriver que E ne soit pas somme directe de droites stables par U , ce qui conduit à la définition des endomorphismes diagonalisables, c'est-à-dire tels qu'il existe une base de E constituée de vecteurs propres de U . On démontre alors que si U admet n valeurs propres distinctes, U est diagonalisable.

Néanmoins, il existe des endomorphismes diagonalisables n'ayant pas n valeurs propres distinctes; les homothéties, les projecteurs, les symétries, fournissent des exemples de tels endomorphismes. L'étude de ces cas fait apparaître que l'ensemble E_λ des vecteurs propres associés à une valeur propre λ de U est un sous-espace vectoriel de E , qui peut être de dimension strictement supérieure à 1. Les sous-espaces vectoriels E_λ jouent un rôle essentiel dans la théorie de la diagonalisation; on les appelle sous-espaces propres de U . On prouve alors que U est diagonalisable si et seulement si E est somme directe des sous-espaces propres de U . C'est pourquoi nous prenons cette caractérisation comme définition des endomorphismes diagonalisables.

Un autre phénomène important apparaît à travers l'étude des projecteurs et des symétries : ces endomorphismes satisfont à des équations simples, à savoir $U^2 = U$ et $U^2 = I_E$, et c'est précisément l'étude de ces équations qui permet de prouver que ces endomorphismes sont diagonalisables et de déterminer leurs valeurs propres. Ceci amène, plus généralement, à étudier les polynômes Q tels que $Q(U) = 0$, ce qui fait l'objet du § 1. On y introduit la notion fondamentale de polynôme minimal d'un endomorphisme.

On étudie ensuite au § 2 les relations qui lient les valeurs propres de U aux racines de Q ; en particulier, on montre que toute valeur propre de U est racine de Q (théorème de Hilbert-Dirac).

Si Q n'a pas de racine dans K , U n'a aucune valeur propre, ce qui conduit à introduire les endomorphismes U tels qu'il existe un polynôme Q scindé sur K satisfaisant à la relation $Q(U) = 0$; ces endomorphismes sont étudiés au § 3, sous le nom d'endomorphismes scindés.

Tout endomorphisme nilpotent non nul U est scindé sans être diagonalisable, car le sous-espace propre $E_0 = \text{Ker}(U)$ n'est pas égal à E . Il apparaît donc que pour étudier les endomorphismes scindés non diagonalisables, la notion de sous-espace propre est insuffisante; on introduit alors le sous-espace spectral F_λ associé à une valeur propre λ de U . On démontre que U est scindé si et seulement si E est somme directe des sous-espaces spectraux de U . C'est pourquoi nous prenons cette caractérisation comme définition des endomorphismes scindés.

Enfin, certains résultats obtenus restent valables sans hypothèse de finitude pour la dimension de E , ce qui permet de les appliquer à d'autres problèmes. C'est pourquoi, dans la première partie de ce chapitre (§§ 1 à 3), nous exposons la théorie générale de la réduction des endomorphismes, tandis qu'au § 4, nous appliquons cette théorie au cas de la dimension finie; dans ce cas particulier, nous montrons comment on peut tirer parti du polynôme caractéristique d'un endomorphisme.

Alors que les résultats des quatre premiers paragraphes concernent les endomorphismes scindés, nous abordons au § 5 la réduction des endomorphismes des espaces vectoriels sur \mathbf{R} , ce qui nécessite la complexification des espaces vectoriels réels. L'outil principal est ici la notion d'endomorphismes conjugués, qui, dans ce cas particulier, montre l'importance de la théorie de Galois dans ces questions. Le cas des espaces vectoriels sur un corps quelconque nécessite une technique plus approfondie des extensions algébriques (cf. chap. III.3).

Le § 6 est consacré aux méthodes pratiques de réduction des matrices.

A titre de complément, nous exposons au § 7 la réduction de Jordan sur un corps quelconque. A cet effet, nous utilisons la structure de $K[X]$ -module définie par U sur l'espace vectoriel E . La théorie des facteurs invariants et des invariants de similitude est rejetée en exercice. Le lecteur intéressé par le calcul explicite de ces invariants pourra se reporter à [2], [3] ou [5].

Enfin, dans le § 8, nous montrons comment les théories précédentes s'appliquent aux équations aux différences finies linéaires et aux équations différentielles linéaires.

A. CAS GÉNÉRAL

§ 1. ENDOMORPHISMES ANNULANT UN POLYNÔME

1. DÉCOMPOSITION DU NOYAU D'UN POLYNÔME D'UN ENDOMORPHISME

Nous allons étudier les noyaux des endomorphismes d'un espace vectoriel qui sont des polynômes d'un même endomorphisme. Nous aurons constamment besoin de la

PROPOSITION 5.1. — Stabilité de l'image et du noyau d'un endomorphisme. — Soient U et V deux endomorphismes d'un espace vectoriel E sur K . Si U et V commutent, le noyau et l'image de U sont stables par V .

Soit d'abord x un élément de $\text{Ker}(U)$. Alors

$$U[V(x)] = (UV)(x) = (VU)(x) = V[U(x)] = 0;$$

donc $V(x)$ est encore un élément de $\text{Ker}(U)$.

Soit maintenant x un élément de $\text{Im}(U)$. Il existe un élément y de E tel que $x = U(y)$, d'où

$$V(x) = V[U(y)] = (VU)(y) = (UV)(y) = U[V(y)];$$

donc $V(x)$ est encore un élément de $\text{Im}(U)$.

COROLLAIRE. — Soient U et V deux endomorphismes d'un espace vectoriel E sur K . Si U et V commutent, alors, pour tout élément P de $K[X]$, le noyau et l'image de $P(U)$ sont stables par V .

En effet, l'ensemble des endomorphismes de E commutant à V est une sous-algèbre unitaire de l'algèbre $\mathcal{L}(E)$.

THÉORÈME 5.1. — Théorème fondamental de l'algèbre linéaire. — Soient U un endomorphisme d'un espace vectoriel E sur K , Q_1 et Q_2 deux polynômes non nuls à coefficients dans K , et $Q = Q_1 Q_2$ leur produit.

1. L'intersection des noyaux des endomorphismes $Q_1(U)$ et $Q_2(U)$ n'est autre que le noyau de $D(U)$, où D désigne le P. G. C. D. de Q_1 et Q_2 :

$$\text{Ker}[Q_1(U)] \cap \text{Ker}[Q_2(U)] = \text{Ker}[D(U)].$$

2. Si les polynômes Q_1 et Q_2 sont premiers entre eux, le noyau de l'endomorphisme $Q(U)$ n'est autre que la somme directe des noyaux des endomorphismes $Q_1(U)$ et $Q_2(U)$:

$$\text{Ker } [Q(U)] = \text{Ker } [Q_1(U)] \oplus \text{Ker } [Q_2(U)].$$

3. Si les polynômes Q_1 et Q_2 sont premiers entre eux, et si $Q(U) = 0$, alors E est somme directe des noyaux de $Q_1(U)$ et de $Q_2(U)$:

$$E = \text{Ker } [Q_1(U)] \oplus \text{Ker } [Q_2(U)].$$

De plus, les projecteurs P_1 et P_2 associés à cette décomposition en somme directe sont des polynômes en U .

Enfin,

$$\text{Im } [Q_1(U)] = \text{Ker } [Q_2(U)] \quad \text{et} \quad \text{Im } [Q_2(U)] = \text{Ker } [Q_1(U)];$$

donc

$$E = \text{Im } [Q_1(U)] \oplus \text{Im } [Q_2(U)].$$

Assertion 1. — Du fait que D divise Q_1 et Q_2 , nous déduisons aussitôt que

$$\text{Ker } [Q_1(U)] \cap \text{Ker } [Q_2(U)] \supset \text{Ker } [D(U)].$$

D'autre part, il existe deux éléments A et B de $K[X]$ tels que

$$(1) \quad D = AQ_1 + BQ_2.$$

Soit x un vecteur de E appartenant à $\text{Ker } [Q_1(U)]$ et à $\text{Ker } [Q_2(U)]$; il découle de (1) que x appartient à $\text{Ker } D(U)$. Autrement dit,

$$\text{Ker } [Q_1(U)] \cap \text{Ker } [Q_2(U)] \subset \text{Ker } D(U).$$

Assertion 2. — Si les polynômes Q_1 et Q_2 sont premiers entre eux, $D = 1$, et l'assertion 1 montre que

$$(2) \quad \text{Ker } [Q_1(U)] \cap \text{Ker } [Q_2(U)] = \{ \mathbf{0} \}.$$

De plus, la relation (1) se réduit alors à l'identité de Bezout :

$$(1') \quad 1 = AQ_1 + BQ_2.$$

Considérons maintenant un vecteur x de E , et posons

$$x_1 = [(BQ_2)(U)](x), \quad x_2 = [(AQ_1)(U)](x)$$

La relation (1') s'écrit encore

$$x = x_1 + x_2.$$

Lorsque le vecteur x appartient au noyau de $Q(U)$,

$$[Q_1(U)](x_1) = [(Q_1BQ_2)(U)](x) = [(BQ)(U)](x) = \mathbf{0},$$

et

$$[Q_2(U)](\mathfrak{x}_2) = [(Q_2 A Q_1)(U)](\mathfrak{x}) = [(A Q)(U)](\mathfrak{x}) = \mathbf{0}.$$

Finalement,

$$(3) \quad \text{Ker } [Q(U)] = \text{Ker } [Q_1(U)] + \text{Ker } [Q_2(U)].$$

Les relations (2) et (3) entraînent l'assertion 2.

Assertion 3. — Si les polynômes Q_1 et Q_2 sont premiers entre eux, et si $Q(U) = 0$, l'assertion 2 montre que

$$(4) \quad E = \text{Ker } Q_1(U) \oplus \text{Ker } Q_2(U).$$

Nous savons d'autre part que les projecteurs P_1 et P_2 associés à cette décomposition en somme directe sont définis par les formules

$$P_1(\mathfrak{x}) = \mathfrak{x}_1 \quad \text{et} \quad P_2(\mathfrak{x}) = \mathfrak{x}_2;$$

donc

$$P_1 = (B Q_2)(U) \quad \text{et} \quad P_2 = (A Q_1)(U).$$

Prouvons enfin, par exemple, que $\text{Im } [Q_1(U)] = \text{Ker } [Q_2(U)]$. Considérons d'abord un vecteur \mathfrak{x} de E tel que $[Q_2(U)](\mathfrak{x}) = \mathbf{0}$; il résulte aussitôt de (1') que $\mathfrak{x} = Q_1(U)[A(U)(\mathfrak{x})]$. Donc $\mathfrak{x} \in \text{Im } [Q_1(U)]$.

Réciproquement, considérons un vecteur \mathfrak{x} de E s'écrivant sous la forme $\mathfrak{x} = Q_1(U)(\mathfrak{y})$, où $\mathfrak{y} \in E$; il est évident que

$$[Q_2(U)](\mathfrak{x}) = [Q(U)](\mathfrak{y}) = \mathbf{0}.$$

Donc $\mathfrak{x} \in \text{Ker } [Q_2(U)]$.

On trouvera dans l'exercice 12 des compléments à ce théorème.

Voici deux corollaires, fort utiles en pratique, du théorème fondamental de l'algèbre linéaire :

COROLLAIRE 1. — Théorème de décomposition des noyaux. — Soient U un endomorphisme d'un espace vectoriel E sur K , p un entier strictement positif, $Q_1, \dots, Q_i, \dots, Q_p$ des polynômes à coefficients dans K premiers entre eux deux à deux, et

$$Q = Q_1 \dots Q_i \dots Q_p$$

leur produit. On désigne par N le noyau de $Q(U)$, et, pour tout $i \in [1, p]$, par N_i le noyau de $Q_i(U)$.

Alors le sous-espace vectoriel N est somme directe des sous-espaces vectoriels N_i :

$$N = \bigoplus_{i=1}^p N_i.$$

La démonstration s'effectue par récurrence sur l'entier p . Lorsque $p = 1$, le corollaire est évident. Supposons-le prouvé à l'ordre $p - 1$, où $p \geq 2$, et considérons une suite $(Q_1, \dots, Q_i, \dots, Q_p)$ de p polynômes premiers entre eux deux à deux. Les polynômes $R_1 = Q_1$ et $R_2 = Q_2 \dots Q_i \dots Q_p$ sont donc premiers entre eux. En appliquant l'assertion 2 du théorème 5.1 aux polynômes R_1 et R_2 , nous voyons que

$$N = \text{Ker} [R_1(U)] \oplus \text{Ker} [R_2(U)].$$

Or, $\text{Ker} [R_1(U)] = N_1$, et $\text{Ker} [R_2(U)]$ est somme directe des sous-espaces vectoriels N_i , $i \geq 2$, d'après l'hypothèse de récurrence. Donc

$$N = \bigoplus_{i=1}^p N_i.$$

COROLLAIRE 2. — Théorème de décomposition d'un endomorphisme. — Soient U un endomorphisme d'un espace vectoriel E sur K , et Q un polynôme à coefficients dans K tel que $Q(U) = 0$. On suppose que Q est décomposé en un produit $Q_1 \dots Q_i \dots Q_p$ de polynômes premiers entre eux deux à deux. Pour tout $i \in [1, p]$, on désigne par N_i le noyau de l'endomorphisme $Q_i(U)$.

1. Les sous-espaces vectoriels $N_1, \dots, N_i, \dots, N_p$ sont stables par U , et l'espace vectoriel E est somme directe de ces sous-espaces vectoriels :

$$E = \bigoplus_{i=1}^p N_i.$$

2. Soit $(P_i)_{1 \leq i \leq p}$ le système de projecteurs associé à la décomposition en somme directe précédente. Alors, pour tout $i \in [1, p]$, P_i est un polynôme en U .

L'assertion 1 est une conséquence immédiate de la proposition 5.1 et du corollaire 1.

Assertion 2. — Considérons un élément i de $[1, p]$, et désignons par N'_i la somme directe des sous-espaces vectoriels N_j , $j \neq i$. Il est immédiat que E est somme directe des sous-espaces vectoriels N_i et N'_i ; il résulte du corollaire 1 que N'_i est le noyau de l'endomorphisme $Q'_i(U)$, où

$$Q'_i = \prod_{j \neq i} Q_j.$$

D'autre part, les projecteurs associés à la décomposition en somme directe

$$E = N_i \oplus N'_i.$$

ne sont autres que P_i et P'_i , où

$$P'_i = \sum_{j \neq i} P_j.$$

Enfin, les polynômes Q_i et Q'_i sont premiers entre eux; en leur appliquant l'assertion 3 du théorème 5.1, nous voyons que P_i et P'_i sont des polynômes en U , ce qui achève la démonstration.

REMARQUE. — Ainsi, sous les hypothèses du corollaire 2, nous obtenons une décomposition de l'espace vectoriel E en somme directe de sous-espaces vectoriels stables par U . L'étude de U se ramène alors à celle des restrictions de U à N_i ; c'est pourquoi ce corollaire prend le nom de théorème de décomposition d'un endomorphisme.

Lorsque l'espace vectoriel E est de dimension finie sur K , pour tout $i \in [1, p]$, on peut choisir une base B_i du sous-espace vectoriel N_i ; la matrice associée à l'endomorphisme U dans la base B obtenue en réunissant les vecteurs des bases B_i est alors décomposée en p blocs diagonaux (cf. prop. I.3.67).

Le corollaire 2 nous conduit à étudier plus en détail les endomorphismes U pour lesquels il existe un polynôme Q tel que $Q(U) = 0$, ce qui fait l'objet du sous-paragraphe suivant.

2. POLYNÔME MINIMAL D'UN ENDOMORPHISME

Dans toute la suite de ce chapitre, E désigne un espace vectoriel sur K , non réduit à $\{0\}$.

DÉFINITION 5.1. — **Endomorphismes admettant un polynôme minimal.** — On dit qu'un endomorphisme U d'un espace vectoriel E sur K admet un polynôme minimal s'il existe un élément non nul Q de $K[X]$ tel que $Q(U) = 0$.

Dans ce cas, l'idéal \mathfrak{I} de $K[X]$ constitué des polynômes Q tels que $Q(U) = 0$ n'est pas réduit à $\{0\}$; le générateur π de l'idéal \mathfrak{I} s'appelle polynôme minimal de U .

PROPOSITION 5.2. — **Existence d'un polynôme minimal, en dimension finie.** — Lorsque l'espace vectoriel E est de dimension finie sur K , tout élément U de $\mathfrak{L}(E)$ admet un polynôme minimal.

Nous savons en effet que si E est de dimension n , l'algèbre $\mathfrak{L}(E)$ est de dimension n^2 . Il en découle que les éléments $I_E, U, U^2, \dots, U^{n^2}$ de $\mathfrak{L}(E)$ sont linéairement dépendants; autrement dit, il existe un élément non nul Q de $K[X]$, de degré inférieur ou égal à n^2 , tel que $Q(U) = 0$.

REMARQUE. — Lorsque E n'est pas de dimension finie, il peut arriver qu'un endomorphisme U de E n'admette pas de polynôme minimal. Prenons par exemple pour E l'espace vectoriel $K[X]$ des polynômes à coefficients dans K , et pour U l'unique endomorphisme de $K[X]$ tel que, pour tout entier naturel p , $U(X^p) = X^{p+1}$. Il est immédiat que $U^p(1) = X^p$; les vecteurs $U^p(1)$, où p parcourt \mathbb{N} , sont donc linéairement indépendants. *A fortiori*, les endomorphismes U^p , où p parcourt \mathbb{N} , sont linéairement indépendants.

PROPOSITION 5.3. — **Passage à un sous-espace vectoriel, à un espace vectoriel quotient.** — Soient U un endomorphisme d'un espace vectoriel E sur K , admettant un polynôme minimal π , et E' un sous-espace vectoriel de E stable par U .

1. Soit U' l'endomorphisme de E' coïncidant avec U . Alors U' admet un polynôme minimal, qui divise π .

2. Soient φ l'application linéaire canonique de E sur $F = E/E'$, et V l'unique endomorphisme de F tel que $V \circ \varphi = \varphi \circ U$. Alors V admet un polynôme minimal, qui divise π .

Assertion 1. — Du fait que $\pi(U) = 0$, nous déduisons aussitôt que $\pi(U') = 0$. Il en découle que U' admet un polynôme minimal, et que celui-ci divise π .

Assertion 2. — Il est immédiat que, pour tout élément P de $K[X]$, $P(V) \circ \varphi = \varphi \circ P(U)$. Il en découle que $\pi(V) = 0$, ce qui prouve que V admet un polynôme minimal, et que celui-ci divise π .

On trouvera des compléments dans l'exercice 13.

PROPOSITION 5.4. — Inversibilité d'un endomorphisme admettant un polynôme minimal. — Soient E un espace vectoriel sur K , et U un endomorphisme de E admettant un polynôme minimal

$$\pi(X) = X^n + \alpha_{n-1}X^{n-1} + \dots + \alpha_0.$$

1. Pour que U soit inversible, il faut et il suffit que α_0 soit non nul ; l'inverse de U est alors un polynôme en U .

2. Pour que U soit un diviseur de zéro bilatère, il faut et il suffit que α_0 soit nul ; il existe alors un élément R de $K[X]$ tel que $R(U) \neq 0$ et que $R(U) \cdot U = U \cdot R(U) = 0$.

a) Si $\alpha_0 \neq 0$, la relation $\pi(U) = 0$ peut encore s'écrire

$$UQ(U) = I_E,$$

où

$$Q = -\alpha_0^{-1}(X^{n-1} + \alpha_{n-1}X^{n-2} + \dots + \alpha_1).$$

L'endomorphisme U est donc inversible, et son inverse est un polynôme en U .

b) Si $\alpha_0 = 0$, la relation $\pi(U) = 0$ peut encore s'écrire

$$UR(U) = 0,$$

où

$$R = X^{n-1} + \alpha_{n-1}X^{n-2} + \dots + \alpha_1.$$

Puisque $d^0(R) < d^0(\pi)$, et que π est le polynôme minimal de U , $R(U)$ n'est pas nul ; U est donc un diviseur de zéro bilatère dans $\mathcal{L}(E)$.

Les assertions 1 et 2 se déduisent aussitôt de a) et b).

COROLLAIRE 1. — Endomorphismes inversibles, et diviseurs de zéro, en dimension finie. — Soit E un espace vectoriel de dimension finie sur K . Alors tout élément non nul de l'anneau $\mathcal{L}(E)$ est soit inversible, soit diviseur de zéro bilatère.

En effet, tout endomorphisme de E admet un polynôme minimal (cf. prop. 5.2).

COROLLAIRE 2. — Caractérisation des endomorphismes inversibles admettant un polynôme minimal. — Soient E un espace vectoriel sur K , et U un endomorphisme de E admettant un polynôme minimal. Il est équivalent de dire :

1. *L'endomorphisme U est inversible.*
2. *L'endomorphisme U est inversible à gauche.*
3. *L'endomorphisme U est inversible à droite.*
- 1'. *L'endomorphisme U est bijectif.*
- 2'. *L'endomorphisme U est injectif.*
- 3'. *L'endomorphisme U est surjectif.*
- 1''. *L'endomorphisme U est régulier.*
- 2''. *L'endomorphisme U est régulier à gauche.*
- 3''. *L'endomorphisme U est régulier à droite.*

Nous savons déjà que pour tout endomorphisme U de E , $1 \Rightarrow 1' \Rightarrow 1''$, $2 \Rightarrow 2' \Rightarrow 2''$, $3 \Rightarrow 3' \Rightarrow 3''$, et que $1 \Rightarrow 2$, $1 \Rightarrow 3$, $1'' \Rightarrow 2''$, $1'' \Rightarrow 3''$.

Il reste à prouver que si U admet un polynôme minimal, $2'' \Rightarrow 1$ et $3'' \Rightarrow 1$. Or, si U n'est pas inversible, le polynôme X n'est pas premier avec le polynôme minimal de U ; donc U est un diviseur de zéro bilatère. Il s'ensuit que U n'est pas régulier à gauche, et qu'il n'est pas régulier à droite, ce qu'il fallait prouver.

COROLLAIRE 3. — Caractérisation des endomorphismes inversibles, en dimension finie. — Soit E un espace vectoriel de dimension finie sur K . Alors, dans l'anneau unitaire $\mathcal{L}(E)$ des endomorphismes de E , les notions d'élément inversible, inversible à gauche, inversible à droite, régulier, régulier à gauche, régulier à droite, coïncident.

En pratique, on rencontre souvent des endomorphismes satisfaisant à une condition un peu plus faible que celle de l'existence d'un polynôme minimal.

DÉFINITION 5.2. — Endomorphismes localement finis. — On dit qu'un endomorphisme U d'un espace vectoriel E sur K est localement fini si, pour tout vecteur x de E , il existe un élément P non nul de $K[X]$ tel que $[P(U)](x) = 0$.

En particulier, on dit que U est localement nilpotent si, pour tout vecteur x de E , il existe un entier $n > 0$ tel que $U^n(x) = 0$.

REMARQUE. — Les endomorphismes localement finis sont d'un grand intérêt, tant en algèbre qu'en analyse; leur théorie est esquissée dans l'exercice 15. Cependant, il existe des endomorphismes très simples qui ne sont pas localement finis. C'est le cas pour l'unique endomorphisme U de $K[X]$ tel que, pour tout entier naturel p , $U(X^p) = X^{p+1}$: en effet, pour tout polynôme P , l'endomorphisme $P(U)$ n'est autre que l'application $Q \mapsto PQ$.

§ 2. SOUS-ESPACES SPECTRAUX

PROPOSITION 5.5. — Noyaux et images itérés. — Soient E un espace vectoriel sur K , U un endomorphisme de E , et λ un scalaire. Pour tout entier naturel r , on note $E_{\lambda,r}$ et $E'_{\lambda,r}$ le noyau et l'image de l'endomorphisme $(U - \lambda I_E)^r$. Les sous-espaces vectoriels $E_{\lambda,1}$ et $E'_{\lambda,1}$ sont notés, plus simplement E_λ et E'_λ .

1. La suite des sous-espaces vectoriels $E_{\lambda,r}$, où $r \in \mathbb{N}$, est croissante, et l'ensemble $\bigcup_{r=0}^{+\infty} E_{\lambda,r}$ est un sous-espace vectoriel de E , noté F_λ .

2. La suite des sous-espaces vectoriels $E'_{\lambda,r}$, où $r \in \mathbb{N}$, est décroissante, et l'ensemble $\bigcup_{r=0}^{+\infty} E'_{\lambda,r}$ est un sous-espace vectoriel de E , noté F'_λ .

3. S'il existe un entier naturel r tel que $E_{\lambda,r} = E_{\lambda,r+1}$ (resp. $E'_{\lambda,r} = E'_{\lambda,r+1}$), alors, pour tout entier naturel s ,

$$E_{\lambda,r} = E_{\lambda,r+s} \quad (\text{resp. } E'_{\lambda,r} = E'_{\lambda,r+s}).$$

4. L'endomorphisme $U - \lambda I_E$ est injectif si et seulement si $F_\lambda = \{0\}$; il est surjectif si et seulement si $F'_\lambda = E$.

(Dans ce qui précède, $(U - \lambda I_E)^0$ désigne I_E , et les sous-espaces vectoriels de E sont ordonnés par inclusion.)

Introduisons l'endomorphisme $V = U - \lambda I_E$; alors

$$E_{\lambda,r} = \text{Ker}(V^r) \quad \text{et} \quad E'_{\lambda,r} = \text{Im}(V^r).$$

Les assertions 1 et 2 sont immédiates.

L'assertion 3 se démontre par récurrence sur s . Lorsque $s = 0$, ou $s = 1$, l'assertion est évidente; supposons-la établie à l'ordre s , $s \geq 1$, et prouvons par exemple que $E_{\lambda,r+s+1} = E_{\lambda,r}$, c'est-à-dire que $\text{Ker}(V^{r+s+1}) = \text{Ker}(V^r)$. Soit pour cela \mathfrak{x} un élément de $\text{Ker}(V^{r+s+1})$; alors $V^{r+1}[V^s(\mathfrak{x})] = 0$, donc $V^s(\mathfrak{x})$ appartient au sous-espace $\text{Ker}(V^{r+1}) = \text{Ker}(V^r)$.

Ainsi, $V^{r+s}(\mathfrak{x}) = 0$; autrement dit, \mathfrak{x} appartient à $\text{Ker}(V^{r+s})$. L'assertion en découle, puisque, d'après l'hypothèse de récurrence, $\text{Ker}(V^{r+s}) = \text{Ker}(V^r)$.

L'assertion 4 est un cas particulier de l'assertion 3 : il suffit de prendre $r = 0$. On peut aussi prouver cette assertion en utilisant le fait qu'une composée d'injections (resp. de surjections) est une injection (resp. une surjection).

DÉFINITION 5. 3. — Valeurs propres d'un endomorphisme. — Soient E un espace vectoriel sur K , et U un endomorphisme de E . On dit qu'un scalaire λ est une valeur propre de U si le noyau de $U - \lambda I_E$ n'est pas réduit à $\{0\}$, autrement dit si $E_\lambda \neq \{0\}$. D'après ce qui précède, cela revient encore à dire que $F_\lambda \neq \{0\}$. La partie de K constituée des valeurs propres de U s'appelle spectre de U dans K , et se note $\text{sp}_K(U)$, ou plus simplement $\text{sp}(U)$, lorsqu'aucune confusion n'est à craindre.

DÉFINITION 5.4. — Sous-espaces propres, sous-espaces spectraux. — Soient E un espace vectoriel sur K , U un endomorphisme de E , et λ une valeur propre de U . Le sous-espace vectoriel E_λ s'appelle sous-espace propre associé à la valeur propre λ ; le sous-espace vectoriel F_λ s'appelle sous-espace spectral associé à la valeur propre λ .

DÉFINITION 5.5. — Vecteurs propres d'un endomorphisme. — Soient E un espace vectoriel sur K , U un endomorphisme de E , et λ une valeur propre de U . Les éléments non nuls de E_λ sont appelés vecteurs propres associés à la valeur propre λ .

Autrement dit, pour qu'un élément x de E soit un vecteur propre de U , il faut et il suffit que x soit non nul, et qu'il existe un scalaire λ tel que $U(x) = \lambda x$; un tel scalaire λ est unique, et c'est une valeur propre de U .

REMARQUE 1. — Soit λ une valeur propre d'un endomorphisme U . Le sous-espace propre E_λ est contenu dans le sous-espace spectral F_λ ; il peut arriver que cette inclusion soit stricte.

Considérons par exemple un endomorphisme U nilpotent non nul de K^n , $n \geq 2$. Alors $F_0 = E$, et $E_0 = \text{Ker}(U) \neq E$.

REMARQUE 2. — Soit λ une valeur propre d'un endomorphisme U ; il peut arriver que la suite des sous-espaces vectoriels $E_{\lambda,r}$ soit strictement croissante.

Prenons par exemple pour E l'espace vectoriel $K[X]$ des polynômes à une indéterminée à coefficients dans K , et pour U l'unique endomorphisme de $K[X]$ tel que, pour tout entier $p > 0$, $U(X^p) = X^{p-1}$, et que $U(1) = 0$. Il est immédiat que, pour tout entier $r > 0$, $\text{Ker}(U^r)$ n'est autre que l'espace vectoriel des polynômes de degré strictement inférieur à r . Ainsi $E_{0,r} = \text{Ker}(U^r) \neq K[X]$, tandis que $F_0 = K[X]$.

DÉFINITION 5.6. — Valeurs propres d'indice fini. — Soit λ une valeur propre d'un endomorphisme U d'un espace vectoriel E sur K . On dit que λ est une valeur propre d'indice fini s'il existe un entier $r > 0$ tel que $E_{\lambda,r} = F_\lambda$.

D'après ce qui précède, cela revient à dire que $E_{\lambda,r} = E_{\lambda,r+1}$, ou encore que la suite des sous-espaces vectoriels $E_{\lambda,r}$ est stationnaire. Dans ces conditions, le plus petit des entiers naturels r tels que $E_{\lambda,r} = E_{\lambda,r+1}$ s'appelle indice de la valeur propre λ .

Si le sous-espace spectral F_λ est de dimension finie, la valeur propre λ est évidemment d'indice fini, et son indice $n(\lambda)$ est inférieur ou égal à la dimension de F_λ :

$$n(\lambda) \leq \dim F_\lambda.$$

PROPOSITION 5.6. — Caractérisation des valeurs propres des endomorphismes admettant un polynôme minimal. — Soient E un espace vectoriel sur K , et U un endomorphisme de E admettant un polynôme minimal. Alors les valeurs propres de U sont encore les scalaires λ tels que l'endomorphisme $U - \lambda I_E$ ne soit pas inversible.

En effet, si π est le polynôme minimal de U , le polynôme $\pi_\lambda(X) = \pi(X + \lambda)$ est évidemment le polynôme minimal de $U - \lambda I_E$. Le corollaire 2 de la proposition 5.4 montre alors que $U - \lambda I_E$ est inversible si et seulement s'il est injectif.

Si U n'admet pas de polynôme minimal, ce résultat peut tomber en défaut (cf. exercice 6); c'est pourquoi on introduit aussi les *valeurs spectrales* d'un endomorphisme U : ce sont les scalaires λ tels que $U - \lambda I_E$ ne soit pas inversible.

Ainsi, toute valeur propre d'un endomorphisme U en est une valeur spectrale, la réciproque étant valable en dimension finie, ou, plus généralement, lorsque U admet un polynôme minimal.

Nous allons comparer les valeurs propres d'un endomorphisme aux valeurs propres d'un polynôme de cet endomorphisme :

THÉORÈME 5.2. — Théorème de Hilbert-Dirac. — *Soient U un endomorphisme d'un espace vectoriel E sur K , et P un polynôme à coefficients dans K .*

Pour tout scalaire λ , et pour tout entier naturel r , le noyau de l'endomorphisme $[P(U) - P(\lambda)I_E]^r$ contient le noyau de l'endomorphisme $(U - \lambda I_E)^r$.

En particulier, soit λ une valeur propre de U . Alors $P(\lambda)$ est une valeur propre de $P(U)$, le sous-espace propre de U associé à λ est contenu dans le sous-espace propre de $P(U)$ associé à $P(\lambda)$, et le sous-espace spectral de U associé à λ est contenu dans le sous-espace spectral de $P(U)$ associé à $P(\lambda)$.

Considérons le polynôme $P(X) - P(\lambda)$; ce polynôme, admettant λ pour racine, est divisible par $X - \lambda$. Ainsi, il existe un polynôme Q tel que

$$P(X) - P(\lambda) = Q(X) \cdot (X - \lambda).$$

Il en découle que, pour tout entier naturel r ,

$$[P(X) - P(\lambda)]^r = [Q(X)]^r \cdot (X - \lambda)^r.$$

Dans cette relation, substituons U à l'indéterminée X :

$$[P(U) - P(\lambda)I_E]^r = [Q(U)]^r \cdot (U - \lambda I_E)^r.$$

Il en résulte aussitôt que le noyau de $(U - \lambda I_E)^r$ est contenu dans le noyau de $[P(U) - P(\lambda)I_E]^r$, ce qu'il fallait prouver.

REMARQUE. — Lorsque le corps K est algébriquement clos, on peut préciser les conclusions de ce théorème; cf. exercice 10.

COROLLAIRE. — *Soit U un endomorphisme d'un espace vectoriel E sur K . S'il existe un polynôme P à coefficients dans K tel que $P(U) = 0$, les valeurs propres de U sont des racines dans K du polynôme P .*

Appliquons maintenant aux sous-espaces spectraux et aux sous-espaces propres les résultats du § 1. La proposition 5.1 fournit aussitôt la

PROPOSITION 5.7. — Stabilité des noyaux et images itérés. — Soient U et V deux endomorphismes d'un espace vectoriel E sur K . Si U et V commutent, alors, pour tout scalaire λ et pour tout entier naturel r , les sous-espaces vectoriels

$$E_{\lambda,r}(U) = \text{Ker} [(U - \lambda I_E)^r] \quad \text{et} \quad E'_{\lambda,r}(U) = \text{Im} [(U - \lambda I_E)^r]$$

sont stables par V .

COROLLAIRE. — Stabilité des sous-espaces propres et des sous-espaces spectraux. — Soient U et V deux endomorphismes d'un espace vectoriel E sur K . Si U et V commutent, les sous-espaces propres et les sous-espaces spectraux de U sont stables par V .

En particulier, les sous-espaces propres et les sous-espaces spectraux d'un endomorphisme U sont stables par U .

PROPOSITION 5.8. — Indépendance linéaire des noyaux itérés. — Soient U un endomorphisme d'un espace vectoriel E sur K , p un entier strictement supérieur à 1, $(\lambda_1, \dots, \lambda_i, \dots, \lambda_p)$ une suite de scalaires distincts deux à deux, et $(r_1, \dots, r_i, \dots, r_p)$ une suite d'entiers strictement positifs. Alors la somme des sous-espaces vectoriels

$$\text{Ker} [(U - \lambda_i I_E)^{r_i}]$$

est directe.

Considérons pour tout $i \in [1, p]$ le polynôme $P_i = (X - \lambda_i)^{r_i}$. Les polynômes P_i sont premiers entre eux deux à deux. Le théorème de décomposition des noyaux (cor. 1 du th. 5.1) montre que la somme des noyaux des endomorphismes $P_i(U)$ est directe, ce qu'il fallait prouver.

COROLLAIRE 1. — Indépendance linéaire des sous-espaces propres. — Soit U un endomorphisme d'un espace vectoriel E sur K . Alors la somme des sous-espaces propres $E_\lambda = \text{Ker} (U - \lambda I_E)$, où λ parcourt le spectre de U dans K , est directe.

Autrement dit : soient $\lambda_1, \dots, \lambda_i, \dots, \lambda_p$ des valeurs propres de U distinctes deux à deux, et $\mathbf{x}_1, \dots, \mathbf{x}_i, \dots, \mathbf{x}_p$ des vecteurs propres associés respectivement à ces valeurs propres. Alors les vecteurs $\mathbf{x}_1, \dots, \mathbf{x}_i, \dots, \mathbf{x}_p$ sont linéairement indépendants.

Sous cette dernière forme, le corollaire 1 est une conséquence immédiate de la proposition, appliquée au cas où les entiers r_i sont tous égaux à 1.

REMARQUE. — On peut donner du corollaire 1 une démonstration plus élémentaire, par récurrence sur l'entier p :

Pour $p = 1$, l'assertion est évidente; supposons-la prouvée à l'ordre $p - 1$, $p > 1$, et considérons une relation linéaire

$$(1) \quad \alpha_1 \mathbf{x}_1 + \dots + \alpha_i \mathbf{x}_i + \dots + \alpha_p \mathbf{x}_p = \mathbf{0}$$

entre les vecteurs propres $\mathbf{x}_1, \dots, \mathbf{x}_i, \dots, \mathbf{x}_p$.

En appliquant l'endomorphisme U aux deux membres, nous obtenons la relation

$$(2) \quad \lambda_1 \alpha_1 \mathbf{x}_1 + \dots + \lambda_i \alpha_i \mathbf{x}_i + \dots + \lambda_p \alpha_p \mathbf{x}_p = \mathbf{0}.$$

Multiplions la relation (1) par le scalaire λ_p , et retranchons-la de la relation (2) :

$$(\lambda_1 - \lambda_p) \alpha_1 \mathbf{x}_1 + \dots + (\lambda_i - \lambda_p) \alpha_i \mathbf{x}_i + \dots + (\lambda_{p-1} - \lambda_p) \alpha_{p-1} \mathbf{x}_{p-1} = \mathbf{0}.$$

D'après l'hypothèse de récurrence, les scalaires $(\lambda_i - \lambda_p) \alpha_i$ sont nuls, quel que soit $i \in [1, p-1]$. Comme les scalaires $\lambda_i - \lambda_p$ ne sont pas nuls, il en découle que $\alpha_i = 0$, pour tout $i \in [1, p-1]$.

La relation (1) s'écrit alors $\alpha_p \mathbf{x}_p = \mathbf{0}$; donc $\alpha_p = 0$.

COROLLAIRE 2. — Indépendance linéaire des sous-espaces spectraux. — Soit U un endomorphisme d'un espace vectoriel E sur K . Alors la somme des sous-espaces spectraux F_λ de U , où λ parcourt le spectre de U dans K , est directe.

Autrement dit : soient $\lambda_1, \dots, \lambda_i, \dots, \lambda_p$ des valeurs propres de U distinctes deux à deux et, pour tout $i \in [1, p]$, \mathbf{x}_i un vecteur non nul du sous-espace spectral F_{λ_i} ; alors les vecteurs $\mathbf{x}_1, \dots, \mathbf{x}_i, \dots, \mathbf{x}_p$ sont linéairement indépendants.

Considérons en effet les vecteurs $\mathbf{x}_1, \dots, \mathbf{x}_i, \dots, \mathbf{x}_p$; pour tout $i \in [1, p]$, il existe un entier r_i tel que \mathbf{x}_i appartienne au noyau de l'endomorphisme $(U - \lambda_i I_E)^{r_i}$. La proposition montre que la somme de ces noyaux est directe, ce qui équivaut à l'assertion énoncée.

REMARQUE. — Existence de valeurs propres. — Nous venons de voir que la somme des sous-espaces spectraux de U est directe. Mais il peut arriver que cette somme ne soit pas égale à E tout entier; il se peut même que cette somme soit réduite à $\{\mathbf{0}\}$, ce qui revient à dire que le spectre de U est vide. Voici deux exemples d'endomorphismes dont le spectre est vide :

1. Soit U l'unique endomorphisme de $K[X]$ tel que, pour tout entier $p \geq 0$,

$$U(X^p) = X^{p+1}.$$

Il est immédiat que U ne possède aucune valeur propre.

2. Soit U l'endomorphisme de \mathbf{R}^2 canoniquement associé à la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Il est facile de voir que $U^2 = -I_E$. Toute valeur propre de U est nécessairement une racine dans \mathbf{R} du polynôme $X^2 + 1$. L'endomorphisme U ne possède donc aucune valeur propre. On est alors conduit à considérer l'endomorphisme $U_{\mathbf{C}}$ de \mathbf{C}^2 défini par la même matrice, dont le spectre dans \mathbf{C} est constitué des points i et $-i$; ce point de vue sera développé au paragraphe 5.5.

§ 3. RÉDUCTION DES ENDOMORPHISMES

1. ENDOMORPHISMES SCINDÉS

DÉFINITION 5.7. — Endomorphismes scindés. — Soit U un endomorphisme d'un espace vectoriel E sur K . On dit que U est scindé sur K si l'espace vectoriel E est somme directe des sous-espaces spectraux F_λ de U , où λ parcourt le spectre de U dans K .

Les projecteurs P_λ associés à cette décomposition de E en somme directe sont appelés projecteurs spectraux de U . Ces projecteurs satisfont donc aux relations fondamentales suivantes :

1. Pour tout élément λ de $\text{sp}(U)$,

$$(1) \quad P_\lambda^2 = P_\lambda.$$

2. Pour tout couple (λ, μ) d'éléments distincts de $\text{sp}(U)$,

$$(2) \quad P_\lambda P_\mu = P_\mu P_\lambda = 0.$$

3. L'application identique de E est égale à la somme des projecteurs P_λ :

$$(3) \quad I_E = \sum_{\lambda \in \text{sp}(U)} P_\lambda.$$

4. L'image de P_λ est le sous-espace spectral F_λ , et le noyau de P_λ est la somme directe des sous-espaces spectraux F_μ , où $\mu \neq \lambda$:

$$(4) \quad \text{Im}(P_\lambda) = F_\lambda \quad \text{et} \quad \text{Ker}(P_\lambda) = \bigoplus_{\mu \neq \lambda} F_\mu.$$

5. Pour tout élément λ de $\text{sp}(U)$, et pour tout endomorphisme V de E commutant à U , les endomorphismes V et P_λ commutent :

$$(5) \quad VP_\lambda = P_\lambda V.$$

Les propriétés 1, 2, 3 et 4 résultent de la proposition I.3.18. La propriété 5 exprime que V laisse stables tous les sous-espaces vectoriels F_λ ; elle résulte donc du corollaire de la proposition 5.7.

Les formules précédentes sont très utiles en pratique, car elles permettent de traiter les problèmes concernant les sous-espaces spectraux d'un endomorphisme scindé au moyen d'un formalisme algébrique.

THÉORÈME 5.3. — Caractérisation des endomorphismes scindés sur K . — Soit U un endomorphisme d'un espace vectoriel E sur K . Il est équivalent de dire :

1. L'endomorphisme U est scindé sur K .

2. Pour tout vecteur \mathfrak{x} de E , il existe un élément non nul P de $K[X]$ scindé sur K et tel que $P(U)(\mathfrak{x}) = 0$.

$1 \Rightarrow 2$: soit \mathbf{x} un vecteur de E ; il existe par hypothèse une partie finie S de $\text{sp}(U)$ et une famille $(\mathbf{x}_\lambda)_{\lambda \in S}$ de vecteurs de E telles que $\mathbf{x} = \sum_{\lambda \in S} \mathbf{x}_\lambda$, et que, pour tout $\lambda \in S$, $\mathbf{x}_\lambda \in F_\lambda$. Il en découle que, pour tout $\lambda \in S$, il existe un entier strictement positif n_λ tel que $(U - \lambda I_E)^{n_\lambda}(\mathbf{x}_\lambda) = \mathbf{0}$. Le polynôme

$$P = \prod_{\lambda \in S} (X - \lambda)^{n_\lambda}$$

est scindé sur K , et il est immédiat que $P(U)(\mathbf{x}) = \mathbf{0}$.

$2 \Rightarrow 1$: il s'agit de prouver que E est somme directe des sous-espaces spectraux F_λ , où λ parcourt $\text{sp}(U)$, ou encore que E est somme directe des sous-espaces vectoriels F_λ , où λ parcourt K . Considérons pour cela un vecteur \mathbf{x} de E ; il existe par hypothèse un élément non nul P de $K[X]$ scindé sur K et tel que $P(U)(\mathbf{x}) = \mathbf{0}$. Le polynôme P peut donc s'écrire sous la forme

$$P = \beta \prod_{\lambda \in T} (X - \lambda)^{r_\lambda},$$

où T est une partie finie de K , β un scalaire non nul, et r_λ un entier strictement positif, pour tout élément λ de T . Le théorème de décomposition des noyaux montre alors que

$$\text{Ker } P(U) = \bigoplus_{\lambda \in T} \text{Ker } (U - \lambda I_E)^{r_\lambda}.$$

Il en découle que

$$\text{Ker } P(U) \subset \bigoplus_{\lambda \in T} F_\lambda \subset \bigoplus_{\lambda \in K} F_\lambda,$$

ce qu'il fallait prouver.

COROLLAIRE. — Cas des corps algébriquement clos. — Soit U un endomorphisme d'un espace vectoriel E sur un corps K algébriquement clos. Pour que U soit scindé sur K , il faut et il suffit que U soit localement fini.

En particulier, tout endomorphisme admettant un polynôme minimal est scindé.

Cela résulte aussitôt du théorème 5.3, et du fait que tout élément de $K[X]$ est scindé sur K .

PROPOSITION 5.9. — Calcul du spectre d'un endomorphisme scindé. — Soient U un endomorphisme d'un espace vectoriel E sur K , $(\mu_i)_{i \in I}$ une famille de scalaires et $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E stables par U , telles que E soit somme directe des sous-espaces vectoriels F_i et que, pour tout élément i de I , l'endomorphisme de F_i coïncidant avec $U - \mu_i I_E$ soit localement nilpotent. Alors U est scindé sur K . En outre, le spectre de U dans K n'est autre que l'ensemble des scalaires λ satisfaisant à la condition suivante : il existe un élément i de I tel que $\mu_i = \lambda$, et que $F_i \neq \{\mathbf{0}\}$; enfin, pour toute valeur propre λ de U , le sous-espace spectral F_λ de U associé à λ n'est autre que la somme directe des sous-espaces vectoriels F_i , où i est tel que $\mu_i = \lambda$.

Introduisons l'ensemble S des scalaires λ pour lesquels il existe un élément i de I tel que $\mu_i = \lambda$, et que $F_i \neq \{0\}$. Puisque $E \neq \{0\}$, et que $E = \bigoplus_{i \in I} F_i$, l'ensemble S est non vide. Considérons maintenant, pour tout élément λ de S , la somme directe G_λ des sous-espaces vectoriels F_i tels que $\mu_i = \lambda$. Alors, pour tout $\lambda \in S$, G_λ n'est pas réduit à $\{0\}$, E est somme directe des sous-espaces vectoriels G_λ où λ parcourt S , et le sous-espace vectoriel G_λ est contenu dans le sous-espace vectoriel

$$F_\lambda = \bigcup_{r=0}^{+\infty} \text{Ker}(U - \lambda I_E)^r.$$

Comme G_λ est non réduit à $\{0\}$, le scalaire λ est une valeur propre de U , et l'inclusion précédente signifie que G_λ est contenu dans le sous-espace spectral F_λ de U associé à λ . Puisque E est somme directe des sous-espaces G_λ , nous voyons que la somme des sous-espaces spectraux de U est égale à E tout entier; ainsi, l'endomorphisme U est scindé sur K .

Il nous reste à démontrer que toute valeur propre λ de U appartient à S , et qu'alors $G_\lambda = F_\lambda$. Cela résulte du lemme suivant, où l'on prendra $I = S$, et $J = \text{sp}(U)$.

LEMME. — Soient E un espace vectoriel sur un corps K , I une partie d'un ensemble J , $(E_i)_{i \in I}$ une famille de sous-espaces vectoriels de E , et $(E'_j)_{j \in J}$ une famille de sous-espaces vectoriels de E non réduits à $\{0\}$. Si, pour tout $i \in I$, E_i est contenu dans E'_i , et si E est somme directe de la famille $(E_i)_{i \in I}$, ainsi que de la famille $(E'_j)_{j \in J}$, alors $J = I$, et, pour tout $i \in I$, $E_i = E'_i$.

Soient j un élément de J , et x un élément non nul de E'_j . Puisque $E = \bigoplus_{i \in I} E_i$, le vecteur x s'écrit d'une manière et d'une seule sous la forme $x = \sum_{i \in I} x_i$, où, pour tout $i \in I$, $x_i \in E_i$. Comme $x \neq 0$, il existe un élément i_0 de I tel que $x_{i_0} \neq 0$. D'autre part, pour tout $i \in I$, x_i appartient à E'_i . Par unicité de la décomposition de x suivant la somme directe $E = \bigoplus_{j \in J} E'_j$, nous voyons que $x_i = 0$ si $i \neq i_0$, que $i_0 = j$, et que $x = x_{i_0}$. Il s'ensuit que $j \in I$, et que $x \in E_{i_0}$, ce qui achève la démonstration.

COROLLAIRE 1. — **Caractérisation des sous-espaces spectraux d'un endomorphisme scindé.** — Soient U un endomorphisme d'un espace vectoriel E sur K , $(\mu_i)_{i \in I}$ une famille finie de scalaires distincts deux à deux, et $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E non réduits à $\{0\}$ et stables par U , telles que E soit somme directe des sous-espaces vectoriels F_i , et que, pour tout $i \in I$, l'endomorphisme de F_i coïncidant avec $U - \mu_i I_E$ soit localement nilpotent. Alors l'application $i \mapsto \mu_i$ est une bijection de I sur le spectre de U dans K et, pour tout $i \in I$, F_i n'est autre que le sous-espace spectral de U associé à la valeur propre μ_i .

COROLLAIRE 2. — Polynômes d'un endomorphisme scindé. — Soient U un endomorphisme scindé d'un espace vectoriel E sur K et Q un élément de $K[X]$. Alors l'endomorphisme $Q(U)$ est scindé, le spectre de $Q(U)$ n'est autre que l'image par la fonction polynomiale Q du spectre de U , et pour toute valeur propre λ de $Q(U)$, le sous-espace spectral $F_\lambda[Q(U)]$ n'est autre que la somme directe des sous-espaces spectraux $F_\mu(U)$ tels que $Q(\mu) = \lambda$.

En effet, par hypothèse, $E = \bigoplus_{\mu \in \text{sp}(U)} F_\mu(U)$. Or, le théorème de Hilbert-Dirac montre que $F_\mu(U)$ est contenu dans $F_{Q(\mu)}[Q(U)]$. Donc la somme directe des sous-espaces vectoriels $F_{Q(\mu)}[Q(U)]$, où μ parcourt $\text{sp}(U)$, est égale à E tout entier. Il suffit alors d'appliquer la proposition 5.9.

2. ENDOMORPHISMES DIAGONALISABLES

Soit U un endomorphisme d'un espace vectoriel E sur K . Nous savons que la somme des sous-espaces propres de U est directe. Cependant, même si E est de dimension finie sur K et si U est scindé sur K , il peut arriver que cette somme directe ne soit pas égale à E tout entier : c'est le cas lorsque U est un endomorphisme nilpotent non nul. Nous sommes ainsi conduit à la

DÉFINITION 5.8. — Endomorphismes diagonalisables. — Soit U un endomorphisme d'un espace vectoriel E sur K . On dit que U est diagonalisable sur K (ou plus simplement diagonalisable, lorsque aucune confusion n'est à craindre) si l'espace vectoriel E est somme directe des sous-espaces propres $E_\lambda(U)$, où λ parcourt le spectre de U dans K .

Voici un résultat d'une importance capitale :

THÉORÈME 5.4. — Caractérisation des endomorphismes diagonalisables sur K . — Soit U un endomorphisme d'un espace vectoriel E sur K . Il est équivalent e dire :

1. L'endomorphisme U est diagonalisable sur K .
2. L'endomorphisme U est scindé sur K , et toute valeur propre de U est d'indice 1 ; autrement dit, U est scindé sur K , et pour toute valeur propre λ de U , le sous-espace propre E_λ est égal au sous-espace spectral F_λ .
3. L'endomorphisme U est scindé sur K , et il est lié à ses projecteurs spectraux P_λ par la formule suivante, dite formule de décomposition spectrale de U :

$$(1) \quad U = \sum_{\lambda \in \text{sp}(U)} \lambda P_\lambda.$$

4. Pour tout vecteur \mathfrak{x} de E , il existe un élément non nul P de $K[X]$ scindé sur K , ayant toutes ses racines simples, et tel que $[P(U)](\mathfrak{x}) = 0$.

$1 \Leftrightarrow 2$: nous savons que, pour tout élément λ de $\text{sp}(U)$, $E_\lambda \subset F_\lambda$, et que la somme des sous-espaces spectraux F_λ est directe. Il en découle que $E = \bigoplus_{\lambda \in \text{sp}(U)} E_\lambda$ si et seulement si $E = \bigoplus_{\lambda \in \text{sp}(U)} F_\lambda$ et $E_\lambda = F_\lambda$ pour tout $\lambda \in \text{sp}(U)$.

$2 \Rightarrow 3$: soit \mathbf{x} un vecteur de E , écrit sous la forme

$$\mathbf{x} = \sum_{\lambda \in \text{sp}(U)} \mathbf{x}_\lambda,$$

où, pour tout $\lambda \in \text{sp}(U)$, \mathbf{x}_λ appartient à E_λ . Par définition de E_λ , $U(\mathbf{x}_\lambda) = \lambda \mathbf{x}_\lambda$, et, par définition de P_λ , $P_\lambda(\mathbf{x}) = \mathbf{x}_\lambda$. Il en découle aussitôt que

$$U(\mathbf{x}) = \sum_{\lambda \in \text{sp}(U)} \lambda P_\lambda(\mathbf{x}).$$

$3 \Rightarrow 2$: la formule (1) montre que la restriction de $U - \lambda I_E$ à F_λ est nulle. Il en résulte que $E_\lambda = F_\lambda$, ce qu'il fallait prouver.

$1 \Rightarrow 4$: soit \mathbf{x} un vecteur de E ; il existe par hypothèse une partie finie S de $\text{sp}(U)$ et une famille $(\mathbf{x}_\lambda)_{\lambda \in S}$ de vecteurs de E telles que $\mathbf{x} = \sum_{\lambda \in S} \mathbf{x}_\lambda$, et que, pour tout $\lambda \in S$, $\mathbf{x}_\lambda \in E_\lambda$. Le polynôme $P = \prod_{\lambda \in S} (X - \lambda)$ est scindé sur K , il a toutes ses racines simples, et il est immédiat que $[P(U)](\mathbf{x}) = \mathbf{0}$.

$4 \Rightarrow 1$: comme nous savons que la somme des sous-espaces vectoriels E_λ est directe, il suffit de prouver que tout vecteur \mathbf{x} de E appartient à cette somme. Or, il existe un élément non nul P de $K[X]$ scindé sur K , ayant toutes ses racines simples, et tel que \mathbf{x} appartienne au noyau de $P(U)$. Il existe donc une partie finie T de K telle que

$$P = \beta \prod_{\lambda \in T} (X - \lambda),$$

où β est un scalaire non nul. Le théorème de décomposition des noyaux montre que

$$\text{Ker}[P(U)] = \bigoplus_{\lambda \in T} \text{Ker}(U - \lambda I_E).$$

Le vecteur \mathbf{x} appartient donc à $\bigoplus_{\lambda \in T} E_\lambda(U)$, ce qu'il fallait prouver.

COROLLAIRE. — Cas des corps algébriquement clos. — Soit U un endomorphisme d'un espace vectoriel E sur un corps algébriquement clos K . Pour que U soit diagonalisable sur K , il faut et il suffit que U soit localement fini et que toutes les valeurs propres de U soient d'indice 1.

PROPOSITION 5.10. — Calcul du spectre d'un endomorphisme diagonalisable. — Soit U un endomorphisme d'un espace vectoriel E sur K .

1. Soient $(\mu_i)_{i \in I}$ une famille de scalaires et $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E stables par U , telles que E soit somme directe des sous-espaces vectoriels F_i et que, pour tout élément i de I , l'endomorphisme de F_i coïncidant avec U soit l'homothétie de rapport μ_i . Alors U est diagonalisable sur K . En outre, le spectre de U dans K n'est autre que l'ensemble S des scalaires λ

satisfaisant à la condition suivante : il existe un élément i de I tel que $\mu_i = \lambda$ et que $F_i \neq \{0\}$; enfin, pour toute valeur propre λ de U , le sous-espace propre E_λ de U associé à λ n'est autre que la somme directe des sous-espaces vectoriels F_i où i est tel que $\mu_i = \lambda$.

2. Soient $(\mu_i)_{i \in I}$ une famille de scalaires et $(P_i)_{i \in I}$ un système de projecteurs de E tels que

$$U = \sum_{i \in I} \mu_i P_i.$$

Alors U est diagonalisable sur K , et, pour toute valeur propre λ de U , le projecteur spectral P_λ de U associé à λ n'est autre que la somme des projecteurs P_i où i est tel que $\mu_i = \lambda$.

Assertion 1. — D'après la proposition 5.9, le spectre de U dans K n'est autre que S , U est scindé sur K , et, pour toute valeur propre λ de U , le sous-espace spectral F_λ de U n'est autre que le sous-espace vectoriel G_λ somme directe des sous-espaces vectoriels F_i , où i est tel que $\mu_i = \lambda$. Il découle aussitôt de l'hypothèse que, pour tout $\lambda \in S$, G_λ est contenu dans $\text{Ker}(U - \lambda I_E)$; autrement dit, G est contenu dans le sous espace propre E_λ de U associé à λ . Il s'ensuit que les trois sous-espaces vectoriels E_λ , F_λ , G_λ coïncident, ce qui achève la démonstration.

L'assertion 2 se ramène aussitôt à l'assertion 1; il suffit de poser $F_i = \text{Im}(P_i)$.

COROLLAIRE 1. — Caractérisation des sous-espaces propres d'un endomorphisme diagonalisable. — Soient $(\mu_i)_{i \in I}$ une famille de scalaires distincts deux à deux et $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E non réduits à $\{0\}$ et stables par U , telles que E soit somme directe des sous-espaces vectoriels F_i , et que, pour tout $i \in I$, l'endomorphisme de F_i coïncidant avec U soit l'homothétie de rapport μ_i . Alors l'application $i \mapsto \mu_i$ est une bijection de I sur le spectre de U dans K , et, pour tout $i \in I$, F_i n'est autre que le sous-espace propre de U associé à la valeur propre μ_i .

COROLLAIRE 2. — Caractérisation des projecteurs spectraux d'un endomorphisme diagonalisable. — Soient $(\mu_i)_{i \in I}$ une famille de scalaires distincts deux à deux et $(P_i)_{i \in I}$ un système de projecteurs non nuls de E tels que

$$(2) \quad U = \sum_{i \in I} \mu_i P_i.$$

Alors l'application $i \mapsto \mu_i$ est une bijection de I sur le spectre de U dans K , et, pour tout $i \in I$, P_i n'est autre que le projecteur spectral de U associé à la valeur propre μ_i . La formule (2) est donc la formule de décomposition spectrale de l'endomorphisme U .

COROLLAIRE 3. — Polynômes d'un endomorphisme diagonalisable. — Soient U un endomorphisme diagonalisable d'un espace vectoriel E sur K , $U = \sum_{\mu \in \text{sp}(U)} \mu P_\mu$ la décomposition spectrale de U , et Q un élément de $K[X]$. Alors

l'endomorphisme $Q(U)$ est diagonalisable, le spectre de $Q(U)$ n'est autre que l'image par la fonction polynomiale Q du spectre de U , et pour toute valeur propre λ de $Q(U)$, le sous-espace propre $E_\lambda[Q(U)]$ n'est autre que la somme directe des sous-espaces propres $E_\mu(U)$ tels que $Q(\mu) = \lambda$. De plus,

$$(3) \quad Q(U) = \sum_{\mu \in \text{sp}(U)} Q(\mu)P_\mu.$$

En effet, tout vecteur \mathfrak{x} de E peut s'écrire sous la forme

$$\mathfrak{x} = \sum_{\mu \in \text{sp}(U)} \mathfrak{x}_\mu,$$

où, pour tout $\mu \in \text{sp}(U)$, \mathfrak{x}_μ appartient à $E_\mu(U)$. Le théorème de Hilbert-Dirac montre que $Q(U)(\mathfrak{x}_\mu) = Q(\mu)\mathfrak{x}_\mu$; de plus, par définition de P_μ , $P_\mu(\mathfrak{x}) = \mathfrak{x}_\mu$. Il en découle aussitôt que

$$Q(U)(\mathfrak{x}) = \sum_{\mu \in \text{sp}(U)} Q(\mu)P_\mu(\mathfrak{x}),$$

ce qui prouve la formule (3).

3. STRUCTURE DES SOUS-ESPACES VECTORIELS STABLES

THÉORÈME 5.5. — Structure des sous-espaces vectoriels stables. — *Soient U un endomorphisme d'un espace vectoriel E sur K , G un sous-espace vectoriel de E stable par U , et V l'endomorphisme de G coïncidant avec U .*

1. *Le spectre de V est constitué des éléments λ du spectre de U tels que $G \cap F_\lambda(U)$ ne soit pas réduit à $\{0\}$, ou encore tels que $G \cap E_\lambda(U)$ ne soit pas réduit à $\{0\}$. Pour toute valeur propre λ de V , le sous-espace spectral $F_\lambda(V)$ n'est autre que $G \cap F_\lambda(U)$, et le sous-espace propre $E_\lambda(V)$ n'est autre que $G \cap E_\lambda(U)$.*

2. *Si U est scindé sur K , il en est de même de V , et le sous-espace vectoriel G est somme directe de ses intersections avec les sous-espaces spectraux $F_\lambda(U)$:*

$$(1) \quad G = \bigoplus_{\lambda \in \text{sp}(U)} G \cap F_\lambda(U).$$

3. *Si U est diagonalisable sur K , il en est de même de V , et le sous-espace vectoriel G est somme directe de ses intersections avec les sous-espaces propres $E_\lambda(U)$:*

$$(2) \quad G = \bigoplus_{\lambda \in \text{sp}(U)} G \cap E_\lambda(U).$$

Ainsi, lorsque U est diagonalisable, tout sous-espace vectoriel stable G est somme directe de sous-espaces vectoriels G_λ des sous-espaces propres $E_\lambda(U)$; réciproquement, si pour tout élément λ de $\text{sp}(U)$ on considère un sous-espace vectoriel G_λ de $E_\lambda(U)$, la somme directe des sous-espaces G_λ est stable par U .

L'assertion 1 est immédiate.

Assertion 2. — Supposons que U soit scindé sur K . Grâce au théorème de caractérisation des endomorphismes scindés (cf. th. 5.3), nous voyons que V est scindé sur K . Cela signifie que

$$G = \bigoplus_{\lambda \in \text{sp}(V)} F_{\lambda}(V).$$

La formule (1) en découle, vu l'assertion 1.

Assertion 3. — Supposons que U soit diagonalisable sur K . Grâce au théorème de caractérisation des endomorphismes diagonalisables (cf. th. 5.4), nous voyons que V est diagonalisable sur K . Cela signifie que

$$G = \bigoplus_{\lambda \in \text{sp}(V)} E_{\lambda}(V).$$

La formule (2) en découle, vu l'assertion 1.

Nous allons appliquer ce théorème à l'étude de l'existence de sous-espaces vectoriels stables supplémentaires d'un sous-espace vectoriel stable :

DÉFINITION 5.9. — Endomorphismes semi-simples. — *On dit qu'un endomorphisme U d'un espace vectoriel E sur K est semi-simple si, pour tout sous-espace vectoriel F de E stable par U , il existe un sous-espace vectoriel G supplémentaire de F dans E stable par U .*

PROPOSITION 5.11. — Caractérisation des endomorphismes semi-simples. — *Soient E un espace vectoriel de dimension finie sur K et U un endomorphisme de E . Pour que U soit diagonalisable sur K , il faut et il suffit que U soit semi-simple et scindé sur K .*

En particulier, si K est algébriquement clos, les notions d'endomorphisme diagonalisable et d'endomorphisme semi-simple coïncident.

Supposons d'abord que U soit diagonalisable sur K , et considérons un sous-espace vectoriel F de E stable par U . D'après le théorème de structure des sous-espaces vectoriels stables (cf. th. 5.5),

$$F = \bigoplus_{\lambda \in \text{sp}(U)} F \cap E_{\lambda}(U).$$

Pour tout élément λ de $\text{sp}(U)$, considérons un sous-espace vectoriel G_{λ} supplémentaire de $F \cap E_{\lambda}(U)$ dans $E_{\lambda}(U)$. Il est clair que $G = \bigoplus_{\lambda \in \text{sp}(U)} G_{\lambda}$ est un sous-espace vectoriel de E stable par U , et que $E = F \oplus G$.

Réciproquement, supposons que U soit semi-simple et scindé sur K . Il est clair que le sous-espace vectoriel $F = \bigoplus_{\lambda \in \text{sp}(U)} E_{\lambda}(U)$ est stable par U . Le sous-espace vectoriel F admet donc un sous-espace vectoriel supplémentaire G stable par U . Supposons par l'absurde que G ne soit pas réduit à $\{0\}$. Puisque U est

scindé sur K , l'endomorphisme V de G coïncidant avec U est scindé sur K (cf. th. 5.5). Puisque $G \neq \{0\}$, le spectre de V dans K n'est pas vide. Soit λ_0 un élément de $\text{sp}(U)$; le sous-espace vectoriel E_{λ_0} est non réduit à $\{0\}$, il est contenu dans G , et dans F , ce qui contredit la relation $E = F \oplus G$.

REMARQUE 1. — Il est inutile de supposer que E est de dimension finie sur K . La même démonstration s'applique, mais, cette fois, l'existence de sous-espaces vectoriels supplémentaires est assurée par l'exercice I.3.3.

REMARQUE 2. — Lorsque le corps K n'est pas algébriquement clos, il faut se garder de croire que tout endomorphisme semi-simple soit diagonalisable sur K . Considérons par exemple l'endomorphisme U de \mathbf{R}^2 canoniquement associé à la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Les seuls sous-espaces vectoriels de \mathbf{R}^2 stables par U sont $\{0\}$ et \mathbf{R}^2 : en effet, s'il existait une droite D stable par U , il existerait un élément λ de \mathbf{R} et un élément non nul x de D tels que $U(x) = \lambda x$, ce qui est absurde puisque le spectre de U dans \mathbf{R} est vide. L'endomorphisme U est donc semi-simple; néanmoins, il n'est pas scindé sur \mathbf{R} .

On trouvera plus loin (cf. th. 5.17) une caractérisation des endomorphismes semi-simples sur un corps quelconque.

Exercices conseillés : 17 à 30.

B. CAS DE LA DIMENSION FINIE

§ 4. RÉDUCTION DES ENDOMORPHISMES, EN DIMENSION FINIE

1. CONSÉQUENCES DE LA THÉORIE GÉNÉRALE

Tout endomorphisme d'un espace vectoriel de dimension finie admet un polynôme minimal (cf. prop. 5.2), ce qui permet de renforcer le corollaire du théorème de Hilbert-Dirac de la manière suivante :

THÉORÈME 5.6. — **Spectre d'un endomorphisme, en dimension finie.** — Soit U un endomorphisme d'un espace vectoriel E de dimension finie n sur K .

1. Le spectre de U dans K est un ensemble fini, dont le cardinal est inférieur ou égal à n ; il est constitué des racines dans K du polynôme minimal π de U .

2. Toute valeur propre λ de U est d'indice fini, et cet indice $n(\lambda)$ n'est autre que la multiplicité de la racine λ du polynôme π ; de plus, $n(\lambda)$ est inférieur ou égal à la dimension du sous-espace spectral F_λ de U associé à la valeur propre λ . Enfin,

$$(1) \quad \sum_{\lambda \in \text{sp}(U)} n(\lambda) \leq \sum_{\lambda \in \text{sp}(U)} \dim F_\lambda \leq n.$$

3. Soit λ une valeur propre de U d'indice p ; le sous-espace vectoriel spectral $F_\lambda = \text{Ker} [(U - \lambda I_E)^p]$ et le sous-espace vectoriel $F'_\lambda = \text{Im} [(U - \lambda I_E)^p]$ sont supplémentaires dans E .

Assertions 1 et 2. — Puisque $\pi(U) = 0$, il résulte du théorème de Hilbert-Dirac que toute valeur propre de U est racine de π .

Réciproquement, considérons une racine λ de π , et désignons par p sa multiplicité. Le polynôme π s'écrit donc sous la forme

$$\pi(X) = (X - \lambda)^p Q(X),$$

où Q est un polynôme unitaire, premier avec $X - \lambda$. Introduisons enfin, pour tout entier naturel r , le noyau $E_{\lambda,r}$ de l'endomorphisme $(U - \lambda I_E)^r$. Lorsque $r \geq p$, le P. G. C. D. de $(X - \lambda)^r$ et de π est égal à $(X - \lambda)^p$. D'après l'assertion 1 du théorème 5.1, le sous-espace vectoriel $E_{\lambda,r}$ est égal au noyau de $(U - \lambda I_E)^p$, c'est-à-dire à $E_{\lambda,p}$. Ainsi, pour tout entier $r \geq p$, $E_{\lambda,r} = F_\lambda$. L'ensemble des entiers naturels r tels que $E_{\lambda,r} = F_\lambda$ admet donc un plus petit élément q , et q est inférieur ou égal à p .

Considérons alors le polynôme $\pi' = (X - \lambda)^q Q(X)$. D'après le théorème de décomposition des noyaux,

$$\text{Ker} [\pi'(U)] = E_{\lambda,q} \oplus \text{Ker} [Q(U)],$$

et

$$E = \text{Ker} [\pi(U)] = E_{\lambda,p} \oplus \text{Ker} [Q(U)].$$

Or, $E_{\lambda,q} = E_{\lambda,p} = F_\lambda$. Il s'ensuit que $\text{Ker} [\pi'(U)] = E$, c'est-à-dire que $\pi'(U) = 0$. Comme π est le polynôme minimal de U , cela implique que π divise π' ; par suite p est inférieur ou égal à q .

Finalement, $q = p$. Comme p est strictement positif, λ est une valeur propre de U . D'après la définition de q , cette valeur propre est d'indice fini égal à q .

Enfin, d'après le corollaire 2 de la proposition 5.8, la somme F des sous-espaces spectraux F_λ est directe; d'où il découle que

$$\sum_{\lambda \in \text{sp}(U)} \dim F_\lambda = \dim F \leq \dim E = n,$$

ce qui achève la démonstration des assertions 1 et 2.

L'assertion 3 résulte alors aussitôt du théorème fondamental de l'algèbre linéaire (cf. th. 5.1).

COROLLAIRE. — Caractérisation des valeurs propres d'indice 1. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , et λ un scalaire. Il est équivalent de dire :

1. Le scalaire λ est une valeur propre de U , et le sous-espace propre E_λ de U associé à λ est égal au sous-espace spectral F_λ de U associé à λ .

2. Le scalaire λ est une racine simple du polynôme minimal de U .

Le théorème de caractérisation des endomorphismes scindés (cf. th. 5.3) fournit l'énoncé suivant :

THÉORÈME 5.7. — Caractérisation des endomorphismes scindés, en dimension finie. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie n sur K . Il est équivalent de dire :

1. L'endomorphisme U est scindé sur K ; autrement dit, E est somme directe des sous-espaces spectraux F_λ de U , où λ parcourt le spectre de U dans K .
2. Le polynôme minimal de U est scindé sur K .
3. Il existe un polynôme Q non nul scindé sur K tel que $Q(U) = 0$.
4. Il existe une famille $(\mu_i)_{i \in I}$ de scalaires et une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels de E stables par U , telles que E soit somme directe des sous-espaces vectoriels F_i , et que, pour tout $i \in I$, l'endomorphisme de F_i coïncidant avec $U - \mu_i I_E$ soit nilpotent.

En outre, si ces conditions équivalentes sont satisfaites :

- a) Les projecteurs spectraux P_λ de l'endomorphisme U sont des polynômes en U .
- b) La décomposition en facteurs irréductibles sur K du polynôme minimal π de U est donnée par la formule suivante :

$$(1) \quad \pi(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda)^{n(\lambda)},$$

où $n(\lambda)$ désigne l'indice de la valeur propre λ de U .

- c) Le polynôme minimal π_λ de l'endomorphisme U_λ de F_λ coïncidant avec U n'est autre que $(X - \lambda)^{n(\lambda)}$.

En particulier, tout endomorphisme d'un espace vectoriel de dimension finie sur un corps algébriquement clos est scindé.

$1 \Rightarrow 4$ est évident.

$4 \Rightarrow 3$: par hypothèse, pour tout $i \in I$, il existe un entier naturel n_i tel que l'endomorphisme de F_i coïncidant avec $(U - \mu_i I_E)^{n_i}$ soit nul. Considérons le polynôme

$$Q(X) = \prod_{i \in I} (X - \mu_i)^{n_i};$$

ce polynôme est scindé sur K , et il est immédiat que, pour tout $i \in I$, la restriction de $Q(U)$ à F_i est nulle. Comme E est somme directe des sous-espaces vectoriels F_i , il en découle que $Q(U) = 0$, ce qu'il fallait prouver.

$3 \Rightarrow 2$: en effet, tout polynôme à coefficients dans K divisant un polynôme scindé sur K est lui-même scindé sur K .

$2 \Rightarrow 1$ découle du théorème 5.3.

Les assertions a) et b) résultent respectivement du corollaire 2 du théorème 5.1 et du théorème 5.6.

c) Nous savons que $F_\lambda = \text{Ker} [(U - \lambda I_E)^{n(\lambda)}]$. Donc $(U_\lambda - \lambda I_{F_\lambda})^{n(\lambda)} = 0$, ce qui montre que π_λ divise $(X - \lambda)^{n(\lambda)}$. Or, d'après la définition de $n(\lambda)$, pour tout entier $p < n(\lambda)$, $(U_\lambda - \lambda I_{F_\lambda})^p \neq 0$; il en découle que $\pi_\lambda = (X - \lambda)^{n(\lambda)}$.

REMARQUE 1. — Soit U un endomorphisme scindé sur K . Choisissons pour tout $\lambda \in \text{sp}(U)$ une base B_λ du sous-espace spectral F_λ de U . Alors la matrice $M_B(U)$ associée à l'endomorphisme U dans la base $B = \bigcup_{\lambda \in \text{sp}(U)} B_\lambda$ est décomposée en blocs diagonaux M_λ . De plus, pour toute valeur propre λ de U , la matrice $M_\lambda - \lambda I_{m(\lambda)}$, où $m(\lambda)$ désigne la dimension de F_λ , est nilpotente.

Nous verrons plus loin qu'en choisissant convenablement les bases B_λ , on peut donner aux matrices M_λ une forme particulièrement simple.

REMARQUE 2. — Lorsque la somme des indices $n(\lambda)$ des valeurs propres de U est égale à n , l'endomorphisme U est scindé sur K ; cela résulte aussitôt du théorème 5.6.

De même, le théorème de caractérisation des endomorphismes diagonalisables (cf. th. 5.4) fournit l'énoncé suivant :

THÉORÈME 5.8. — Caractérisation des endomorphismes diagonalisables, en dimension finie. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie n sur K . Il est équivalent de dire :

1. L'endomorphisme U est diagonalisable sur K ; autrement dit, E est somme directe des sous-espaces propres E_λ de U , où λ parcourt le spectre de U dans K .
2. Le polynôme minimal de U est scindé sur K , et toutes ses racines sont simples.
3. L'endomorphisme U est scindé sur K , et il est lié à ses projecteurs spectraux P_λ par la formule

$$(1) \quad U = \sum_{\lambda \in \text{sp}(U)} \lambda P_\lambda.$$

4. Il existe un polynôme Q non nul scindé sur K , ayant toutes ses racines simples et tel que $Q(U) = 0$.

5. Il existe une famille $(\mu_i)_{i \in I}$ de scalaires et une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels de E stables par U telles que E soit somme directe des sous-espaces vectoriels F_i et que, pour tout $i \in I$, l'endomorphisme de F_i coïncidant avec U soit l'homothétie de rapport μ_i .

6. Il existe une famille $(\mu_i)_{i \in I}$ de scalaires et un système $(P_i)_{i \in I}$ de projecteurs de E telles que

$$(2) \quad U = \sum_{i \in I} \mu_i P_i.$$

7. Il existe une base de E constituée de vecteurs propres de U .

8. Il existe une base de E dans laquelle la matrice associée à U est diagonale.

En outre, si ces conditions équivalentes sont satisfaites :

a) Les projecteurs spectraux P_λ de l'endomorphisme U sont des polynômes en U . Plus précisément, pour tout élément λ de $\text{sp}(U)$,

$$(3) \quad P_\lambda = Q_\lambda(U),$$

où

$$Q_\lambda = \frac{\prod_{\mu \neq \lambda} (X - \mu)}{\prod_{\mu \neq \lambda} (\lambda - \mu)}.$$

b) La décomposition en facteurs irréductibles sur K du polynôme minimal π de U est donnée par la formule suivante :

$$(4) \quad \pi(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda).$$

En particulier, lorsque K est algébriquement clos, un endomorphisme de E est diagonalisable si et seulement si les racines de son polynôme minimal sont simples.

L'équivalence des conditions 1, 3, 4, 5, 6, 7 et 8 résulte aussitôt du théorème de caractérisation des endomorphismes diagonalisables (cf. th. 5.4).

Il est d'autre part évident que $2 \Leftrightarrow 4$.

Les assertions a) et b) découlent alors des assertions correspondantes du théorème 5.7; enfin, pour établir la formule (3), il suffit de noter que, pour tout élément Q de $K[X]$,

$$Q(U) = \sum_{\lambda \in \text{sp}(U)} Q(\lambda) P_\lambda$$

(cf. cor. 3 de la prop. 5.10) et d'appliquer cette formule au polynôme Q_λ .

REMARQUE 1. — Plus généralement, on peut calculer les projecteurs spectraux d'un endomorphisme scindé grâce aux polynômes d'interpolation de Lagrange-Sylvester; cf. exercice 20.

REMARQUE 2. — Une base $B = (e_1, e_2, \dots, e_n)$ de E est constituée de vecteurs propres de U si et seulement si la matrice $M_B(U)$ est de la forme

$$M_B(U) = \begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_i & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Alors le spectre de U est constitué des scalaires λ_i , et, pour tout élément λ de $\text{sp}(U)$, le sous-espace propre E_λ de U associé à λ admet pour base B_λ l'ensemble des vecteurs e_i tels que $\lambda_i = \lambda$.

COROLLAIRE. — Cas où toutes les valeurs propres sont simples. — Soit U un endomorphisme d'un espace vectoriel E de dimension n sur K , admettant n valeurs propres $\lambda_1, \lambda_2, \dots, \lambda_n$ distinctes deux à deux. Alors U est diagonalisable sur K , et tous ses sous-espaces propres sont de dimension 1. De plus le polynôme minimal π de U est donné par la formule

$$(1) \quad \pi(X) = \prod_{i=1}^n (X - \lambda_i).$$

Considérons en effet, pour tout $i \in [1, n]$, un vecteur propre x_i associé à la valeur propre λ_i . D'après le corollaire 1 de la proposition 5.8, ces vecteurs sont linéairement indépendants; étant au nombre de n , ils constituent une base B de E . L'endomorphisme U est donc diagonalisable sur K , et le polynôme minimal π de U est donné par la formule (1). Comme E est somme directe des droites Kx_i , où i parcourt $[1, n]$, le théorème de caractérisation des sous-espaces propres (cf. prop. 5.10) s'applique, et montre que le sous-espace propre de U associé à la valeur propre λ_i n'est autre que Kx_i .

EXEMPLE. — Symétries. — On se propose d'étudier les endomorphismes U d'un espace vectoriel E de dimension finie sur K tels que $U^2 = I_E$.

a) Lorsque K est de caractéristique différente de 2, le polynôme $Q(X) = X^2 - 1$ est un polynôme scindé sur K , ayant deux racines simples, à savoir 1 et -1 . L'endomorphisme U est donc diagonalisable sur K . Désignons par E_1 le noyau de $U - I_E$, et par E_{-1} le noyau de $U + I_E$; soient P_1 et P_{-1} les projecteurs associés à la décomposition en somme directe $E = E_1 \oplus E_{-1}$. Nous savons que $U = P_1 - P_{-1}$; il en résulte aussitôt que

$$P_1 = \frac{1}{2}(I_E + U) \quad \text{et} \quad P_{-1} = \frac{1}{2}(I_E - U).$$

L'endomorphisme U n'est autre que la symétrie par rapport au sous-espace vectoriel E_1 parallèlement au sous-espace vectoriel E_{-1} .

Les valeurs propres éventuelles de U sont 1 et -1 ; trois cas peuvent se présenter :

- le sous-espace vectoriel E_{-1} est réduit à $\{0\}$; alors $U = I_E$;
- le sous-espace vectoriel E_1 est réduit à $\{0\}$; alors $U = -I_E$;
- les scalaires 1 et -1 sont valeurs propres de U , les sous-espaces propres associés étant E_1 et E_{-1} .

Dans le premier cas, le polynôme minimal π de U est égale à $X - 1$; dans le deuxième cas, il est égal à $X + 1$, et dans le troisième, à $X^2 - 1$.

b) Lorsque K est de caractéristique 2, la situation est très différente : en effet, le polynôme Q est scindé sur K , mais il admet 1 comme racine double. L'endomorphisme U est scindé sur K , et il admet 1 comme unique valeur propre.

De plus, $(U - I_E)^2 = 0$; l'indice de la valeur propre 1 est donc inférieur ou égal à 2. Deux cas se présentent donc :

- la valeur propre 1 est d'indice 1; alors $U = I_E$;
- la valeur propre 1 est d'indice 2; l'endomorphisme U n'est pas diagonalisable.

Le deuxième cas se rencontre dans l'exemple suivant : $E = K^2$, et U est l'endomorphisme de K^2 canoniquement associé à la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Dans le premier cas, le polynôme minimal π de U est égal à $X - 1$; dans le deuxième cas, il est égal à $X^2 - 1 = (X - 1)^2$.

PROPOSITION 5.12. — Spectre du transposé d'un endomorphisme. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K .

1. Le polynôme minimal de l'endomorphisme tU transposé de U n'est autre que le polynôme minimal de U .
2. Le spectre de tU est égal au spectre de U , et, pour tout élément λ de $\text{sp}(U)$, λ a même indice pour U et tU .
3. Pour que U soit scindé (resp. diagonalisable), il faut et il suffit que tU soit scindé (resp. diagonalisable).

L'assertion 1 est immédiate, puisque, pour tout élément P de $K[X]$, ${}^tP(U) = P({}^tU)$.

L'assertion 2 en découle aussitôt, grâce au théorème 5.6, ainsi que l'assertion 3, grâce au théorème de caractérisation des endomorphismes scindés (resp. diagonalisables) (cf. th. 5.7 et 5.8).

THÉORÈME 5.9. — Calcul fonctionnel sur les endomorphismes diagonalisables. — Soit U un endomorphisme diagonalisable d'un espace vectoriel E de dimension finie sur K . On désigne par $\mathcal{F}[\text{sp}(U)]$ l'algèbre unitaire des applications de $\text{sp}(U)$ dans K , et par j l'injection canonique de $\text{sp}(U)$ dans K .

1. Il existe un morphisme φ et un seul de l'algèbre unitaire $\mathcal{F}[\text{sp}(U)]$ dans l'algèbre unitaire $\mathcal{L}(E)$ tel que $\varphi(j) = U$. Plus précisément, soit

$$(1) \quad U = \sum_{\lambda \in \text{sp}(U)} \lambda P_\lambda$$

la décomposition spectrale de U . Alors, pour tout élément f de $\mathcal{F}[\text{sp}(U)]$,

$$(2) \quad \varphi(f) = \sum_{\lambda \in \text{sp}(U)} f(\lambda) P_\lambda.$$

2. Le morphisme φ est injectif, et son image n'est autre que la sous-algèbre unitaire de $\mathcal{L}(E)$ engendrée par U .

3. Soient P un élément de $K[X]$ et f la fonction polynomiale sur $\text{sp}(U)$ définie par P . Alors

$$(3) \quad \varphi(f) = P(U).$$

C'est pourquoi, dans le cas général, l'endomorphisme $\varphi(f)$ se note $f(U)$. Les propriétés du morphisme φ se traduisent alors de la manière suivante :

a) Pour tout élément f de $\mathcal{F}[\text{sp}(U)]$, $f(U)$ est un endomorphisme diagonalisable, et

$$(2') \quad f(U) = \sum_{\lambda \in \text{sp}(U)} f(\lambda)P_\lambda.$$

b) L'application $f \mapsto f(U)$ est un morphisme injectif de l'algèbre unitaire $\mathcal{F}[\text{sp}(U)]$ dans l'algèbre unitaire $\mathcal{L}(E)$, dont l'image est constituée des polynômes en U .

4. Pour tout élément f de $\mathcal{F}[\text{sp}(U)]$, le spectre de $f(U)$ est constitué des scalaires $f(\lambda)$, où λ parcourt $\text{sp}(U)$. De plus, pour toute valeur propre μ de $f(U)$,

$$(4) \quad E_\mu[f(U)] = \bigoplus_{f(\lambda)=\mu} E_\lambda(U).$$

5. Pour tout élément f de $\mathcal{F}[\text{sp}(U)]$ et pour tout élément g de $\mathcal{F}[f(\text{sp}(U))]$,

$$(5) \quad g[f(U)] = (g \circ f)(U).$$

6. Pour tout élément f de $\mathcal{F}[\text{sp}(U)]$,

$$(6) \quad f({}^tU) = {}^t[f(U)].$$

Assertion 1. — Unicité de φ . — Soit φ un morphisme de l'algèbre unitaire $\mathcal{F}[\text{sp}(U)]$ dans l'algèbre unitaire $\mathcal{L}(E)$ tel que $\varphi(j) = U$. Pour tout élément λ de $\text{sp}(U)$, désignons par χ_λ l'élément de $\mathcal{F}[\text{sp}(U)]$ défini par les relations

$$\begin{aligned} \chi_\lambda(\mu) &= 1 & \text{si } \mu &= \lambda, \\ \chi_\lambda(\mu) &= 0 & \text{si } \mu &\neq \lambda. \end{aligned}$$

Comme l'ensemble $\text{sp}(U)$ est fini, la famille $(\chi_\lambda)_{\lambda \in \text{sp}(U)}$ est une base de l'espace vectoriel $\mathcal{F}[\text{sp}(U)]$. Plus précisément, pour tout élément f de $\mathcal{F}[\text{sp}(U)]$,

$$f = \sum_{\lambda \in \text{sp}(U)} f(\lambda)\chi_\lambda.$$

Puisque φ est linéaire, nous en déduisons que

$$(7) \quad \varphi(f) = \sum_{\lambda \in \text{sp}(U)} f(\lambda)\varphi(\chi_\lambda).$$

Pour calculer $\varphi(\chi_\lambda)$, considérons, pour tout élément λ de $\text{sp}(U)$, le polynôme d'interpolation de Lagrange Q_λ défini par la relation

$$Q_\lambda(X) = \frac{\prod_{\mu \neq \lambda} (X - \mu)}{\prod_{\mu \neq \lambda} (\lambda - \mu)}.$$

Pour tout élément μ de $\text{sp}(U)$, $\chi_\lambda(\mu) = Q_\lambda(\mu)$; autrement dit, $\chi_\lambda = Q_\lambda(j)$. Puisque φ est un morphisme d'algèbres unitaires, il en résulte que

$$\varphi(\chi_\lambda) = \varphi[Q_\lambda(j)] = Q_\lambda[\varphi(j)] = Q_\lambda(U).$$

Or, nous savons que $Q_\lambda(U) = P_\lambda$. Finalement,

$$(8) \quad \varphi(\chi_\lambda) = P_\lambda.$$

Des formules (7) et (8), il découle que $\varphi(f)$ est nécessairement donné par la formule (2), ce qui prouve l'unicité de φ .

Existence de φ . — L'application φ définie par la formule (2) convient, car les projecteurs spectraux P_λ constituent un système de projecteurs.

Assertions 2 et 3. — La relation (2) montre que le morphisme φ est injectif, car il est immédiat que les projecteurs spectraux P_λ sont linéairement indépendants dans $\mathfrak{L}(E)$; elle montre aussi que, pour tout élément f de $\mathcal{F}[\text{sp}(U)]$, l'endomorphisme $\varphi(f)$ est un polynôme en U puisque, pour tout $\lambda \in \text{sp}(U)$, P_λ est un polynôme en U . Réciproquement, soient Q un élément de $K[X]$ et f l'application de $\text{sp}(U)$ dans K définie par la formule $f(\mu) = Q(\mu)$. Alors

$$\varphi(f) = \sum_{\lambda \in \text{sp}(U)} Q(\lambda) P_\lambda = Q(U).$$

L'assertion 4 découle aussitôt de la formule (2) et de la proposition 5.10.

Assertion 5. — Les applications $g \mapsto g[f(U)]$ et $g \mapsto (g \circ f)(U)$ sont deux morphismes de l'algèbre unitaire $\mathcal{F}[f(\text{sp}(U))]$ dans l'algèbre unitaire $\mathfrak{L}(E)$ prenant la même valeur, à savoir $f(U)$, lorsque g est l'injection canonique de $f[\text{sp}(U)]$ dans K . L'assertion 1 montre que ces deux morphismes sont égaux, ce qu'il fallait prouver.

Assertion 6. — Nous savons (cf. prop. 5.12) que $\text{sp}({}^tU) = \text{sp}(U)$. Soit f un élément de $\mathcal{F}[\text{sp}(U)]$; il existe un élément Q de $K[X]$ tel que f soit la fonction polynomiale sur $\text{sp}(U)$ associée à Q . Il en découle que

$$f({}^tU) = Q({}^tU) = {}^t[Q(U)] = {}^t[f(U)].$$

On trouvera esquissé dans l'exercice 65 le calcul fonctionnel sur les endomorphismes scindés, dans le cas où les fonctions considérées sont rationnelles.

2. POLYNÔME CARACTÉRISTIQUE D'UN ENDOMORPHISME

Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur un corps K , et λ un élément de K . Nous savons que λ est une valeur propre de U si et seulement si l'endomorphisme $U - \lambda I_E$ n'est pas inversible. D'après le corollaire 1 du théorème 3.5, cela revient à dire que le scalaire $\text{Det}(\lambda I_E - U)$ est nul. Nous sommes donc amené à étudier la fonction $\lambda \mapsto \text{Det}(\lambda I_E - U)$; plus précisément, nous allons montrer que cette fonction est une fonction polynomiale.

Considérons d'abord une matrice carrée $M = (\alpha_{ij})$ d'ordre n à éléments dans K , et introduisons le corps $K(X)$ des fractions rationnelles à une indéterminée à coefficients dans K . La formule du développement du déterminant d'une matrice carrée (cf. § 3.2) montre que le déterminant de la matrice carrée $XI_n - M$, considérée comme élément de $M_n[K(X)]$, est un élément de $K[X]$.

DÉFINITION 5.10. — Polynôme caractéristique d'une matrice carrée. — *Le polynôme $\text{Det}(XI_n - M)$ est appelé polynôme caractéristique de la matrice M ; on le note δ_M :*

$$\delta_M(X) = \begin{vmatrix} X - \alpha_{11} & -\alpha_{12} & \dots & -\alpha_{1i} & \dots & -\alpha_{1n} \\ -\alpha_{21} & X - \alpha_{22} & \dots & -\alpha_{2i} & \dots & -\alpha_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ -\alpha_{i1} & -\alpha_{i2} & \dots & X - \alpha_{ii} & \dots & -\alpha_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ -\alpha_{n1} & -\alpha_{n2} & \dots & -\alpha_{ni} & \dots & X - \alpha_{nn} \end{vmatrix}.$$

En outre, ce polynôme est unitaire et de degré n ; il peut donc s'écrire sous la forme :

$$\delta_M(X) = X^n - \sigma_1(M)X^{n-1} + \dots + (-1)^p \sigma_p(M)X^{n-p} + \dots + (-1)^n \sigma_n(M),$$

où, pour tout $p \in [1, n]$, $\sigma_p(M) \in K$. De plus, l'application σ_p est une fonction polynomiale homogène de degré p des éléments α_{ij} de la matrice M .

En particulier,

$$\sigma_1(M) = \text{Tr } M$$

$$\sigma_n(M) = \text{Det } M.$$

PROPOSITION 5.13. — Polynôme caractéristique d'un endomorphisme. — *Soient U un endomorphisme d'un espace vectoriel E de dimension finie n sur K , B une base de E , et $M_B(U)$ la matrice associée à U dans cette base.*

Alors le polynôme $\text{Det}[XI_n - M_B(U)]$ est indépendant de la base B ; on l'appelle polynôme caractéristique de l'endomorphisme U , et on le note δ_U , ou plus simplement δ , lorsque aucune confusion n'est à craindre. On le note encore $\text{Det}(XI_E - U)$.

Les scalaires $\sigma_p[M_B(U)]$ sont indépendants de B ; on les note $\sigma_p(U)$.

Soient en effet B' une autre base de E , et P la matrice de passage de B à B' . Les matrices $M_B(U)$ et $M_{B'}(U)$ sont donc liées par la relation

$$M_{B'}(U) = P^{-1} M_B(U) P.$$

Il en découle que

$$XI_n - M_{B'}(U) = P^{-1} [XI_n - M_B(U)] P.$$

Donc

$$\text{Det} [XI_n - M_{B'}(U)] = \text{Det} (P^{-1}) \cdot \text{Det} [XI_n - M_B(U)] \cdot \text{Det} P = \text{Det} [XI_n - M_B(U)],$$

ce qu'il fallait prouver.

Les résultats précédents s'énoncent alors sous la forme suivante :

PROPOSITION 5.14. — Propriétés du polynôme caractéristique d'un endomorphisme. — *Soit U un endomorphisme d'un espace vectoriel E de dimension finie non nulle n sur K .*

1. *Le polynôme caractéristique δ_U de U est un polynôme unitaire de degré n à coefficients dans K ; il est donné par la formule*

$$(1) \quad \delta_U(X) = X^n - \sigma_1(U)X^{n-1} + \dots + (-1)^p \sigma_p(U)X^{n-p} + \dots + (-1)^n \sigma_n(U)$$

De plus,

$$(2) \quad \sigma_1(U) = \text{Tr } U,$$

$$(3) \quad \sigma_n(U) = \text{Det } U.$$

2. *Pour tout élément α de K ,*

$$(4) \quad \delta_U(\alpha) = \text{Det} (\alpha I_E - U).$$

3. *Le spectre de U dans K est constitué des racines dans K du polynôme caractéristique de U .*

Pour toute valeur propre λ de U dans K , la multiplicité $m(\lambda)$ de la racine λ du polynôme δ_U s'appelle multiplicité de la valeur propre λ .

4. *Lorsque le polynôme caractéristique de U est scindé sur K , la décomposition de δ_U en facteurs irréductibles sur K est donnée par la formule*

$$(5) \quad \delta_U(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda)^{m(\lambda)}.$$

Soit donc $(\lambda_1, \lambda_2, \dots, \lambda_n)$ une suite d'éléments de $\text{sp}(U)$ possédant la propriété suivante : pour tout élément λ de $\text{sp}(U)$, le cardinal de l'ensemble des éléments j de $[1, n]$ tels que $\lambda_j = \lambda$ est égal à $m(\lambda)$. La relation (5) s'écrit encore

$$(5') \quad \delta_U(X) = \prod_{j=1}^n (X - \lambda_j).$$

Par suite, pour tout entier $p \in [1, n]$,

$$(6) \quad \sigma_p(U) = S_p(\lambda_1, \lambda_2, \dots, \lambda_n),$$

où $S_p(X_1, X_2, \dots, X_n)$ désigne le $p^{\text{ième}}$ polynôme symétrique élémentaire à n indéterminées.

En particulier,

$$(7) \quad \sigma_1(U) = \sum_{j=1}^n \lambda_j,$$

$$(8) \quad \sigma_n(U) = \prod_{j=1}^n \lambda_j.$$

PROPOSITION 5.15. — Polynôme caractéristique de la restriction d'un endomorphisme à un sous-espace stable. — Soient E un espace vectoriel de dimension finie sur K , et U un endomorphisme de E . Soient d'autre part F un sous-espace vectoriel de E stable par U , et G un supplémentaire de F . On désigne par P_F et P_G les projecteurs associés à la décomposition $E = F \oplus G$, par U_1 l'endomorphisme de F coïncidant avec U , et par U_2 l'endomorphisme de G défini par la formule $U_2(z) = P_G \circ U(z)$, pour tout vecteur z appartenant à G . Alors

$$\delta_U = \delta_{U_1} \cdot \delta_{U_2}.$$

Choisissons une base $B_1 = (e_1, e_2, \dots, e_p)$ de F , et une base $B_2 = (e_{p+1}, e_{p+2}, \dots, e_n)$ de G . Alors $B = (e_1, e_2, \dots, e_n)$ est une base de E . Puisque U laisse stable F , il résulte de la proposition I.3.65 que la matrice $M_B(U)$ associée à U dans la base B s'écrit

$$M_B(U) = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

où $A \in M_p(K)$, $D \in M_{n-p}(K)$, et $B \in M_{p, n-p}(K)$. De plus, la matrice A n'est autre que $M_{B_1}(U_1)$ et la matrice D n'est autre que $M_{B_2}(U_2)$.

Le résultat annoncé provient de la formule

$$\text{Det} \begin{pmatrix} XI_p - A & -B \\ 0 & XI_{n-p} - D \end{pmatrix} = \text{Det}(XI_p - A) \cdot \text{Det}(XI_{n-p} - D).$$

COROLLAIRE 1. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , et F un sous-espace vectoriel de E non réduit à $\{0\}$ et stable par U . Alors le polynôme caractéristique de l'endomorphisme de F coïncidant avec U divise celui de U .

COROLLAIRE 2. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Si E est somme directe de sous-espaces vectoriels F_1, F_2, \dots, F_p non réduits à $\{0\}$ et stables par U , et si l'on désigne par $U_1, U_2, \dots,$

U_p les endomorphismes de ces sous-espaces vectoriels coïncidant avec U , alors le polynôme caractéristique de l'endomorphisme U est le produit des polynômes caractéristiques des endomorphismes U_i :

$$\delta_U = \prod_{i=1}^p \delta_{U_i}.$$

3. ENDOMORPHISMES TRIGONALISABLES

DÉFINITION 5.11. — Endomorphismes trigonalisables. — On dit qu'un endomorphisme U d'un espace vectoriel E de dimension finie sur K est trigonalisable s'il existe une base de E dans laquelle la matrice M associée à U est trigonale supérieure :

$$M = \begin{pmatrix} \lambda_1 & & & * \\ & \ddots & & \\ & & \lambda_i & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Le polynôme caractéristique de U est alors égal à

$$\delta_U(X) = \text{Det}(XI_n - M) = \prod_{i=1}^n (X - \lambda_i).$$

Ainsi, le spectre de l'endomorphisme U est constitué des scalaires λ_i .

THÉORÈME 5.10. — Caractérisation des endomorphismes trigonalisables. — Soient E un espace vectoriel de dimension finie n sur K , et U un endomorphisme de E . Il est équivalent de dire :

1. L'endomorphisme U est trigonalisable.
2. Il existe une suite croissante $(E_i)_{1 \leq i \leq n}$ de sous-espaces vectoriels de E stables par U tels que, pour tout $i \in [1, n]$, $\dim E_i = i$.
3. L'endomorphisme U est scindé sur K .

$2 \Rightarrow 1$: soit $(E_i)_{1 \leq i \leq n}$ une suite de sous-espaces vectoriels stables par U et tels que, pour tout $i \in [1, n]$, $\dim E_i = i$. Posons $E_0 = \{0\}$. Pour chaque entier i , il existe un élément e_i de E_i n'appartenant pas à E_{i-1} . La famille $(e_1, e_2, \dots, e_i, \dots, e_n)$ est une base de E dans laquelle la matrice associée à U est trigonale supérieure, d'après la proposition I.3.60.

$1 \Rightarrow 3$: soit B une base de E dans laquelle la matrice $M_B(U)$ s'écrit

$$M_B(U) = \begin{pmatrix} \lambda_1 & & & * \\ & \ddots & & \\ & & \lambda_i & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Pour tout $i \in [1, n]$, désignons par E_i le sous-espace vectoriel engendré par e_1, e_2, \dots, e_i , et posons $E_0 = \{0\}$. Comme, pour tout $i \in [1, n]$, $(U - \lambda_i I_E)(E_i)$ est contenu dans E_{i-1} , nous voyons que le polynôme $\delta_U(X) = \prod_{i=1}^n (X - \lambda_i)$ annule l'endomorphisme U . Puisque δ_U est scindé sur K , il en est de même de U (cf. th. 5.7).

$3 \Rightarrow 2$: c'est le point principal de la démonstration. Prouvons-le par récurrence sur la dimension de l'espace vectoriel E . Lorsque E est de dimension 1, l'assertion est évidente. Soit donc n un entier strictement supérieur à 1 ; supposons que l'assertion soit vraie pour tout espace vectoriel F de dimension $n - 1$ et pour tout endomorphisme V de F scindé sur K . Considérons alors un espace vectoriel E de dimension n et un endomorphisme U de E scindé sur K . D'après la proposition 5.12, tU est aussi scindé sur K . Soient λ une valeur propre de tU , et y^* un vecteur propre de tU associé à λ . Le noyau F de la forme linéaire y^* est un hyperplan de E ; de plus, puisque la droite Ky^* est stable par tU , le sous-espace vectoriel F est stable par U . Soit V l'endomorphisme de F coïncidant avec U . Puisque U est scindé sur K , V l'est aussi (cf. th. 5.5). Nous pouvons donc appliquer l'hypothèse de récurrence à l'endomorphisme V de F : il existe une suite croissante $(E_i)_{1 \leq i \leq n-1}$ de sous-espaces vectoriels de F stables par V telle que, pour tout $i \in [1, n - 1]$, $\dim E_i = i$. La suite $(E_1, \dots, E_{n-1}, E_n)$, où $E_n = E$, convient visiblement.

COROLLAIRE 1. — *Soit E un espace vectoriel de dimension finie sur un corps K algébriquement clos. Alors tout endomorphisme de E est trigonalisable.*

COROLLAIRE 2. — Théorème de Hamilton-Cayley. — *Tout endomorphisme U d'un espace vectoriel E de dimension finie sur K annule son polynôme caractéristique. En d'autres termes, le polynôme minimal de U divise le polynôme caractéristique de U .*

Le cas où l'endomorphisme U est scindé sur K a été traité au cours de la démonstration du théorème précédent. Le cas général s'y ramène de la manière suivante :

* Introduisons une base $B = (e_1, e_2, \dots, e_n)$ de E . Soient M la matrice associée à U dans la base B , et $\delta(X) = \text{Det}(XI_n - M)$. Tout revient à prouver que $\delta(M) = 0$. Considérons en effet un corps de rupture K' du polynôme minimal π de U (cf. chap. III.1), la base canonique B' de K'^n , et l'endomorphisme U' de K'^n canoniquement associé à la matrice M . Puisque $\pi(U) = 0$, $\pi(M) = M_B[\pi(U)] = 0$; donc $M_{B'}[\pi(U')] = \pi(M) = 0$. Il s'ensuit que $\pi(U') = 0$; ainsi U' est scindé sur K' , et, par suite, $\delta(U') = 0$, ce qui entraîne aussitôt l'assertion. *

On trouvera d'autres démonstrations du théorème de Hamilton-Cayley dans les exercices 52 et 64.

COROLLAIRE 3. — *Pour toute valeur propre λ d'un endomorphisme U d'un espace vectoriel de dimension finie sur K , l'indice $n(\lambda)$ est inférieur ou égal à la multiplicité $m(\lambda)$.*

En effet, $n(\lambda)$ est la multiplicité de la racine λ du polynôme minimal π , $m(\lambda)$ est celle de la racine λ du polynôme caractéristique δ , et π divise δ , d'après le théorème de Hamilton-Cayley.

COROLLAIRE 4. — **Autre caractérisation des endomorphismes scindés.** — *Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Pour que U soit scindé sur K , il faut et il suffit que le polynôme caractéristique de U soit scindé sur K .*

Ainsi, lorsque U est scindé sur K , le polynôme caractéristique de U est égal à

$$\delta_U(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda)^{m(\lambda)},$$

tandis que le polynôme minimal de U est égal à

$$\pi_U(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda)^{n(\lambda)},$$

où, pour tout $\lambda \in \text{sp}(U)$, $1 \leq n(\lambda) \leq m(\lambda)$.

Si U est scindé sur K , il existe une base de E dans laquelle la matrice M associée à U est trigonale supérieure. Il en résulte aussitôt que $\delta_U(X) = \text{Det}(XI_n - M)$ est scindé sur K .

Supposons réciproquement que δ_U soit scindé sur K . D'après le théorème de Hamilton-Cayley, $\delta_U(U) = 0$; il découle alors du théorème de caractérisation des endomorphismes scindés (cf. th. 5.7) que U est scindé sur K .

COROLLAIRE 5. — **Caractérisation des endomorphismes nilpotents.** — *Soit U un endomorphisme d'un espace vectoriel de dimension finie n sur K . Il est équivalent de dire :*

1. *L'endomorphisme U est nilpotent.*
2. *Il existe une base B de E dans laquelle la matrice associée à U est trigonale supérieure nilpotente.*
3. *Le polynôme caractéristique de U est égal à X^n .*

Si ces conditions sont vérifiées, alors $U^n = 0$.

$1 \Rightarrow 2$: si U est nilpotent, U est scindé sur K ; il existe donc une base de E dans laquelle la matrice M associée à U est trigonale supérieure :

$$M = \begin{pmatrix} \lambda_1 & & & * \\ & \ddots & & \\ & & \lambda_i & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Les scalaires $\lambda_1, \lambda_2, \dots, \lambda_n$ étant les valeurs propres de U , sont tous nuls, d'après le théorème de Hilbert-Dirac.

$2 \Rightarrow 3$ est évident.

$3 \Rightarrow 1$: comme $\delta_U(X) = X^n$, le théorème de Hamilton-Cayley montre que $U^n = 0$.

REMARQUE. — Les endomorphismes unipotents peuvent être caractérisés de manière analogue.

COROLLAIRE 6. — Polynôme caractéristique d'un polynôme d'endomorphisme. — Soient U un endomorphisme scindé d'un espace vectoriel E de dimension n sur K , $\delta_U(X) = \prod_{i=1}^n (X - \lambda_i)$ son polynôme caractéristique, et P un élément de $K[X]$. Alors le polynôme caractéristique de l'endomorphisme $P(U)$ n'est autre que

$$\delta_{P(U)}(X) = \prod_{i=1}^n [X - P(\lambda_i)].$$

En particulier,

$$\text{Det } [P(U)] = \prod_{i=1}^n P(\lambda_i),$$

$$\text{Tr } [P(U)] = \sum_{i=1}^n P(\lambda_i).$$

Considérons une base B de E dans laquelle la matrice M associée à U est trigonale supérieure. Alors

$$\delta_{P(U)}(X) = \text{Det } (XI_n - P(M)).$$

Le calcul de ce déterminant est immédiat, puisque M , et par suite $P(M)$, sont trigonales supérieures.

On trouvera une généralisation de ce résultat dans l'exercice 65.

COROLLAIRE 7. — Autre caractérisation des endomorphismes nilpotents. — Soient K un corps de caractéristique 0, et U un endomorphisme d'un espace vectoriel E de dimension finie n sur K . Pour que U soit nilpotent, il faut et il suffit que, pour tout élément r de $[1, n]$, $\text{Tr } U^r = 0$.

Si U est nilpotent, il en est de même de U^r , pour tout entier $r \geq 1$. Le polynôme caractéristique de U^r est donc égal à X^n , et il en découle que $\text{Tr } (U^r) = \sigma_1(U^r) = 0$.

Pour démontrer la réciproque, nous nous ramenons au cas où U est scindé sur K , en introduisant le cas échéant le corps de rupture K' de K . Considérons alors une base (e_1, e_2, \dots, e_n) de E dans laquelle la matrice M associée à U est trigonale supérieure :

$$M = \begin{pmatrix} \lambda_1 & & & * \\ & \ddots & & \\ & & \lambda_i & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}.$$

Il en résulte que, pour tout entier $r \geq 1$,

$$\text{Tr}(U^r) = \text{Tr}(M^r) = \sum_{i=1}^n \lambda_i^r.$$

Or, d'après le corollaire de la proposition 2.41, la seule suite $(\lambda_1, \lambda_2, \dots, \lambda_n)$ d'éléments d'un corps K de caractéristique 0 satisfaisant pour tout entier $r \in [1, n]$ à la relation $\sum_{i=1}^n \lambda_i^r = 0$ est la suite $(0, 0, \dots, 0)$. Nous voyons donc que M est une matrice trigonale supérieure nilpotente; il s'ensuit que U est nilpotent.

THÉOREME 5.11. — Dimension des sous-espaces spectraux. — *Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Pour toute valeur propre λ de U , la dimension du sous-espace spectral F_λ de U associé à λ n'est autre que la multiplicité $m(\lambda)$ de la racine λ du polynôme caractéristique de U .*

En effet, d'après le théorème 5.6, le sous-espace spectral $F = F_\lambda$ de U associé à λ admet un sous-espace vectoriel supplémentaire G stable par U . Désignons par V et W les endomorphismes de F et G coïncidant avec U . D'après le corollaire 2 de la proposition 5.15,

$$(1) \quad \delta_U = \delta_V \delta_W.$$

Notons d'abord que

$$\delta_U(X) = (X - \lambda)^{m(\lambda)} Q(X), \quad \text{où} \quad Q(\lambda) \neq 0.$$

Remarquons ensuite que l'endomorphisme $V - \lambda I_F$ de F est nilpotent; il en découle (cf. cor. 5 du th. 5.10) que le polynôme caractéristique de $V - \lambda I_F$ est égal à $X^{m'}$, où m' désigne la dimension du sous-espace spectral $F = F_\lambda$. Ainsi,

$$\delta_V(X) = (X - \lambda)^{m'}.$$

Enfin, le scalaire λ n'appartient pas au spectre de W : soit en effet \mathfrak{x} un vecteur de G tel que $W(\mathfrak{x}) = \lambda \mathfrak{x}$; alors $U(\mathfrak{x}) = \lambda \mathfrak{x}$, et, par suite, \mathfrak{x} appartient à $F = F_\lambda$; il en découle que $\mathfrak{x} = 0$, puisque F et G sont supplémentaires dans E . Ainsi, $\delta_W(\lambda) \neq 0$.

La relation (1) s'écrit donc

$$(X - \lambda)^{m(\lambda)} Q(X) = (X - \lambda)^{m'} \delta_W(X), \quad \text{où} \quad Q(\lambda) \neq 0 \quad \text{et} \quad \delta_W(\lambda) \neq 0.$$

Il en résulte aussitôt que $m' = m(\lambda)$, ce qu'il fallait prouver.

COROLLAIRE. — Autre caractérisation des endomorphismes diagonalisables. *Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K .*

1. *Pour toute valeur propre λ de U , la dimension du sous-espace propre E_λ de U associée à λ est inférieure ou égale à la multiplicité $m(\lambda)$ de la racine λ du polynôme caractéristique de U .*

2. Pour que U soit diagonalisable, il faut et il suffit que son polynôme caractéristique δ_U soit scindé sur K , et que, pour toute valeur propre λ de U , la dimension de E_λ soit égale à $m(\lambda)$.

L'assertion 1 résulte aussitôt du théorème 5.11, puisque E_λ est contenu dans F_λ .

Assertion 2. — D'après le théorème 5.8, pour que U soit diagonalisable, il faut et il suffit que U soit scindé sur K , et que, pour toute valeur propre λ de U ,

$$\dim E_\lambda = \dim F_\lambda.$$

L'assertion en découle, puisque U est scindé sur K si et seulement si δ_U est scindé sur K (cf. cor. 4 du th. 5.10), et que $\dim F_\lambda = m(\lambda)$ d'après le théorème 5.11.

Des théorèmes 5.7 et 5.10, nous déduisons aussitôt le résultat fondamental de la théorie de la réduction des endomorphismes des espaces vectoriels de dimension finie :

THÉORÈME 5.12. — Réduction des endomorphismes scindés. — Soit U un endomorphisme scindé d'un espace vectoriel E de dimension finie $n > 0$ sur K .

1. Pour toute valeur propre λ de U , il existe une base B_λ du sous-espace spectral F_λ de U telle que la matrice M_λ associée dans B_λ à l'endomorphisme obtenu par restriction de U à F_λ soit de la forme

$$M_\lambda = \lambda I_{m(\lambda)} + N_\lambda,$$

où N_λ est une matrice trigonale supérieure nilpotente.

Alors la matrice $M_B(U)$ associée à U dans la base $B = \bigcup_{\lambda \in \text{sp}(U)} B_\lambda$ est décomposée en les blocs diagonaux M_λ :

$$M = \begin{pmatrix} M_{\lambda_1} & 0 & \dots & 0 \\ 0 & M_{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_{\lambda_r} \end{pmatrix},$$

$$M_\lambda = \begin{pmatrix} \lambda & & & N_\lambda \\ & \lambda & & \\ & & \ddots & \\ 0 & & & \lambda \end{pmatrix}.$$

2. Réciproquement, soient (F_1, F_2, \dots, F_p) une suite de sous-espaces vectoriels de E dont E est somme directe, et, pour tout $j \in [1, p]$, B_j une base de F_j satisfaisant aux conditions suivantes :

a) la matrice associée à U dans la base $B = \bigcup_{j=1}^p B_j$ de E est décomposée en blocs diagonaux M_j ;

b) pour tout $j \in [1, p]$, il existe un scalaire λ_j tel que M_j soit de la forme

$$M_j = \begin{pmatrix} \lambda_j & & * \\ & \ddots & \\ 0 & & \lambda_j \end{pmatrix}.$$

Alors le spectre de U est constitué des scalaires λ_j , et, pour toute valeur propre λ de U , le sous-espace spectral F_λ n'est autre que la somme directe des sous-espaces vectoriels F_j où j est tel que $\lambda_j = \lambda$.

Exercices conseillés : 50 à 57.

4. RÉDUCTION D'UNE FAMILLE COMMUTATIVE D'ENDOMORPHISMES

PROPOSITION 5.16. — Diagonalisation simultanée. — Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} un ensemble non vide d'endomorphismes de E . Il est équivalent de dire :

1. Il existe une base B de E constituée de vecteurs propres communs à tous les éléments de \mathcal{A} .
2. Il existe une base B de E telle que, pour tout élément U de \mathcal{A} , $M_B(U)$ soit une matrice diagonale.
3. L'ensemble \mathcal{A} est constitué d'endomorphismes diagonalisables commutant deux à deux.

Il est évident que $1 \Rightarrow 2$ et que $2 \Rightarrow 3$.

$3 \Rightarrow 1$: raisonnons par récurrence sur la dimension de E . Lorsque $\dim E = 1$, l'assertion est évidente. Soit donc n un entier strictement supérieur à 1 ; supposons l'assertion démontrée pour tous les espaces vectoriels de dimension strictement inférieure à n , et considérons un espace vectoriel E de dimension n . Deux cas se présentent :

a) Il existe un élément U de \mathcal{A} dont le spectre n'est pas réduit à un seul élément. Soient alors λ un élément de $\text{sp}(U)$, E_λ le sous-espace propre de U associé à la valeur propre λ , et E'_λ la somme directe des sous-espaces propres de U associés aux valeurs propres distinctes de λ . Puisque U est diagonalisable, $E = E_\lambda \oplus E'_\lambda$. Les sous-espaces vectoriels E_λ et E'_λ sont stables par tout endomorphisme de E commutant à U , donc par les éléments de \mathcal{A} . De plus, $\dim E_\lambda < \dim E$, et $\dim E'_\lambda < \dim E$. Désignons par \mathcal{B} (resp. \mathcal{B}') l'ensemble des endomorphismes de E_λ (resp. de E'_λ) coïncidant avec les éléments de \mathcal{A} . Les éléments de \mathcal{B} , ou de \mathcal{B}' , commutent évidemment deux à deux, et ils sont diagonalisables (cf. th. 5.5). En appliquant l'hypothèse de récurrence, nous voyons qu'il existe une base B_1 de E_λ constituée de vecteurs propres communs à tous les éléments de \mathcal{B} , et une base B'_1 de E'_λ constituée de vecteurs propres communs à tous les éléments de \mathcal{B}' . La base de E obtenue en réunissant les bases B_1 et B'_1 convient visiblement.

b) Pour tout élément U de \mathcal{A} , le spectre de U est réduit à un seul élément. Puisque U est diagonalisable, cela signifie que U est une homothétie; l'assertion est alors triviale.

PROPOSITION 5.17. — Existence d'un vecteur propre commun. — Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} un ensemble non vide d'endomorphismes de E commutant deux à deux et scindés sur K . Il existe alors un vecteur propre commun à tous les éléments de \mathcal{A} .

Raisonnons encore par récurrence sur la dimension de E . Comme dans la proposition précédente, deux cas se présentent :

a) Il existe un élément U de \mathcal{A} et une valeur propre λ de U tels que $E_\lambda(U) \neq E$. Le sous-espace vectoriel $E_\lambda(U)$ est stable pour tout endomorphisme de E commutant à U , donc par les éléments de \mathcal{A} . De plus, $\dim E_\lambda(U) < \dim E$. Désignons par \mathcal{B} l'ensemble des endomorphismes de $E_\lambda(U)$ coïncidant avec les éléments de \mathcal{A} . Les éléments de \mathcal{B} commutent deux à deux, et ils sont scindés sur K (cf. th. 5.5). En appliquant l'hypothèse de récurrence, nous voyons qu'il existe un élément de $E_\lambda(U)$ qui est vecteur propre commun à tous les éléments de \mathcal{B} . Ce vecteur convient évidemment.

b) Pour tout élément U de \mathcal{A} , il existe une valeur propre λ de U telle que $E_\lambda(U) = E$. Cela signifie que tous les éléments de \mathcal{A} sont des homothéties; l'assertion est donc triviale.

COROLLAIRE 1. — Trigonalisation simultanée. — Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} un ensemble non vide d'endomorphismes de E commutant deux à deux et scindés sur K . Il existe alors une suite (E_1, E_2, \dots, E_n) de sous-espaces vectoriels de E stables par tous les éléments de \mathcal{A} telle que, pour tout $i \in [1, n]$, $\dim E_i = i$. Autrement dit, il existe une base B de E telle que, pour tout élément U de \mathcal{A} , la matrice $M_B(U)$ soit trigonale supérieure.

La démonstration est calquée sur celle du théorème 5.10. Raisonnons par récurrence sur la dimension de E . Considérons la famille \mathcal{A}^* d'endomorphismes de E^* constituée des transposés des éléments de \mathcal{A} . Puisque les éléments de \mathcal{A} commutent deux à deux, il en est de même des éléments de \mathcal{A}^* . De même, puisque les éléments de \mathcal{A} sont scindés, il en est de même des éléments de \mathcal{A}^* (cf. prop. 5.12). Il existe donc un vecteur propre y^* commun à tous les éléments de \mathcal{A}^* . Le noyau F de y^* est alors un hyperplan de E stable par tous les éléments de \mathcal{A} . Soit \mathcal{B} l'ensemble des endomorphismes de F coïncidant avec les éléments de \mathcal{A} . Les éléments de \mathcal{B} commutent deux à deux, et ils sont scindés (cf. th. 5.5). L'hypothèse de récurrence montre qu'il existe une suite croissante $(E_1, E_2, \dots, E_{n-1})$ de sous-espaces vectoriels de F stables par les éléments de \mathcal{B} telle que, pour tout $i \in [1, n-1]$, $\dim E_i = i$. La suite $(E_1, E_2, \dots, E_{n-1}, E_n)$, où $E_n = E$, convient visiblement.

COROLLAIRE 2. — Trigonalisation simultanée d'endomorphismes nilpotents. Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} un ensemble non vide d'endomorphismes nilpotents de E commutant deux à deux. Il existe alors une base B de E telle que, pour tout élément U de \mathcal{A} , la matrice $M_B(U)$ soit trigonale supérieure nilpotente.

Cela résulte aussitôt du corollaire 1, puisque, si U est nilpotent et si $M_B(U)$ est trigonale, tous les éléments diagonaux de $M_B(U)$ sont nuls.

On trouvera dans les exercices 23 et 24 des généralisations des propositions 5.16 et 5.17.

REMARQUE. — Contrairement au cas des endomorphismes diagonalisables (cf. prop. 5.16), les corollaires 1 et 2 ne donnent pas une *condition nécessaire et suffisante* pour que des endomorphismes soient simultanément trigonalisables. L'étude d'une telle condition requiert quelques notions sur les algèbres de Lie; on pourra consulter à ce sujet les exercices 70 à 73.

PROPOSITION 5.18. — Réduction simultanée. — *Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} un ensemble non vide d'endomorphismes de E , commutant deux à deux et scindés sur K . Il existe alors une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels de E dont E est somme directe, et satisfaisant aux conditions suivantes :*

1. *Pour tout $i \in I$, le sous-espace vectoriel F_i est stable par tous les éléments de \mathcal{A} .*

2. *Pour tout $i \in I$, il existe une base B_i de F_i telle que, pour tout élément U de \mathcal{A} , la matrice $M_i(U)$ associée dans la base B_i à l'endomorphisme de F_i coïncidant avec U soit de la forme*

$$M_i(U) = \lambda_i(U) \cdot I_{n_i} + N_i(U),$$

où $n_i = \dim F_i$, où $\lambda_i(U)$ est un scalaire, et où $N_i(U)$ est une matrice triangulaire supérieure nilpotente.

Alors, pour tout élément U de \mathcal{A} , la matrice $M_B(U)$ associée à U dans la base $B = \bigcup_{i \in I} B_i$ est décomposée en les blocs diagonaux $M_i(U)$:

$$M_B(U) = \begin{pmatrix} M_1(U) & & 0 \\ & M_2(U) & \\ 0 & & \ddots \\ & & & M_r(U) \end{pmatrix},$$

$$M_i(U) = \begin{pmatrix} \lambda_i(U) & & N_i(U) \\ & \lambda_i(U) & \\ 0 & & \ddots \\ & & & \lambda_i(U) \end{pmatrix}.$$

Raisonnons encore par récurrence sur la dimension n de E . Le cas où $n = 1$ est évident. Supposons la proposition démontrée pour tous les espaces vectoriels de dimension strictement inférieure à n , $n > 1$, et considérons un espace vectoriel E de dimension n . Deux cas se présentent :

a) *Il existe un élément U de \mathcal{A} dont le spectre n'est pas réduit à un seul élément.* Soient alors λ un élément de $\text{sp}(U)$, F_λ le sous-espace spectral de U associé à λ , et F'_λ la somme directe des autres sous-espaces spectraux de U . Puisque U est scindé, $E = F_\lambda \oplus F'_\lambda$. Les sous-espaces vectoriels F_λ et F'_λ sont stables par tout endomorphisme de E commutant à U , donc par les éléments de \mathcal{A} . Dès lors, on suit pas à pas la démonstration de la proposition 5.16 dans le cas a).

b) *Pour tout élément U de \mathcal{A} , le spectre de U est réduit à un seul élément $\lambda(U)$.* Alors U s'écrit sous la forme

$$U = \lambda(U) \cdot I_E + V,$$

où V est nilpotent. Les endomorphismes V commutent deux à deux, et la proposition résulte dans ce cas du corollaire 2 de la proposition 5.17.

5. DÉCOMPOSITIONS ADDITIVE ET MULTIPLICATIVE D'UN ENDOMORPHISME

THÉORÈME 5.13. — Décomposition additive d'un endomorphisme. — Soit U un endomorphisme scindé d'un espace vectoriel E de dimension finie sur K .

1. Il existe un couple (D, N) et un seul d'endomorphismes de E satisfaisant aux conditions suivantes :

a) l'endomorphisme D est diagonalisable, et l'endomorphisme N est nilpotent ;

b) les endomorphismes D et N commutent, et

$$(1) \quad U = D + N.$$

Les endomorphismes D et N s'appellent respectivement composante diagonalisable (ou semi-simple) et composante nilpotente de l'endomorphisme U .

2. L'endomorphisme D est lié aux projecteurs spectraux P_λ de U par la relation suivante :

$$(2) \quad D = \sum_{\lambda \in \text{sp}(U)} \lambda P_\lambda$$

Son polynôme minimal n'est autre que $\prod_{\lambda \in \text{sp}(U)} (X - \lambda)$; son polynôme caractéristique est égal à celui de U .

3. Les endomorphismes D et N sont des polynômes en U .

Existence. — Définissons l'endomorphisme D par la formule (2).

Il est clair que D est diagonalisable, et que son polynôme minimal est égal à

$$\prod_{\lambda \in \text{sp}(U)} (X - \lambda).$$

Posons ensuite $N = U - D$. La matrice associée à N dans la base construite au théorème 5.12 est décomposée en les blocs N_λ ; il s'ensuit que cette matrice est trigonale supérieure nilpotente, et que N est nilpotent.

Comme les projecteurs spectraux sont des polynômes en U (cf. th. 5.7), nous voyons qu'il en est de même pour D et N ; en particulier, D et N commutent.

Le polynôme caractéristique de D est égal à celui de U , puisque, pour toute valeur propre λ de U , $m(\lambda) = \dim F_\lambda$.

Unicité. — Soient (D, N) le couple que nous venons de construire, et (D', N') un autre couple d'endomorphismes de E satisfaisant aux conditions a) et b).

L'endomorphisme D' commute à N' ; il commute donc à $U = N' + D'$, et par suite à D , qui est un polynôme en U . Ainsi, les endomorphismes D et D' sont diagonalisables, et ils commutent; il résulte alors de la proposition 5.16 que $D - D'$ est diagonalisable.

De même, N' commute à D' ; il commute donc à $U = D' + N'$, et par suite à N , qui est un polynôme en U . Ainsi, les endomorphismes N et N' sont nilpotents, *et ils commutent*. Il en résulte que $N' - N$ est nilpotent; de manière plus précise, si $N^p = 0$ et si $(N')^q = 0$, la formule du binôme montre que $(N' - N)^r = 0$ dès que

$$r \geq p + q - 1.$$

Or, les relations $U = D + N$ et $U = D' + N'$ montrent que $D - D' = N' - N$. Ainsi, l'endomorphisme $W = D - D' = N' - N$ est à la fois diagonalisable et nilpotent, ce qui prouve que $W = 0$.

COROLLAIRE. — **Décomposition multiplicative d'un automorphisme.** — Soit U un automorphisme scindé d'un espace vectoriel E de dimension finie sur K .

1. Il existe un couple (D, V) et un seul d'automorphismes de E satisfaisant aux conditions suivantes :

- a) l'automorphisme D est diagonalisable, et l'automorphisme V est unipotent ;
- b) les automorphismes D et V commutent, et

$$(1) \quad U = DV.$$

L'automorphisme D n'est autre que la composante diagonalisable de l'automorphisme U ; l'automorphisme V s'appelle composante unipotente de l'automorphisme U .

2. La composante unipotente V de U et la composante nilpotente N de U sont liées par la relation

$$V = I_E + D^{-1}N.$$

3. La composante unipotente de U est un polynôme en U .

Unicité. — Soit (D, V) un couple satisfaisant aux conditions a) et b). Puisque V est unipotent, $N' = V - I_E$ est nilpotent; la relation $U = DV$ s'écrit encore

$$U = D + DN'.$$

Puisque V commute à D , N' commute à D ; il s'ensuit que $N = DN'$ est nilpotent et que N commute à D . Le couple (D, N) satisfait donc aux conditions a) et b) du théorème 5.13, ce qui montre que D est nécessairement la composante diagonalisable de U , et que N est sa composante nilpotente. La relation $V = I_E + D^{-1}N$ s'en déduit.

Existence. — Puisque U est un automorphisme, 0 n'appartient pas au spectre de U . La composante diagonalisable D de U , ayant les mêmes valeurs propres que U , est donc un automorphisme, et

$$D^{-1} = \sum_{\lambda \in \text{sp}(U)} \lambda^{-1} P_\lambda$$

est encore un polynôme en U . Définissons alors V par la formule $V = I_E + D^{-1}N$. Puisque N et D commutent, $D^{-1}N$ est nilpotent; donc V est unipotent. Puisque D^{-1} et N sont des polynômes en U , V est un polynôme en U . Enfin, la relation $U = D + N$ fournit aussitôt la relation $U = DV$.

On trouvera des compléments dans l'exercice 29.

§ 5. RÉDUCTION DES ENDOMORPHISMES D'UN ESPACE VECTORIEL SUR LE CORPS DES RÉELS

1. EXTENSION COMPLEXE D'UN ESPACE VECTORIEL SUR LE CORPS DES RÉELS

Soit E un espace vectoriel sur le corps des complexes. La restriction à $\mathbf{R} \times E$ de l'application de $\mathbf{C} \times E$ dans E définissant la loi externe de E permet de munir E d'une structure de \mathbf{R} -espace vectoriel, dite *sous-jacente* à la structure de \mathbf{C} -espace vectoriel.

Dans ce chapitre, on a pu voir le rôle éminent joué par les espaces vectoriels sur les corps algébriquement clos. Du fait que le corps des réels n'est pas algébriquement clos, on est amené à poser le problème suivant :

Soit F un espace vectoriel sur le corps des réels ; trouver un espace vectoriel E sur le corps des complexes dont F soit un \mathbf{R} -sous-espace vectoriel, et satisfaisant à la propriété universelle suivante :

Pour tout espace vectoriel G sur \mathbf{C} et pour toute application \mathbf{R} -linéaire U de F dans le \mathbf{R} -espace vectoriel sous-jacent à G , il existe une application \mathbf{C} -linéaire \tilde{U} et une seule de E dans G prolongeant U .

Lorsque $F = \mathbf{R}^n$, il s'impose naturellement de prendre $E = \mathbf{C}^n$. Il est immédiat que \mathbf{C}^n satisfait à la propriété universelle précédente : pour le voir, on utilise uniquement le fait que tout vecteur z de \mathbf{C}^n s'écrit d'une manière et d'une seule sous la forme $z = x + iy$, où x et y appartiennent à \mathbf{R}^n , autrement dit, que le \mathbf{R} -espace vectoriel sous-jacent à \mathbf{C}^n est somme directe des sous-espaces vectoriels \mathbf{R}^n et $i\mathbf{R}^n$.

Plus généralement :

PROPOSITION 5.19. — *Soient F un espace vectoriel sur \mathbf{R} et E un espace vectoriel sur \mathbf{C} tel que le \mathbf{R} -espace vectoriel sous-jacent à E soit somme directe des \mathbf{R} -sous-espaces vectoriels F et iF . Alors E satisfait à la propriété universelle suivante :*

Pour tout espace vectoriel G sur \mathbf{C} et pour toute application \mathbf{R} -linéaire U de F dans le \mathbf{R} -espace vectoriel sous-jacent à G , il existe une application \mathbf{C} -linéaire \tilde{U} et une seule de E dans G prolongeant U .

De plus, \tilde{U} n'est autre que l'application qui à tout vecteur z de E , écrit sous la forme $z = x + iy$, où x et y appartiennent à F , associe le vecteur

$$(1) \quad \tilde{U}(z) = U(x) + iU(y).$$

Unicité de \tilde{U} . — Tout élément z de E s'écrit d'une manière et d'une seule sous la forme $z = x + iy$, où x et $y \in F$; comme \tilde{U} est \mathbf{C} -linéaire, nous voyons que

$$\tilde{U}(z) = \tilde{U}(x) + i\tilde{U}(y).$$

Puisque $\tilde{U}(x) = U(x)$, et que $\tilde{U}(y) = U(y)$, l'endomorphisme \tilde{U} est donné par la formule (1).

Existence de \tilde{U} . — Définissons \tilde{U} par la formule (1). Il est immédiat que \tilde{U} est \mathbf{R} -linéaire, et que \tilde{U} prolonge U . Il reste donc à prouver que, pour tout élément z de E , $\tilde{U}(iz) = i\tilde{U}(z)$.

Écrivons pour cela z sous la forme $z = x + iy$, où x et $y \in F$; alors $iz = -y + ix$, et, par suite,

$$\tilde{U}(iz) = -U(y) + iU(x).$$

D'autre part,

$$i\tilde{U}(z) = i[U(x) + iU(y)] = -U(y) + iU(x),$$

ce qui achève la démonstration.

Ainsi, la recherche d'une solution du problème universel posé précédemment se ramène à l'existence d'un \mathbf{C} -espace vectoriel E tel que $E = F \oplus iF$. Supposons d'abord acquise cette existence, et reconstituons F à partir de E :

a) L'application φ de $F \times F$ dans E qui à tout couple (x, y) de vecteurs de F associe le vecteur $x + iy$ est bijective.

b) Calculons maintenant la somme de deux éléments z et z' de E , et le produit d'un vecteur z de E par un nombre complexe λ . Écrivons pour cela

$$z = x + iy, \quad z' = x' + iy', \quad \lambda = \alpha + i\beta,$$

où x, y, x', y' appartiennent à F , α et β appartiennent à \mathbf{R} . Alors

$$z + z' = (x + x') + i(y + y')$$

$$\lambda z = (\alpha + i\beta)(x + iy) = (\alpha x - \beta y) + i(\alpha y + \beta x).$$

Autrement dit, si $z = \varphi(x, y)$ et $z' = \varphi(x', y')$, alors

$$(1) \quad z + z' = \varphi(x + x', y + y')$$

$$(2) \quad \lambda z = \varphi(\alpha x - \beta y, \alpha y + \beta x).$$

Ces considérations nous amènent à la proposition suivante :

PROPOSITION 5.20. — Extension complexe d'un espace vectoriel réel. — Soit F un espace vectoriel sur le corps des réels.

1. L'ensemble $F \times F$, muni de la loi interne

$$((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')) \mapsto (\mathbf{x} + \mathbf{x}', \mathbf{y} + \mathbf{y}'),$$

et de la loi externe, application de $\mathbb{C} \times (F \times F)$ dans $F \times F$,

$$(\alpha + i\beta, (\mathbf{x}, \mathbf{y})) \mapsto (\alpha\mathbf{x} - \beta\mathbf{y}, \alpha\mathbf{y} + \beta\mathbf{x}),$$

est un espace vectoriel sur le corps des complexes ; on l'appelle extension complexe de F , et on le note $F_{\mathbb{C}}$.

2. L'application j de F dans $F_{\mathbb{C}}$ qui à tout vecteur \mathbf{x} associe le vecteur $(\mathbf{x}, \mathbf{0})$ est un isomorphisme du \mathbb{R} -espace vectoriel F sur le \mathbb{R} -sous-espace vectoriel de $F_{\mathbb{C}}$ constitué des couples $(\mathbf{x}, \mathbf{0})$, où $\mathbf{x} \in F$.

3. Tout vecteur \mathbf{z} de $F_{\mathbb{C}}$ se décompose d'une manière et d'une seule sous la forme

$$\mathbf{z} = (\mathbf{x}, \mathbf{0}) + i(\mathbf{y}, \mathbf{0}),$$

où $\mathbf{x}, \mathbf{y} \in F$.

4. Soit S une partie de F ; pour que S soit libre (resp. génératrice) dans F , il faut et il suffit que $j(S)$ soit libre (resp. génératrice) dans $F_{\mathbb{C}}$. En particulier, pour que S soit une base de F , il faut et il suffit que $j(S)$ soit une base de $F_{\mathbb{C}}$.

Enfin, si B est une base de F , $B \cup iB$ est une base du \mathbb{R} -espace vectoriel sous-jacent à $F_{\mathbb{C}}$.

Assertion 1. — Le seul axiome des espaces vectoriels dont la vérification n'est pas évidente est :

$$\forall \lambda, \lambda' \in \mathbb{C}, \quad \forall \mathbf{z} \in F_{\mathbb{C}}, \quad (\lambda\lambda')\mathbf{z} = \lambda(\lambda'\mathbf{z}).$$

Pour le vérifier, écrivons $\mathbf{z} = (\mathbf{x}, \mathbf{y})$, $\lambda = \alpha + i\beta$, $\lambda' = \alpha' + i\beta'$; alors

$$\begin{aligned} (\lambda\lambda')\mathbf{z} &= [(\alpha\alpha' - \beta\beta') + i(\alpha\beta' + \beta\alpha')] \cdot (\mathbf{x}, \mathbf{y}) \\ &= [(\alpha\alpha' - \beta\beta')\mathbf{x} - (\alpha\beta' + \beta\alpha')\mathbf{y}, (\alpha\alpha' - \beta\beta')\mathbf{y} + (\alpha\beta' + \beta\alpha')\mathbf{x}], \end{aligned}$$

et

$$\begin{aligned} \lambda(\lambda'\mathbf{z}) &= (\alpha + i\beta)(\alpha'\mathbf{x} - \beta'\mathbf{y}, \alpha'\mathbf{y} + \beta'\mathbf{x}) \\ &= [\alpha(\alpha'\mathbf{x} - \beta'\mathbf{y}) - \beta(\alpha'\mathbf{y} + \beta'\mathbf{x}), \alpha(\alpha'\mathbf{y} + \beta'\mathbf{x}) + \beta(\alpha'\mathbf{x} - \beta'\mathbf{y})], \end{aligned}$$

d'où l'égalité annoncée.

Les assertions 2 et 3 sont immédiates.

Assertion 4. — Soit S une partie de F . Il est évident que si S n'est pas libre, alors $j(S)$ n'est pas libre ; supposons réciproquement que S soit libre, et

considérons une relation linéaire $\sum_{k=1}^p \lambda_k j(\mathbf{x}_k) = \mathbf{0}$, où, pour tout $k \in [1, p]$, $\mathbf{x}_k \in S$ et $\lambda_k \in \mathbb{C}$. En écrivant λ_k sous la forme $\lambda_k = \alpha_k + i\beta_k$, où α_k et $\beta_k \in \mathbb{R}$, et en posant

$$\mathbf{x} = \sum_{k=1}^p \alpha_k \mathbf{x}_k \quad \text{et} \quad \mathbf{y} = \sum_{k=1}^p \beta_k \mathbf{x}_k,$$

nous voyons que la relation précédente s'écrit $j(\mathbf{x}) + ij(\mathbf{y}) = \mathbf{0}$. Il s'ensuit que $j(\mathbf{x}) = j(\mathbf{y}) = \mathbf{0}$, et, comme j est un isomorphisme, que $\mathbf{x} = \mathbf{y} = \mathbf{0}$. Les vecteurs \mathbf{x}_k étant par hypothèse linéairement indépendants, il en découle que, pour tout $k \in [1, p]$, $\alpha_k = \beta_k = 0$, ce qu'il fallait prouver.

Il résulte aussitôt de l'assertion 3 que si S est une partie génératrice de F , $j(S)$ est une partie génératrice de $F_{\mathbb{C}}$. Réciproquement, si $j(S)$ est génératrice dans $F_{\mathbb{C}}$, pour tout vecteur \mathbf{x} de F , le vecteur $j(\mathbf{x})$ peut s'écrire sous la forme

$$j(\mathbf{x}) = \sum_{k=1}^p \mu_k j(\mathbf{x}_k), \text{ où, pour tout } k \in [1, p], \mathbf{x}_k \in S \text{ et } \mu_k \in \mathbb{C}. \text{ Il découle faci-}$$

lement de l'assertion 3 que $j(\mathbf{x}) = \sum_{k=1}^p \operatorname{Re}(\mu_k) \cdot j(\mathbf{x}_k)$. Comme j est un isomorphisme d'espaces vectoriels réels, cette égalité signifie encore que

$$\mathbf{x} = \sum_{k=1}^p \operatorname{Re}(\mu_k) \cdot \mathbf{x}_k,$$

ce qu'il fallait prouver.

Le reste de l'assertion est maintenant évident.

REMARQUE. — On notera l'analogie de la construction de $F_{\mathbb{C}}$ avec celle de \mathbb{C} (cf. § I.4.11).

On identifie souvent, grâce à l'isomorphisme j , l'espace vectoriel F au \mathbb{R} -sous-espace vectoriel de $F_{\mathbb{C}}$ constitué des vecteurs de la forme $(\mathbf{x}, \mathbf{0})$, où $\mathbf{x} \in F$. C'est pourquoi les vecteurs de cette forme sont appelés *vecteurs réels* de $F_{\mathbb{C}}$.

COROLLAIRE 1. — *Si l'espace vectoriel F est de dimension finie n sur \mathbb{R} , alors $F_{\mathbb{C}}$ est de dimension n sur \mathbb{C} , et de dimension $2n$ sur \mathbb{R} .*

COROLLAIRE 2. — *L'extension complexe de \mathbb{R}^n est isomorphe à \mathbb{C}^n .*

La proposition 5.19 fournit aussitôt le

THÉORÈME 5.14. — **Propriété universelle de l'extension complexe d'un espace vectoriel réel.** — *Soient F un espace vectoriel sur \mathbb{R} , $F_{\mathbb{C}}$ son extension complexe, et j_F l'application canonique de F dans $F_{\mathbb{C}}$. Alors, pour tout espace vectoriel G sur \mathbb{C} , et pour toute application \mathbb{R} -linéaire U de F dans le \mathbb{R} -espace*

vectorel sous-jacent à G , il existe une application \mathbb{C} -linéaire \tilde{U} et une seule de $F_{\mathbb{C}}$ dans G telle que $\tilde{U} \circ j_F = U$:

$$\begin{array}{ccc} F & \xrightarrow{j_F} & F_{\mathbb{C}} \\ & \searrow U & \downarrow \tilde{U} \\ & & G \end{array}$$

Lorsqu'on identifie F au sous-espace des vecteurs réels de $F_{\mathbb{C}}$, la relation précédente signifie simplement que \tilde{U} prolonge U . Alors, pour tout vecteur z de $F_{\mathbb{C}}$ écrit sous la forme $z = x + iy$, où x et $y \in F$, $\tilde{U}(z)$ est donné par la formule

$$(1) \quad \tilde{U}(z) = U(x) + iU(y).$$

THÉORÈME 5.15. — Extension complexe d'une application linéaire. — Soient F et F' deux espaces vectoriels sur \mathbb{R} , $F_{\mathbb{C}}$ et $F'_{\mathbb{C}}$ leurs extensions complexes, j_F et $j_{F'}$ les applications canoniques de F dans $F_{\mathbb{C}}$ et de F' dans $F'_{\mathbb{C}}$.

1. Pour toute application \mathbb{R} -linéaire U de F dans F' , il existe une application \mathbb{C} -linéaire $U_{\mathbb{C}}$ et une seule de $F_{\mathbb{C}}$ dans $F'_{\mathbb{C}}$ telle que

$$U_{\mathbb{C}} \circ j_F = j_{F'} \circ U :$$

$$\begin{array}{ccc} F & \xrightarrow{U} & F' \\ j_F \downarrow & & \downarrow j_{F'} \\ F_{\mathbb{C}} & \xrightarrow{U_{\mathbb{C}}} & F'_{\mathbb{C}} \end{array}$$

On identifiera désormais F et F' aux sous-espaces vectoriels des vecteurs réels de $F_{\mathbb{C}}$ et de $F'_{\mathbb{C}}$. La relation précédente signifie alors que $U_{\mathbb{C}}$ prolonge U ; c'est pourquoi $U_{\mathbb{C}}$ s'appelle extension complexe de l'application linéaire U .

Pour tout vecteur z de $F_{\mathbb{C}}$ écrit sous la forme $z = x + iy$, où $x, y \in F$, $U_{\mathbb{C}}(z)$ est donné par la formule

$$(2) \quad U_{\mathbb{C}}(z) = U(x) + iU(y).$$

2. Le noyau de $U_{\mathbb{C}}$ n'est autre que l'extension complexe du noyau de U , et l'image de $U_{\mathbb{C}}$ n'est autre que l'extension complexe de l'image de U .

3. Soient F, F' et F'' trois espaces vectoriels sur \mathbb{R} , $F_{\mathbb{C}}, F'_{\mathbb{C}}$ et $F''_{\mathbb{C}}$ leurs extensions complexes, U une application \mathbb{R} -linéaire de F dans F' , et V une application \mathbb{R} -linéaire de F' dans F'' . Alors l'extension complexe de $V \circ U$ n'est autre que $V_{\mathbb{C}} \circ U_{\mathbb{C}}$:

$$(V \circ U)_{\mathbb{C}} = V_{\mathbb{C}} \circ U_{\mathbb{C}}.$$

4. Soit F un espace vectoriel de dimension finie sur \mathbb{R} , muni d'une base B . On sait que B est aussi une base du \mathbb{C} -espace vectoriel $F_{\mathbb{C}}$. Alors, pour tout

endomorphisme U de F , les matrices associées à U et à U_C dans cette base sont égales :

$$M_B(U_C) = M_B(U).$$

En particulier,

$$\text{Det}(U_C) = \text{Det}(U).$$

Assertion 1. — Pour démontrer l'existence et l'unicité de U_C , il suffit d'appliquer la proposition précédente et l'espace vectoriel $G = F'_C$ et à l'application \mathbf{R} -linéaire $j_F \circ U$ de F dans F'_C .

Assertion 2. — La formule (2) montre aussitôt que si z appartient à $[\text{Ker}(U)]_C$, c'est-à-dire si $z = x + iy$, où x et y appartiennent à $\text{Ker}(U)$, alors $U_C(z) = 0$. Réciproquement, soit $z = x + iy$ un élément de $\text{Ker}(U_C)$; la même formule montre que $U(x) = U(y) = 0$; donc z appartient à $[\text{Ker}(U)]_C$.

On prouvera de même que $\text{Im}(U_C) = [\text{Im}(U)]_C$.

Les autres assertions sont immédiates.

2. INVOLUTION CANONIQUE D'UNE EXTENSION COMPLEXE

PROPOSITION 5.21. — Involution canonique d'une extension complexe. — Soient F un espace vectoriel sur \mathbf{R} , $E = F_C$ son extension complexe, et j_F l'involution canonique de E , qui à tout élément $z = x + iy$ de E associe l'élément $\bar{z} = x - iy$. (Le vecteur \bar{z} est dit conjugué du vecteur z .)

1. Pour que z soit égal à son conjugué, il faut et il suffit que z appartienne à F , c'est-à-dire que z soit un vecteur réel de E .

2. Pour tout sous-espace vectoriel G de E , $j_F(G)$ est encore un sous-espace vectoriel de E , appelé sous-espace vectoriel conjugué de G , et noté \bar{G} . Pour que $\bar{G} = G$, il faut et il suffit que G soit égal à $(F \cap G)_C$. On dit alors que G est un sous-espace vectoriel réel de E .

Si G est un sous-espace vectoriel de dimension finie de E , pour que G soit réel, il faut et il suffit qu'il existe une base de G constituée de vecteurs réels.

3. Soit $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de F . Pour que F soit somme directe des sous-espaces vectoriels F_i , il faut et il suffit que E soit somme directe de la famille $(E_i)_{i \in I}$ des complexifiés des sous-espaces vectoriels F_i .

PROPOSITION 5.22. — Applications linéaires conjuguées. — Soient F et F' deux espaces vectoriels sur \mathbf{R} , $E = F_C$ et $E' = F'_C$ leurs extensions complexes, V une application linéaire de F_C dans F'_C , et \bar{V} l'application linéaire de F_C dans F'_C , dite conjuguée de V , qui à tout vecteur $z = x + iy$ de F_C associe le vecteur

$$\bar{V}(x + iy) = \bar{V}(x) + i\bar{V}(y).$$

1. Pour tout élément z de F_C ,

$$\overline{\bar{V}(z)} = \bar{V}(\bar{z}).$$

De plus, le noyau de \bar{V} n'est autre que le sous-espace vectoriel conjugué du noyau de V , et l'image de \bar{V} n'est autre que le sous-espace vectoriel conjugué de l'image de V .

Enfin,

$$\overline{\lambda V + \lambda' V'} = \bar{\lambda} \bar{V} + \bar{\lambda}' \bar{V}',$$

et

$$\overline{W \circ V} = \bar{W} \circ \bar{V}.$$

En particulier, l'application $V \mapsto \bar{V}$ est un automorphisme involutif de l'anneau unitaire $\mathfrak{L}(\mathbb{C})$. Il en découle que, pour tout élément P de $\mathbb{C}[X]$,

$$\overline{P(V)} = P(\bar{V}).$$

2. On dit que V est réelle si $\bar{V} = V$; pour que V soit réelle, il faut et il suffit que $V(F)$ soit contenu dans F' . De plus, l'application $U \mapsto U_{\mathbb{C}}$ est un isomorphisme du \mathbf{R} -espace vectoriel $\mathfrak{L}_{\mathbf{R}}(F, F')$ sur le \mathbf{R} -sous-espace vectoriel de $\mathfrak{L}_{\mathbb{C}}(E, E')$ constitué des applications linéaires réelles de E dans E' .

Soit en particulier F un espace vectoriel sur \mathbf{R} . Alors l'application $U \mapsto U_{\mathbb{C}}$ est un isomorphisme de l'algèbre unitaire $\mathfrak{L}_{\mathbf{R}}(F)$ sur la \mathbf{R} -sous-algèbre unitaire de $\mathfrak{L}_{\mathbb{C}}(E)$ constituée des endomorphismes réels. Il en découle que $U_{\mathbb{C}}$ est inversible si et seulement si U l'est.

3. Si F et F' sont de dimension finie et munis respectivement de bases B et B' , les matrices $M_{B, B'}(V) = (\alpha_{ij})$ et $M_{B, B'}(\bar{V}) = (\beta_{ij})$ satisfont aux relations $\beta_{ij} = \overline{\alpha_{ij}}$, pour tout couple (i, j) d'indices. Il en découle que

$$\text{Det}(\bar{V}) = \overline{\text{Det}(V)}.$$

DÉFINITION 5.12. — Matrices conjuguées. — Soit $M = (\alpha_{ij})$ un élément de $\mathbf{M}_{n,p}(\mathbb{C})$. On appelle matrice conjuguée de M , et on note \bar{M} , l'élément (β_{ij}) de $\mathbf{M}_{n,p}(\mathbb{C})$ défini par les relations

$$\beta_{ij} = \overline{\alpha_{ij}}.$$

Évidemment, pour que $\bar{M} = M$, il faut et il suffit que tous les éléments de M soient réels.

De ce qui précède, nous déduisons aussitôt que

1. Pour tout couple (M, M') d'éléments de $\mathbf{M}_{n,p}(\mathbb{C})$, et pour tout couple (λ, λ') de nombres complexes,

$$\overline{(\lambda M + \lambda' M')} = \bar{\lambda} \bar{M} + \bar{\lambda}' \bar{M}'$$

2. Pour tout élément M de $\mathbf{M}_{n,p}(\mathbb{C})$ et pour tout élément N de $\mathbf{M}_{m,n}(\mathbb{C})$,

$$\overline{NM} = \bar{N} \bar{M}.$$

3. L'application $M \mapsto \bar{M}$ est un automorphisme involutif de l'anneau unitaire $\mathbf{M}_n(\mathbb{C})$.

4. Pour tout élément M de $M_n(\mathbb{C})$,

$$\text{Det}(\overline{M}) = \overline{\text{Det}(M)}.$$

PROPOSITION 5.23. — Spectre du conjugué d'un endomorphisme. — Soient F un espace vectoriel sur \mathbb{R} , E son extension complexe, V un endomorphisme de E , et \overline{V} l'endomorphisme conjugué de V .

1. Pour qu'un nombre complexe λ soit une valeur propre de V , il faut et il suffit que $\bar{\lambda}$ soit une valeur propre de \overline{V} . Le sous-espace spectral $F_{\bar{\lambda}}(\overline{V})$ associé à $\bar{\lambda}$ n'est autre que le conjugué du sous-espace spectral $F_{\lambda}(V)$ associé à λ . De même, le sous-espace propre $E_{\bar{\lambda}}(\overline{V})$ n'est autre que le conjugué du sous-espace propre $E_{\lambda}(V)$.

Pour que λ soit une valeur propre d'indice fini de V , il faut et il suffit que $\bar{\lambda}$ soit une valeur propre d'indice fini de \overline{V} ; leurs indices sont alors égaux.

Pour que V soit scindé, ou diagonalisable, il faut et il suffit que \overline{V} le soit.

2. Pour que V admette un polynôme minimal, il faut et il suffit que \overline{V} en admette un; ces deux polynômes sont alors conjugués.

3. Si F est de dimension finie, les polynômes caractéristiques de V et de \overline{V} sont conjugués.

4. Si F est de dimension finie, les composantes diagonalisable et nilpotente de \overline{V} ne sont autres que les conjuguées des composantes diagonalisable et nilpotente de V . De même, si V est un automorphisme de E , la composante unipotente de \overline{V} n'est autre que la conjuguée de la composante unipotente de V .

Assertion 1. — Nous savons que, pour tout élément P de $\mathbb{C}[X]$, $\overline{P(\overline{V})} = \overline{P}(\overline{V})$. En appliquant cette relation au cas où $P = (X - \lambda)^r$, nous voyons que le noyau de $(\overline{V} - \bar{\lambda}I_E)^r$ n'est autre que le sous-espace vectoriel conjugué du noyau de $(V - \lambda I_E)^r$. L'assertion en découle aussitôt.

Assertion 2. — La relation $\overline{P(\overline{V})} = \overline{P}(\overline{V})$ montre que la relation $P(V) = 0$ équivaut à la relation $\overline{P}(\overline{V}) = 0$. L'assertion s'en déduit facilement.

Assertion 3. — Considérons une base B de F , et désignons par M la matrice associée à V dans la base B . La matrice associée à \overline{V} dans la base B n'est autre que \overline{M} . L'assertion est donc une conséquence immédiate de la relation

$$\text{Det}(XI_n - \overline{M}) = \overline{\text{Det}(XI_n - M)}.$$

Assertion 4. — Soient D et N les composantes diagonalisable et nilpotente de V . Puisque $V = D + N$ et que $DN = ND$, $\overline{V} = \overline{D} + \overline{N}$ et $\overline{DN} = \overline{ND}$. Comme N est nilpotent, il en est de même de \overline{N} ; comme D est diagonalisable, il en est de même de \overline{D} . L'assertion en résulte, par unicité des composantes diagonalisable et nilpotente de \overline{V} .

Le cas des composantes unipotentes se traite de manière analogue.

COROLLAIRE. — Cas des endomorphismes réels. — Soient F un espace vectoriel sur \mathbb{R} , E son extension complexe et V un endomorphisme réel de E , c'est-à-dire un endomorphisme de E laissant stable F .

1. Pour toute valeur propre λ de V , $\bar{\lambda}$ est aussi une valeur propre de V , ayant même indice que λ si λ est d'indice fini. Les sous-espaces spectraux $F_\lambda(V)$ et $F_{\bar{\lambda}}(V)$ sont conjugués, ainsi que les sous-espaces propres $E_\lambda(V)$ et $E_{\bar{\lambda}}(V)$.

En particulier, si λ est réel, $F_\lambda(V)$ et $E_\lambda(V)$ sont des sous-espaces vectoriels réels.

2. Si V admet un polynôme minimal, ce polynôme est à coefficients réels.

3. Si F est de dimension finie, le polynôme caractéristique de V est à coefficients réels.

4. Si F est de dimension finie, les composantes diagonalisable et nilpotente de V sont des endomorphismes réels.

PROPOSITION 5.24. — Propriétés des endomorphismes diagonalisables réels. Soient F un espace vectoriel sur \mathbf{R} , E son extension complexe, et V un endomorphisme réel de E . Si V est diagonalisable, tout sous-espace vectoriel réel E' de E stable par V admet un sous-espace vectoriel supplémentaire réel stable par V .

Posons $R = \text{sp}(V) \cap \mathbf{R}$ et $D = \text{sp}(V) \cap \{z \mid \text{Im}(z) > 0\}$. Puisque V est réel et diagonalisable, et que E' est stable par V , le théorème 5.5. montre que

$$E' = \left[\bigoplus_{\lambda \in R} E'_\lambda \right] \oplus \left[\bigoplus_{\mu \in D} (E'_\mu \oplus \overline{E'_\mu}) \right],$$

où, pour tout élément v de $\text{sp}(V)$,

$$E'_v = E' \cap E_v(V).$$

Puisque E' est un sous-espace vectoriel réel, pour tout élément λ de R , E'_λ est un sous-espace vectoriel réel et, pour tout élément μ de D , $E'_\mu = \overline{E'_\mu}$. Pour tout élément λ de R , considérons un sous-espace vectoriel réel E''_λ supplémentaire de E'_λ dans $E_\lambda(V)$ et, pour tout élément μ de D , considérons un sous-espace vectoriel E''_μ supplémentaire de E'_μ dans $E_\mu(V)$. Il est immédiat que le sous-espace vectoriel

$$E'' = \left[\bigoplus_{\lambda \in R} E''_\lambda \right] \oplus \left[\bigoplus_{\mu \in D} (E''_\mu \oplus \overline{E''_\mu}) \right]$$

est réel et stable par V , et que E est somme directe de E' et de E'' .

3. RÉDUCTION DES ENDOMORPHISMES D'UN ESPACE VECTORIEL SUR LE CORPS DES RÉELS

Nous étudions maintenant les relations qui lient le spectre d'un endomorphisme au spectre de son extension complexe.

PROPOSITION 5.25. — Spectre de l'extension complexe d'un endomorphisme. Soient F un espace vectoriel sur \mathbf{R} , $F_{\mathbf{C}}$ son extension complexe, U un endomorphisme de F , et $U_{\mathbf{C}}$ l'extension complexe de U .

1. Pour toute valeur propre λ de $U_{\mathbb{C}}$, $\bar{\lambda}$ est aussi une valeur propre de $U_{\mathbb{C}}$, ayant même indice que λ si λ est d'indice fini. Les sous-espaces spectraux $F_{\lambda}(U_{\mathbb{C}})$ et $F_{\bar{\lambda}}(U_{\mathbb{C}})$ sont conjugués, ainsi que les sous-espaces propres $E_{\lambda}(U_{\mathbb{C}})$ et $E_{\bar{\lambda}}(U_{\mathbb{C}})$.

2. Pour qu'un nombre réel λ soit une valeur propre de $U_{\mathbb{C}}$, il faut et il suffit que λ soit une valeur propre de U . Alors le sous-espace spectral $F_{\lambda}(U_{\mathbb{C}})$ n'est autre que l'extension complexe du sous-espace spectral $F_{\lambda}(U)$; de même, le sous-espace propre $E_{\lambda}(U_{\mathbb{C}})$ n'est autre que l'extension complexe du sous-espace propre $E_{\lambda}(U)$.

En particulier, si λ est une valeur propre réelle de $U_{\mathbb{C}}$, et si $E_{\lambda}(U_{\mathbb{C}})$ est de dimension finie, il existe une base de cet espace vectoriel constituée de vecteurs réels.

3. Pour que U admette un polynôme minimal, il faut et il suffit que $U_{\mathbb{C}}$ en admette un; ces deux polynômes sont alors égaux.

4. Si F est de dimension finie, le polynôme caractéristique de $U_{\mathbb{C}}$ n'est autre que celui de U .

L'assertion 1 résulte aussitôt du corollaire de la proposition 5.23, puisque $U_{\mathbb{C}}$ est un endomorphisme réel.

L'assertion 2 découle du fait que, pour tout nombre réel λ , et pour tout entier naturel r , le noyau de $(U_{\mathbb{C}} - \lambda I_{F_{\mathbb{C}}})^r$ n'est autre que le complexifié du noyau de $(U - \lambda I_F)^r$.

Assertion 3. — Soit P un élément de $\mathbb{R}[X]$ tel que $P(U) = 0$. Alors

$$P(U_{\mathbb{C}}) = [P(U)]_{\mathbb{C}} = 0.$$

Il s'ensuit que si U admet un polynôme minimal π , il en est de même de $U_{\mathbb{C}}$, et que le polynôme minimal π' de $U_{\mathbb{C}}$ divise π dans $\mathbb{C}[X]$. Supposons réciproquement que $U_{\mathbb{C}}$ admet un polynôme minimal π' . D'après le corollaire de la proposition 5.23, π' est réel. De la relation $\pi'(U_{\mathbb{C}}) = 0$, nous déduisons que $\pi'(U) = 0$, car, pour tout vecteur \mathbf{x} de F , $U_{\mathbb{C}}(\mathbf{x}) = U(\mathbf{x})$. Donc U admet un polynôme minimal π et π divise π' dans $\mathbb{R}[X]$. Enfin, comme π' est à coefficients réels, et comme π' divise π dans $\mathbb{C}[X]$, π' divise π dans $\mathbb{R}[X]$. Puisque π et π' sont unitaires, $\pi = \pi'$.

L'assertion 4 est une conséquence immédiate du fait que, pour toute base B de F ,

$$M_B(U_{\mathbb{C}}) = M_B(U).$$

COROLLAIRE. — Caractérisation des endomorphismes scindés sur \mathbb{R} . — Soient F un espace vectoriel sur \mathbb{R} , $F_{\mathbb{C}}$ son extension complexe, U un endomorphisme de F admettant un polynôme minimal, et $U_{\mathbb{C}}$ son extension complexe. Pour que U soit scindé sur \mathbb{R} , il faut et il suffit que le spectre de $U_{\mathbb{C}}$ soit contenu dans \mathbb{R} . Alors, U est diagonalisable si et seulement si $U_{\mathbb{C}}$ est diagonalisable.

En effet, d'après le théorème 5.7, U est scindé sur \mathbb{R} si et seulement si son polynôme minimal π est scindé sur \mathbb{R} . Or, π est aussi le polynôme minimal de $U_{\mathbb{C}}$, et les racines de π dans \mathbb{C} ne sont autres que les valeurs propres de $U_{\mathbb{C}}$.

La dernière assertion est alors immédiate, puisqu'un endomorphisme est diagonalisable si et seulement si son polynôme minimal a toutes ses racines simples.

Étudions maintenant le cas où U n'est pas nécessairement scindé.

PROPOSITION 5.26. — Caractérisation des endomorphismes semi-simples sur \mathbf{R} . — Soient F un espace vectoriel de dimension finie sur \mathbf{R} , $E = F_{\mathbf{C}}$ son extension complexe et U un endomorphisme de F . Pour que U soit semi-simple, il faut et il suffit que son extension complexe $U_{\mathbf{C}}$ soit diagonalisable.

Supposons d'abord que l'endomorphisme U est semi-simple. Considérons le sous-espace vectoriel E' de E somme directe des sous-espaces propres de $U_{\mathbf{C}}$. Puisque $U_{\mathbf{C}}$ est un endomorphisme réel, E' est un sous-espace vectoriel réel de E ; donc E' n'est autre que le complexifié de $F' = E' \cap F$. Comme E' et F sont stables par $U_{\mathbf{C}}$, F' est stable par U . Puisque U est semi-simple, il existe un sous-espace vectoriel F'' supplémentaire de F' dans F stable par U . Le complexifié E'' de F'' est stable par $U_{\mathbf{C}}$, et E est somme directe de E' et de E'' . Il suffit de prouver que $E'' = \{0\}$. S'il n'en était pas ainsi, l'endomorphisme V de E'' coïncidant avec $U_{\mathbf{C}}$ admettrait au moins une valeur propre, puisque le corps des complexes est algébriquement clos. Le sous-espace propre associé à cette valeur propre serait un sous-espace propre de U non contenu dans E' , ce qui contredirait la définition de E' .

Supposons réciproquement que l'endomorphisme $U_{\mathbf{C}}$ est diagonalisable. Considérons un sous-espace vectoriel F' de F stable par U . Alors le complexifié E' de F' est un sous-espace vectoriel réel de E stable par $U_{\mathbf{C}}$. Puisque $U_{\mathbf{C}}$ est réel et diagonalisable, il résulte de la proposition 5.24 que E' admet un sous-espace vectoriel supplémentaire réel E'' stable par $U_{\mathbf{C}}$. Le sous-espace vectoriel $F'' = E'' \cap F$ est un supplémentaire de F' stable par U , ce qu'il fallait prouver.

COROLLAIRE. — Décomposition additive d'un endomorphisme d'un espace vectoriel réel. — Soit U un endomorphisme d'un espace vectoriel F de dimension finie sur \mathbf{R} . Il existe alors un couple (D, N) et un seul d'endomorphismes de F satisfaisant aux conditions suivantes :

- a) l'endomorphisme D est semi-simple, et l'endomorphisme N est nilpotent ;
- b) les endomorphismes D et N commutent, et

$$U = D + N.$$

Unicité. — Soit (D, N) un couple satisfaisant aux conditions de l'énoncé. Alors $U_{\mathbf{C}} = D_{\mathbf{C}} + N_{\mathbf{C}}$, et $D_{\mathbf{C}}$ et $N_{\mathbf{C}}$ commutent. D'autre part, puisque N est nilpotent, il en est de même de $N_{\mathbf{C}}$. Enfin, d'après la proposition précédente, puisque D est semi-simple, $D_{\mathbf{C}}$ est diagonalisable. Par suite, $D_{\mathbf{C}}$ et $N_{\mathbf{C}}$ sont les composantes diagonalisable et nilpotente de $U_{\mathbf{C}}$. L'unicité du couple (D, N) s'en déduit aussitôt.

Existence. — Considérons l'extension complexe $U_{\mathbb{C}}$ de U . D'après le corollaire de la proposition 5.23, les composantes diagonalisable et nilpotente D' et N' de $U_{\mathbb{C}}$ sont des endomorphismes réels; il existe donc un couple (D, N) et un seul d'endomorphismes de F tel que $D' = D_{\mathbb{C}}$ et que $N' = N_{\mathbb{C}}$. Puisque $U_{\mathbb{C}} = D_{\mathbb{C}} + N_{\mathbb{C}}$ et que $D_{\mathbb{C}}$ et $N_{\mathbb{C}}$ commutent, $U = D + N$ et D et N commutent. D'autre part, puisque $N_{\mathbb{C}}$ est nilpotent, il en est de même de N . Enfin, d'après la proposition précédente, puisque $D_{\mathbb{C}}$ est diagonalisable, D est semi-simple.

THÉORÈME 5.16. — Réduction des endomorphismes semi-simples sur \mathbb{R} . — Soient F un espace vectoriel de dimension finie non nulle n sur \mathbb{R} , et U un endomorphisme de F tel que l'extension complexe $U_{\mathbb{C}}$ de U soit diagonalisable. Le polynôme caractéristique de U s'écrit sous la forme

$$\delta_U = \prod_{j=1}^r (X - \lambda_j) \cdot \prod_{h=1}^d (X - \mu_h)(X - \bar{\mu}_h),$$

où, pour tout $j \in [1, r]$, λ_j est réel, où, pour tout $h \in [1, d]$, $\text{Im}(\mu_h) > 0$, et où les entiers r et d sont liés par la relation $r + 2d = n$. Pour tout $h \in [1, d]$, on pose $\mu_h = \alpha_h + i\beta_h$, où $\alpha_h \in \mathbb{R}$ et $\beta_h \in \mathbb{R}^*$.

1. Il existe une base $(e_k)_{1 \leq k \leq n}$ de $F_{\mathbb{C}}$ telle que

a) pour tout $j \in [1, r]$, e_j appartienne à F , et $U_{\mathbb{C}}(e_j) = \lambda_j e_j$;

b) pour tout $h \in [1, d]$, e_{h+d+r} soit conjugué de e_{h+r} , et $U_{\mathbb{C}}(e_{h+r}) = \mu_h e_{h+r}$.

2. Pour tout $h \in [1, d]$, on pose

$$(1) \quad \begin{aligned} f_h &= \frac{1}{2i}(e_{h+r} - e_{h+d+r}) \\ g_h &= \frac{1}{2}(e_{h+r} + e_{h+d+r}). \end{aligned}$$

Alors la famille $(e_1, e_2, \dots, e_r, f_1, g_1, f_2, g_2, \dots, f_d, g_d)$ est une base de F dans laquelle la matrice associée à U est de la forme

$$M_B(U) = \begin{pmatrix} \lambda_1 & & & & & & 0 \\ & \lambda_2 & & & & & \\ & & \ddots & & & & \\ & & & \lambda_r & & & \\ & & & & M_1 & & \\ & & & & & M_2 & \\ & & & & & & \ddots \\ & & & & & & & M_d \\ 0 & & & & & & & & \end{pmatrix},$$

où, pour tout $h \in [1, d]$,

$$M_h = \begin{pmatrix} \alpha_h & -\beta_h \\ \beta_h & \alpha_h \end{pmatrix}.$$

Autrement dit, si, pour tout $j \in [1, r]$, on pose $F_j = \mathbf{R}e_j$, et pour tout $h \in [1, d]$, on pose $F_{h+r} = \mathbf{R}f_h \oplus \mathbf{R}g_h$, l'espace vectoriel F est somme directe des sous-espaces vectoriels F_m , où m parcourt $[1, r + d]$. De plus,

a) pour tout $j \in [1, r]$, la droite F_j est stable par U , et l'endomorphisme de F_j obtenu par restriction de U à F_j n'est autre que l'homothétie de rapport λ_j ;

b) pour tout $h \in [1, d]$, le plan F_{h+r} est stable par U , et l'endomorphisme de F_{h+r} coïncidant avec U admet M_h pour matrice dans la base (f_h, g_h) .

Assertion 1. — Posons $R = \text{sp}(U_C) \cap \mathbf{R}$, $D = \text{sp}(U_C) \cap \{z \mid \text{Im}(z) > 0\}$, et, pour tout $\lambda \in \text{sp}(U_C)$, $E_\lambda = E_\lambda(U_C)$. Puisque U_C est diagonalisable,

$$F_C = \left[\bigoplus_{\lambda \in R} E_\lambda \right] \oplus \left[\bigoplus_{\mu \in D} (E_\mu \oplus E_{\bar{\mu}}) \right].$$

a) Comme, pour tout $\lambda \in R$, E_λ est un sous-espace vectoriel réel, il existe une base B_λ de ce sous-espace vectoriel constituée de vecteurs de F ; prenons pour (e_1, e_2, \dots, e_r) la famille obtenue en réunissant les bases B_λ , où λ parcourt R .

b) Comme, pour tout $\mu \in D$, le sous-espace vectoriel E_μ est conjugué du sous-espace vectoriel $E_{\bar{\mu}}$, pour toute base B_μ de E_μ , $\overline{B_\mu}$ est une base de $E_{\bar{\mu}}$; prenons pour $(e_{r+1}, e_{r+2}, \dots, e_{r+d})$ la famille obtenue en réunissant les bases B_μ , où μ parcourt D . Pour tout $h \in [1, d]$, posons $e_{r+d+h} = \overline{e_{r+h}}$. La famille $(e_k)_{1 \leq k \leq n}$ convient visiblement.

Assertion 2. — Les relations (1) montrent que la famille

$$B = (e_1, e_2, \dots, e_r, f_1, g_1, g_2, \dots, f_r, g_r)$$

est une base de F_C . De plus, comme $e_{h+d+r} = \overline{e_{h+r}}$, il est immédiat que les vecteurs $f_1, g_1, f_2, g_2, \dots, f_r, g_r$ appartiennent à F . Déterminons enfin les vecteurs colonnes de la matrice $M_B(U)$:

a) pour tout $j \in [1, r]$,

$$(2) \quad U(e_j) = U_C(e_j) = \lambda_j e_j;$$

b) pour tout $h \in [1, d]$,

$$(3) \quad U_C(e_{h+r}) = \mu_h e_{h+r}.$$

Or, $e_{h+r} = g_h + if_h$, et $\mu_h = \alpha_h + i\beta_h$. En prenant les parties réelle et imaginaire de la relation (3), nous obtenons les relations suivantes :

$$\begin{aligned} U(g_h) &= -\beta_h f_h + \alpha_h g_h, \\ U(f_h) &= \alpha_h f_h + \beta_h g_h, \end{aligned}$$

ce qui achève la démonstration.

REMARQUE 1. — Soit x un vecteur propre de U_C , associé à une valeur propre λ . Si x est réel, alors λ est réel.

En effet, $U_C(\mathbf{x}) = \lambda \mathbf{x}$; donc $\overline{U_C(\mathbf{x})} = \overline{\lambda \mathbf{x}}$, c'est-à-dire $U_C(\mathbf{x}) = \overline{\lambda} \mathbf{x}$, puisque \mathbf{x} et $U_C(\mathbf{x})$ sont réels. La relation $(\lambda - \overline{\lambda})\mathbf{x} = \mathbf{0}$ montre que λ est réel.

Il en découle que tout vecteur propre réel de U_C appartient nécessairement au sous-espace vectoriel engendré par e_1, e_2, \dots, e_r .

REMARQUE 2. — Soient, plus généralement, U un endomorphisme d'un espace vectoriel E sur un corps K , et K' une extension galoisienne de K (cf. chap. III.1). Les méthodes précédentes permettent d'effectuer la réduction de U lorsque le polynôme minimal de U est scindé sur K' .

Exercices conseillés : 58 et 59.

§ 6. RÉDUCTION DES MATRICES

Soient E un espace vectoriel de dimension finie non nulle n sur K , B_1 et B_2 deux bases de E , et P la matrice de passage de B_1 à B_2 . Soient d'autre part U un endomorphisme de E , M_1 et M_2 les matrices associées à U dans les bases B_1 et B_2 . Nous savons (cf. § I.3.16) que M_1 et M_2 sont liées par la relation

$$M_2 = P^{-1}M_1P.$$

Ceci nous conduit à introduire dans l'ensemble $\mathbf{M}_n(K)$ la relation binaire définie par les couples (M, M') tels qu'il existe un élément inversible Q de $\mathbf{M}_n(K)$ tel que

$$M' = QMQ^{-1}.$$

Il est immédiat que cette relation binaire est une relation d'équivalence dans $\mathbf{M}_n(K)$.

DÉFINITION 5.13. — **Matrices semblables.** — *Deux matrices carrées d'ordre n à éléments dans K sont dites semblables si elles sont liées par la relation précédente. Cette relation est appelée relation de similitude, et les classes d'équivalence sont appelées classes de similitude.*

REMARQUE 1. — Pour que deux matrices M et M' soient semblables, il faut et il suffit que leurs transposées tM et ${}^tM'$ le soient.

REMARQUE 2. — **Automorphismes intérieurs de $\mathbf{M}_n(K)$.** — Soit Q une matrice carrée inversible d'ordre n . Alors l'application

$$\sigma_Q : M \mapsto QMQ^{-1}$$

est un automorphisme de l'algèbre unitaire $M_n(K)$. Un tel automorphisme est appelé automorphisme intérieur de $M_n(K)$. De plus, l'application

$$\sigma : Q \mapsto \sigma_Q$$

est un morphisme du groupe multiplicatif $GL_n(K)$ des matrices carrées inversibles d'ordre n dans le groupe multiplicatif des automorphismes de l'algèbre unitaire $M_n(K)$.

On peut d'ailleurs prouver le résultat suivant (cf. exercice 3.35) : *Tous les automorphismes de l'algèbre $M_n(K)$ sont intérieurs, c'est-à-dire que σ est un morphisme surjectif ; de plus, le noyau du morphisme σ est constitué des matrices scalaires non nulles* (cf. exercice I.3.55).

PROPOSITION 5.27. — Interprétation vectorielle de la similitude des matrices. Soient M_1 et M_2 deux matrices carrées d'ordre n , supposées semblables. On désigne par B_1 la base canonique de K^n , et par U l'endomorphisme de K^n canoniquement associé à M_1 . (La matrice M_1 n'est autre que la matrice associée à U dans la base B_1 .) Il existe alors une base B_2 de K^n telle que M_2 soit la matrice associée à U dans la base B_2 .

Supposons en effet que les matrices M_1 et M_2 soient liées par la relation

$$M_2 = QM_1Q^{-1}.$$

Il existe une base B_2 et une seule de K^n telle que Q soit la matrice de passage de B_2 à B_1 . La matrice associée à U dans la base B_2 n'est autre que $QM_1Q^{-1} = M_2$ ce qu'il fallait prouver.

REMARQUE 1. — Deux matrices semblables sont *a fortiori* équivalentes (au sens de la déf. 4.5), mais la réciproque n'est pas vraie : par exemple une matrice carrée M d'ordre n est équivalente à la matrice unité I_n si et seulement si M est inversible, tandis que M est semblable à I_n si et seulement si $M = I_n$.

REMARQUE 2. — Au paragraphe 4.1, nous avons pu caractériser de façon simple les matrices équivalentes à une matrice donnée (cf. corollaire 2 du théorème 4.1). Il est beaucoup plus délicat de caractériser les matrices semblables à une matrice donnée : cette caractérisation fait l'objet de la théorie des invariants de similitude, qu'on trouvera esquissée dans l'exercice 64.

DÉFINITION 5.14. — Spectre d'une matrice carrée. — Soient M une matrice carrée d'ordre n à éléments dans K , et U l'endomorphisme de K^n canoniquement associé à M . On appelle valeurs propres, sous-espaces propres, sous-espaces spectraux ... de M les valeurs propres, sous-espaces propres, sous-espaces spectraux... de U .

De même, on appelle polynôme caractéristique de M le polynôme caractéristique de U ; les valeurs propres de M sont donc les racines du polynôme caractéristique de M .

Enfin, on dit que M est scindée (resp. diagonalisable, resp. trigonalisable) sur K si U est scindé (resp. diagonalisable, resp. trigonalisable) sur K .

PROPOSITION 5.28. — Spectre des matrices associées à un endomorphisme. Soient E un espace vectoriel de dimension finie non nulle n sur K , U un endomorphisme de E , B une base de E , et $M_B(U)$ la matrice associée à U dans la base B . Le polynôme minimal de $M_B(U)$ est égal à celui de U . Ainsi, pour que la matrice $M_B(U)$ soit diagonalisable (resp. trigonalisable), il faut et il suffit que U soit diagonalisable (resp. trigonalisable).

En effet, pour tout élément P de $K[X]$, les relations $P(U) = 0$, $M_B[P(U)] = 0$ et $P[M_B(U)] = 0$ sont équivalentes.

PROPOSITION 5.29. — Spectres de deux matrices semblables. — Soient M et M' deux matrices carrées d'ordre n , liées par la relation $M' = QMQ^{-1}$, où $Q \in \text{GL}_n(K)$.

1. Les matrices M et M' ont même polynôme minimal; elles sont donc simultanément diagonalisables ou trigonalisables.

Le spectre de M' dans K est égal au spectre de M dans K .

2. Pour tout scalaire λ , et pour tout entier naturel r ,

$$(1) \quad E_{\lambda,r}(M') = Q[E_{\lambda,r}(M)].$$

En particulier, le sous-espace propre (resp. spectral) de M' associé à une valeur propre λ de M' (ou de M) est l'image par Q du sous-espace propre (resp. spectral) de M associé à λ .

Ainsi, pour qu'un vecteur \mathbf{x} de K^n soit un vecteur propre de M' associé à une valeur propre λ de M' (ou de M) il faut et il suffit que $Q^{-1}(\mathbf{x})$ soit un vecteur propre de M associé à λ .

Assertion 1. — Pour tout élément Q de $\text{GL}_n(K)$, l'application $\sigma_Q: M \mapsto QMQ^{-1}$ est un automorphisme de l'algèbre unitaire $\mathbf{M}_n(K)$. Il en découle aussitôt que M et M' ont même polynôme minimal, car, pour tout élément P de $K[X]$, la relation $P(M) = 0$ équivaut à la relation $P(M') = 0$.

Assertion 2. — Comme σ_Q est un automorphisme de l'algèbre unitaire $\mathbf{M}_n(K)$, pour tout scalaire λ et pour tout entier naturel r ,

$$(M' - \lambda I_n)^r = Q(M - \lambda I_n)^r Q^{-1}.$$

La formule (1) en résulte aussitôt.

La théorie des endomorphismes scindés (cf. th. 5.12) nous conduit à poser la

DÉFINITION 5.15. — Matrices trigonales supérieures réduites. — On dit qu'une matrice carrée d'ordre n à éléments dans K est une matrice trigonale supérieure réduite si elle est décomposée en r blocs diagonaux M_1, M_2, \dots, M_r , d'ordres m_1, m_2, \dots, m_r , et si, pour tout $j \in [1, r]$, M_j est de la forme

$$M_j = \lambda_j I_{m_j} + N_j,$$

où $\lambda_j \in K$, et où N_j est une matrice trigonale supérieure nilpotente.

Les scalaires $\lambda_1, \lambda_2, \dots, \lambda_r$ sont alors les valeurs propres de M , et, pour tout élément μ de $\text{sp}(M)$, la multiplicité $m(\mu)$ de la valeur propre μ est égale à la somme des entiers m_j , où j est tel que $\lambda_j = \mu$.

PROPOSITION 5.30. — Caractérisation des matrices diagonalisables, et des matrices scindées. — Soient M une matrice carrée d'ordre n à éléments dans K , U l'endomorphisme de K^n canoniquement associé à M , et B la base canonique de K^n .

1. Pour que M soit diagonalisable sur K , il faut et il suffit que M soit semblable à une matrice diagonale.

Plus précisément, si M est diagonalisable, il existe une base $B' = (f_1, f_2, \dots, f_n)$ de K^n constituée de vecteurs propres de U . Ainsi, pour tout $j \in [1, n]$, $U(f_j) = \lambda_j f_j$. Soient D la matrice diagonale ayant pour éléments $\lambda_1, \lambda_2, \dots, \lambda_n$, et P la matrice de passage de B à B' ; alors

$$M = PDP^{-1}.$$

2. Pour que M soit scindée sur K , ou trigonalisable sur K , il faut et il suffit que M soit semblable à une matrice trigonale supérieure.

Plus précisément, si M est scindée sur K , il existe une base $B' = (f_1, f_2, \dots, f_n)$ de K^n telle que $T = M_{B'}(U)$ soit une matrice trigonale supérieure réduite. Soit P la matrice de passage de B à B' ; alors

$$M = PTP^{-1}.$$

Assertion 1. — Il est immédiat qu'une matrice diagonale est diagonalisable. Or, toute matrice semblable à une matrice diagonalisable est diagonalisable (cf. prop. 5.29). Par suite, toute matrice semblable à une matrice diagonale est diagonalisable.

L'assertion 2 se prouve exactement de la même façon.

Notons enfin le résultat suivant, souvent utile :

PROPOSITION 5.31. — Densité des matrices diagonalisables. — On suppose que K est algébriquement clos. Soient n un entier strictement positif, et P un élément de $K[(X_{ij})]$, où (i, j) parcourt $[1, n] \times [1, n]$. Pour tout élément $M = (\alpha_{ij})$ de $M_n(K)$, on désigne par P_M le scalaire obtenu en substituant les scalaires α_{ij} aux indéterminées X_{ij} dans P .

Si P_M est nul pour toute matrice M diagonalisable, alors P_M est nul pour toute matrice M .

Soit en effet \mathcal{E} l'ensemble des matrices M ayant n valeurs propres distinctes. Le corps K étant algébriquement clos, \mathcal{E} n'est autre que l'ensemble des matrices M telles que le discriminant Δ_M du polynôme caractéristique de M soit non nul (cf. chap. III.1). Le principe de prolongement des identités algébriques (cf. cor. 1 du th. 2.10) montre alors que si $P_M = 0$ pour tout élément M de \mathcal{E} , $P_M = 0$ pour tout élément M de $M_n(K)$. Or, le corollaire du théorème 5.8 montre aussitôt que \mathcal{E} est contenu dans l'ensemble des matrices diagonalisables, ce qui achève la démonstration.

Méthodes pratiques de réduction des matrices. — Soient $M = (\alpha_{ij})$ une matrice carrée d'ordre n à éléments dans K , et U l'endomorphisme de K^n canoniquement associé à M . Par définition, diagonaliser (resp. trigonaliser, resp. réduire) M , c'est déterminer une matrice diagonale D (resp. une matrice trigonale supérieure T , resp. une matrice trigonale supérieure réduite T') et un élément P de $\text{GL}_n(K)$ tels que

$$M = PDP^{-1} \text{ (resp. } M = PTP^{-1}, \text{ resp. } M = PT'P^{-1}).$$

Cela revient à déterminer une base (f_1, f_2, \dots, f_n) de K^n dans laquelle la matrice associée à U soit diagonale (resp. trigonale supérieure, resp. trigonale supérieure réduite).

Voici une méthode pratique de construction d'une telle base :

a) On forme le polynôme caractéristique de M , et on détermine ses racines $\lambda_1, \lambda_2, \dots, \lambda_r$, avec leurs multiplicités $m(\lambda_1), m(\lambda_2), \dots, m(\lambda_r)$.

Dans toute la suite, nous supposons que M est scindée sur K ; pour cela, il faut et il suffit que son polynôme caractéristique soit scindé sur K .

b) Pour chaque valeur propre de M , c'est-à-dire pour chaque racine λ , du polynôme caractéristique de M , on détermine une base du sous-espace propre $E_\lambda(U)$. Pour cela, on résout le système d'équations linéaires homogènes

[illegible]

dont le déterminant est nul. Soit $m_1(\lambda_j)$ la dimension du sous-espace vectoriel $E_{\lambda_j,1}(U)$.

c) La matrice M est diagonalisable si et seulement si la réunion des diverses bases ainsi obtenues est constituée de n vecteurs $\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_n$; cela revient à dire que, pour toute valeur propre λ_j , $m_1(\lambda_j) = m(\lambda_j)$.

d) Dans le cas contraire, pour toute valeur propre λ_j telle que $m_1(\lambda_j)$ soit strictement inférieur à $m(\lambda_j)$, on complète la base de $E_{\lambda_j,1}(U)$ en une base de $E_{\lambda_j,2}(U)$. Soit $m_2(\lambda_j)$ la dimension de $E_{\lambda_j,2}(U)$. Si $m_2(\lambda_j) = m(\lambda_j)$, on a ainsi déterminé une base du sous-espace spectral $F_{\lambda_j}(U)$. Sinon, on réitère ce procédé, en déterminant une base du sous-espace vectoriel $E_{\lambda_j,p}(U)$ jusqu'à ce que $m_p(\lambda_j)$ soit égal à $m(\lambda_j)$.

En réunissant les bases des sous-espaces spectraux $F_{\lambda_j}(U)$ ainsi construites, on obtient une base (f_1, f_2, \dots, f_n) de K^n dans laquelle la matrice associée à U est trigonale supérieure réduite.

REMARQUE 1. — Voici comment on peut compléter une base de $E_{\lambda_j,1}(U)$ en une base de $E_{\lambda_j,2}(U)$, lorsque $m_1(\lambda_j) = m(\lambda_j) - 1$: on résout le système linéaire

$$U(\mathbf{x}) - \lambda_j \mathbf{x} = \mathbf{a}_j,$$

où a_j est un élément non nul de $E_{\lambda_j,1}(U)$, qu'on décompose dans la base déjà construite de $E_{\lambda_j,1}(U)$.

EXEMPLE. — Trigonaliser la matrice à éléments complexes

$$M = \begin{pmatrix} 2 & -2 & 3 \\ 10 & -4 & 5 \\ 5 & -4 & 6 \end{pmatrix}.$$

Le polynôme caractéristique de M est

$$X^3 - 4X^2 + 5X - 2 = (X - 1)^2(X - 2).$$

Le sous-espace propre associé à la valeur propre 2 est la droite engendrée par le vecteur $f_1 = (4, 15, 10)$. Le sous-espace propre associé à la valeur propre 1 est la droite engendrée par le vecteur $f_2 = (1, 5, 3)$. La résolution du système linéaire

$$U(x) - x = f_2$$

montre que $f_3 = (0, -2, -1)$ est un élément de $E_{1,2}(U)$. La matrice associée à U dans la base (f_1, f_2, f_3) est donc

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

La matrice P admet pour colonnes les composantes de f_1, f_2, f_3 ; donc

$$P = \begin{pmatrix} 4 & 1 & 0 \\ 15 & 5 & -2 \\ 10 & 3 & -1 \end{pmatrix}.$$

REMARQUE 2. — Dans de nombreux exemples, il est plus simple d'utiliser une interprétation géométrique, afin de déterminer directement les vecteurs propres, et par la même occasion les valeurs propres.

EXEMPLE. — Diagonaliser la matrice à éléments complexes

$$M = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}.$$

Soit $x = (\xi_1, \xi_2, \dots, \xi_n)$ un élément de C^n ; alors $U(x) = \sum_{j=1}^n \xi_j U(e_j)$.

Or, pour tout $j \in [1, p]$, l'image par U du vecteur e_j est le vecteur $f = (1, 1, \dots, 1)$.
Donc

$$U(x) = \left(\sum_{j=1}^n \xi_j \right) f.$$

Si le vecteur x est un vecteur propre, deux cas se présentent :

a) le vecteur x est colinéaire à f ; le vecteur f est effectivement un vecteur propre, associé à la valeur propre n ;

b) le vecteur $U(\mathbf{x})$ est nul; l'hyperplan H , d'équation $\sum_{j=1}^n \xi_j = 0$ est un sous-espace propre, associé à la valeur propre 0.

Il s'ensuit que M est diagonalisable. On obtient une base de vecteurs propres en réunissant le vecteur f et une base de H .

REMARQUE 3. — Notons enfin que si une matrice M est de la forme $P(N)$, où P est un polynôme et N une autre matrice, la diagonalisation de M se ramène aussitôt à celle de N , d'après le théorème de Hilbert-Dirac.

EXEMPLE. — Soit

$$M = \begin{pmatrix} \alpha & \beta & \beta \\ \beta & \alpha & \beta \\ \beta & \beta & \alpha \end{pmatrix}.$$

La matrice M peut s'écrire sous la forme $M = \alpha I_3 + \beta N$, où

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

La diagonalisation de M se ramène à celle de N .

Voici enfin une méthode de calcul pratique d'un polynôme matriciel :

PROPOSITION 5.32. — **Substitution d'une matrice carrée dans un polynôme.** Soient M un élément de $M_n(K)$ et P un élément de $K[X]$.

1. Si M est scindé, il en est de même de $P(M)$.
2. Si M est diagonalisable sur K , il en est de même de $P(M)$.
3. Si T est une matrice trigonale supérieure réduite, décomposée en les blocs diagonaux M_1, M_2, \dots, M_s , où, pour tout $j \in [1, s]$,

$$M_j = \lambda_j I_{m_j} + N_j,$$

la matrice N_j étant trigonale supérieure nilpotente, alors $P(T)$ est encore une matrice trigonale supérieure réduite; elle est décomposée en les blocs diagonaux

$$P(M_1), P(M_2), \dots, P(M_s).$$

Enfin, pour tout $j \in [1, s]$, $P(M_j)$ peut être calculée grâce à son développement taylorien

$$P(M_j) = P(\lambda_j)I_{m_j} + \frac{P'(\lambda_j)}{1!} N_j + \dots + \frac{P^{(p)}(\lambda_j)}{p!} N_j^p + \dots$$

4. Si D est une matrice diagonale, de la forme

$$D = \begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_j & \\ & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix},$$

alors $P(D)$ est une matrice diagonale, et

$$P(D) = \begin{pmatrix} P(\lambda_1) & & & 0 \\ & \ddots & & \\ & & P(\lambda_j) & \\ & & & \ddots \\ 0 & & & & P(\lambda_n) \end{pmatrix}.$$

Ainsi, pour calculer $P(M)$, on peut utiliser la méthode suivante :

a) Si M est diagonalisable, on diagonalise M ; autrement dit, on met M sous la forme

$$M = ADA^{-1},$$

où $A \in \text{GL}_n(K)$, et où D est une matrice diagonale. Alors

$$P(M) = AP(D)A^{-1}.$$

b) Dans le cas contraire, on réduit M ; autrement dit, on écrit M sous la forme

$$M = ATA^{-1},$$

où $A \in \text{GL}_n(K)$, et où T est une matrice trigonale supérieure réduite. Alors

$$P(M) = AP(T)A^{-1}.$$

REMARQUE. — Cette proposition permet en particulier de calculer pour tout entier $p > 0$ la puissance $p^{\text{ième}}$ d'une matrice carrée. Elle se généralise facilement au cas où l'on effectue une substitution d'un endomorphisme, ou d'une matrice carrée, dans une fraction rationnelle; cf. exercices 65 et 66.

Nous verrons (cf. *Analyse* III) comment on peut effectuer une substitution d'un endomorphisme ou d'une matrice carrée dans une série entière, ou même dans une fonction analytique.

Exercices conseillés : 31 à 49.

§ 7. RÉDUITE DE JORDAN

La théorie de la réduction exposée au § 4 suffit pour la plupart des applications pratiques. Cependant, pour certaines questions (caractérisation des matrices semblables, étude générale des systèmes de suites récurrentes ou des systèmes d'équations différentielles, par exemple), on a besoin d'un résultat plus précis. A cet effet, nous utiliserons la

DÉFINITION 5.16. — **Sous-espace vectoriel stable engendré par un vecteur.** Soient U un endomorphisme d'un espace vectoriel E sur K et x un vecteur

de E . L'ensemble des sous-espaces vectoriels de E contenant \mathfrak{x} et stables par U admet un plus petit élément, à savoir l'intersection de tous les sous-espaces vectoriels de E contenant \mathfrak{x} et stables par U ; on l'appelle sous-espace vectoriel stable par U engendré par \mathfrak{x} .

Ce sous-espace vectoriel n'est autre que l'ensemble des vecteurs $[P(U)](\mathfrak{x})$, où P parcourt $K[X]$.

DÉFINITION 5.17. — Sous-espaces vectoriels monogènes. — Soit U un endomorphisme d'un espace vectoriel E sur K . On dit qu'un sous-espace vectoriel F de E stable par U est monogène relativement à U , ou encore U -monogène, s'il existe un élément \mathfrak{x} de F tel que le sous-espace vectoriel stable par U engendré par \mathfrak{x} soit égal à F . On dit alors que \mathfrak{x} est un U -générateur de F .

PROPOSITION 5.33. — Annulateur d'un vecteur. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , et \mathfrak{x} un vecteur de E .

1. L'idéal $\mathfrak{I}_{\mathfrak{x}}$ constitué des éléments P de $K[X]$ tels que \mathfrak{x} appartienne au noyau de $P(U)$ n'est pas réduit à $\{0\}$. Son générateur est un polynôme unitaire, noté $\pi_{\mathfrak{x}}$, divisant le polynôme minimal π de U ; on l'appelle annulateur de \mathfrak{x} relativement à U .

2. Soit $E_{\mathfrak{x}}$ le sous-espace vectoriel de E stable par U engendré par \mathfrak{x} . Le polynôme $\pi_{\mathfrak{x}}$ n'est autre que le polynôme minimal de l'endomorphisme $U_{\mathfrak{x}}$ de $E_{\mathfrak{x}}$ coïncidant avec U .

3. Soient r le degré de $\pi_{\mathfrak{x}}$ et, pour tout élément j de $[1, r]$, $e_j = U^{r-j}(\mathfrak{x})$. Alors la famille $B = (e_j)_{1 \leq j \leq r}$ est une base de l'espace vectoriel $E_{\mathfrak{x}}$. En particulier,

$$(1) \quad \dim E_{\mathfrak{x}} = d^0(\pi_{\mathfrak{x}}).$$

En outre, lorsque $\pi_{\mathfrak{x}}$ est écrit sous la forme

$$\pi_{\mathfrak{x}} = X^r + \sum_{p=0}^{r-1} \alpha_p X^p,$$

la matrice associée à $U_{\mathfrak{x}}$ dans la base B est égale à

$$\begin{pmatrix} -\alpha_{r-1} & 1 & 0 & \dots & 0 & 0 \\ -\alpha_{r-2} & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -\alpha_1 & 0 & 0 & \dots & 0 & 1 \\ -\alpha_0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

Cette matrice est appelée matrice canonique associée au polynôme unitaire

$$X^r + \sum_{p=0}^{r-1} \alpha_p X^p.$$

Réciproquement, soient F un sous-espace vectoriel de E stable par U et V l'endomorphisme de F coïncidant avec U . S'il existe une base $B = (e_j)_{1 \leq j \leq r}$ de F dans laquelle la matrice associée à V est de la forme précédente, F est monogène relativement à U , et e_r est un U -générateur de F .

L'assertion 1 est immédiate.

Assertion 2. — Soit π' le polynôme minimal de $U_{\mathfrak{x}}$. Puisque $[\pi'(U)](\mathfrak{x}) = 0$, $\pi_{\mathfrak{x}}$ divise π' . D'autre part, puisque tout vecteur y de $E_{\mathfrak{x}}$ est de la forme $[Q(U)](\mathfrak{x})$, où $Q \in K[X]$, et que $[\pi_{\mathfrak{x}}(U)](\mathfrak{x}) = 0$, nous voyons que $[\pi_{\mathfrak{x}}(U)](y) = 0$; donc π' divise $\pi_{\mathfrak{x}}$. Comme π' et $\pi_{\mathfrak{x}}$ sont unitaires, il en découle que $\pi' = \pi_{\mathfrak{x}}$.

Assertion 3. — La famille B est libre : en effet, s'il existait une relation linéaire non triviale de la forme $\sum_{p=0}^{r-1} \beta_p U^p(\mathfrak{x}) = 0$, le polynôme $Q = \sum_{p=0}^{r-1} \beta_p X^p$ appartiendrait à $\mathfrak{I}_{\mathfrak{x}}$, ce qui est impossible.

Soit F le sous-espace vectoriel de E engendré par B . Puisque $[\pi_{\mathfrak{x}}(U)](\mathfrak{x}) = 0$, $U^r(\mathfrak{x})$ appartient à F . Il en découle aussitôt que F est stable par U . Comme \mathfrak{x} appartient à F , il s'ensuit que F contient $E_{\mathfrak{x}}$. L'inclusion opposée étant évidente, $F = E_{\mathfrak{x}}$, ce qui prouve que B est une base de $E_{\mathfrak{x}}$. Le reste de l'assertion est immédiat.

Nous nous proposons maintenant de réduire les endomorphismes d'un espace vectoriel E sur un corps K non nécessairement algébriquement clos. La notion de vecteur propre n'est plus adaptée à ce cas; il convient de la remplacer par la notion suivante :

DÉFINITION 5.18. — Sous-espaces vectoriels irréductibles. — Soient U un endomorphisme d'un espace vectoriel E sur K et F un sous-espace vectoriel de E stable par U . On dit que F est irréductible relativement à U si F n'est pas réduit à $\{0\}$ et si les seuls sous-espaces vectoriels de F stables par U sont $\{0\}$ et F .

Cela équivaut à dire que F n'est pas réduit à $\{0\}$ et que tout vecteur non nul de F est un U -générateur de F .

Les droites de E stables par U sont des sous-espaces vectoriels irréductibles; si le corps K est algébriquement clos, ce sont les seuls sous-espaces vectoriels irréductibles, car, pour tout sous-espace vectoriel de F non réduit à $\{0\}$ et stable par U , il existe au moins un vecteur propre de U appartenant à F .

PROPOSITION 5.34. — Caractérisation des sous-espaces vectoriels irréductibles. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , F un sous-espace vectoriel de E non réduit à $\{0\}$ et stable par U , et V l'endomorphisme de F coïncidant avec U . Pour que F soit irréductible, il faut et il suffit que F soit monogène et que le polynôme minimal π de V soit irréductible. Le polynôme π s'appelle type de F .

Supposons d'abord que F est irréductible. Alors, tout vecteur non nul \mathfrak{x} de F est un U -générateur de F ; donc F est monogène. Le polynôme minimal π de V est de la forme P^r , où P est irréductible et où $r \in \mathbb{N}^*$: dans le cas contraire, le théorème de décomposition des noyaux (cf. th. 5.1) fournirait une décomposition de F en somme directe de sous-espaces vec-

toriels stables par U et non réduits à $\{0\}$, ce qui contredirait l'irréductibilité de F . Enfin, l'entier r est égal à 1 : dans le cas contraire, le noyau de $P(V)$ serait un sous-espace vectoriel de F stable par U , différent de F et non réduit à $\{0\}$, ce qui contredirait encore l'irréductibilité de F .

Supposons réciproquement que F est monogène et que le polynôme minimal π de V est irréductible. Considérons un U -générateur x de F . Alors, d'après la proposition 5.33, $\dim F = d^0(\pi_x) = d^0(\pi)$. Soient y un élément non nul de F et E_y le sous-espace vectoriel stable par U engendré par y . L'annulateur π_y de y divise π . Puisque π est irréductible, $\pi_y = \pi$. Donc $\dim E_y = d^0(\pi_y) = d^0(\pi) = \dim F$. Il en découle que $E_y = F$, ce qu'il fallait prouver.

REMARQUE. — Il peut arriver qu'un sous-espace vectoriel soit monogène sans être irréductible. Soit par exemple U l'endomorphisme de \mathbb{C}^2 défini par les relations $U(e_2) = e_1$ et $U(e_1) = 0$. Alors \mathbb{C}^2 est U -monogène sans être irréductible, puisque la droite $D = \mathbb{C}e_1$ est stable par U .

Le théorème suivant fournit une caractérisation remarquable des endomorphismes semi-simples à l'aide des sous-espaces vectoriels irréductibles, qui généralise au cas des corps non nécessairement algébriquement clos la caractérisation des endomorphismes diagonalisables (cf. th. 5.8) :

THÉORÈME 5.17. — Caractérisation des endomorphismes semi-simples. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K et π le polynôme minimal de U . Il est équivalent de dire :

1. L'espace vectoriel E est somme de sous-espaces vectoriels irréductibles.
2. L'espace vectoriel E est somme directe d'une famille finie de sous-espaces vectoriels irréductibles.
3. L'endomorphisme U est semi-simple.
4. Pour tout polynôme irréductible P , la valuation $v_P(\pi)$ est inférieure ou égale à 1.

Si ces conditions équivalentes sont réalisées, tout sous-espace vectoriel de E stable par U est somme directe d'une famille finie de sous-espaces vectoriels irréductibles.

Pour démontrer que $1 \Rightarrow 2$ et que $1 \Rightarrow 3$, nous utiliserons le

LEMME. — Soit $(E_i)_{i \in I}$ une famille de sous-espaces vectoriels irréductibles de E dont la somme est E . Alors, pour tout sous-espace vectoriel F de E stable par U , il existe une partie finie J de I telle que $E = F \oplus \left(\bigoplus_{i \in J} E_i \right)$.

Soit \mathfrak{E} l'ensemble des parties finies H de I telles que la somme $F + \left(\sum_{i \in H} E_i \right)$ soit directe.

Il est clair que $\text{card}(H) \leq \dim E$. L'ensemble des nombres $\text{card}(H)$, où H parcourt \mathfrak{E} , admet donc un plus grand élément p . Soit J un élément de \mathfrak{E} tel que $\text{card}(J) = p$. Le sous-espace vectoriel $G = F \oplus \left(\bigoplus_{i \in J} E_i \right)$ est évidemment stable par U . Il reste à prouver que $G = E$. Supposons par l'absurde que $G \neq E$. Puisque E est somme des sous-espaces vectoriels E_i , il existe un élément i de I tel que E_i ne soit pas contenu dans G . Comme $E_i \cap G$ est un sous-espace vectoriel de E_i stable par U et différent de E_i , et que E_i est irréductible, $E_i \cap G = \{0\}$. Il en découle que $J \cup \{i\}$ est un élément de \mathfrak{E} contenant strictement J , ce qui contredit la définition de p .

$1 \Rightarrow 2$ s'en déduit aussitôt : il suffit de prendre $F = \{0\}$.

$1 \Rightarrow 3$ s'en déduit aussi : le sous-espace vectoriel $\bigoplus_{i \in J} E_i$ est un supplémentaire de F stable par U .

$2 \Rightarrow 1$ est évident.

$3 \Rightarrow 1$. Il est immédiat que le sous-espace vectoriel E' de E somme de tous les sous-espaces vectoriels irréductibles de E est stable par U . Supposons par l'absurde que $E' \neq E$. Puisque U est semi-simple, E' admet un supplémentaire E'' stable par U et non réduit à $\{0\}$. Considérons l'ensemble \mathcal{F} des sous-espaces vectoriels de E'' stables par U et non réduits à $\{0\}$, et un élément E_1 de \mathcal{F} de dimension minimale. Le sous-espace vectoriel E_1 est irréductible, et $E' \cap E_1 = \{0\}$, ce qui contredit la définition de E' .

$2 \Rightarrow 4$. Soit $(E_i)_{i \in I}$ une famille finie de sous-espaces vectoriels irréductibles dont E est somme directe. D'après la proposition 5.34, pour tout élément i de I , le polynôme minimal de l'endomorphisme de E_i coïncidant avec U est irréductible. Soit alors \mathcal{E} l'ensemble des polynômes minimaux de ces endomorphismes. Il est immédiat que $\pi = \prod_{p \in \mathcal{E}} P$, ce qu'il fallait prouver.

$4 \Rightarrow 1$. Décomposons π en facteurs irréductibles : $\pi = P_1 P_2 \dots P_r$. D'après le théorème de décomposition des noyaux (cf. th. 5.1), E est somme directe des noyaux E_i des endomorphismes $P_i(U)$. Il suffit donc de prouver que, pour tout élément i de $[1, r]$ et pour tout élément non nul x de E_i , le sous-espace vectoriel stable E_x engendré par x est irréductible. Or, le polynôme minimal π' de l'endomorphisme V de E_x coïncidant avec U divise P_i , et P_i est irréductible. Donc π' est irréductible, et, d'après la proposition 5.34, le sous-espace vectoriel E_x est irréductible.

Soit enfin F un sous-espace vectoriel de E stable par U . Si U satisfait à la condition 4, il en est évidemment de même de l'endomorphisme V de F coïncidant avec U . Le sous-espace vectoriel F est donc somme directe de sous-espaces vectoriels irréductibles relativement à V , ce qui achève la démonstration du théorème.

REMARQUE. — L'équivalence des assertions 1, 2 et 3 résulte de la théorie des modules semi-simples; cf. exercice I.3.96. Il suffit de munir E de la structure de $K[X]$ -module définie par l'application $(P, x) \mapsto [P(U)](x)$. La notion de sous-espace vectoriel stable (resp. de sous-espace vectoriel monogène, resp. de sous-espace vectoriel irréductible) correspond alors à celle de sous-module (resp. de sous-module monogène, resp. de sous-module semi-simple). Pour que l'endomorphisme U soit semi-simple, il faut et il suffit que ce module soit semi-simple.

COROLLAIRE. — Cas des endomorphismes dont le polynôme minimal est irréductible. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K , dont le polynôme minimal π est irréductible. Il existe alors une famille (E_1, E_2, \dots, E_p) de sous-espaces vectoriels irréductibles de E dont E est somme directe. Ces sous-espaces vectoriels sont tous de type π . En particulier, $\dim E = p \, d^0(\pi)$.

D'après le théorème précédent, il existe une famille finie (E_1, E_2, \dots, E_p) de sous-espaces vectoriels irréductibles de E dont E est somme directe. Pour tout élément i de $[1, p]$, le polynôme minimal de l'endomorphisme V_i de E_i coïncidant avec U divise π . Comme π est irréductible, ce polynôme est égal à π . Il en résulte que $\dim E_i = d^0(\pi)$, et, par suite, que $\dim E = p \, d^0(\pi)$.

Considérons maintenant un endomorphisme quelconque U d'un espace vectoriel E de dimension finie sur K . Soit

$$\pi = \prod_{i=1}^p P_i^{q_i}$$

la décomposition en facteurs irréductibles sur K du polynôme minimal π de U . D'après le théorème de décomposition des noyaux (cf. cor. 2 du th. 5.1), l'espace vectoriel E est somme directe des noyaux des endomorphismes $Q_i(U)$, où, pour tout élément i de $[1, p]$, $Q_i = P_i^{q_i}$. Il en découle que le polynôme minimal de l'endomorphisme de E_i coïncidant avec U est égal à Q_i . L'étude de U se ramène ainsi à celle d'endomorphismes dont le polynôme minimal est une puissance d'un polynôme irréductible.

Nous sommes ainsi amené à poser la

DÉFINITION 5.19. — Endomorphismes de Jordan. — Soient P un élément irréductible de $K[X]$ et r un entier naturel. On dit qu'un endomorphisme U d'un espace vectoriel E de dimension finie sur K non réduit à $\{0\}$ est un endomorphisme de Jordan de type P^r si E est U -monogène et si le polynôme minimal de U est égal à P^r .

Soient \mathfrak{x} un vecteur U -générateur de E , n le degré de P^r et, pour tout élément j de $[1, n]$, $e_j = U^{n-j}(\mathfrak{x})$. La famille $(e_j)_{1 \leq j \leq n}$ est alors une base de E ; en particulier, $\dim E = r \operatorname{d}^\circ(P)$. La matrice associée à U dans cette base s'appelle matrice de Jordan de type P^r .

EXEMPLE 1. — Cas des endomorphismes scindés. — Soit U un endomorphisme scindé d'un espace vectoriel E de dimension finie n sur K . Si U est un endomorphisme de Jordan, le polynôme minimal de U est de la forme $(X - \lambda)^n$, où $\lambda \in K$. On dit alors plus simplement que U est de type (λ, n) . La matrice associée à U dans la base précédemment définie est égale à la matrice $J_{\lambda, n}$ suivante :

$$J_{\lambda, n} = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Cette matrice s'appelle matrice de Jordan de type (λ, n) .

Soit en effet P^r le polynôme minimal de U . Puisque U est scindé, P^r est un polynôme scindé; donc P est de la forme $X - \lambda$, où $\lambda \in K$. La relation $\dim E = r \operatorname{d}^\circ(P)$ montre alors que $r = n$.

REMARQUE. — Si K est algébriquement clos, ce résultat s'applique à tout endomorphisme de Jordan de E .

EXEMPLE 2. — Si l'espace vectoriel E est irréductible relativement à U , U est un endomorphisme de Jordan, dont le polynôme minimal est irréductible.

La notion d'endomorphismes de Jordan permet d'effectuer la réduction des endomorphismes dont le polynôme minimal est une puissance d'un polynôme irréductible, qui généralisent au cas des corps non nécessairement algébriquement clos les endomorphismes n'ayant qu'une seule valeur propre :

THÉOREME 5.18. — Réduction des endomorphismes dont le polynôme minimal est une puissance d'un polynôme irréductible. — Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K , dont le polynôme minimal π est de la forme P^p , où P est irréductible et où p est un entier naturel non nul.

1. Il existe une famille finie $(E_i)_{i \in I}$ de sous-espaces vectoriels de E non réduits à $\{0\}$, stables par U et monogènes, telle que E soit somme directe des sous-espaces vectoriels E_i . De plus, pour tout élément i de I , l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan de type P^{r_i} , où r_i appartient à $[1, p]$.

Par suite, pour tout élément i de I , il existe une base B_i de E_i telle que la matrice M_i associée à U_i soit une matrice de Jordan. La matrice associée à U dans la base B obtenue en réunissant les bases B_i est décomposée en les blocs diagonaux M_i . Une telle base s'appelle base de Jordan pour l'endomorphisme U .

2. Soit, pour tout élément r de $[1, p]$, m_r le nombre des éléments i de I tels que $r_i = r$. Alors la suite (m_1, m_2, \dots, m_p) est indépendante du choix de la famille $(E_i)_{i \in I}$.

Assertion 1. — La démonstration s'effectue par récurrence sur l'entier p . Lorsque $p = 1$, le polynôme minimal π de U est égal à P . Comme P est irréductible, E est somme directe d'une famille finie $(E_i)_{i \in I}$ de sous-espaces vectoriels irréductibles, donc monogènes. De plus, ces sous-espaces vectoriels sont de type P . En particulier, l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan de type P .

Soit donc p un entier strictement supérieur à 1. Supposons l'assertion démontrée pour tout couple (F, V) constitué d'un espace vectoriel F et d'un endomorphisme V de F dont le polynôme minimal est égal à P^r , où $r < p$, et considérons un endomorphisme U de E dont le polynôme minimal est égal à P^p . Introduisons l'espace vectoriel quotient $F = E/\text{Ker } P(U)$, et l'application canonique φ de E sur F . Puisque $\text{Ker } P(U)$ est stable par U , il existe un endomorphisme V de F et un seul tel que $V \circ \varphi = \varphi \circ U$:

$$\begin{array}{ccc} & U & \\ E & \longrightarrow & E \\ \varphi \downarrow & & \downarrow \varphi \\ & V & \\ F & \longrightarrow & F \end{array}$$

Nous procédons alors en plusieurs étapes :

a) Le polynôme minimal π' de V est égal à P^{p-1} . — En effet, pour tout élément y de F , écrit sous la forme $y = \varphi(x)$, où $x \in E$,

$$[P^{p-1}(V)](y) = [P^{p-1}(V)](\varphi(x)) = \varphi[P^{p-1}(U)(x)].$$

Or, puisque $P^p(U) = 0$, le vecteur $[P^{p-1}(U)](x)$ appartient à $\text{Ker } P(U) = \text{Ker } (\varphi)$. Donc $P^{p-1}(V) = 0$, ce qui prouve que π' divise P^{p-1} .

Réciproquement, considérons un élément x de E . Alors

$$\varphi[(\pi'(U))(x)] = [\pi'(V)](\varphi(x)) = 0.$$

Par suite, le vecteur $[\pi'(U)](x)$ appartient à $\text{Ker } (\varphi) = \text{Ker } P(U)$. Il en découle que $\pi = P^p$ divise $P\pi'$, et donc que P^{p-1} divise π' .

Finalement, comme P et π' sont unitaires, nous voyons que $\pi' = P^{p-1}$.

b) L'hypothèse de récurrence s'applique donc au couple (F, V) . — Il existe une famille finie $(F_j)_{j \in J}$ de sous-espaces vectoriels de F non réduits à $\{0\}$, stables par V et monogènes, telle que F soit somme directe des sous-espaces vectoriels F_j . Alors, pour tout élément j de J , l'endomorphisme V_j de F_j coïncidant avec V est un endomorphisme de Jordan de type P^{r_j} , où r_j appartient à $[1, p-1]$, car son polynôme minimal divise celui de V , à savoir P^{p-1} . Pour tout élément j de J , introduisons un vecteur y_j de F_j générateur relativement à V_j , et un vecteur x_j de E tel que $\varphi(x_j) = y_j$. Désignons par E'_j le sous-espace vectoriel de E stable par U engendré par x_j , et par U'_j l'endomorphisme de E'_j coïncidant avec U .

c) Pour tout élément j de J , $\varphi[E'_j] = F_j$. — Soit en effet $z_j = [Q_j(U)](x_j)$ un élément de E'_j , où Q_j appartient à $K[X]$. Alors

$$\varphi(z_j) = \varphi[Q_j(U)(x_j)] = [Q_j(V)](\varphi(x_j)) = [Q_j(V)](y_j).$$

Donc $\varphi(z_j)$ appartient à F_j , et $\varphi(E'_j) \subset F_j$. D'autre part, le sous-espace vectoriel $\varphi(E'_j)$ est stable par V , car $V[\varphi(z_j)] = \varphi[U(z_j)]$. Comme y_j appartient à $\varphi(E'_j)$, il en découle que F_j est contenu dans $\varphi(E'_j)$. Ainsi, $\varphi(E'_j) = F_j$.

d) La somme des sous-espaces vectoriels E'_j est directe. — Soit en effet $(z_j)_{j \in J}$ une famille d'éléments de E telle que $\sum_{j \in J} z_j = 0$ et que, pour tout élément j de J , z_j appartiennent à E'_j .

Il en découle que $\sum_{j \in J} \varphi(z_j) = 0$. Puisque $\varphi(z_j)$ appartient à F_j et que la somme des sous-espaces vectoriels F_j est directe, nous en déduisons que, pour tout élément j de J , $\varphi(z_j) = 0$, c'est-à-dire que $z_j \in E'_j \cap \text{Ker } P(U)$. Or, pour tout élément j de J , z_j peut s'écrire sous la forme $z_j = [Q_j(U)](x_j)$, où Q_j appartient à $K[X]$. La relation $\varphi(z_j) = 0$ s'écrit alors $[Q_j(V)](y_j) = 0$, ce qui montre que P^{r_j} divise Q_j . Comme $r_j \geq 1$, z_j peut s'écrire sous la forme $z_j = [P(U)](w_j)$, où w_j appartient à E'_j . La relation $\sum_{j \in J} z_j = 0$ implique alors que

$\sum_{j \in J} \varphi(w_j) = 0$. Puisque $\varphi(w_j)$ appartient à F_j et que la somme des sous-espaces vectoriels F_j est directe, nous en déduisons que, pour tout élément j de J , $\varphi(w_j) = 0$, c'est-à-dire que $z_j = [P(U)](w_j) = 0$, ce qui achève la démonstration.

e) Existence de la famille $(E_i)_{i \in I}$. — Puisque $F = \bigoplus_{j \in J} F_j$ et que, pour tout élément j de J , $\varphi(E'_j) = F_j$, E est somme du sous-espace vectoriel $E' = \bigoplus_{j \in J} E'_j$ et de $\text{Ker } P(U)$. Le sous-espace vectoriel $E' \cap \text{Ker } P(U)$ est stable par U . Comme P est irréductible, l'endomorphisme U' de $E' \cap \text{Ker } P(U)$ coïncidant avec U est semi-simple (cf. th. 5.17). Le sous-espace vectoriel $E' \cap \text{Ker } P(U)$ admet donc un supplémentaire E'' dans $\text{Ker } P(U)$ stable par U' , c'est-à-dire stable par U . Alors $E = E' \oplus E''$. Enfin, l'endomorphisme U'' de E'' coïncidant avec U admet P pour polynôme minimal. Puisque P est irréductible, E'' est somme directe d'une famille finie $(E''_h)_{h \in H}$ de sous-espaces vectoriels irréductibles, tous de type P . Ces sous-espaces vec-

toriels sont donc monogènes, et, pour tout élément h de H , l'endomorphisme U_h'' de E_h'' coïncidant avec U est de Jordan de type P . La famille $(E_i)_{i \in I}$ obtenue en réunissant les familles $(E_j')_{j \in J}$ et $(E_h'')_{h \in H}$ convient visiblement.

Assertion 2. — Pour tout élément r de $[1, p]$, considérons le triplet (F_r, φ_r, V_r) défini par récurrence de la manière suivante : $F_1 = F$, $\varphi_1 = \varphi$, $V_1 = V$; pour tout entier $r > 1$, $F_r = F_{r-1}/\text{Ker } P(V_{r-1})$, φ_r est l'application canonique de F_{r-1} sur F_r , et V_r est l'unique endomorphisme de F_r tel que $V_r \circ \varphi_r = \varphi_r \circ V_{r-1}$. La démonstration de l'assertion 1 montre que

$$\dim \text{Ker } [P(U)] = (m_1 + m_2 + \dots + m_p) d^0(P).$$

Le même raisonnement, appliqué au couple (F_r, V_r) , montre que, pour tout élément r de $[1, p]$,

$$(1) \quad \dim \text{Ker } [P(V_r)] = (m_{r+1} + m_{r+2} + \dots + m_p) d^0(P).$$

Les équations (1) déterminent de manière unique les entiers m_1, m_2, \dots, m_p en fonction des nombres $\dim \text{Ker } [P(V_r)]$, lesquels sont indépendants de la décomposition $(E_i)_{i \in I}$ choisie. La suite (m_1, m_2, \dots, m_p) est donc aussi indépendante du choix de la famille $(E_i)_{i \in I}$.

Lorsque le corps K est algébriquement clos, le polynôme minimal π de U est nécessairement de la forme $(X - \lambda)^p$; autrement dit, $U - \lambda I_E$ est nilpotent et admet X^p pour polynôme minimal, ce qui montre l'importance du

COROLLAIRE. — Réduction des endomorphismes nilpotents. — Soient U un endomorphisme nilpotent d'un espace vectoriel E de dimension finie sur K , et X^p son polynôme minimal.

1. Il existe une famille finie $(E_i)_{i \in I}$ de sous-espaces vectoriels de E non réduits à $\{0\}$, stables par U et monogènes relativement à U , telle que E soit somme directe des sous-espaces vectoriels E_i . De plus, pour tout élément i de I , l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan de type $(0, r_i)$, où r_i appartient à $[1, p]$, et $\dim E_i = r_i$.

Par suite, pour tout élément i de I , il existe une base B_i de E_i telle que la matrice M_i associée à U_i soit une matrice de Jordan :

$$M_i = J_{0, r_i} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

La matrice associée à U dans la base B obtenue en réunissant les bases B_i est décomposée en les blocs diagonaux M_i :

$$M_B(U) = \begin{pmatrix} M_1 & & & 0 \\ & \ddots & & \\ & & M_i & \\ 0 & & & M_s \end{pmatrix}.$$

2. Soit, pour tout élément r de $[1, p]$, m_r le nombre des éléments i de I tels que $\dim E_i = r$. Alors la suite (m_1, m_2, \dots, m_r) est indépendante du choix de la famille $(E_i)_{i \in I}$.

On trouvera esquissée dans l'exercice 60 une démonstration plus élémentaire de ce corollaire, fournissant en outre un algorithme permettant de construire une base de Jordan.

Grâce au théorème précédent, on peut donner une interprétation intéressante des endomorphismes de Jordan. A cet effet, nous introduisons la

DÉFINITION 5.20. — Sous-espaces vectoriels indécomposables. — Soit U un endomorphisme d'un espace vectoriel E sur K . On dit qu'un sous-espace vectoriel F de E stable par U est indécomposable relativement à U s'il n'est pas réduit à $\{0\}$ et s'il n'existe pas de décomposition de F en somme directe de deux sous-espaces vectoriels stables par U et non réduits à $\{0\}$.

Les sous-espaces vectoriels irréductibles sont évidemment indécomposables. La réciproque est vraie si U est semi-simple. Dans le cas général, il n'en est pas toujours ainsi :

THÉOREME 5.19. — Caractérisation des sous-espaces vectoriels indécomposables. — Soient U un endomorphisme d'un espace vectoriel E sur K , F un sous-espace vectoriel de E stable par U et V l'endomorphisme de F coïncidant avec U . Pour que F soit indécomposable relativement à U , il faut et il suffit que F soit U -monogène et que V soit un endomorphisme de Jordan.

Supposons d'abord que V est un endomorphisme de Jordan. Son polynôme minimal est alors de la forme P^r , où P est un élément irréductible de $K[X]$ et r un entier naturel non nul, et $\dim F = r d^0(P)$. Soit (F', F'') un couple de sous-espaces vectoriels de F stables par V dont F est somme directe. Supposons par l'absurde que F' et F'' ne soient pas réduits à $\{0\}$, et considérons deux vecteurs non nuls x' et x'' appartenant respectivement à F' et à F'' . L'annulateur de x' divise P^r , donc est de la forme $P^{r'}$, où $r' \leq r$. De plus, $r' \neq r$, car, dans le cas contraire, le sous-espace vectoriel stable par U engendré par x' aurait pour dimension $r d^0(P)$, ce qui est impossible, puisque $\dim F' < \dim F = r d^0(P)$. Ainsi, $[P^{r-1}(U)](x') = 0$. De même, $[P^{r-1}(U)](x'') = 0$. Comme tout vecteur x de F peut s'écrire sous la forme $x = x' + x''$, où $x' \in F'$ et $x'' \in F''$, il en résulterait que $P^{r-1}(V) = 0$, ce qui contredit la définition de r .

Supposons réciproquement que F est un sous-espace vectoriel indécomposable. Le théorème de décomposition des noyaux (cf. cor. 2 du th. 5.1) montre que le polynôme minimal de V est de la forme P^r , où P est irréductible et r strictement supérieur à 1. Le théorème 5.18 montre alors que F est monogène relativement à V , c'est-à-dire relativement à U . Donc V est un endomorphisme de Jordan.

L'intérêt des sous-espaces vectoriels indécomposables apparaît dans le théorème fondamental suivant :

THÉOREME 5.20. — Réduction de Jordan d'un endomorphisme. — Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , et π le poly-

nôme minimal de U . Il existe une famille finie $(E_i)_{i \in I}$ de sous-espaces vectoriels de E indécomposables relativement à U telle que E soit somme directe des sous-espaces vectoriels E_i . De plus, pour tout élément i de I , l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan de type $P_i^{r_i}$, où P_i est un diviseur irréductible de π et où r_i appartient à $[1, v_{P_i}(\pi)]$.

Par suite, pour tout élément i de I , il existe une base B_i de E_i telle que la matrice M_i associée à U_i soit une matrice de Jordan. La matrice associée à U dans la base B obtenue en réunissant les bases B_i est décomposée en les blocs diagonaux M_i . Une telle base s'appelle base de Jordan pour l'endomorphisme U .

Vu le théorème de caractérisation des endomorphismes indécomposables (cf. th. 5.19), il suffit de prouver que E est somme directe d'une famille de sous-espaces vectoriels indécomposables. Pour cela, on raisonne par récurrence sur la dimension n de E . Lorsque $n = 1$, cette assertion est évidente, puisqu'une droite est toujours indécomposable. Soit donc n un entier strictement supérieur à 1. Supposons l'assertion démontrée pour tout couple (F, V) constitué d'un espace vectoriel F de dimension strictement inférieure à n et d'un endomorphisme V de F , et considérons un endomorphisme U d'un espace vectoriel E de dimension n . Si E est indécomposable, l'assertion est encore évidente. Sinon, il existe un couple (F, G) de sous-espaces vectoriels de E non réduits à $\{0\}$, stables par U , dont E est somme directe. Soient V et W les endomorphismes de F et de G coïncidant avec U . Il suffit alors d'appliquer l'hypothèse de récurrence aux couples (F, V) et (G, W) .

COROLLAIRE. — Réduction de Jordan d'un endomorphisme scindé. — Soit U un endomorphisme scindé d'un espace vectoriel E de dimension finie sur K . Il existe une famille $(E_i)_{i \in I}$ de sous-espaces vectoriels de E indécomposables relativement à U , dont E est somme directe. De plus, pour tout élément i de I , l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan; il existe donc une base B_i de E_i telle que la matrice M_i associée à U_i soit de la forme

$$M_i = \lambda_i I_{n_i} + N_i,$$

où $n_i = \dim E_i$, où λ_i est un scalaire et N_i une matrice de Jordan :

$$M_i = \begin{pmatrix} \lambda_i & 1 & & 0 \\ & \lambda_i & 1 & \\ & & \ddots & \ddots \\ 0 & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix}.$$

La matrice associée à U dans la base B obtenue en réunissant les bases B_i est décomposée en les blocs diagonaux M_i :

$$M_B(U) = \begin{pmatrix} M_1 & & 0 \\ & M_2 & \\ & & \ddots \\ 0 & & & M_s \end{pmatrix}.$$

Il suffit d'appliquer le théorème précédent, et de noter que, pour tout élément i de I , l'endomorphisme U_i de E_i coïncidant avec U est un endomorphisme de Jordan scindé.

REMARQUE. — Réduction de Jordan des matrices. — Soient M une matrice carrée d'ordre n à éléments dans K et U l'endomorphisme de K^n canoniquement associé à M . On dit qu'un sous-espace vectoriel de K^n est monogène, irréductible ou indécomposable relativement à M s'il l'est relativement à U . On dit qu'une base de K^n est une base de Jordan pour M si c'est une base de Jordan pour U .

Le théorème de réduction de Jordan des endomorphismes fournit aussitôt l'énoncé suivant :

Pour tout élément M de $M_n(K)$, il existe une base de Jordan pour M . Autrement dit, tout élément M de $M_n(K)$ est semblable à une matrice diagonale de matrices de Jordan.

La proposition 5.32 se précise alors en la

PROPOSITION 5.35. — Substitution d'une matrice carrée dans un polynôme. Soit T une matrice triangulaire supérieure réduite, décomposée en les blocs diagonaux M_1, M_2, \dots, M_s , où, pour tout élément j de $[1, s]$, M_j est égale à la matrice de Jordan J_{λ_j, r_j} . Alors, pour tout élément P de $K[X]$, $P(T)$ est encore une matrice triangulaire supérieure réduite, décomposée en les blocs diagonaux $P(M_1), P(M_2), \dots, P(M_s)$. Enfin, pour tout élément j de $[1, s]$,

$$P(M_j) = P(\lambda_j)I_{r_j} + \frac{DP(\lambda_j)}{1!}J + \frac{D^2P(\lambda_j)}{2!}J^2 + \dots + \frac{D^{r_j-1}P(\lambda_j)}{(r_j-1)!}J^{r_j-1},$$

où J désigne la matrice de Jordan $J_{0,1}$.

Exercices conseillés : 60 à 64.

§ 8. APPLICATIONS DE LA THÉORIE DE LA RÉDUCTION

On suppose que le corps K est de caractéristique 0.

1. ÉQUATIONS AUX DIFFÉRENCES FINIES LINÉAIRES A COEFFICIENTS CONSTANTS

Dans ce sous-paragraphe, p désigne un entier naturel non nul, et T l'endomorphisme de $E = \mathcal{F}(\mathbf{N}, K)$ défini par la formule

$$(Tf)(n) = f(n+1).$$

On appelle *équation aux différences finies linéaire d'ordre p* une équation de la forme

$$(1) \quad (T^p + a_{p-1}T^{p-1} + \dots + a_0)(f) = g,$$

où a_0, a_1, \dots, a_{p-1} et g sont des éléments donnés de $\mathcal{F}(\mathbb{N}, K)$. L'équation (1) signifie donc que, pour tout entier naturel n ,

$$(1') \quad f(n+p) + a_{p-1}(n)f(n+p-1) + \dots + a_0(n)f(n) = g(n).$$

Lorsque les suites a_0, a_1, \dots, a_{p-1} sont des constantes $\alpha_0, \alpha_1, \dots, \alpha_{p-1}$, on dit que l'équation (1) est à coefficients constants. Le polynôme

$$P = X^p + \alpha_{p-1}X^{p-1} + \dots + \alpha_0$$

s'appelle alors polynôme caractéristique de l'équation (1).

PROPOSITION 5.36. — Existence et unicité des solutions d'une équation aux différences finies linéaire. — Soit $(a_0, a_1, \dots, a_{p-1})$ une suite de p éléments de $\mathcal{F}(\mathbb{N}, K)$.

1. Pour tout élément $\mathbf{b} = (\beta_0, \beta_1, \dots, \beta_{p-1})$ de K^p , il existe un élément $f_{\mathbf{b}}$ et un seul de $\mathcal{F}(\mathbb{N}, K)$ satisfaisant pour tout entier naturel n à la relation

$$(2) \quad f(n+p) + a_{p-1}(n)f(n+p-1) + \dots + a_0(n)f(n) = 0$$

et tel que, pour tout élément j de $[0, p-1]$,

$$(3) \quad f(j) = \beta_j.$$

La fonction $f_{\mathbf{b}}$ s'appelle solution de (2) associée à la condition initiale \mathbf{b} .

2. L'application $\varphi : \mathbf{b} \mapsto f_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel K^p sur l'espace vectoriel F des solutions de l'équation (2). En particulier, la dimension de F est égale à p .

Soient $(\mathbf{e}_0, \mathbf{e}_1, \dots, \mathbf{e}_{p-1})$ la base canonique de K^p et, pour tout élément j de $[0, p-1]$, f_j la solution de l'équation (2) associée à la condition initiale \mathbf{e}_j . La famille $(f_0, f_1, \dots, f_{p-1})$ est une base de l'espace vectoriel F , dite canonique.

3. Pour tout élément \mathbf{b} de K^p et pour tout élément g de $\mathcal{F}(\mathbb{N}, K)$, il existe un élément f de $\mathcal{F}(\mathbb{N}, K)$ et un seul vérifiant les relations (1) et (3).

L'assertion 1 est immédiate.

Assertion 2. — L'application φ est linéaire : soient en effet $(\mathbf{b}, \mathbf{b}')$ un couple d'éléments de K^p et (α, α') un couple de scalaires. Alors la fonction $\alpha\varphi(\mathbf{b}) + \alpha'\varphi(\mathbf{b}')$ est solution de (2), car l'équation (2) est linéaire, et admet pour condition initiale $\alpha\mathbf{b} + \alpha'\mathbf{b}'$. D'après l'assertion 1, il en découle que

$$\alpha\varphi(\mathbf{b}) + \alpha'\varphi(\mathbf{b}') = \varphi(\alpha\mathbf{b} + \alpha'\mathbf{b}').$$

L'injectivité de φ résulte encore de l'assertion 1,

Soit enfin f un élément de F . Posons $\mathbf{b} = (f(0), f(1), \dots, f(p-1))$. Il résulte de l'assertion 1 que les fonctions f et $f_{\mathbf{b}}$ sont égales, ce qui montre la surjectivité de φ .

L'assertion 3 est immédiate.

Lorsque l'équation (2) est à coefficients constants et que son polynôme caractéristique est scindé, cette proposition peut se préciser de la manière suivante :

THÉORÈME 5.21. — Structure de l'espace vectoriel des solutions d'une équation homogène à coefficients constants. — Soit

$$P = X^p + \alpha_{p-1}X^{p-1} + \dots + \alpha_0$$

un polynôme scindé sur K tel que $P(0) \neq 0$, décomposé en facteurs irréductibles sous la forme

$$P = \prod_{i=1}^r (X - \lambda_i)^{p_i},$$

où, pour tout élément i de $[1, r]$, λ_i est un scalaire non nul.

1. *L'espace vectoriel F des solutions de l'équation*

$$[P(T)](f) = 0$$

est somme directe des noyaux N_i des endomorphismes $(T - \lambda_i I_E)^{p_i}$, où i parcourt $[1, r]$.

2. *Pour tout élément i de $[1, r]$, le sous-espace vectoriel N_i est de dimension p_i . Plus précisément, soit, pour tout élément j de $[0, p_i - 1]$, f_{ij} la fonction définie par la formule*

$$f_{ij}(n) = \lambda_i^n n^j.$$

Alors la famille (f_{ij}) est une base du sous-espace vectoriel N_i .

En particulier, les éléments de F ne sont autres que les fonctions f de la forme

$$f(n) = \sum_{i=1}^r \lambda_i^n Q_i(n),$$

où, pour tout élément i de $[1, r]$, Q_i est un polynôme de degré strictement inférieur à p_i .

L'assertion 1 résulte aussitôt du théorème de décomposition des noyaux (cf. th. 5.1), appliqué à l'endomorphisme $P(T)$.

Assertion 2. — Nous utiliserons le

LEMME. — Soit $\Delta = T - I_E$. Pour tout entier naturel q , le noyau de l'endomorphisme Δ^q de E est constitué des fonctions polynomiales de degré strictement inférieur à q , c'est-à-dire des fonctions de la forme

$$n \mapsto \sum_{s=0}^{q-1} \gamma_s n^s.$$

En effet, si f est une fonction polynomiale de degré s , Δf est une fonction polynomiale de degré inférieur ou égal à $s - 1$. Il en découle que le sous-

espace vectoriel E_q de E constitué des fonctions polynomiales de degré strictement inférieur à q est contenu dans le noyau de Δ^q . Or, $\dim E_q = q$, et, d'après la proposition 5.36, $\dim \text{Ker}(\Delta^q) = q$. Par suite, $\text{Ker}(\Delta^q) = E_q$, ce qui achève la démonstration du lemme.

Considérons maintenant un scalaire non nul λ . Il est immédiat que $\text{Ker}(T - \lambda I_E)$ n'est autre que la droite engendrée par la fonction $e_\lambda : n \mapsto \lambda^n$. Pour déterminer le noyau de $(T - \lambda I_E)^q$ lorsque $q > 1$, considérons un élément g de E , et calculons $(T - \lambda I_E)(e_\lambda \cdot g)$:

$$\begin{aligned} [(T - \lambda I_E)(e_\lambda \cdot g)](n) &= (e_\lambda \cdot g)(n+1) - \lambda(e_\lambda \cdot g)(n) \\ &= \lambda^{n+1}[g(n+1) - g(n)] = \lambda e_\lambda(n) \cdot (\Delta g)(n). \end{aligned}$$

Donc

$$(T - \lambda I_E)(e_\lambda \cdot g) = \lambda e_\lambda \cdot \Delta g.$$

Par récurrence sur q , nous en déduisons que, pour tout entier q strictement supérieur à 1,

$$(4) \quad (T - \lambda I_E)^q(e_\lambda \cdot g) = \lambda^q e_\lambda \cdot \Delta^q g.$$

Soit f un élément de E . Nous pouvons écrire f sous la forme $f = e_\lambda \cdot g$, où $g \in E$. D'après la formule (4), pour que f appartienne au noyau de $(T - \lambda I_E)^q$, il faut et il suffit que g appartienne au noyau de Δ^q , ou encore que g soit une fonction polynomiale de degré strictement inférieur à q , ce qui achève la démonstration.

Étudions maintenant les systèmes d'équations aux différences finies linéaires.

On appelle *système de p équations aux différences finies linéaires d'ordre 1* un système d'équations de la forme

$$(5) \quad T(f_i) = \sum_{j=1}^p a_{ij} f_j + g_i, \quad i \in [1, p],$$

où, pour tout couple (i, j) d'éléments de $[1, p]$, a_{ij} est un élément donné de $\mathcal{F}(\mathbb{N}, K)$ et où, pour tout élément i de $[1, p]$, g_i est un élément donné de $\mathcal{F}(\mathbb{N}, K)$. Le système (5) signifie donc que, pour tout entier naturel n ,

$$(5') \quad f_i(n+1) = \sum_{j=1}^p a_{ij}(n) f_j(n) + g_i(n), \quad i \in [1, p].$$

Lorsque les suites a_{ij} sont des scalaires α_{ij} , on dit que le système (5) est à coefficients constants. La matrice $M = (\alpha_{ij})$ s'appelle alors matrice associée au système (5), et son polynôme caractéristique s'appelle polynôme caractéristique de ce système. Le système (5) équivaut alors à l'équation suivante :

$$(5'') \quad T(f) = U(f) + g,$$

où $f = (f_1, f_2, \dots, f_p)$, où $g = (g_1, g_2, \dots, g_p)$, et où U est l'endomorphisme de K^p canoniquement associé à M .

PROPOSITION 5.37. — Existence et unicité des solutions d'un système d'équations aux différences finies linéaires. — Soit (a_{ij}) une famille d'éléments de $\mathcal{F}(\mathbf{N}, K)$, où i et j parcourent $[1, p]$.

1. Pour tout élément $\mathbf{b} = (\beta_1, \beta_2, \dots, \beta_p)$ de K^p , il existe une suite $\mathbf{f}_{\mathbf{b}} = (f_1, f_2, \dots, f_p)$ et une seule d'éléments de $\mathcal{F}(\mathbf{N}, K)$ satisfaisant aux relations

$$(6) \quad f_i(n+1) = \sum_{j=1}^p a_{ij}(n) f_j(n), \quad i \in [1, p],$$

et telle que

$$(7) \quad \mathbf{f}(0) = \mathbf{b}$$

L'application $\mathbf{f}_{\mathbf{b}}$ s'appelle solution de (6) associée à la condition initiale \mathbf{b} .

2. L'application $\varphi : \mathbf{b} \mapsto \mathbf{f}_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel K^p sur le sous-espace vectoriel F de l'espace vectoriel $\mathcal{F}(\mathbf{N}, K^p)$ constitué des solutions de l'équation (6). En particulier, la dimension de F est égale à p .

Soient enfin (e_1, e_2, \dots, e_p) la base canonique de K^p et, pour tout élément j de $[1, p]$, \mathbf{f}_j la solution de l'équation (6) associée à la condition initiale e_j . La famille $(\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_p)$ est une base de l'espace vectoriel F , dite canonique.

3. Pour tout élément \mathbf{b} de K^p et pour tout élément g de $\mathcal{F}(\mathbf{N}, K)$, il existe une suite $\mathbf{f} = (f_1, f_2, \dots, f_p)$ d'éléments de $\mathcal{F}(\mathbf{N}, K)$ et une seule vérifiant les relations (5) et (7).

La démonstration est calquée sur celle de la proposition 5.36.

Lorsque le système (6) est à coefficients constants et que son polynôme caractéristique est scindé, cette proposition peut se préciser de la manière suivante :

THÉORÈME 5.22. — Structure de l'espace vectoriel des solutions d'un système homogène à coefficients constants. — Soient U un endomorphisme de K^p et φ l'isomorphisme canonique de K^p sur l'espace vectoriel F des solutions de l'équation

$$(6) \quad T(\mathbf{f}) = U(\mathbf{f}).$$

1. Pour tout élément \mathbf{b} de K^p et pour tout entier naturel n ,

$$(8) \quad \mathbf{f}_{\mathbf{b}}(n) = U^n(\mathbf{b}).$$

2. On suppose que l'endomorphisme U est scindé. Soit (E_1, E_2, \dots, E_r) une suite de sous-espaces vectoriels de K^p stables par U , de dimensions respectives p_1, p_2, \dots, p_r , dont K^p est somme directe, telle que, pour tout élément m de $[1, r]$, l'endomorphisme U_m de E_m coïncidant avec U soit de la forme

$$U_m = \lambda_m I_{E_m} + N_m,$$

où N_m est nilpotent. Soient enfin $B_m = (e_{mh})$ une base de E_m et f_{mh} l'image par φ de e_{mh} . Alors la famille (f_{mh}) est une base de l'espace vectoriel F . De plus, pour tout entier naturel n ,

$$(9) \quad f_{mh}(n) = (\lambda_m I_{E_m} + N_m)^n(e_{mh}).$$

En particulier, pour toute solution f de l'équation (6), il existe une suite (c_{mq}) , où $q \in [0, p_m - 1]$, telle que, pour tout entier naturel n ,

$$(10) \quad f(n) = \sum_{m=1}^r \lambda_m^n \sum_{q=0}^{p_m-1} n^q c_{mq}.$$

3. On suppose que U est diagonalisable, et on considère une base $B = (e_m)$ de K^p constituée de vecteurs propres de U . Soit f_m l'image par φ de e_m . Alors la famille (f_m) est une base de l'espace vectoriel F . De plus, pour tout entier naturel n ,

$$(11) \quad f_m(n) = \lambda_m^n e_m.$$

En particulier, pour toute solution f de l'équation (6), il existe une suite (c_m) d'éléments de K^p telle que, pour tout entier naturel n ,

$$(12) \quad f(n) = \sum_{m=1}^p \lambda_m^n c_m.$$

L'assertion 1 est évidente.

Assertion 2. — La famille (f_{mh}) est une base de F , car φ est un isomorphisme. On obtient la formule (9) en appliquant la relation (8) au cas où $b = e_{mh}$. Puisque $N_m^{p_m} = 0$, nous déduisons de la formule (9) qu'il existe une suite (d_{mhq}) , où $q \in [0, p_m - 1]$, telle que, pour tout entier naturel n ,

$$f_{mh}(n) = \lambda_m^n \sum_{q=0}^{p_m-1} n^q d_{mhq}.$$

La formule (10) en résulte aussitôt.

L'assertion 3 découle aussitôt de la formule (8).

REMARQUE 1. — On peut appliquer l'assertion 2 au cas où les sous-espaces vectoriels E_1, E_2, \dots, E_r sont les sous-espaces vectoriels spectraux (cf. th. 5.12), et aussi au cas où ils sont indécomposables (cf. cor. du th. 5.20).

REMARQUE 2. — **Méthode pratique de résolution d'un système homogène.** — Considérons un élément scindé $M = (\alpha_{ij})$ de $M_p(K)$ et un élément $b = (\beta_1, \beta_2, \dots, \beta_p)$ de K^p . Pour déterminer l'unique solution f_b du système d'équations

$$(6') \quad f_i(n+1) = \sum_{j=1}^p \alpha_{ij} f_j(n), \quad i \in [1, p]$$

$$(7') \quad f_i(0) = \beta_i, \quad i \in [1, p],$$

2. ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES A COEFFICIENTS CONSTANTS

Dans ce sous-paragraphe, p désigne un entier naturel non nul, et D la dérivation canonique de $K[[X]]$.

On appelle *équation différentielle linéaire d'ordre p* une équation de la forme

$$(1) \quad (D^p + A_{p-1}D^{p-1} + \dots + A_0)(S) = T,$$

où A_0, A_1, \dots, A_{p-1} et T sont des éléments donnés de $K[[X]]$. Lorsque les séries entières formelles A_0, A_1, \dots, A_{p-1} sont des scalaires $\alpha_0, \alpha_1, \dots, \alpha_{p-1}$, on dit que l'équation (1) est à coefficients constants. Le polynôme

$$P = X^p + \alpha_{p-1}X^{p-1} + \dots + \alpha_0$$

s'appelle alors polynôme caractéristique de l'équation (1).

PROPOSITION 5.38. — Existence et unicité des solutions d'une équation différentielle linéaire. — Soit $(A_0, A_1, \dots, A_{p-1})$ une suite de p éléments de $K[[X]]$.

1. Pour tout élément $\mathbf{b} = (\beta_0, \beta_1, \dots, \beta_{p-1})$ de K^p , il existe un élément $S_{\mathbf{b}}$ et un seul de $K[[X]]$ solution de l'équation

$$(2) \quad D^p(S) + A_{p-1}D^{p-1}(S) + \dots + A_0S = 0$$

et tel que, pour tout élément j de $[0, p-1]$,

$$(3) \quad [D^j(S)](0) = \beta_j.$$

La série entière formelle $S_{\mathbf{b}}$ s'appelle solution de (2) associée à la condition initiale \mathbf{b} .

2. L'application $\varphi : \mathbf{b} \mapsto S_{\mathbf{b}}$ est un isomorphisme de l'espace vectoriel K^p sur l'espace vectoriel F des solutions de l'équation (2). En particulier, la dimension de F est égale à p .

Soient $(e_0, e_1, \dots, e_{p-1})$ la base canonique de K^p et, pour tout élément j de $[0, p-1]$, S_j la solution de l'équation (2) associée à la condition initiale e_j . La famille $(S_0, S_1, \dots, S_{p-1})$ est une base de l'espace vectoriel F , dite canonique.

3. Pour tout élément \mathbf{b} de K^p et pour tout élément T de $K[[X]]$, il existe un élément S de $K[[X]]$ et un seul vérifiant les relations (1) et (3).

Assertion 1. — D'après la formule de Maclaurin, pour qu'une série entière formelle $S = \sum_{n=0}^{+\infty} \gamma_n \frac{X^n}{n!}$ satisfasse à la relation (2), il faut et il suffit que, pour tout entier naturel n ,

$$[D^n(C)](0) = 0,$$

où $C = D^p(S) + A_{p-1}D^{p-1}(S) + \dots + A_0S$, ou encore que

$$\gamma_{n+p} + \lambda_{p-1,n}\gamma_{n+p-1} + \dots + \lambda_{0,n}\gamma_n = 0, \text{ où } \lambda_{j,n} \in K.$$

Ces relations, jointes aux relations

$$\gamma_j = \beta_j \quad \text{pour tout } j \in [0, p-1],$$

montrent l'existence et l'unicité de S .

La démonstration de l'assertion 2 est calquée sur le cas des équations aux différences finies.

L'assertion 3 se démontre comme l'assertion 1.

Lorsque l'équation (2) est à coefficients constants et que son polynôme caractéristique est scindé, la proposition 5.38 peut se préciser de la manière suivante :

THÉORÈME 5.23. — **Structure de l'espace vectoriel des solutions d'une équation homogène à coefficients constants.** — *Soit*

$$P = X^p + \alpha_{p-1}X^{p-1} + \dots + \alpha_0$$

un polynôme scindé sur K , décomposé en facteurs irréductibles sous la forme

$$P = \prod_{i=1}^r (X - \lambda_i)^{p_i}.$$

1. *L'espace vectoriel F des solutions de l'équation*

$$[P(D)](S) = 0$$

est somme directe des noyaux N_i des endomorphismes $(D - \lambda_i I_E)^{p_i}$, où $E = K[[X]]$ et où i parcourt $[1, r]$.

2. *Pour tout élément i de $[1, r]$, le sous-espace vectoriel N_i est de dimension p_i . Plus précisément, soit, pour tout élément j de $[0, p_i - 1]$, E_{ij} la série entière formelle définie par la formule*

$$E_{ij} = \exp(\lambda_i X) \cdot X^j.$$

Alors la famille (E_{ij}) est une base du sous-espace vectoriel N_i .

En particulier, les éléments de F ne sont autres que les séries entières formelles S de la forme

$$S = \sum_{i=1}^r \exp(\lambda_i X) Q_i,$$

où, pour tout élément i de $[1, r]$, Q_i est un polynôme de degré strictement inférieur à p_i .

L'assertion 1 résulte aussitôt du théorème de décomposition des noyaux (cf. th. 5.1), appliqué à l'endomorphisme $P(D)$.

Assertion 2. — Considérons un scalaire λ . D'après le corollaire du théorème 1.17, le noyau de $D - \lambda I_E$ n'est autre que la droite engendrée par la série entière formelle $E_\lambda = \exp(\lambda X)$. Pour déterminer le noyau de $(D - \lambda I_E)^q$ lorsque $q > 1$, considérons un élément T de E , et calculons $(D - \lambda I_E)(E_\lambda \cdot T)$:

$$(D - \lambda I_E)(E_\lambda \cdot T) = \lambda E_\lambda \cdot T + E_\lambda D(T) - \lambda E_\lambda T = E_\lambda \cdot D(T).$$

Par récurrence sur q , nous en déduisons que, pour tout entier q strictement supérieur à 1,

$$(4) \quad (D - \lambda I_E)^q(E_\lambda \cdot T) = E_\lambda \cdot D^q(T).$$

Soit S un élément de E . Puisque E_λ est inversible dans $K[[X]]$, nous pouvons écrire S sous la forme $S = E_\lambda T$, où $T \in K[[X]]$. D'après la formule (4), pour que S appartienne au noyau de $(D - \lambda I_E)^q$, il faut et il suffit que T appartienne au noyau de D^q , ou encore que T soit un polynôme de degré strictement inférieur à q , ce qui achève la démonstration.

Étudions maintenant les systèmes d'équations différentielles linéaires.

On appelle *système de p équations différentielles linéaires d'ordre 1* un système d'équations de la forme

$$(5) \quad D(S_i) = \sum_{j=1}^p A_{ij} S_j + B_i \quad i \in [1, p],$$

où, pour tout couple (i, j) d'éléments de $[1, p]$, A_{ij} est un élément donné de $K[[X]]$ et où, pour tout élément i de $[1, p]$, B_i est un élément donné de $K[[X]]$. Lorsque les séries entières formelles A_{ij} sont des scalaires α_{ij} , on dit que le système (5) est à coefficients constants. La matrice $M = (\alpha_{ij})$ s'appelle alors matrice associée au système (5), et son polynôme caractéristique s'appelle polynôme caractéristique de ce système. Le système (5) équivaut alors à l'équation suivante :

$$(5') \quad D(S) = U(S) + B,$$

où $S = (S_1, S_2, \dots, S_p)$, où $B = (B_1, B_2, \dots, B_p)$, et où U est l'endomorphisme de K^p canoniquement associé à M .

PROPOSITION 5.39. — Existence et unicité des solutions d'un système d'équations différentielle linéaires. — Soit (A_{ij}) une famille d'éléments de $K[[X]]$, où i et j parcourent $[1, p]$.

1. Pour tout élément $b = (\beta_1, \beta_2, \dots, \beta_p)$ de K^p , il existe une suite $S_b = (S_1, S_2, \dots, S_p)$ d'éléments de $K[[X]]$ et une seule satisfaisant aux relations

$$(6) \quad D(S_i) = \sum_{j=1}^p A_{ij} S_j, \quad i \in [1, p],$$

et telle que

$$(7) \quad S(0) = b.$$

La série formelle S_b s'appelle *solution de (6) associée à la condition initiale b* .

2. L'application $\varphi : \mathbf{b} \mapsto S_{\mathbf{b}}$ est un isomorphisme de K^p sur le sous-espace vectoriel F de l'espace vectoriel $K^p[[X]]$ constitué des solutions de l'équation (6). En particulier, la dimension de F est égale à p .

Soient (e_1, e_2, \dots, e_p) la base canonique de K^p et, pour tout élément j de $[1, p]$, S_j la solution de l'équation (6) associée à la condition initiale e_j . La famille (S_1, S_2, \dots, S_p) est une base de l'espace vectoriel F , dite canonique.

3. Pour tout élément \mathbf{b} de K^p et pour toute suite $\mathbf{B} = (B_1, B_2, \dots, B_p)$ d'éléments de $K[[X]]$, il existe une suite $\mathbf{S} = (S_1, S_2, \dots, S_p)$ d'éléments de $K[[X]]$ et une seule vérifiant les relations (5) et (7).

Assertion 1. — D'après la formule de Maclaurin, pour que \mathbf{S} satisfasse à (6), il faut et il suffit que, pour tout entier naturel n et pour tout élément i de $[1, p]$,

$$D^{n+1}(S_i)(0) = \sum_{j=1}^p D^n(A_{ij}S_j)(0).$$

Ces relations, jointes à (7), montrent l'existence et l'unicité de \mathbf{S} .

La démonstration de l'assertion 2 est calquée sur celle de la proposition 5.38.

L'assertion 3 se démontre comme l'assertion 1.

Pour étudier les systèmes d'équations différentielles linéaires à coefficients constants, nous utiliserons la

PROPOSITION 5.40. — **Exponentielle formelle d'un endomorphisme.** — Soit U un endomorphisme de K^p .

1. Pour tout élément \mathbf{S} de $K^p[[X]]$, la suite des séries entières formelles \mathbf{B}_n à coefficients dans K^p définie par la relation

$$\mathbf{B}_n = \frac{X^n}{n!} U^n(\mathbf{S})$$

est sommable. L'application qui à tout élément \mathbf{S} de $K^p[[X]]$ associe $\sum_{n=0}^{+\infty} \mathbf{B}_n$ est un endomorphisme du $K[[X]]$ -module $K^p[[X]]$; on l'appelle exponentielle formelle de XU , et on la note $\exp(XU)$.

2. On suppose que U est scindé sur K . Soit (E_1, E_2, \dots, E_r) une suite de sous-espaces vectoriels de K^p stables par U , de dimensions respectives p_1, p_2, \dots, p_r , dont K^p est somme directe, telle que, pour tout élément m de $[1, r]$, l'endomorphisme U_m de E_m coïncidant avec U soit de la forme

$$U_m = \lambda_m I_{E_m} + N_m,$$

où N_m est nilpotent. Alors, pour tout élément m de $[1, r]$ et pour tout élément \mathbf{y} de E_m ,

$$\exp(XU)(\mathbf{y}) = \exp(\lambda_m X) \cdot \sum_{q=0}^{p_m-1} X^q \frac{N_m^q(\mathbf{y})}{q!}.$$

3. On suppose que U est diagonalisable sur K , et on considère une base $B = (e_m)$ de K^p constituée de vecteurs propres de U . Alors, pour tout élément m de $[1, r]$,

$$[\exp(XU)](e_m) = [\exp(\lambda_m X)] \cdot e_m.$$

L'assertion 1 est immédiate, puisque, pour tout entier naturel n , $v_0(B_n) \geq n$.

Assertion 2. — Calculons $\exp(XU)(y)$:

$$\begin{aligned} \exp(XU)(y) &= \sum_{n=0}^{+\infty} \frac{X^n}{n!} (\lambda_m I_{E_m} + N_m)^n(y) = \sum_{n=0}^{+\infty} \frac{X^n}{n!} \sum_{q=0}^{p_m-1} C_n^q \lambda_m^{n-q} N_m^q(y) \\ &= \sum_{q=0}^{p_m-1} \left(\sum_{n=q}^{+\infty} \lambda_m^{n-q} \frac{X^n}{(n-q)!} \right) \frac{N_m^q(y)}{q!} = \exp(\lambda_m X) \sum_{q=0}^{p_m-1} X^q \frac{N_m^q(y)}{q!}, \end{aligned}$$

ce qu'il fallait prouver.

L'assertion 3 s'en déduit aussitôt.

REMARQUE. — Soient M un élément de $M_p(K)$ et U l'endomorphisme de K^p canoniquement associé à M . On appelle exponentielle de XM , et on note $\exp(XM)$, la matrice associée à l'endomorphisme $\exp(XU)$ du $K[[X]]$ -module $K^p[[X]]$ dans la base canonique de ce module.

Il est immédiat que, pour tout élément inversible P de $M_p(K)$,

$$\exp(XPMP^{-1}) = P \exp(XM) P^{-1}.$$

Lorsque la matrice M est trigonale supérieure réduite, décomposée en les blocs diagonaux M_1, M_2, \dots, M_r , où, pour tout élément m de $[1, r]$, $M_m = \lambda_m I_{p_m} + V_m$, V_m étant nilpotente, la matrice $\exp(XM)$ est encore une matrice trigonale supérieure réduite, décomposée en les blocs diagonaux $\exp(XM_1), \exp(XM_2), \dots, \exp(XM_r)$. Enfin, pour tout élément m de $[1, r]$,

$$\exp(XM_m) = \exp(\lambda_m X) \sum_{q=0}^{p_m-1} X^q \frac{V_m^q}{q!}.$$

Nous pouvons alors énoncer le

THÉORÈME 5.24. — Structure de l'espace vectoriel des solutions d'un système homogène à coefficients constants. — Soient U un endomorphisme de K^p et φ l'isomorphisme canonique de K^p sur l'espace vectoriel F des solutions de l'équation

$$(6) \quad D(S) = U(S).$$

1. Pour tout élément b de K^p ,

$$(8) \quad S_b = [\exp(XU)](b).$$

2. On suppose que l'endomorphisme U est scindé. Soit (E_1, E_2, \dots, E_r) une suite de sous-espaces vectoriels de K^p stables par U , de dimensions respectives

p_1, p_2, \dots, p_r , dont K^p est somme directe, telle que, pour tout élément m de $[1, r]$, l'endomorphisme de E_m coïncidant avec U soit de la forme

$$U_m = \lambda_m I_{E_m} + N_m,$$

où N_m est nilpotent. Soient enfin $B_m = (e_{mh})$ une base de E_m et S_{mh} l'image par φ de e_{mh} . Alors la famille (S_{mh}) est une base de l'espace vectoriel F des solutions de l'équation (6). De plus,

$$(9) \quad S_{mh} = [\exp (XU_m)](e_{mh}).$$

En particulier, pour toute solution S de l'équation (6), il existe une suite (c_{mq}) d'éléments de K^p , où $q \in [0, p_m - 1]$, telle que

$$(10) \quad S = \sum_{m=1}^r \exp (\lambda_m X) \sum_{q=0}^{p_m-1} X^q c_{mq}.$$

3. On suppose que U est diagonalisable, et on considère une base $B = (e_m)$ de K^p constituée de vecteurs propres de U . Soit S_m l'image par φ de e_m . Alors la famille (S_m) est une base de l'espace vectoriel F des solutions de l'équation (6). De plus,

$$(11) \quad S_m = \exp (\lambda_m X) e_m.$$

En particulier, pour toute solution S de l'équation (6), il existe une suite (c_m) d'éléments de K^p telle que

$$(12) \quad S = \sum_{m=1}^p \exp (\lambda_m X) c_m.$$

Assertion 1. — Posons

$$S = \exp (XU)(b) = \sum_{n=0}^{+\infty} U^n(b) \frac{X^n}{n!}.$$

Alors

$$D(S) = \sum_{n=1}^{+\infty} U^n(b) \frac{X^{n-1}}{(n-1)!} = U(S)$$

et $S(0) = b$. Par unicité de S_b , nous en déduisons que $S = S_b$.

Assertion 2. — La famille (S_{mh}) est une base de F , car φ est un isomorphisme. On obtient la formule (9) en appliquant la relation (8) au cas où $b = e_{mh}$. On en déduit la formule (10), grâce à la proposition 5.40.

L'assertion 3 découle aussitôt de la formule (2).

REMARQUE 1. — On peut appliquer l'assertion 1 au cas où les sous-espaces vectoriels E_1, E_2, \dots, E_r sont les sous-espaces vectoriels spectraux, et aussi au cas où ils sont indécomposables.

REMARQUE 2. — **Méthode pratique de résolution d'un système homogène.** — Considérons un élément scindé $M = (\alpha_{ij})$ de $\mathbf{M}_p(K)$ et un élément $b = (\beta_1, \beta_2, \dots, \beta_p)$ de K^p . Pour déterminer l'unique solution S_b du système d'équations

$$(6') \quad D(S_i) = \sum_{j=1}^p \alpha_{ij} S_j \quad i \in [1, p]$$

$$(7') \quad S_i(0) = \beta_i, \quad i \in [1, p],$$

on utilise la méthode suivante :

a) On réduit la matrice M à la forme de Jordan, c'est-à-dire qu'on détermine un élément inversible P de $\mathbf{M}_p(K)$ et une matrice diagonale R de matrices de Jordan tels que $M = PRP^{-1}$.

b) On calcule $\exp(RX)$ comme il a été dit dans la proposition 5.40 et on en déduit

$$\exp(XM) = P \exp(XR)P^{-1}.$$

On obtient ainsi les composantes de S_b puisque $S_b = \exp(XU)(b)$, où U désigne l'endomorphisme de K^p canoniquement associé à M .

Pour calculer S_b , on peut aussi utiliser le fait que la série entière formelle S_b s'écrit sous la forme (10), en procédant par identification.

REMARQUE 3. — Le cas d'une équation d'ordre p peut se ramener à l'étude d'un système de p équations d'ordre 1. Considérons en effet une suite $(\alpha_0, \alpha_1, \dots, \alpha_{p-1})$ d'éléments de K et un élément $b = (\beta_0, \beta_1, \dots, \beta_{p-1})$ de K^p . Soit S_b l'unique solution de l'équation

$$(2') \quad D^p(T) + \alpha_{p-1}D^{p-1}(T) + \dots + \alpha_0 T = 0$$

telle que, pour tout élément j de $[0, p-1]$,

$$(3') \quad D^p(T)(0) = \beta_j.$$

A tout élément T de $K[[X]]$, associons l'élément $S = (S_1, S_2, \dots, S_p)$ de $K^p[[X]]$ défini par les formules

$$S_i = D^{i-1}(T), \quad i \in [1, p].$$

Pour que T satisfasse aux relations (2') et (3'), il faut et il suffit que S satisfasse au système

$$(6') \quad \begin{cases} D(S_1) = S_2 \\ D(S_2) = S_3 \\ \dots\dots\dots \\ D(S_p) = -\alpha_0 S_1 - \alpha_1 S_2 - \dots - \alpha_{p-1} S_p \end{cases}$$

et aux relations

$$(7') \quad S_i(0) = \beta_{i-1}, \quad i \in [1, p].$$

En procédant comme dans le cas des systèmes aux différences finies, on retrouve le résultat du théorème 5.23.

EXERCICES

VALEURS PROPRES, VECTEURS PROPRES

- *1. Soit E l'espace vectoriel des fonctions $f_{\alpha,\beta}$ définies sur \mathbf{R} par la relation

$$f_{\alpha,\beta}(x) = e^{-x}(\alpha \operatorname{ch} x + \beta \operatorname{sh} x), \quad \alpha, \beta \in \mathbf{R}.$$

Montrer que la restriction à E de la dérivation des fonctions d'une variable réelle définit un endomorphisme de E , dont on déterminera les valeurs propres et les vecteurs propres.*

2. Soit U l'application de $K[X]$ dans lui-même qui à tout polynôme P associe $(2X + 1)P - (X^2 - 1)D(P)$. Montrer que U est un endomorphisme de $K[X]$, dont on déterminera les vecteurs propres et les valeurs propres.

- *3. Soit E l'espace vectoriel des fonctions continues sur \mathbf{R} à valeurs complexes.

1. On considère l'endomorphisme U de E qui à tout élément f associe l'élément g défini par la formule

$$g(x) = \int_0^1 e^{x-t} f(t) dt.$$

Déterminer les valeurs propres et les vecteurs propres de U .

2. Reprendre la question précédente lorsque

$$g(x) = \int_0^1 \sin(x-t) f(t) dt.*$$

- *4. Soit E l'espace vectoriel des fonctions continues sur $[0, 1]$ à valeurs complexes. On considère l'endomorphisme U de E qui à tout élément f associe l'élément g défini par la formule

$$g(x) = \int_0^1 \inf(x, t) f(t) dt.$$

Déterminer les valeurs propres et les vecteurs propres de U .*

5. Soient n un entier naturel strictement supérieur à 1 et E l'espace vectoriel des polynômes à une indéterminée à coefficients réels de degré inférieur ou égal à $n - 1$.

1. On note D l'endomorphisme de E qui à tout polynôme P de E associe le polynôme dérivé P' . Déterminer le polynôme minimal de l'endomorphisme D .

2. Soit T l'endomorphisme de E défini par la formule

$$T(P) = P(X + 1).$$

Calculer T en fonction de D et déterminer le polynôme minimal de T .

6. *Exemples d'endomorphismes sans valeur propre admettant des valeurs spectrales.*

1. Soit A une K -algèbre commutative unitaire. Pour tout élément x de A , on désigne par T_x l'endomorphisme $y \mapsto xy$ de l'espace vectoriel A . Caractériser les valeurs propres et les valeurs spectrales de T_x . En déduire que si A est intègre et n'est pas un corps, il existe des éléments x de A tels que T_x admette des valeurs spectrales, mais n'admette aucune valeur propre.

2. *Applications.* — Soit P un polynôme à coefficients dans K . Déterminer les valeurs propres et les valeurs spectrales de l'endomorphisme $Q \mapsto PQ$ de l'espace vectoriel $K[X]$. Étudier de même l'endomorphisme $S \mapsto RS$ de $K(X)$, où R est une fraction rationnelle.

Étudier enfin l'endomorphisme $g \mapsto fg$ de l'espace vectoriel $C(\mathbf{R})$ des fonctions continues sur \mathbf{R} à valeurs complexes, où f est une fonction polynomiale.

7. On considère l'espace vectoriel $\mathcal{D}([-a, a])$ des fonctions indéfiniment dérivables sur l'intervalle $[-a, a]$ (où $a > 0$), à valeurs complexes.

Déterminer les valeurs propres et les valeurs spectrales de l'endomorphisme U qui à tout élément f de $\mathcal{D}([-a, a])$ associe la fonction g définie par la relation

$$g(x) = \int_0^x f(t) dt.$$

8. Soient α et β deux scalaires, et U l'application de $K[X]$ dans lui-même qui à tout polynôme P associe $D[(\alpha X + \beta)P]$. Montrer que U est un endomorphisme de l'espace vectoriel $K[X]$, dont on déterminera les valeurs propres et les vecteurs propres.

9. Soit E un espace vectoriel sur un corps K de caractéristique nulle. On suppose qu'il existe un couple (U, V) d'endomorphismes de E tel que

$$UV - VU = I_E.$$

1. Montrer que pour tout entier strictement positif n ,

$$UV^n - V^nU = nV^{n-1}.$$

2. Soit P un élément de $K[X]$. Montrer que

$$UP(V) - P(V)U = P'(V).$$

3. En déduire que l'espace vectoriel E n'est pas de dimension finie, et que U et V n'admettent pas de polynôme minimal. Retrouver le premier résultat en utilisant la notion de trace.

4. Prouver aussi que U et V ne sont pas de rang fini, et qu'il n'existe aucun polynôme non constant P tel que $P(U)$ soit de rang fini, ou que $P(V)$ soit de rang fini.

10 A. *Théorème de Hilbert-Dirac, dans le cas des corps algébriquement clos.*

Soient U un endomorphisme d'un espace vectoriel E sur un corps K algébriquement clos, et P un polynôme non constant à coefficients dans K .

1. Soit μ un scalaire. En utilisant la décomposition en facteurs irréductibles du polynôme $P(X) - \mu$, déterminer le noyau de l'endomorphisme $[P(U) - \mu I_E]^r$, pour tout entier $r > 0$.

2. En déduire que le spectre de l'endomorphisme $P(U)$ n'est autre que l'image par la fonction polynomiale P du spectre de U .

3. En déduire que le sous-espace spectral de $P(U)$ associé à une valeur propre μ de $P(U)$ n'est autre que la somme directe des sous-espaces spectraux F_λ de U , où λ parcourt la partie de $\text{sp}(U)$ constituée des valeurs propres λ telles que $P(\lambda) = \mu$.

4. Les sous-espaces propres de $P(U)$ peuvent-ils être calculés de la même manière? On examinera en particulier le cas où l'endomorphisme U est diagonalisable.

11 A. Théorème de Hilbert-Dirac, pour les valeurs spectrales.

1. Soient E un ensemble, f_1, f_2, \dots, f_p des applications de E dans lui-même commutant deux à deux (pour la loi de composition des applications, et $f = f_1 \circ f_2 \circ \dots \circ f_p$ leur composée. Montrer que f est injective (resp. surjective, resp. bijective) si et seulement si, pour tout $i \in [1, p]$, f_i est injective (resp. surjective, resp. bijective).

2. Soient U un endomorphisme d'un espace vectoriel E sur K , et P un polynôme non constant à coefficients dans K . Montrer que si λ est une valeur propre (resp. spectrale) de U , $P(\lambda)$ est une valeur propre (resp. spectrale) de $P(U)$.

3. Montrer que, lorsque K est algébriquement clos, on obtient ainsi toutes les valeurs propres (resp. spectrales) de $P(U)$.

12. Soient U un endomorphisme d'un espace vectoriel E sur K , A et B deux polynômes non nuls à coefficients dans K . Soient D le P. G. C. D. de A et B , et M leur P. P. C. M.

1. Montrer que le sous-espace vectoriel somme des noyaux de $A(U)$ et de $B(U)$ n'est autre que le noyau de $M(U)$:

$$\text{Ker}[A(U)] + \text{Ker}[B(U)] = \text{Ker}[M(U)].$$

2. Montrer que le sous-espace vectoriel intersection des images des endomorphismes $A(U)$ et $B(U)$ n'est autre que l'image de $M(U)$:

$$\text{Im}[A(U)] \cap \text{Im}[B(U)] = \text{Im}[M(U)],$$

et que le sous-espace vectoriel somme des images de $A(U)$ et de $B(U)$ n'est autre que l'image de $D(U)$:

$$\text{Im}[A(U)] + \text{Im}[B(U)] = \text{Im}[D(U)].$$

13 A. Polynôme minimal de la restriction d'un endomorphisme.

Soient U un endomorphisme d'un espace vectoriel E admettant un polynôme minimal π , et Q_1, Q_2, \dots, Q_p des polynômes premiers entre eux deux à deux tels que π divise le produit $Q = Q_1 Q_2 \dots Q_p$. Pour tout $i \in [1, p]$, on pose $R_i = \text{P. G. C. D.}(\pi, Q_i)$, on désigne par N_i le noyau de $Q_i(U)$, et par U_i l'endomorphisme de N_i coïncidant avec U .

1. Prouver que π est divisible par le polynôme $R = R_1 R_2 \dots R_p$.

2. Prouver que le noyau de $R_i(U)$ est égal au noyau de $Q_i(U)$. En déduire que $R(U) = 0$, et que $R = \pi$.

3. Prouver enfin que R_i n'est autre que le polynôme minimal π_i de U_i . Quel résultat retrouve-t-on lorsque Q_i est de la forme $(X - \lambda_i)^{n_i}$?

14. Existence d'un polynôme minimal.

Soient E un espace vectoriel sur K , et U un endomorphisme de E .

1. Montrer que si U admet un polynôme minimal, il en est de même de tout élément de la sous-algèbre pleine de $\mathcal{L}(E)$ engendrée par U .

Prouver réciproquement que s'il existe un élément non constant R de $K(X)$ dans lequel U est substituable et tel que $R(U)$ admette un polynôme minimal, alors U admet un polynôme minimal.

2. Montrer que si U est de rang fini, U admet un polynôme minimal.

15 A. Endomorphismes localement finis.

Soient E un espace vectoriel sur K et U un endomorphisme de E .

1. Prouver que si U est localement fini et injectif, U est bijectif. En déduire que toute valeur spectrale de U est une valeur propre de U .

2. Soit U l'unique endomorphisme de $K[X]$ tel que $U(1) = 0$ et que, pour tout entier strictement positif p , $U(X^p) = X^{p-1}$. Montrer que U est surjectif et localement nilpotent.

3. Soit R une fraction rationnelle dans laquelle U est substituable. Montrer que si U est localement fini, il en est de même de $R(U)$. (Étant donné un élément α de E , il existe un élément P non nul de $K[X]$ tel que $[P(U)](\alpha) = 0$. On pourra considérer les restrictions de U et de $R(U)$ au sous-espace vectoriel $\text{Ker } [P(U)]$.)

16 A. Théorème de Hilbert-Dirac pour les fractions rationnelles d'un endomorphisme.

Soient U un endomorphisme d'un espace vectoriel E sur K , et R un élément de $K(X)$ dans lequel U est substituable.

1. Prouver que si λ est une valeur spectrale de U , λ est substituable dans R , et que $R(\lambda)$ est une valeur spectrale de $R(U)$.

2. Montrer que si λ est une valeur propre de U , $R(\lambda)$ est une valeur propre de $R(U)$, et que le sous-espace propre (resp. spectral) de U associé à λ est contenu dans le sous-espace propre (resp. spectral) de $R(U)$ associé à $R(\lambda)$.

3. Prouver que lorsque K est algébriquement clos, pour toute valeur propre (resp. spectrale) μ de $R(U)$, il existe une valeur propre (resp. spectrale) λ de U telle que $\mu = R(\lambda)$. Déterminer le sous-espace spectral de U associé à λ .

RÉDUCTION DES ENDOMORPHISMES

17. Soient n un entier naturel non nul, K un corps de caractéristique 0, α , β et γ trois éléments de K tels que $\alpha \neq \beta$, et U l'endomorphisme de $K[X]$ défini par la formule

$$U(P) = (X - \alpha)(X - \beta)P' - [2nX - n(\alpha + \beta) + \gamma]P.$$

Prouver que le sous-espace vectoriel E_{2n} de $K[X]$ constitué des polynômes de degré inférieur ou égal à $2n$ est stable par U . Déterminer les valeurs propres et les vecteurs propres de U , et montrer que ceux-ci appartiennent à E_{2n} . Montrer enfin que l'endomorphisme de E_{2n} coïncidant avec U est diagonalisable.

18. Soient K un corps de caractéristique 0, (a, b) un couple d'entiers naturels et U l'endomorphisme de $K[X]$ défini par la formule

$$U(P) = X^2P'' - (a + b - 1)XP' + abP.$$

Déterminer les valeurs propres et les vecteurs propres de U , et montrer que U est diagonalisable.

19. Soient K un corps de caractéristique 0, α un élément de K , et U l'endomorphisme de $K[X]$ défini par la formule

$$U(P) = (X - \alpha)[P' + P'(\alpha)] - 2[P - P(\alpha)].$$

1. Déterminer le noyau et l'image de U .
2. Trouver les valeurs propres et les vecteurs propres de U , et montrer que U est diagonalisable.

20 B. *Interpolation de Lagrange-Sylvester pour les polynômes d'un endomorphisme scindé.*

Soit U un endomorphisme scindé d'un espace vectoriel E sur K , admettant un polynôme minimal

$$\pi(X) = \prod_{\lambda \in \text{sp}(U)} (X - \lambda)^{n(\lambda)}.$$

Soit I la partie de $\text{sp}(U) \times \mathbb{N}$ constituée des couples (λ, h) tels que $h \in [0, n(\lambda) - 1]$; on pose $n = \text{card}(I)$.

1. Soient P et Q deux éléments de $K[X]$. Montrer que $P(U) = Q(U)$ si et seulement si, pour tout élément (λ, h) de I ,

$$D^h(P)(\lambda) = D^h(Q)(\lambda).$$

2. Pour tout élément P de $K[X]$, on désigne par $b(P)$ le vecteur de K^I dont les composantes sont les scalaires $D^h(P)(\lambda)$, et par L_P le polynôme d'interpolation de Lagrange-Sylvester associé au vecteur $b(P)$. On note ψ l'application linéaire de $K[X]$ dans l'espace vectoriel F_n des polynômes à coefficients dans K de degré strictement inférieur à n qui à P associe L_P . Déterminer l'image et le noyau de l'application linéaire ψ . En déduire que la relation $P(U) = Q(U)$ équivaut à la relation $L_P = L_Q$. En particulier, $P(U) = L_P(U)$.

3. Pour tout $\lambda \in \text{sp}(U)$, on désigne par b_λ l'élément $e_{\lambda,0}$ de la base canonique de K^I et par Q_λ le polynôme d'interpolation de Lagrange-Sylvester associé au vecteur b_λ . Prouver que $Q_\lambda(U)$ n'est autre que le projecteur spectral P_λ de U associé à la valeur propre λ .

21 A. *Spectre du transposé d'un endomorphisme.*

Soit U un endomorphisme d'un espace vectoriel E .

1. Montrer que toute valeur spectrale de U est une valeur spectrale de tU , et réciproquement. Montrer que si U est localement nilpotent et surjectif, tU n'admet pas de valeur propre; donner un exemple d'un tel endomorphisme.

2. Montrer que tU admet un polynôme minimal si et seulement si U en admet un, et qu'alors le polynôme minimal de tU est égal à celui de U .

3. Prouver que si U admet un polynôme minimal, alors, pour tout scalaire λ et pour tout entier naturel n ,

$$E_{\lambda,n}({}^tU) = [\text{Im} [(U - \lambda E)^n]]^\perp.$$

En déduire que si, de plus, U est scindé,

$$F_\lambda({}^tU) = \bigcap_{\mu \neq \lambda} [F_\mu(U)]^\perp.$$

22 A. Familles commutatives d'endomorphismes nilpotents.

Soit \mathcal{A} un ensemble d'endomorphismes d'un espace vectoriel E sur K , commutant deux à deux.

1. Montrer que si tous les éléments de \mathcal{A} sont nilpotents (resp. localement nilpotents), tout élément du sous-espace vectoriel de $\mathcal{L}(E)$ engendré par \mathcal{A} est nilpotent (resp. localement nilpotent).

2. Soient U et V deux endomorphismes permutables de E . Montrer que si U est nilpotent (resp. localement nilpotent), UV est nilpotent (resp. localement nilpotent).

23 A. Existence d'un vecteur propre commun à un ensemble d'endomorphismes commutant deux à deux.

Soit \mathcal{B} un ensemble non vide d'endomorphismes d'un espace vectoriel E sur K , commutant deux à deux. On dit qu'un sous-espace vectoriel F de E est \mathcal{B} -propre s'il satisfait aux deux conditions suivantes :

a) *Le sous-espace vectoriel F est stable par tout endomorphisme V de E commutant à tous les éléments de \mathcal{B} .*

b) *Pour tout élément U de \mathcal{B} , il existe un scalaire λ tel que F soit contenu dans le sous-espace propre $E_\lambda(U)$.*

1. Soient F un sous-espace vectoriel \mathcal{B} -propre non réduit à $\{0\}$, V un endomorphisme scindé de E commutant à tous les éléments de \mathcal{B} , et $\mathcal{B}' = \mathcal{B} \cup \{V\}$. Prouver qu'il existe une valeur propre λ de V telle que $F' = F \cap E_\lambda(V)$ ne soit pas réduit à $\{0\}$, et qu'alors F' est \mathcal{B}' -propre.

2. Prouver que si \mathcal{B} est un ensemble fini dont tous les éléments sont des endomorphismes scindés, il existe un sous-espace vectoriel de E \mathcal{B} -propre non réduit à $\{0\}$.

3. En déduire le résultat plus général suivant :

Soit \mathcal{A} un ensemble non vide d'endomorphismes d'un espace vectoriel E sur K , commutant deux à deux, et scindés sur K . Si le sous-espace vectoriel de $\mathcal{L}(E)$ engendré par \mathcal{A} est de dimension finie, il existe un sous-espace vectoriel de E \mathcal{A} -propre non réduit à $\{0\}$.

En particulier, il existe un vecteur propre commun à tous les éléments de \mathcal{A} .

(On pourra considérer une partie finie \mathcal{B} de \mathcal{A} telle que tout élément de \mathcal{A} soit combinaison linéaire d'éléments de \mathcal{B} , et prouver que tout sous-espace vectoriel \mathcal{B} -propre est \mathcal{A} -propre. Mais ce résultat peut tomber en défaut si le sous-espace vectoriel de $\mathcal{L}(E)$ engendré par \mathcal{A} n'est pas de dimension finie; cf. exercice 25.)

24 B. Réduction simultanée d'un ensemble d'endomorphismes commutant deux à deux.

Soit \mathcal{B} un ensemble non vide d'endomorphismes d'un espace vectoriel E sur K , commutant deux à deux.

On dit qu'une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels de E est \mathcal{B} -spectrale si elle satisfait aux trois conditions suivantes :

a) *Pour tout $i \in I$, et pour tout endomorphisme V de E commutant à tous les éléments de \mathcal{B} , le sous-espace vectoriel F_i est stable par V .*

b) *Tout sous-espace vectoriel G de E stable par \mathcal{B} , c'est-à-dire stable par tous les éléments de \mathcal{B} , est somme directe de ses intersections avec les sous-espaces vectoriels F_i :*

$$G = \bigoplus_{i \in I} (G \cap F_i).$$

(En particulier, E est somme directe des sous-espaces vectoriels F_i .)

c) *Pour tout élément i de I , et pour tout élément U de \mathcal{B} , il existe un scalaire λ tel que F_i soit contenu dans le sous-espace spectral $F_\lambda(U)$.*

On dit qu'une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels de E est \mathcal{B} -propre si elle satisfait aux conditions a), b) et

c') Pour tout élément i de I , et pour tout élément U de \mathcal{B} , il existe un scalaire λ tel que F_i soit contenu dans le sous-espace propre $E_\lambda(U)$.

1. Montrer que s'il existe une famille $(F_i)_{i \in I}$ de sous-espaces vectoriels \mathcal{B} -spectrale (resp. \mathcal{B} -propre), tout élément de \mathcal{B} est un endomorphisme scindé (resp. diagonalisable).

2. Soient $(F_i)_{i \in I}$ une famille \mathcal{B} -spectrale de sous-espaces vectoriels de E , V un endomorphisme scindé commutant à tous les éléments de \mathcal{B} , et $\mathcal{B}' = \mathcal{B} \cup \{V\}$. On pose $I' = I \times \text{sp}(V)$ et, pour tout élément $j = (i, \lambda)$ de I' , on désigne par F'_j le sous-espace vectoriel $F_i \cap F_\lambda(V)$. Prouver que la famille $(F'_j)_{j \in I'}$ est \mathcal{B}' -spectrale, et que, si $(F_i)_{i \in I}$ est \mathcal{B} -propre et V diagonalisable, $(F'_j)_{j \in I'}$ est \mathcal{B}' -propre.

3. Prouver que si \mathcal{B} est un ensemble fini dont tous les éléments sont des endomorphismes scindés (resp. diagonalisables), il existe une famille $(F_i)_{i \in I}$ \mathcal{B} -spectrale (resp. \mathcal{B} -propre) de sous-espaces vectoriels de E .

4. En déduire le résultat plus général suivant :

Soit \mathcal{A} un ensemble non vide d'endomorphismes d'un espace vectoriel E sur K , commutant deux à deux, et scindés (resp. diagonalisables) sur K . Si le sous-espace vectoriel de $\mathcal{L}(E)$ engendré par \mathcal{A} est de dimension finie, il existe une famille $(F_i)_{i \in I}$ \mathcal{A} -spectrale (resp. \mathcal{A} -propre) de sous-espaces vectoriels de E .

(On pourra considérer une partie finie \mathcal{B} de \mathcal{A} telle que tout élément de \mathcal{A} soit combinaison linéaire d'éléments de \mathcal{B} , et prouver que toute famille $(F_i)_{i \in I}$ \mathcal{B} -spectrale (resp. \mathcal{B} -propre) de sous-espaces vectoriels de E est \mathcal{A} -spectrale (resp. \mathcal{A} -propre); pour le premier cas, on pourra utiliser l'exercice 22.)

25 B. Exemples de familles commutatives d'endomorphismes sans vecteur propre commun.

Soit A l'algèbre $P_{\mathbb{N}}(K)$ des polynômes construits sur \mathbb{N} à coefficients dans K (cf. exercice 2.59). Pour tout $n \in \mathbb{N}$, on désigne par H_n l'endomorphisme $P \mapsto X_n P$ de l'espace vectoriel A .

1. Soient \mathcal{I} l'idéal de A engendré par les polynômes X_n^2 , où $n \in \mathbb{N}$, E l'espace vectoriel A/\mathcal{I} , et φ l'application canonique de A sur E .

Montrer que, pour tout $n \in \mathbb{N}$, il existe un endomorphisme U_n et un seul de E tel que $U_n \circ \varphi = \varphi \circ H_n$. Déterminer l'image et le noyau de U_n . Prouver que les endomorphismes U_n commutent deux à deux, que pour tout $n \in \mathbb{N}$, $U_n^2 = 0$, mais qu'il n'existe aucun vecteur propre commun aux endomorphismes U_n .

2. Soient \mathcal{J} l'idéal de A engendré par les polynômes $X_n^2 - X_n$, où $n \in \mathbb{N}$, F l'espace vectoriel A/\mathcal{J} , et ψ l'application canonique de A sur F .

Montrer que, pour tout $n \in \mathbb{N}$, il existe un endomorphisme V_n et un seul de F tel que $V_n \circ \psi = \psi \circ H_n$. Déterminer l'image et le noyau de V_n . Prouver que les endomorphismes V_n commutent deux à deux, que pour tout $n \in \mathbb{N}$, V_n est un projecteur, mais qu'il n'existe aucun vecteur propre commun aux endomorphismes V_n .

3. Reprendre les deux questions précédentes lorsque A est l'algèbre $K[X_1, X_2, \dots, X_p]$.

26 B. Projecteurs minimaux d'une algèbre commutative d'endomorphismes diagonalisables.

Soient E un espace vectoriel de dimension finie sur K , et \mathcal{A} une sous-algèbre commutative unitaire de $\mathcal{L}(E)$ dont tous les éléments sont des endomorphismes diagonalisables.

Sur l'ensemble des projecteurs de $\mathcal{L}(E)$ on considère la relation d'ordre $P \leq Q$ définie par les couples (P, Q) tels que $P = PQ = QP$ (cf. exercice I.3.32). Soient \mathcal{T} l'ensemble des projecteurs appartenant à \mathcal{A} et \mathcal{M} l'ensemble des éléments minimaux de $\mathcal{T} - \{0\}$. Cet ensemble \mathcal{M} s'appelle ensemble des projecteurs minimaux de \mathcal{A} .

1. Prouver que pour tout couple (P, Q) d'éléments distincts de \mathcal{M} , $PQ = QP = 0$. En déduire que \mathcal{M} est un ensemble fini.

2. Prouver que pour tout projecteur non nul P_1 de \mathcal{T} , il existe un projecteur P de \mathcal{M} tel que $P \leq P_1$. En déduire que $I_E = \sum_{P \in \mathcal{M}} P$.

3. Montrer que tout projecteur non nul P_1 de \mathcal{T} est somme d'éléments de \mathcal{M} . En déduire que tout élément U de \mathcal{A} peut s'écrire sous la forme

$$(1) \quad U = \sum_{P \in \mathcal{M}} \alpha_P \cdot P,$$

où pour tout $P \in \mathcal{M}$, α_P appartient à K .

Retrouver ainsi le théorème de diagonalisation simultanée (cf. prop. 5.16).

La formule (1) s'appelle *formule de décomposition spectrale de \mathcal{A}* .

4. Prouver que le commutant \mathcal{A}' de \mathcal{A} est constitué des endomorphismes V de E tels que, pour tout $P \in \mathcal{M}$, $\text{Im}(P)$ soit stable par V . A l'aide de l'exercice I. 3.55, prouver que le bicommutant \mathcal{A}'' de \mathcal{A} est égal à \mathcal{A} .

Examiner le cas particulier où \mathcal{A} est la sous-algèbre unitaire de $\mathcal{L}(E)$ engendrée par un endomorphisme diagonalisable U .

27 A. Endomorphismes scindés dont toutes les valeurs propres sont d'indice fini.

Soit U un endomorphisme d'un espace vectoriel E sur K . Montrer que si U est scindé sur K , et que si toutes les valeurs propres de U sont d'indice fini, il est équivalent de dire : U est inversible, U est injectif, U est surjectif, U est inversible à gauche, U est inversible à droite, U est régulier, U est régulier à gauche, U est régulier à droite.

28 A. Projecteurs spectraux des endomorphismes scindés.

Soient U et V deux endomorphismes d'un espace vectoriel E sur K . On dit que V est localement un polynôme en U si, pour tout sous-espace vectoriel F de E de dimension finie, il existe un élément Q_F de $K[X]$ tel que, pour tout élément x de F , $V(x) = [Q_F(U)](x)$.

Prouver que si U est scindé sur K , les projecteurs spectraux de U sont localement des polynômes en U .

(On pourra d'abord prouver qu'étant donné un sous-espace vectoriel F de E de dimension finie, il existe un élément P non nul de $K[X]$ tel que F soit contenu dans le noyau G de $P(U)$. On pourra alors étudier l'endomorphisme V de G obtenu par restriction de U à G .)

29 B. Décompositions additive et multiplicative d'un endomorphisme.

I. — Soit U un endomorphisme scindé d'un espace vectoriel E , admettant un polynôme minimal.

1. En s'inspirant du cas où E est de dimension finie (cf. th. 5.13), prouver qu'il existe un couple (D, N) et un seul d'endomorphismes de E satisfaisant aux conditions suivantes :

- a) l'endomorphisme D est diagonalisable, et l'endomorphisme N est nilpotent;
- b) les endomorphismes D et N commutent, et $U = D + N$.

2. Prouver que D et N sont des polynômes en U . Prouver ensuite qu'il existe un élément P de $K[X]$ tel que $P(0) = 0$ et que $D = P(U)$. (On pourra distinguer deux cas suivant que le terme constant du polynôme minimal de U est nul ou non nul.)

3. Généraliser le théorème de décomposition multiplicative d'un automorphisme (cor. du th. 5.13).

II. — Soit U un endomorphisme scindé d'un espace vectoriel E sur K .

1. Prouver qu'il existe un couple (D, N) et un seul d'endomorphismes de E satisfaisant aux conditions suivantes :

a) l'endomorphisme D est diagonalisable, et l'endomorphisme N est localement nilpotent;

b) les endomorphismes D et N commutent, et $U = D + N$.

2. Prouver que D et N sont localement des polynômes en U (cf. exercice 28).

3. Généraliser le théorème de décomposition multiplicative d'un automorphisme.

30 A. Représentations des groupes finis.

Soient G un groupe fini d'ordre n , E un espace vectoriel sur un corps K de caractéristique 0 et $\varphi : g \mapsto U_g$ un morphisme de G dans le groupe $\text{GL}(E)$.

1. Pour tout endomorphisme U de E , on pose

$$\tilde{U} = \frac{1}{n} \sum_{g \in G} U_g U U_g^{-1}.$$

Prouver que, pour tout élément h de G , \tilde{U} commute avec U_h . Soit V un endomorphisme de E tel que, pour tout élément h de G , V commute avec U_h . Montrer que, pour tout endomorphisme U de E , $\tilde{U}V = \tilde{U}V$.

2. Soit F un sous-espace vectoriel de E invariant par G , c'est-à-dire stable par U_g pour tout élément g de G . Soit P un projecteur de E dont l'image est égale à F . Montrer que, pour tout élément y de F , $\tilde{P}(y) = y$ et que l'image de \tilde{P} est contenue dans F . En déduire que \tilde{P} est un projecteur de E dont l'image est égale à F .

Prouver le résultat suivant :

Tout sous-espace vectoriel de E invariant par G admet un sous-espace vectoriel supplémentaire invariant par G .

Prouver que, pour tout élément g de G , U_g est un endomorphisme semi-simple. (On pourra introduire le sous-groupe cyclique engendré par U_g .)

3. On dit qu'un sous-espace vectoriel F de E non réduit à $\{0\}$ est irréductible relativement à G s'il est invariant par G et si $\{0\}$ et F sont les seuls sous-espaces vectoriels de F invariants par G .

Montrer qu'il existe une famille $(E_i)_{i \in I}$ de sous-espaces vectoriels de E dont E est somme directe, telle que, pour tout élément i de I , E_i soit irréductible relativement à G .

4. Montrer que si le groupe G est commutatif et le corps K algébriquement clos, les endomorphismes U_g sont simultanément diagonalisables.

RÉDUCTION DES MATRICES

31. Soit α un nombre réel. Déterminer les valeurs propres, les sous-espaces propres, les sous-espaces spectraux et le polynôme minimal de la matrice

$$\begin{pmatrix} 0 & \sin \alpha & \sin 2\alpha \\ \sin \alpha & 0 & \sin 2\alpha \\ \sin 2\alpha & \sin \alpha & 0 \end{pmatrix}.$$

32. Montrer que les éléments de $M_3(\mathbb{C})$ de la forme

$$M_\alpha = \begin{pmatrix} 1 & 0 & \alpha \\ -\alpha & 1 & -\frac{\alpha^2}{2} \\ 0 & 0 & 1 \end{pmatrix}$$

constituent un groupe multiplicatif.

Déterminer pour toute valeur de α le polynôme caractéristique, le polynôme minimal, les valeurs propres et les vecteurs propres de la matrice M_α .

33. Déterminer les valeurs propres, les sous-espaces propres, les sous-espaces spectraux et le polynôme minimal des éléments suivants de $M_3(\mathbb{C})$:

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 2 & 0 \\ \beta & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & \alpha & 1 \\ 0 & 1 & \beta \\ 0 & 0 & \gamma \end{pmatrix}, \quad \begin{pmatrix} \alpha+1 & \beta & \gamma \\ \alpha & \beta+1 & \gamma \\ \alpha & \beta & \gamma+1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & \alpha \\ \alpha & 0 & 1 \\ 1 & \alpha & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & \alpha \\ \alpha-1 & -\alpha-1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \alpha & \beta \\ \alpha & 0 & \beta \\ \alpha & \beta & 0 \end{pmatrix}.$$

$$\begin{pmatrix} 0 & \alpha & \alpha^2 \\ \frac{1}{\alpha} & 0 & \alpha \\ \frac{1}{\alpha^2} & \frac{1}{\alpha} & 0 \end{pmatrix}.$$

34. On considère l'élément suivant de $M_3(\mathbb{R})$:

$$M = \begin{pmatrix} 3 & -3 & 2 \\ -1 & 5 & -2 \\ -1 & 3 & 0 \end{pmatrix}.$$

1. Trouver son polynôme caractéristique.
2. Trouver son polynôme minimal.
3. Montrer que M est inversible, et calculer son inverse.
4. Calculer M^n , où $n \in \mathbb{Z}$.

35. Déterminer les suites $(\alpha, \beta, \alpha', \beta', \alpha'', \beta'')$ des nombres complexes telles que la matrice

$$\begin{pmatrix} 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \\ 1 & \alpha'' & \beta'' \end{pmatrix}$$

admette pour vecteurs propres les vecteurs $(1, 1, 1)$, $(1, 0, -1)$ et $(1, -1, 1)$.

36. Diagonaliser les éléments suivants de $M_3(\mathbb{C})$:

$$\begin{pmatrix} 4 & -1 & 0 \\ 1 & 1 & 1 \\ 2 & 5 & -4 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & -2 & 1 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 7 & -6 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & -1 \\ 3 & -3 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}.$$

37. Diagonaliser l'élément suivant de $M_3(\mathbb{R})$, où a, b, c sont trois nombres réels strictement positifs différents de 1 :

$$\begin{pmatrix} 1 & \log_a b & \log_a c \\ \log_b a & 1 & \log_b c \\ \log_c a & \log_c b & 1 \end{pmatrix}.$$

38. Pour chacune des matrices carrées M à éléments complexes suivantes, calculer le polynôme caractéristique et le polynôme minimal. Déterminer les valeurs propres, les sous-espaces propres, les sous-espaces spectraux, et une matrice carrée inversible P telle que la matrice PMP^{-1} soit réduite.

$$\begin{pmatrix} -3 & 2 & -4 \\ 4 & -3 & 4 \\ 2 & -3 & 5 \end{pmatrix}, \quad \begin{pmatrix} 3 & 8 & 7 \\ 1 & 4 & 3 \\ -2 & -6 & -5 \end{pmatrix}, \quad \begin{pmatrix} 3 & -1 & 0 \\ -1 & 3 & 1 \\ 4 & -4 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 4 & 1 & 2 \\ -5 & 0 & -2 \\ 2 & -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -3 & 1 & 1 \\ -3 & 0 & 2 \\ -2 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 3 & -1 & 1 & -1 \\ 1 & 3 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & -3 & 5 \end{pmatrix}.$$

39. Diagonaliser l'élément suivant de $M_4(\mathbb{R})$:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Déterminer les valeurs propres, les sous-espaces propres, les sous-espaces spectraux et le polynôme minimal des éléments suivants de $M_4(\mathbb{C})$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \beta & \beta' & 1 & 0 \\ \gamma & \gamma' & \gamma'' & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \beta & \beta' & 2 & 0 \\ \gamma & \gamma' & \gamma'' & 2 \end{pmatrix}.$$

40. Mettre chacune des matrices carrées à éléments complexes suivantes sous la forme réduite de Jordan, en explicitant la matrice de passage correspondante :

$$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 12 & -6 & -2 \\ 18 & -9 & -3 \\ 18 & -9 & -3 \end{pmatrix}, \quad \begin{pmatrix} 3 & 2 & -3 \\ 4 & 10 & -12 \\ 3 & 6 & -7 \end{pmatrix}, \quad \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}, \quad \begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & -1 & 2 & -1 \\ 2 & 0 & 1 & -4 & -1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & -3 & 3 & -1 \end{pmatrix}.$$

41. Soit n un entier naturel.

1. Calculer les puissances $n^{\text{ièmes}}$ des matrices suivantes :

$$\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \quad \begin{pmatrix} -7 & -6 \\ 12 & 10 \end{pmatrix}.$$

2. Soient α et β deux nombres réels. Calculer les puissances $n^{\text{ièmes}}$ des matrices suivantes :

$$\begin{pmatrix} 0 & -\alpha \\ \beta & \alpha + \beta \end{pmatrix} \quad \begin{pmatrix} \alpha & 1 - \alpha \\ 1 - \beta & \beta \end{pmatrix}.$$

42. On considère l'élément suivant de $M_3(\mathbf{R})$:

$$M = \begin{pmatrix} 9 & 0 & 0 \\ -5 & 4 & 0 \\ -8 & 0 & 1 \end{pmatrix}.$$

Déterminer tous les éléments N de $M_3(\mathbf{R})$ diagonalisables et tels que $N^2 = M$.

43. On considère l'élément suivant de $M_4(\mathbf{R})$:

$$M = \begin{pmatrix} 7 & 4 & 0 & 0 \\ -12 & -7 & 0 & 0 \\ 20 & 11 & -6 & -12 \\ -12 & -6 & 6 & 11 \end{pmatrix}.$$

1. Trouver les valeurs propres de M . On désignera par $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ ces valeurs propres, avec $\lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \lambda_4$. Déterminer les vecteurs propres de M .

2. Soit U l'endomorphisme de \mathbf{R}^4 dont la matrice associée dans la base canonique B est M . On choisit une nouvelle base B' de \mathbf{R}^4 dans laquelle la matrice D associée à U est diagonale, les éléments sur la diagonale principale étant rangés dans l'ordre $\lambda_1, \lambda_2, \lambda_3, \lambda_4$. Déterminer B' de telle sorte que les colonnes de la matrice de passage P soient formées d'entiers rationnels premiers entre eux dans leur ensemble, le premier élément non nul de chaque colonne étant positif.

Vérifier la relation $D = P^{-1}MP$.

3. Soit n un entier rationnel. Montrer que la matrice M^n peut se mettre sous la forme

$$M^n = \lambda_1^n M_1 + \lambda_2^n M_2 + \lambda_3^n M_3 + \lambda_4^n M_4,$$

où M_1, M_2, M_3, M_4 sont des éléments de $M_4(\mathbf{R})$ indépendants de n , que l'on explicitera. Examiner le cas où $n = 0$.

4. Calculer les produits $M_i M_j$, où i et j parcourent l'intervalle $[1, 4]$ de \mathbf{N} .

Soient $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ quatre nombres réels. Trouver une condition nécessaire et suffisante pour que la matrice

$$N = \alpha_1 M_1 + \alpha_2 M_2 + \alpha_3 M_3 + \alpha_4 M_4$$

soit inversible. Calculer alors son inverse.

44. 1. Soient a, b, c trois nombres rationnels. On considère les nombres complexes suivants :

$$\begin{aligned} \alpha &= a + b \sqrt[3]{2} + c \sqrt[3]{4}, \\ \beta &= a + bj \sqrt[3]{2} + cj^2 \sqrt[3]{4}, \\ \gamma &= a + bj^2 \sqrt[3]{2} + cj \sqrt[3]{4}. \end{aligned}$$

Former un polynôme du troisième degré admettant ces nombres pour racines.

Montrer que si l'un des nombres α, β, γ est nul, alors $a = b = c = 0$. (En supposant cette relation non satisfaite, on remarquera que l'hypothèse entraîne l'existence d'une racine commune aux polynômes $X^3 - 2$ et $cX^2 + bX + a$, donc d'une racine rationnelle pour $X^3 - 2$).

2. Montrer que l'ensemble K des nombres réels de la forme

$$(1) \quad \alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4},$$

où a, b, c parcourent \mathbf{Q} , est un sous-corps de \mathbf{R} . Étudier de même l'ensemble des nombres complexes de la forme β , et l'ensemble des nombres complexes de la forme γ .

3. Les nombres rationnels a, b, c étant fixés, et le nombre α défini par la relation (1), on fait correspondre à tout élément ξ de K le nombre réel $\xi' = \alpha\xi$. On pose

$$\begin{aligned} \xi &= x + y\sqrt[3]{2} + z\sqrt[3]{4}, \\ \xi' &= x' + y'\sqrt[3]{2} + z'\sqrt[3]{4}. \end{aligned}$$

Calculer x', y', z' en fonction de x, y, z .

Montrer que les matrices de la forme

$$M_{a,b,c} = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix},$$

où a, b, c parcourent \mathbf{Q} , forment un corps isomorphe à K .

Calculer le déterminant de $M_{a,b,c}$; montrer qu'il est nul si et seulement si $a = b = c = 0$.

4. Étudier l'ensemble des matrices $M_{a,b,c}$ où a, b, c parcourent \mathbf{R} , puis l'ensemble des matrices $M_{a,b,c}$ où a, b, c parcourent \mathbf{C} . Dans chaque cas, on déterminera les éléments inversibles et les diviseurs de 0; on cherchera les valeurs propres et les vecteurs propres des matrices $M_{a,b,c}$.

5. Soient n un entier rationnel, et a, b, c trois nombres rationnels non tous nuls. On note la matrice $(M_{a,b,c})^n$ sous la forme

$$\begin{pmatrix} a_n & 2c_n & 2b_n \\ b_n & a_n & 2c_n \\ c_n & b_n & a_n \end{pmatrix},$$

Calculer α^n, β^n et γ^n en fonction de a_n, b_n et c_n .

45. Déterminer les valeurs propres et les vecteurs propres de la matrice considérée dans l'exercice 4.17. Montrer que, sauf dans le cas trivial où l'un des deux nombres complexes β et γ est nul, cette matrice est diagonalisable.

46. Soient n un entier naturel non nul, $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ un élément de K^n , M_α l'élément de $M_{n+1}(K)$ défini par la formule

$$M_\alpha = \begin{pmatrix} 0 & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1 & 0 & \alpha_2 & \dots & \alpha_n \\ \alpha_1 & \alpha_2 & 0 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & 0 \end{pmatrix},$$

et U_α l'endomorphisme de K^{n+1} canoniquement associé à M_α .

1. Déterminer les valeurs propres de U_a .

2. On pose $\beta = \sum_{j=1}^n \alpha_j$. Prouver que si, pour tout élément j de $[1, n]$, $\beta \neq -\alpha_j$,

U_a est diagonalisable, et déterminer une base de vecteurs propres. On pourra exprimer ces vecteurs propres à l'aide des vecteurs

$$f_0 = \sum_{j=1}^{n+1} e_j, f_1 = e_1, f_2 = e_1 + e_2, \dots, f_n = \sum_{j=1}^n e_j,$$

où $(e_1, e_2, \dots, e_{n+1})$ désigne la base canonique de K^{n+1} .

3. Dans le cas général, déterminer la matrice T_a associée à U_a dans la base (f_0, f_1, \dots, f_n) . En déduire l'ensemble des éléments a de K^n tels que U_a soit diagonalisable, et déterminer alors une base de vecteurs propres de U_a .

4. Calculer le polynôme minimal de U_a , en discutant suivant les valeurs de a .

47 B. Réduction des matrices stochastiques.

On dit qu'un élément $M = (\alpha_{ij})$ de $M_{n,p}(\mathbf{R})$ est une *matrice stochastique* si, pour tout élément (i, j) de $[1, n] \times [1, p]$, $\alpha_{ij} \geq 0$ et si, pour tout élément j de $[1, p]$,

$$\sum_{i=1}^n \alpha_{ij} = 1.$$

1. Montrer que, pour toute suite (M_1, M_2, \dots, M_r) de matrices stochastiques appartenant à $M_{n,p}(\mathbf{R})$ et pour toute suite $(\beta_1, \beta_2, \dots, \beta_r)$ de nombres réels positifs dont la

somme est égale à 1, la matrice $\sum_{h=1}^r \beta_h M_h$ est encore stochastique.

2. Soient M et N deux matrices stochastiques, appartenant respectivement à $M_{n,p}(\mathbf{R})$ et à $M_{m,n}(\mathbf{R})$. Prouver que la matrice NM est stochastique. En particulier, si M est une matrice stochastique appartenant à $M_n(\mathbf{R})$, il en est de même de M^q , pour tout entier naturel q .

3. On considère la norme sur C^n qui à tout vecteur $x = (\xi_1, \xi_2, \dots, \xi_n)$ associe $\|x\|_1 = \sum_{i=1}^n |\xi_i|$. Soient M une matrice stochastique appartenant à $M_n(\mathbf{R})$, et U l'endomorphisme de C^n canoniquement associé à M . Prouver que, pour tout vecteur x de C^n , $\|U(x)\|_1 \leq \|x\|_1$, et caractériser les vecteurs de C^n pour lesquels cette inégalité devient une égalité.

4. Soit M une matrice stochastique appartenant à $M_n(\mathbf{R})$, considérée comme un élément de $M_n(\mathbf{C})$. Prouver que 1 est valeur propre de M , et que le vecteur $f = (1, 1, \dots, 1)$ est un vecteur propre de M associé à cette valeur propre. Prouver que le spectre de M est contenu dans le disque fermé de centre 0 et de rayon 1. Prouver que toute valeur propre λ de M telle que $|\lambda| = 1$ est d'indice 1, et qu'il existe un entier naturel non nul q tel que $\lambda^q = 1$. (On pourra considérer un vecteur propre $x = (\xi_1, \xi_2, \dots, \xi_n)$ associé à λ , et introduire un élément k de $[1, n]$ tel que, pour tout élément j de $[1, n]$, $|\xi_j| \leq |\xi_k|$.)

48 A. Réduction de la matrice complémentaire d'une matrice.

Soient K un corps algébriquement clos, $M = (\alpha_{ij})$ un élément de $M_n(K)$ et \tilde{M} la matrice complémentaire de M . Déterminer le spectre de \tilde{M} à l'aide de celui de M , ainsi

que les sous-espaces propres et les sous-espaces spectraux de \tilde{M} . (On pourra distinguer trois cas suivant que $\text{rang } M = n$, $\text{rang } M = n - 1$, $\text{rang } M < n - 1$, et utiliser l'exercice 4.44.)

49 A. Localisation du spectre (disques de Gerchgorine).

Soit $M = (\alpha_{ij})$ un élément de $M_n(\mathbb{C})$, où $n > 1$.

1. Montrer que le spectre de M est contenu dans la réunion des disques fermés $B'_{\alpha_{ii}}(\beta_i)$, où, pour tout élément i de $[1, n]$,

$$\beta_i = \sum_{j \neq i} |\alpha_{ij}|.$$

(On pourra utiliser le théorème d'Hadamard; cf. exercice 4.37.)

2. Montrer que le spectre de M est contenu dans la réunion des ovales de Cassini d'équation

$$|z - \alpha_{ii}| \cdot |z - \alpha_{jj}| \leq \beta_i \beta_j,$$

où (i, j) parcourt l'ensemble des couples d'éléments distincts de $[1, n]$.

RÉDUCTION DES ENDOMORPHISMES, EN DIMENSION FINIE

50 A. Trigonalisation d'un endomorphisme.

On se propose de donner une démonstration directe du théorème suivant :

Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K dont le polynôme caractéristique est scindé sur K . Alors U est trigonalisable.

On démontrera cette assertion par récurrence sur la dimension n de E .

On suppose donc qu'elle est démontrée en dimension $n - 1$, et on considère un endomorphisme U d'un espace vectoriel E de dimension n , $n > 1$. Soient λ une valeur propre de U , e_1 un vecteur propre associé à la valeur propre λ , et G un sous-espace vectoriel supplémentaire de la droite Ke_1 dans E . On désigne par V l'endomorphisme de G défini par la formule $V(z) = P_G[U(z)]$, où P_G est le projecteur sur G parallèlement à Ke_1 . Calculer le polynôme caractéristique de V , et prouver que l'hypothèse de récurrence s'applique à V .

51 A. Bases adaptées à une suite de sous-espaces vectoriels stables.

Soit U un endomorphisme scindé d'un espace vectoriel E de dimension finie n sur K .

1. Soit F un sous-espace vectoriel de E de dimension p , stable par U . Montrer qu'il existe une base $B = (e_1, e_2, \dots, e_n)$ de E dans laquelle la matrice associée à U est triangulaire supérieure, et telle que (e_1, e_2, \dots, e_p) soit une base de F . (On pourra d'abord construire une suite croissante (E_1, E_2, \dots, E_p) de sous-espaces vectoriels de E stables par U telle que $E_p = F$, et que, pour tout $q \in [1, p]$, $\dim E_q = q$. On construira alors une suite croissante $(G_1, G_2, \dots, G_{n-p})$ de sous-espaces vectoriels de E^* stables par tU , telle que $G_{n-p} = F^\perp$, et que, pour tout $q \in [1, n - p]$, $\dim G_q = q$.)

2. Soit plus généralement (F_1, F_2, \dots, F_r) une suite strictement croissante de sous-espaces vectoriels de E stables par U . Pour tout $i \in [1, r]$, on note p_i la dimension de F_i . Montrer qu'il existe une suite croissante (E_1, E_2, \dots, E_n) de sous-espaces vectoriels de E stables par U telle que, pour tout $q \in [1, n]$ $\dim E_q = q$, et que, pour tout $i \in [1, r]$, $E_{p_i} = F_i$.

52. Théorème de Hamilton-Cayley.

1. Soit (A_0, A_1, \dots, A_r) une suite d'éléments de $M_n(K)$, considérés comme éléments de $M_n(K')$, où $K' = K(X)$. Prouver que la relation

$$A_0 + XA_1 + \dots + X^r A_r = 0$$

est équivalente aux relations

$$A_0 = A_1 = \dots = A_r = 0.$$

2. Soient E un espace vectoriel de dimension finie non nulle n sur K , U un endomorphisme de E , B une base de E , et M la matrice associée à U dans la base B . On désigne par $N = (P_{ij}(X))$ l'élément de $M_n(K')$ défini par la relation $N = XI_n - M$, et par \tilde{N} la matrice complémentaire de N . En utilisant la relation

$$N\tilde{N} = (\text{Det } N) \cdot I_n,$$

prouver le théorème de Hamilton-Cayley.

3. Soit P un élément de $K[X]$. Prouver que $P(U) = 0$ si et seulement si, pour tout couple (i, j) d'éléments de $[1, n]$, $P \cdot P_{ij}$ est un multiple de δ_{ij} . (On pourra écrire

$$P(X) \cdot I_n - P(M) = NN',$$

où N' est une matrice dont les éléments sont des polynômes à coefficients dans K .)

53. Soient E un espace vectoriel de dimension finie sur K , U et N deux endomorphismes de E tels que $UN = NU$, N étant nilpotent.

1. Prouver que $U + N$ est inversible si et seulement si U est inversible.

a) Si K est algébriquement clos, on pourra trigonaliser simultanément U et N .

b) Dans le cas général, on pourra noter que si U n'est pas inversible, les noyaux de U et N ont une intersection non réduite à $\{0\}$.

2. Prouver que

$$\text{Det}(U + N) = \text{Det}(U).$$

(On pourra d'abord établir cette relation lorsque U est inversible.)

En déduire que U et $U + N$ ont même polynôme caractéristique.

54. Soient E et F deux espaces vectoriels sur K , U une application linéaire de E dans F et V une application linéaire de F dans E .

1. Montrer que si l'endomorphisme $I_F - UV$ est inversible dans $\mathcal{L}(F)$, l'endomorphisme $I_E - VU$ est inversible dans $\mathcal{L}(E)$, et que

$$(I_E - VU)^{-1} = I_E + V(I_F - UV)^{-1}U.$$

En déduire que les valeurs spectrales non nulles de VU coïncident avec celles de UV .

2. On suppose désormais que les espaces vectoriels E et F sont de dimension finie. Montrer que les valeurs propres non nulles de VU coïncident avec celles de UV et que, si $E = F$, les spectres des endomorphismes VU et UV sont égaux. Montrer que si $\dim E \neq \dim F$, il existe des couples (U, V) tels que UV soit injective et que VU ne le soit pas.

3. Prouver que $\text{Tr}(UV) = \text{Tr}(VU)$ et que, pour tout entier naturel m ,

$$\text{Tr}[(UV)^m] = \text{Tr}[(VU)^m].$$

4. On suppose que $E = F$ et que U est un automorphisme de E . En utilisant la relation $VU = U^{-1}(UV)U$, prouver que les polynômes caractéristiques de VU et de UV sont égaux. Montrer que ces polynômes sont encore égaux lorsque U est un endomorphisme quelconque de E .

5. Comparer les polynômes caractéristiques de VU et de UV . (On pourra introduire une base $(e)_{1 \leq j \leq p}$ de E et une base $(f_i)_{1 \leq i \leq n}$ de F telles que, pour tout élément j de $[1, r]$, $U(e_j) = f_j$ et que, pour tout élément j de $[r+1, p]$, $U(e_j) = 0$, où $r = \text{rang}(U)$.)

55. Réduction des endomorphismes de translation.

Soient E un espace vectoriel de dimension finie n sur K , et U un endomorphisme de E . On désigne par U_g (resp. par U_d) l'endomorphisme de l'espace vectoriel $\mathfrak{L}(E)$ défini par la formule $U_g(V) = U \circ V$ (resp. $U_d(V) = V \circ U$).

1. Déterminer les noyaux de U_g et de U_d à l'aide du noyau et de l'image de U . En déduire que les spectres de U_g et de U_d coïncident avec celui de U .

2. Soit λ une valeur propre de U . Déterminer les sous-espaces propres de U_g et de U_d associés à λ , et calculer leurs dimensions en fonction de celle du sous-espace propre de U associé à λ . Reprendre la même question pour les sous-espaces spectraux de U_g et de U_d .

3. Prouver que si U est scindé, ou diagonalisable, il en est de même de U_g et de U_d .

4. Prouver que si U est scindé, les polynômes caractéristiques de U_g et de U_d sont égaux à δ_U^n . Lorsque K est algébriquement clos, retrouver ce résultat en le démontrant d'abord lorsque U est diagonalisable, et en utilisant la densité des endomorphismes diagonalisables.

56 B. Réduction des extensions tensorielle, symétrique et extérieure d'un endomorphisme.

1. Soient E et F deux espaces vectoriels de dimension finie sur K , U une application linéaire de E dans F , p un entier naturel non nul et U_p l'application linéaire de $\mathcal{M}_p(F)$ dans $\mathcal{M}_p(E)$ extension $p^{\text{ième}}$ de U . Déterminer le noyau et l'image de U_p à l'aide du noyau et de l'image de U . (On pourra introduire des bases convenables de E et de F .)

2. Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Déterminer le spectre de l'endomorphisme U_p à l'aide du spectre de l'endomorphisme U .

Prouver que si U est diagonalisable sur K , il en est de même de U_p . Déterminer alors les sous-espaces propres de U_p à l'aide des sous-espaces propres de U .

Prouver que si U est scindé sur K , il en est de même de U_p . Déterminer alors les sous-espaces spectraux de U_p à l'aide des sous-espaces spectraux de U , et le polynôme caractéristique de U_p à l'aide de celui de U .

3. Reprendre les deux questions précédentes en remplaçant l'espace vectoriel $\mathcal{M}_p(E)$ par l'espace vectoriel $\mathcal{P}_p(E)$, puis par l'espace vectoriel $\mathcal{A}_p(E)$.

57. Soient n un entier naturel non nul, r un entier naturel strictement supérieur à 1 et $(U_p)_{1 \leq p \leq r}$ une suite d'endomorphismes de l'espace vectoriel $E = \mathbb{C}^n$ satisfaisant aux relations suivantes :

— pour tout élément p de $[1, r]$, $U_p^2 = -I_E$;

— pour tout couple (p, q) d'éléments distincts de $[1, r]$, $U_p U_q = -U_q U_p$.

1. Montrer que, pour tout élément p de $[1, r]$, la trace de U_p est nulle, et que n est pair.

2. Montrer que, pour tout élément p de $[1, r]$, U_p est diagonalisable, et que ses valeurs propres sont i et $-i$ avec la multiplicité $\frac{n}{2}$.

58. Pour tout élément M de $M_n(\mathbb{C})$, on pose $M = A + iB$, où A et $B \in M_n(\mathbb{R})$. Soit φ l'application de $M_n(\mathbb{C})$ dans $M_{2n}(\mathbb{R})$ qui associe à M la matrice

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix}.$$

Montrer que φ est un morphisme de \mathbb{R} -algèbres unitaires, et que son image est l'ensemble des éléments de $M_{2n}(\mathbb{R})$ commutant avec la matrice

$$\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

59. Soit E un espace vectoriel de dimension finie sur \mathbb{R} .

1. Soit U un endomorphisme de E tel que $U^2 = -I_E$. On définit une application de $\mathbb{C} \times E$ dans E qui au couple d'un nombre complexe $\alpha + i\beta$ et d'un vecteur x de E associe $\alpha x - \beta U(x)$. Montrer que, muni de l'addition et de cette loi externe, E est un espace vectoriel sur \mathbb{C} , que l'on note E_U .

2. Soit V un endomorphisme du \mathbb{R} -espace vectoriel E . Montrer qu'il est équivalent de dire :

- l'application V commute avec U ;
- l'application V est un endomorphisme du \mathbb{C} -espace vectoriel E_U .

3. Prouver que si (x_1, x_2, \dots, x_n) est une base du \mathbb{C} -espace vectoriel E_U , alors $(x_1, \dots, x_n, U(x_1), \dots, U(x_n))$ est une base du \mathbb{R} -espace vectoriel E .

Soient F le sous-espace vectoriel de E engendré par x_1, x_2, \dots, x_n , et G le sous-espace vectoriel de E engendré par $U(x_1), U(x_2), \dots, U(x_n)$. Prouver que F et G sont supplémentaires dans E , que $U(F) = G$ et que $U(G) = F$.

4. En déduire que E est de dimension paire sur \mathbb{R} .

5. Prouver qu'il existe une application linéaire j et une seule du \mathbb{C} -espace vectoriel $F_{\mathbb{C}}$ sur le \mathbb{C} -espace vectoriel E_U telle que, pour tout couple (x, y) d'éléments de F , $j(x + iy) = x - U(y)$. Trouver l'automorphisme de $F_{\mathbb{C}}$ auquel s'identifie l'automorphisme U par j .

Retrouver par cette méthode le résultat de la question 2.

6. Étendre ces résultats au cas où E n'est pas nécessairement de dimension finie.

RÉDUCTION DE JORDAN

60 A. Réduction de Jordan d'un endomorphisme nilpotent.

Soient U un endomorphisme nilpotent d'un espace vectoriel E de dimension finie n sur K , et p le plus petit des entiers s tels que $U^s = 0$. Pour tout entier naturel q , on pose $E_q = \text{Ker}(U^q)$, et $n_q = \dim E_q$.

1. Soient m un élément de $[1, p]$, et G un sous-espace vectoriel de E tel que $G \cap E_m = \{0\}$. Prouver que $U(G) \cap E_{m-1} = \{0\}$.

2. En déduire qu'il existe une suite $(G_q)_{1 \leq q \leq p}$ de sous-espaces vectoriels de E telle que

$$\begin{aligned} E_p &= G_1 \oplus E_{p-1} \\ E_{p-1} &= U(G_1) \oplus G_2 \oplus E_{p-2} \\ &\dots\dots\dots \\ E_{p-q+1} &= U^{q-1}(G_1) \oplus U^{q-2}(G_2) \oplus \dots \oplus U(G_{q-1}) \oplus G_q \oplus E_{p-q} \\ &\dots\dots\dots \\ E_1 &= U^{p-1}(G_1) \oplus U^{p-2}(G_2) \oplus \dots \oplus U(G_{p-1}) \oplus G_p. \end{aligned}$$

3. Pour tout entier $q \in [1, p]$, on pose

$$H_q = G_q \oplus U(G_q) \oplus \dots \oplus U^{p-q}(G_q).$$

Montrer que H_q est stable par U , et que

$$E = E_p = H_1 \oplus H_2 \oplus \dots \oplus H_p.$$

4. On considère maintenant une base $B = (e_i)_{i \in I}$ du sous-espace vectoriel $\bigoplus_{q=1}^p G_q$ adaptée à cette décomposition en somme directe : ainsi, pour tout $q \in [1, p]$, $B_q = (e_i)_{i \in I_q}$ est une base de G_q , où I_q désigne l'ensemble des éléments i de I tels que $e_i \in G_q$. Pour tout $i \in I$, on désigne par F_i le sous-espace vectoriel de E engendré par les vecteurs $U^j(e_i)$, où $j \in \mathbb{N}$. Montrer que les sous-espaces vectoriels F_i sont stables par U , et monogènes relativement à U .

Prouver, par récurrence sur l'entier j , que, pour tout $j \in [1, p - q]$,

$$U^j(G_q) = \bigoplus_{i \in I_q} F_i,$$

et que

$$E = \bigoplus_{i \in I} F_i.$$

On obtient ainsi le résultat suivant (cf. cor. du th. 5.18) :

Pour tout endomorphisme nilpotent U d'un espace vectoriel E de dimension finie n sur K , il existe une famille finie $(F_i)_{i \in I}$ de sous-espaces vectoriels de E non réduits à $\{0\}$, stables par U et monogènes relativement à U , telle que E soit somme directe des sous-espaces vectoriels F_i . De plus, pour tout $i \in I$, il existe une base B_i de F_i telle que la matrice M_i associée à l'endomorphisme V_i de F_i obtenu par restriction de U à F_i soit une matrice de Jordan.

5. Prouver que si $(F_i)_{i \in I}$ est une telle suite, le degré du polynôme minimal de U n'est autre que la plus grande des dimensions des sous-espaces vectoriels F_i .

Plus généralement, montrer que, pour tout $r \in [1, n]$, le nombre m_r des éléments i de I tels que $\dim F_i = r$ est donné par la relation

$$m_r = 2n_r - n_{r+1} - n_{r-1}.$$

61 A. Effet d'un automorphisme intérieur sur la décomposition de Jordan.

Soit E un espace vectoriel de dimension finie sur K .

1. Soient U un endomorphisme de E , V un automorphisme de E , et $U' = VUV^{-1}$. Montrer qu'un sous-espace vectoriel F de E est stable par U si et seulement si $V(F)$ est stable par U' , que F est U -monogène si et seulement si $V(F)$ est U' -monogène, et que, dans ces conditions, un vecteur x de E est un U -générateur de F si et seulement si $V(x)$

est un U' -générateur de $V(F)$. Prouver de même que F est irréductible (resp. indécomposable) relativement à U si et seulement si $V(F)$ est irréductible (resp. indécomposable) relativement à U' .

2. Soient U et U' deux endomorphismes de E ayant même polynôme minimal et tels que E soit U -monogène et U' -monogène, x un U -générateur de E et x' un U' -générateur de E . On considère l'unique automorphisme V de E tel que, pour tout élément j de $[0, n - 1]$, $V[U^j(x)] = U'^j(x')$. Montrer que $U' = VUV^{-1}$.

62. Sommes de sous-espaces vectoriels monogènes.

Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Soient x et y deux vecteurs de E , dont les annulateurs P et Q sont premiers entre eux, F et G les sous-espaces vectoriels de E stables par U engendrés par x et par y . Montrer que la somme $F + G$ est directe. Prouver que l'annulateur π de $x + y$ n'est autre que PQ (On montrera que π divise PQ , et donc que $\pi = P_1Q_1$, où P_1 divise P et Q_1 divise Q . On prouvera ensuite que P divise P_1 et que Q divise Q_1 , en considérant les transformés de $x + y$ par $(QP_1)(U)$ et par $(Q_1P)(U)$.)

En déduire le résultat suivant :

Soient F et G deux sous-espaces vectoriels U -monogènes de E tels que les polynômes minimaux P et Q des endomorphismes de F et de G coïncidant avec U soient premiers entre eux. Alors la somme $F + G$ est directe, et $F + G$ est U -monogène.

63 A. Sous-espaces vectoriels stables de sous-espaces vectoriels monogènes.

Soient U un endomorphisme d'un espace vectoriel E de dimension finie n sur K tel que E soit U -monogène, π le polynôme minimal de U et x un vecteur U -générateur de E .

1. Soient P un élément de $K[X]$ et $y = P(U)(x)$. On désigne par π_1 le P. G. C. D. de P et de π , et on pose $\pi_2 = \frac{\pi}{\pi_1}$. Prouver que l'annulateur π' de y n'est autre que π_2 . (On prouvera successivement que π' divise π_2 et que π divise $\pi'P$.) En particulier, la dimension du sous-espace vectoriel stable engendré par y est égale à $n - d^\circ(\pi_1)$.

2. Soit F un sous-espace vectoriel de E stable par U . Montrer que l'ensemble des éléments P de $K[X]$ tels que $P(U)(x)$ appartienne à F est un idéal de $K[X]$. Soit D le générateur de cet idéal. Prouver que le vecteur $D(U)(x)$ est un U -générateur de F . En déduire le résultat suivant :

Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Alors tout sous-espace vectoriel de E stable par U contenu dans un sous-espace vectoriel U -monogène est encore U -monogène.

64 B. Invariants de similitude d'un endomorphisme.

Soient U un endomorphisme d'un espace vectoriel E de dimension finie sur K , et π le polynôme minimal de U .

1. A l'aide du théorème de Jordan et de l'exercice 62, prouver qu'il existe deux sous-espaces vectoriels F et G de E stables par U dont E est somme directe, tels que G soit U -monogène et que le polynôme minimal de l'endomorphisme de G coïncidant avec U soit égal à π .

En déduire qu'il existe une suite (E_1, E_2, \dots, E_r) de sous-espaces vectoriels U -monogènes de E dont E est somme directe, telle que, pour tout élément j de $[1, r - 1]$, le polynôme minimal π_j de l'endomorphisme U_j de E_j coïncidant avec U divise π_{j+1} .

2. Soit (E_1, E_2, \dots, E_r) une suite de sous-espaces vectoriels de E satisfaisant aux conditions précédentes. Prouver que le polynôme π_r est égal à π . En déduire que $\dim E_r = d^\circ(\pi)$. Soient $F_1 = E/E_r$, ϕ_1 l'application linéaire canonique de E sur F_1 et V_1 l'unique endomorphisme de F_1 tel que $V_1 \circ \phi_1 = \phi_1 \circ U$. Prouver que π_{r-1} n'est autre que le polynôme minimal de V_1 . Interpréter de même les polynômes $\pi_{r-2}, \pi_{r-3}, \dots, \pi_1$.

3. Soit (E_1, E_2, \dots, E_r) une suite de sous-espaces vectoriels de E satisfaisant aux conditions précédentes. Prouver que le polynôme caractéristique δ_U est égal au produit des polynômes π_j . En déduire une nouvelle démonstration du théorème de Hamilton-Cayley.

4. On introduit sur E la structure de $K[X]$ -module définie par l'endomorphisme U . En appliquant à ce module les résultats de l'exercice I.3.105, et en comparant la suite $(\pi_1, \pi_2, \dots, \pi_r)$ à celle des facteurs invariants de ce module, prouver l'unicité de la suite $(\pi_1, \pi_2, \dots, \pi_r)$, et retrouver son existence.

5. Déduire des questions 1 et 4 le résultat fondamental suivant :

Soit U un endomorphisme d'un espace vectoriel E de dimension finie sur K . Il existe une suite (E_1, E_2, \dots, E_r) de sous-espaces vectoriels U -monogènes de E dont E est somme directe, telle que, pour tout élément j de $[1, r - 1]$, le polynôme minimal π_j de l'endomorphisme U de E_j coïncidant avec U divise π_{j+1} . La suite $(\pi_1, \pi_2, \dots, \pi_r)$ est indépendante du choix de la décomposition (E_1, E_2, \dots, E_r) . De plus, pour que deux endomorphismes U et U' de E soient semblables, il faut et il suffit qu'ils aient même suite $(\pi_1, \pi_2, \dots, \pi_r)$ associée. C'est pourquoi $(\pi_1, \pi_2, \dots, \pi_r)$ s'appelle suite des invariants de similitude de l'endomorphisme U .

6. Soient M un élément de $M_n(K)$, et U l'endomorphisme de K^n canoniquement associé à M . On appelle suite des invariants de similitude de M la suite des invariants de similitude de U . Prouver que deux éléments M et M' de $M_n(K)$ sont semblables si et seulement s'ils ont la même suite d'invariants de similitude. Prouver que, dans chaque classe de similitude de l'ensemble $M_n(K)$, il existe une matrice canonique et une seule.

(Soit $(\pi_1, \pi_2, \dots, \pi_r)$ une suite de r polynômes unitaires non constants à coefficients dans K telle que, pour tout élément j de $[1, r - 1]$, π_j divise π_{j+1} . On appelle matrice canonique associée à la suite $(\pi_1, \pi_2, \dots, \pi_r)$ la matrice décomposée en les blocs diagonaux M_1, M_2, \dots, M_r , où, pour tout élément j de $[1, r]$, M_j est la matrice canonique associée au polynôme π_j .)

7. Expliciter les résultats des questions 5 et 6 lorsque le corps K est algébriquement clos.

Application. — Déterminer les classes de similitude des éléments de $M_5(\mathbb{C})$ qui annulent le polynôme $X^3 - 2X^2 + X$.

CALCUL FONCTIONNEL

65. Substitution d'un endomorphisme dans une fraction rationnelle.

(On utilise les résultats de l'exercice 16.)

Soient U un endomorphisme scindé d'un espace vectoriel E sur K , et R un élément de $K(X)$.

1. Montrer que U est substituable dans R si et seulement si toutes les valeurs propres de U sont substituables dans R .

Dans toute la suite, on suppose cette condition réalisée.

2. Prouver que le spectre de $R(U)$ est constitué des scalaires $R(\lambda)$, où λ parcourt $\text{sp}(U)$. Montrer que $R(U)$ est un endomorphisme scindé, et déterminer ses sous-espaces spectraux.

3. Prouver que si U est diagonalisable, il en est de même de $R(U)$. Déterminer alors la décomposition spectrale de $R(U)$ en fonction de celle de U .

4. On suppose que E est de dimension finie sur K , et que U est substituable dans R . Soit

$$\delta_U = \prod_{i=1}^n (X - \lambda_i)$$

le polynôme caractéristique de U . Prouver que

$$\delta_{R(U)} = \prod_{i=1}^n (X - R(\lambda_i)),$$

et que

$$\text{Tr } [R(U)] = \sum_{i=1}^n R(\lambda_i).$$

(On pourra trigonaliser l'endomorphisme U .)

5. Soit M un élément de $\mathbf{M}_n(K)$ scindé sur K . Prouver que la matrice $XI_n - M$ est inversible dans $\mathbf{M}_n(K(X))$, et que

$$\text{Tr } [(XI_n - M)^{-1}] = \frac{D(\delta_M)}{\delta_M}.$$

66. *Substitution d'une matrice carrée dans une fraction rationnelle.*

(On utilise les résultats de l'exercice 65.)

Soient M un élément scindé de $\mathbf{M}_n(K)$ et R un élément de $K(X)$.

1. Montrer que M est substituable dans R si et seulement si toutes les valeurs propres de M sont substituables dans R .

Dans la suite, on suppose que cette condition est réalisée.

2. Montrer que si M est diagonalisable, il en est de même de $R(M)$, et donner une méthode de calcul de $R(M)$.

3. Montrer que si M est trigonale supérieure réduite, il en est de même de $R(M)$. En déduire une méthode de calcul de $R(M)$, lorsqu'on suppose seulement que M est scindée.

67 A. *Polynômes d'un endomorphisme nilpotent.*

Soient E un espace vectoriel sur K , et P un élément de $K[X]$.

1. On suppose que $P(0) = 0$, et que $P'(0) \neq 0$. Soient N un endomorphisme nilpotent de E , et $K[N]$ la sous-algèbre unitaire engendrée par N . On désigne par n le plus grand des entiers naturels p tels que $N^p \neq 0$. On rappelle (cf. exercice I.3.48) que l'application de l'algèbre A_n des développements limités formels à l'ordre n dans $K[N]$ qui

à $\sum_{p=0}^n \alpha_p X^p$ associe $\sum_{p=0}^n \alpha_p N^p$ est un isomorphisme d'algèbres unitaires. En déduire qu'il existe un polynôme Q tel que $Q(0) = 0$ et que $Q(P(N)) = P[Q(N)] = N$.

Montrer que l'application $N \mapsto P(N)$ est une bijection de l'ensemble des endomorphismes nilpotents de E sur lui-même.

2. Soit λ un élément de K . On suppose que $P'(\lambda) \neq 0$. On désigne par \mathcal{U}_λ l'ensemble des endomorphismes U de E de la forme $U = \lambda I_E + N$, où N est nilpotent. Prouver que, pour tout élément U de \mathcal{U}_λ , $P(U)$ appartient à $\mathcal{U}_{P(\lambda)}$. À l'aide de la question 1, prouver que, pour tout élément U de \mathcal{U}_λ , il existe un élément R de $K[X]$ tel que $R[P(U)] = U$. Prouver que l'application $U \mapsto P(U)$ est une bijection de \mathcal{U}_λ sur $\mathcal{U}_{P(\lambda)}$.

68 B. *Applications polynomiales dans l'algèbre des endomorphismes.*

Soient E un espace vectoriel de dimension finie sur K , A une partie de K et Q un élément de $K[X]$ dont la restriction à A est injective et telle que Q' ne s'annule pas sur A . On pose $B = Q(A)$, et on désigne par $\mathcal{L}_A(E)$ (resp. par $\mathcal{L}_B(E)$) l'ensemble des endomorphismes scindés de E dont le spectre est contenu dans A (resp. dans B).

1. Prouver que, pour tout élément V de $\mathcal{L}_B(E)$, il existe un élément U de $\mathcal{L}_A(E)$ tel que $Q(U) = V$, et que U soit un polynôme en V . (On pourra réduire V .)

2. Soient U un endomorphisme scindé de E , D sa composante diagonalisable, et R un élément de $K[X]$. Prouver que $R(D)$ est la composante diagonalisable de $R(U)$.

3. En déduire que si U est un élément de $\mathcal{L}_A(E)$, les projecteurs spectraux de U sont des polynômes en $Q(U)$.

4. Pour toute valeur propre λ de U , on désigne par P_λ le projecteur spectral sur $F_\lambda(U)$, et on pose $U_\lambda = UP_\lambda$; U_λ s'écrit sous la forme $U_\lambda = \lambda P_\lambda + N_\lambda$, où N_λ est nilpotent. Démontrer que

$$Q(U) \cdot P_\lambda = Q(\lambda I_E + N_\lambda) \cdot P_\lambda.$$

En utilisant l'exercice 67, montrer que N_λ est un polynôme en $Q(\lambda I_E + N_\lambda)$. En déduire que N_λ est un polynôme en $Q(U)$. Prouver enfin que U est un polynôme en $Q(U)$.

5. Soient U et U' deux éléments de $\mathcal{L}_A(E)$ tels que $Q(U) = Q(U')$. Prouver que U et U' commutent. Montrer que U et U' ont même composante diagonalisable. Prouver enfin que $U = U'$.

On obtient ainsi le résultat suivant :

L'application $U \mapsto Q(U)$ est une bijection de $\mathcal{L}_A(E)$ sur $\mathcal{L}_B(E)$.

69. *Surjectivité des fonctions puissances.*

Soient $N_n(K)$ l'ensemble des matrices nilpotentes d'ordre n , et $U_n(K)$ le groupe multiplicatif des matrices unipotentes d'ordre n .

1. A l'aide de l'exercice 68, prouver que, pour tout entier rationnel p non nul, l'application $U \mapsto U^p$ est une application surjective de $U_n(K)$ sur lui-même.

2. Plus généralement, pour tout élément α de K , et pour tout élément U de $U_n(K)$, on pose $U^\alpha = \exp[\alpha \log(U)]$, où \log désigne la bijection inverse de la bijection \exp de $N_n(K)$ sur $U_n(K)$ (cf. exercice I.3.49). Prouver que U^α est un polynôme en U , et que l'application $\alpha \mapsto U^\alpha$ est un morphisme du groupe additif K dans le groupe multiplicatif $U_n(K)$. Prouver d'autre part que si α est non nul, l'application $U \mapsto U^\alpha$ est une application surjective de $U_n(K)$ sur lui-même.

3. On suppose le corps K algébriquement clos. Prouver, en utilisant le théorème de décomposition multiplicative d'un automorphisme (corollaire du th. 5.13), que, pour tout entier strictement positif p , et pour tout élément M de $GL_n(K)$, il existe un élément M' de $GL_n(K)$ tel que $M'^p = M$, et que M' soit un polynôme en M . Déterminer alors toutes les matrices M' satisfaisant à ces relations. En particulier, l'application $M \mapsto M^p$ est une application surjective de $GL_n(K)$ sur lui-même.

4. Soient M un élément non nul de $M_2(K)$ tel que $M^2 = 0$, et p un entier strictement supérieur à 1. Prouver qu'il n'existe aucun élément M' de $M_2(K)$ tel que $M'^p = M$.

ALGÈBRES DE LIE NILPOTENTES ET RÉSOLUBLES

70 A. Algèbres de Lie classiques.

On appelle *K-algèbre de Lie* une *K*-algèbre \mathfrak{g} , dont la multiplication, appelée crochet et notée $(x, y) \mapsto [x, y]$, satisfait aux conditions suivantes :

— pour tout élément x de \mathfrak{g} ,

$$[x, x] = 0;$$

— pour tout triplet (x, y, z) d'éléments de \mathfrak{g} ,

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$$

(identité de Jacobi.)

1. Soit A une *K*-algèbre associative. Prouver que l'application $(x, y) \mapsto [x, y] = xy - yx$ définit sur A une structure de *K*-algèbre de Lie.

En particulier, l'espace vectoriel $\mathfrak{L}(E)$ des endomorphismes d'un espace vectoriel E , muni de la loi $(U, V) \mapsto UV - VU$, est une *K*-algèbre de Lie, notée $\mathfrak{gl}(E)$.

2. Soit E un espace vectoriel de dimension finie n . Montrer que l'ensemble des endomorphismes de trace nulle est un idéal de $\mathfrak{gl}(E)$; on le note $\mathfrak{sl}(E)$.

Montrer que l'ensemble des endomorphismes laissant stable un drapeau $\mathcal{F} = (E_0, E_1, \dots, E_n)$ de E (cf. exercice 4.49) est une sous-algèbre de Lie de $\mathfrak{gl}(E)$, notée $\mathfrak{t}_{\mathcal{F}}(E)$, et que l'ensemble des endomorphismes U de E tels que, pour tout élément i de $[1, n]$, $U(E_i) \subset E_{i-1}$ est un idéal de l'algèbre de Lie $\mathfrak{t}_{\mathcal{F}}(E)$, notée $\mathfrak{n}_{\mathcal{F}}(E)$.

3. Prouver de même que l'espace vectoriel $M_n(K)$ des matrices carrées d'ordre n à éléments dans K , muni de la loi $(M, N) \mapsto MN - NM$, est une *K*-algèbre de Lie, notée $\mathfrak{gl}(n, K)$, que les matrices de trace nulle constituent un idéal de $\mathfrak{gl}(n, K)$, noté $\mathfrak{sl}(n, K)$, que les matrices trigonales supérieures constituent une sous-algèbre de Lie de $\mathfrak{gl}(n, K)$, notée $\mathfrak{t}(n, K)$, et que les matrices trigonales supérieures nilpotentes constituent un idéal de $\mathfrak{t}(n, K)$, noté $\mathfrak{n}(n, K)$.

71 A. Dérivations d'une algèbre de Lie.

On rappelle qu'une dérivation D d'une algèbre de Lie \mathfrak{g} est un endomorphisme de l'espace vectoriel \mathfrak{g} tel que, pour tout couple (x, y) d'éléments de \mathfrak{g} ,

$$D([x, y]) = [Dx, y] + [x, Dy].$$

1. Montrer que l'ensemble des dérivations de \mathfrak{g} est une sous-algèbre de l'algèbre de Lie associée à $\mathfrak{L}(\mathfrak{g})$, appelée algèbre de Lie des dérivations de \mathfrak{g} , et notée $\text{Der}(\mathfrak{g})$.

2. Pour tout élément x de \mathfrak{g} , soit $\text{Ad } x$ l'endomorphisme de l'espace vectoriel \mathfrak{g} défini par la formule

$$(\text{Ad } x)(y) = [x, y].$$

Montrer que $\text{Ad } x$ est une dérivation de \mathfrak{g} , dite *dérivation intérieure* définie par x , et que l'application $x \mapsto \text{Ad } x$ est un morphisme de l'algèbre de Lie \mathfrak{g} dans l'algèbre de Lie $\text{Der}(\mathfrak{g})$, dont le noyau s'appelle *centre de* \mathfrak{g} et dont l'image est un idéal de $\text{Der}(\mathfrak{g})$. Plus précisément, prouver que, pour tout élément x de \mathfrak{g} et pour tout élément D de $\text{Der}(\mathfrak{g})$,

$$[D, \text{Ad } x] = \text{Ad } (Dx).$$

3. Soit \mathfrak{a} une sous-algèbre de Lie de \mathfrak{g} . Montrer que \mathfrak{a} est un idéal si et seulement si \mathfrak{a} est stable par toutes les dérivations intérieures de \mathfrak{g} .

On dit qu'un idéal α est *caractéristique* si α est stable par toutes les dérivations de \mathfrak{g} . Montrer que tout idéal caractéristique d'un idéal (resp. d'un idéal caractéristique) de \mathfrak{g} est un idéal (resp. un idéal caractéristique) de \mathfrak{g} .

4. Soient α et \mathfrak{h} deux idéaux (resp. deux idéaux caractéristiques) de \mathfrak{g} . Montrer que le sous-espace vectoriel de \mathfrak{g} engendré par les éléments $[x, y]$ où $x \in \alpha$ et $y \in \mathfrak{h}$ est un idéal (resp. un idéal caractéristique) de \mathfrak{g} , noté $[\alpha, \mathfrak{h}]$.

On pose

$$\mathcal{D}^0 \mathfrak{g} = \mathfrak{g}, \quad \mathcal{C}^0 \mathfrak{g} = \mathfrak{g}$$

et, pour tout entier naturel non nul p ,

$$\mathcal{D}^p \mathfrak{g} = [\mathcal{D}^{p-1} \mathfrak{g}, \mathcal{D}^{p-1} \mathfrak{g}], \quad \mathcal{C}^p \mathfrak{g} = [\mathfrak{g}, \mathcal{C}^{p-1} \mathfrak{g}].$$

Montrer que, pour tout entier naturel p , $\mathcal{D}^p \mathfrak{g}$ et $\mathcal{C}^p \mathfrak{g}$ sont des idéaux caractéristiques, et que $\mathcal{D}^p \mathfrak{g} \subset \mathcal{C}^p \mathfrak{g}$. La suite $(\mathcal{D}^p \mathfrak{g})$ s'appelle *série dérivée* de \mathfrak{g} , et la suite $(\mathcal{C}^p \mathfrak{g})$ *série centrale descendante* de \mathfrak{g} ; $\mathcal{D}^1 \mathfrak{g}$, égal à $\mathcal{C}^1 \mathfrak{g}$, s'appelle *algèbre de Lie dérivée* de \mathfrak{g} .

5. Prouver que, pour tout idéal (resp. pour tout idéal caractéristique) α de \mathfrak{g} , le commutant α' de α dans \mathfrak{g} , c'est-à-dire l'ensemble des éléments x de \mathfrak{g} tels que, pour tout élément y de α , $[x, y] = 0$, est un idéal (resp. un idéal caractéristique) de \mathfrak{g} . En particulier, le centre de \mathfrak{g} est un idéal caractéristique de \mathfrak{g} .

On pose

$$\mathcal{C}_0 \mathfrak{g} = \{0\}$$

et, pour tout entier naturel non nul p ,

$$\mathcal{C}_p \mathfrak{g} = \varphi_p^{-1}(\mathfrak{g}_p),$$

où φ_p désigne l'application canonique de \mathfrak{g} sur $\mathfrak{g}/\mathcal{C}_{p-1} \mathfrak{g}$, et où \mathfrak{g}_p désigne le centre de cette dernière algèbre. En particulier, $\mathcal{C}_1 \mathfrak{g}$ est le centre de \mathfrak{g} . Montrer que $\mathcal{C}_p \mathfrak{g}$ est un idéal caractéristique de \mathfrak{g} , que la suite $(\mathcal{C}_p \mathfrak{g})$ est croissante et que, pour tout entier naturel non nul p ,

$$[\mathfrak{g}, \mathcal{C}_p \mathfrak{g}] \subset \mathcal{C}_{p-1} \mathfrak{g}.$$

La suite $(\mathcal{C}_p \mathfrak{g})$ s'appelle *série centrale ascendante* de \mathfrak{g} .

72 B. Algèbres de Lie nilpotentes.

On utilise les résultats de l'exercice 71.

Soit \mathfrak{g} une algèbre de Lie. On dit que \mathfrak{g} est *nilpotente* s'il existe une suite décroissante $(\alpha_0, \alpha_1, \dots, \alpha_p)$ d'idéaux de \mathfrak{g} telle que $\alpha_0 = \mathfrak{g}$, $\alpha_p = \{0\}$ et, pour tout élément i de $[0, p-1]$, $[\mathfrak{g}, \alpha_i] \subset \alpha_{i+1}$.

1. Montrer que, sous ces hypothèses, pour tout élément i de $[0, p]$, $\alpha_i \supset \mathcal{C} \mathfrak{g}$ et $\alpha_{p-i} \subset \mathcal{C}_i \mathfrak{g}$.

En particulier, on obtient le résultat suivant :

Soit \mathfrak{g} une algèbre de Lie. Il est équivalent de dire :

- a) \mathfrak{g} est nilpotente;
- b) il existe un entier naturel p tel que $\mathcal{C}^p \mathfrak{g} = \{0\}$;
- c) il existe un entier naturel p tel que $\mathcal{C}_p \mathfrak{g} = \{0\}$;
- d) il existe un entier naturel p tel que, pour toute suite (x_1, x_2, \dots, x_p) d'éléments de \mathfrak{g} ,

$$\text{Ad } x_1 \circ \text{Ad } x_2 \circ \dots \circ \text{Ad } x_p = 0$$

2. Soient E un espace vectoriel de dimension finie n sur K et $\mathcal{F} = (E_0, E_1, \dots, E_n)$ un drapeau de E . Prouver que l'algèbre de Lie $\mathfrak{n}_{\mathcal{F}}(E)$ est nilpotente. (On considérera les idéaux α_r constitués des endomorphismes U de E tels que, pour tout élément i de $[r+1, n]$, $U(E_i) \subset E_{i-r}$.)

3. Soient E un espace vectoriel sur K et U un endomorphisme nilpotent de E . Prouver que $\text{Ad } U$ est un endomorphisme nilpotent de $\mathfrak{L}(E)$.

4. Prouver le résultat suivant (théorème d'Engel) :

Soient E un espace vectoriel sur K non réduit à $\{0\}$ et \mathfrak{g} une sous-algèbre de Lie de dimension finie de $\mathfrak{gl}(E)$ dont tous les éléments sont des endomorphismes nilpotents de E . Il existe alors un élément non nul x de E tel que, pour tout élément U de \mathfrak{g} , $U(x) = 0$.

On pourra raisonner par récurrence sur $n = \dim \mathfrak{g}$, et prouver successivement les résultats suivants :

a) Soit \mathfrak{h} une sous-algèbre de Lie de \mathfrak{g} distincte de \mathfrak{g} . Alors l'ensemble $\mathfrak{n}(\mathfrak{h})$ des éléments U de \mathfrak{g} tels que $\text{Ad } U$ laisse stable \mathfrak{h} est une sous-algèbre de Lie de \mathfrak{g} contenant \mathfrak{h} . En considérant les endomorphismes de $\mathfrak{g}/\mathfrak{h}$ définis par les endomorphismes $\text{Ad } U$, où $U \in \mathfrak{h}$, et en appliquant l'hypothèse de récurrence, montrer qu'il existe un élément V de \mathfrak{g} n'appartenant pas à \mathfrak{h} et appartenant à $\mathfrak{n}(\mathfrak{h})$.

b) Soit \mathfrak{h} une sous-algèbre de Lie de \mathfrak{g} distincte de \mathfrak{g} , de dimension maximale. Prouver à l'aide de a) que \mathfrak{h} est un idéal de \mathfrak{g} . En déduire que $\text{codim}_{\mathfrak{g}} \mathfrak{h} = 1$, et que le sous-espace vectoriel F de E constitué des éléments y tels que $U(y) = 0$ pour tout élément U de \mathfrak{h} est stable par \mathfrak{g} . A l'aide de l'hypothèse de récurrence, prouver que $F \neq \{0\}$.

Soient enfin V un élément de \mathfrak{g} n'appartenant pas à \mathfrak{h} et x un élément non nul de F tel que $V(x) = 0$. Prouver que, pour tout élément U de \mathfrak{g} , $U(x) = 0$.

5. A l'aide du théorème d'Engel, prouver le résultat suivant, qui constitue une réciproque de la question 2 :

Soient E un espace vectoriel de dimension finie sur K et \mathfrak{g} une sous-algèbre de Lie de $\mathfrak{gl}(E)$ dont tous les éléments sont des endomorphismes nilpotents de E . Il existe alors un drapeau \mathcal{F} de E tel que \mathfrak{g} soit contenue dans $\mathfrak{n}_{\mathcal{F}}(E)$.

(On pourra raisonner par récurrence sur la dimension de E .)

En particulier, il existe une base B de E telle que, pour tout élément U de \mathfrak{g} , $M_B(U)$ soit triangulaire supérieure nilpotente.

(Lorsque \mathfrak{g} est commutative, on retrouve le corollaire 2 de la proposition 5.16.)

6. Soit \mathfrak{n} une algèbre de Lie de dimension finie n sur K . On suppose que, pour tout élément x de \mathfrak{n} , $\text{Ad } x$ est un endomorphisme nilpotent de \mathfrak{n} . A l'aide de la question 5, appliquée à $E = \mathfrak{n}$, montrer qu'il existe un drapeau $(\alpha_0, \alpha_1, \dots, \alpha_n)$ de sous-espaces vectoriels de \mathfrak{n} tel que, pour tout élément i de $[1, n]$, $[\mathfrak{n}, \alpha_i] \subset \alpha_{i-1}$. En conclure que \mathfrak{n} est une algèbre de Lie nilpotente.

73 B. Algèbres de Lie résolubles.

On utilise les résultats de l'exercice 71.

Soit \mathfrak{g} une algèbre de Lie. On dit que \mathfrak{g} est *résoluble* s'il existe une suite décroissante $(\alpha_0, \alpha_1, \dots, \alpha_p)$ d'idéaux de \mathfrak{g} telle que, $\alpha_0 = \mathfrak{g}$, $\alpha_p = \{0\}$ et que, pour tout élément i de $[0, p-1]$, $[\alpha_i, \alpha_i] \subset \alpha_{i+1}$.

1. Montrer que, sous les hypothèses précédentes, alors, pour tout élément i de $[0, p]$, $\alpha_i \supset \mathcal{D}^i \mathfrak{g}$. En déduire que $\mathcal{D}^p \mathfrak{g} = \{0\}$.

En particulier, on obtient le résultat suivant :

Soit \mathfrak{g} une algèbre de Lie. Il est équivalent de dire :

a) *\mathfrak{g} est résoluble;*

b) *il existe un entier naturel p tel que $\mathcal{D}^p \mathfrak{g} = 0$.*

Toute algèbre de Lie nilpotente est donc résoluble. Plus généralement, prouver que si $\mathfrak{D}\mathfrak{g}$ est nilpotente, \mathfrak{g} est résoluble.

2. Soient E un espace vectoriel de dimension finie n sur K et $\mathcal{F} = (E_0, E_1, \dots, E_n)$ un drapeau de E . Prouver que $\mathfrak{t}_{\mathcal{F}}(E)$ est résoluble, mais non nilpotente.

3. Prouver le résultat suivant (théorème de Lie) :

Soient E un espace vectoriel non réduit à $\{0\}$ sur un corps de caractéristique 0 et \mathfrak{g} une sous-algèbre de Lie de dimension finie de $\mathfrak{gl}(E)$, constituée d'endomorphismes scindés sur K . Il existe alors un vecteur propre commun à tous les endomorphismes de \mathfrak{g} .

(Lorsque \mathfrak{g} est commutative, on retrouve la proposition 5.16.)

On pourra prouver successivement les résultats suivants :

a) Soient E un espace vectoriel non réduit à $\{0\}$ sur un corps K de caractéristique 0, \mathfrak{g} une sous-algèbre de Lie de $\mathfrak{gl}(E)$ constituée d'endomorphismes localement finis, \mathfrak{h} un idéal de \mathfrak{g} et \mathfrak{x} un vecteur propre commun à tous les éléments de \mathfrak{h} . Soit χ l'application de \mathfrak{h} dans K définie par la relation $U(\mathfrak{x}) = \chi(U)\mathfrak{x}$, pour tout élément U de \mathfrak{h} . Soient enfin V un élément de \mathfrak{g} , F le sous-espace vectoriel de E stable par V engendré par \mathfrak{x} , et p sa dimension. Prouver, par récurrence sur i , que, pour tout élément i de $[0, p]$ et pour tout élément U de \mathfrak{h} ,

$$(UV^i)(\mathfrak{x}) \equiv \chi(U)V^i(\mathfrak{x}) \quad (\text{mod. } E_i),$$

où

$$E_i = \bigoplus_{j=0}^{i-1} KV^j(\mathfrak{x}).$$

En déduire que $E_p = F$ est stable par U et que la trace de l'endomorphisme de F coïncidant avec U est égale à $p\chi(U)$. En conclure que $\chi([V, U]) = 0$.

b) On démontrera alors le théorème de Lie par récurrence sur $n = \dim \mathfrak{g}$. On prouvera que $\mathfrak{D}\mathfrak{g} \neq \mathfrak{g}$, et on en déduira qu'il existe un idéal \mathfrak{h} de \mathfrak{g} de codimension 1. En appliquant l'hypothèse de récurrence, on montrera qu'il existe un vecteur propre \mathfrak{x} de E commun à tous les éléments U de \mathfrak{h} , c'est-à-dire tel que $U(\mathfrak{x}) = \chi(U)\mathfrak{x}$. On prouvera grâce à a) que le sous-espace vectoriel G de E constitué des éléments y tels que $U(y) = \chi(U)y$ pour tout élément U de \mathfrak{h} est un sous-espace vectoriel stable par tous les éléments de \mathfrak{g} , et non réduit à $\{0\}$.

Soit enfin V un élément de \mathfrak{g} n'appartenant pas à \mathfrak{h} . Montrer qu'il existe un vecteur propre z de V appartenant à G , et prouver que z est un vecteur propre commun à tous les éléments de \mathfrak{g} .

4. A l'aide du théorème de Lie, prouver le résultat suivant, qui constitue une réciproque de la question 2 :

Soient E un espace vectoriel de dimension finie n sur un corps K de caractéristique 0 et \mathfrak{g} une sous-algèbre de Lie de $\mathfrak{gl}(E)$ résoluble et constituée d'endomorphismes scindés sur K . Il existe alors un drapeau \mathcal{F} de E tel que \mathfrak{g} soit contenu dans $\mathfrak{t}_{\mathcal{F}}(E)$.

(On pourra raisonner par récurrence sur n .)

En particulier, il existe une base B de E telle que, pour tout élément U de \mathfrak{g} , $M_B(U)$ soit triangulaire supérieure.

5. Soit \mathfrak{t} une algèbre de Lie résoluble de dimension finie n sur un corps algébriquement clos de caractéristique 0. Montrer qu'il existe un drapeau constitué d'idéaux de \mathfrak{t} . En déduire que $\mathfrak{D}\mathfrak{t} = \mathfrak{n}$ est une algèbre de Lie nilpotente (On prouvera que, pour tout élément x de \mathfrak{n} , $\text{Ad } x$ est un endomorphisme nilpotent de \mathfrak{t} , et on appliquera l'exercice 72.)

ÉQUATIONS AUX DIFFÉRENCES FINIES

74. *Équations aux différences finies.*

1. Soient β_0 et β_1 deux nombres complexes. Calculer en fonction de n le terme général de la suite (u_n) de nombres complexes définie par la condition initiale

$$u_0 = \beta_0, \quad u_1 = \beta_1$$

et telle que, pour tout entier $n \geq 2$,

$$u_n = u_{n-1} - u_{n-2}.$$

2. Étudier de même la suite (u_n) de nombres réels définie par la condition initiale

$$u_0 = \beta_0, \quad u_1 = \beta_1$$

et telle que, pour tout entier $n \geq 2$,

$$u_n = \frac{2}{\frac{1}{u_{n-1}} + \frac{1}{u_{n-2}}},$$

β_0 et β_1 étant deux nombres réels strictement positifs.

3. Étudier la suite (u_n) de nombres réels strictement positifs définie par $u_0 = 1$, $u_1 = 2$ et telle que, pour tout entier $n \geq 2$,

$$u_n = \sqrt{u_{n-1}u_{n-2}}.$$

4. Soient a_0, a_1, b_0 et b_1 quatre entiers naturels non nuls. Calculer en fonction de n le terme général de la suite (u_n) définie par

$$u_0 = \frac{a_0}{b_0}, \quad u_1 = \frac{a_1}{b_1}$$

et telle que, pour tout entier $n \geq 2$,

$$u_n = \frac{a_n}{b_n} = \frac{a_{n-1} + a_{n-2}}{b_{n-1} + b_{n-2}}.$$

75. *Systèmes d'équations aux différences finies.*

1. Soient β_1 et β_2 deux nombres complexes. Calculer en fonction de n les termes généraux des suites (u_n) et (v_n) de nombres complexes satisfaisant aux conditions initiales

$$u_0 = \beta_1, \quad v_0 = \beta_2$$

et telles que, pour tout entier naturel non nul n ,

$$\begin{aligned} u_n &= \alpha_1 u_{n-1} + \alpha_2 v_{n-1} \\ v_n &= \alpha_3 u_{n-1} + \alpha_4 v_{n-1}, \end{aligned}$$

où $\alpha_1, \alpha_2, \alpha_3$ et α_4 sont des nombres complexes.

Examiner le cas particulier où $\alpha_1 = \alpha_4$ et $\alpha_2 = -\alpha_3$.

2. Soient β_1 et β_2 deux nombres réels strictement positifs. Calculer en fonction de n les termes généraux des suites (u_n) et (v_n) de nombres réels strictement positifs telles que

$$u_0 = \beta_1, \quad v_0 = \beta_2$$

et que, pour tout entier naturel non nul n ,

$$u_n = u_{n-1} v_{n-1}$$

$$v_n = \frac{u_{n-1}^3}{v_{n-1}}.$$

3. Soient β_1 , β_2 et β_3 trois nombres complexes. Calculer en fonction de n les termes généraux des suites (u_n) , (v_n) et (w_n) de nombres complexes telles que

$$u_0 = \beta_1, \quad v_0 = \beta_2, \quad w_0 = \beta_3$$

et que, pour tout entier naturel non nul n ,

$$u_n = v_{n-1} + w_{n-1}$$

$$v_n = w_{n-1} + u_{n-1}$$

$$w_n = u_{n-1} + v_{n-1}.$$

BIBLIOGRAPHIE

- [1] A. A. ALBERT, *Fundamental concepts of higher algebra*, University of Chicago press.
 - [2] N. BOURBAKI, *Algèbre* (2 vol.), Hermann, Paris.
 - [3] L. CHAMBADAL et J. L. OVAERT, *Algèbre linéaire et algèbre tensorielle*, Dunod, Paris.
 - [4] V. N. FADDEEVA, *Computational methods of linear algebra*, Dover, New York.
 - [5] F. R. GANTMACHER, *Théorie des matrices* (2 vol.), Dunod, Paris.
 - [6] R. GODEMENT, *Cours d'algèbre*, Hermann, Paris.
 - [7] N. JACOBSON, *Lectures in abstract algebra* (3 vol.), van Nostrand, Princeton.
 - [8] S. LANG, *Algebra*, Addison-Wesley, Reading.
 - [9] S. Mac LANE et G. BIRKHOFF, *Algèbre* (2 vol.), Gauthier-Villars, Paris.
 - [10] B. L. van der WAERDEN, *Moderne Algebra* (2 vol.), Springer, Berlin et *Modern algebra* (2 vol.), Ungar, New York.
 - [11] R. S. VARGA, *Matrix iterative analysis*, Prentice-Hall, Englewood Cliffs.
 - [12] O. ZARISKI and P. SAMUEL, *Commutative algebra* (2 vol.), van Nostrand, Princeton.
-

INDEX TERMINOLOGIQUE

ADDITIVE (décomposition) d'un endomorphisme	430	de $C((X))$	88
AFFINITÉ	331	d'une extension complexe	437
(matrice d')	332	(matrice)	453
ALGÈBRE :		CARACTÈRE d'un groupe	185
des formes multilinéaires	296	CARACTÉRISTIQUE :	
des formes multilinéaires alternées ..	298	(déterminant)	353
des formes multilinéaires symétriques	319	(matrice)	353
des polynômes à une indéterminée à coefficients dans un corps	4	(polynôme) d'un endomorphisme ..	418
des polynômes à une indéterminée à coefficients dans un anneau	134	(polynôme) d'une matrice carrée ...	418
des polynômes construits sur un ensemble fini	147	CELLULE du groupe linéaire	381
des séries entières formelles 67,	207	CIRCULAIRE (permutation)	180
des séries entières formelles généralisées	75	CLOS (corps algébriquement)	58
ALGÈBRIQUES (prolongement des identités)	161	COEFFICIENT :	
ALTERNÉ(E) :		d'un polynôme	3
(application p -linéaire)	258	d'une série entière formelle	67
(forme multilinéaire)	298	COFACTEUR(s) :	
(forme p -linéaire)	263	d'un élément d'une matrice carrée ..	286
(groupe)	189	(matrice des)	286
ANNULATEUR d'un vecteur	453	COMPLÉMENTAIRE (matrice)	286
ANTISYMETRIQUE :		COMPLEXE (extension) :	
(application p -linéaire)	258	d'un espace vectoriel réel	434
(forme p -linéaire)	263	d'une application linéaire	436
(fraction rationnelle)	205	COMPOSÉ(E) :	
(polynôme)	192	de deux fractions rationnelles	18
ANTISYMETRISATION (opérateur d')	262	de deux polynômes	11
ANTISYMETRISÉE d'une application p -linéaire	262	de deux séries entières formelles ...	72
APPELL (polynôme d')	226	COMPOSITION (opérateur de)	222
BERNOULLI :		CONJUGUÉ(E) :	
(nombre de)	228	d'une application linéaire	437
(polynôme de)	228	d'une fraction rationnelle	63
BEZOUT (identité de)	23	d'une matrice	438
BORDANTE (matrice)	328	d'un polynôme	63
BRUHAT (décomposition de)	383	d'une série entière formelle	88
CANONIQUE (involution) :		d'un vecteur	437
de $C[X]$, de $C(X)$	63	CONVOLUTION :	
		(algèbre de) d'un monoïde	92
		(produit de)	92
		CORPS :	
		des fractions rationnelles à une indéterminée	8
		des fractions rationnelles à plusieurs indéterminées	154
		des séries entières formelles généralisées	76

CRAMER :		DIVISEUR (plus grand commun)	27
(formules de)	352	DIVISION suivant les puissances crois-	
(système de)	350	santes	52
CYCLE	178	DOMINANT (coefficient)	8
		DRAPEAU d'un espace vectoriel	382
D'ALEMBERT-GAUSS (théorème de) . . .	61		
DÉCOMPOSABLE (forme p -linéaire)	265	EISENSTEIN (règle d'irréductibilité d') ..	145
DÉCOMPOSITION :		ÉLÉMENTAIRE :	
d'une permutation en produit de		(application linéaire)	291
cycles	181	(fraction rationnelle)	48
en facteurs unitaires irréductibles		(opération)	333
d'un polynôme	25	(polynôme symétrique)	193
en facteurs unitaires irréductibles		(transposition)	185
d'une fraction rationnelle	33	ENGEL (théorème d')	502
DEGRÉ :		ENGENDRÉ (sous-espace vectoriel sta-	
d'une fraction rationnelle	9	ble) par un vecteur	452
d'un polynôme	5, 153	ENTIÈRE (partie) d'une fraction ration-	
DÉRIVATION :		nelle	35
canonique de l'algèbre des fractions		ÉQUIVALENTES (matrices)	329
rationnelles	45	EUCLIDIENNE (division)	20
canonique de l'algèbre des polynômes		EULER :	
.	40	(identité d')	170
canonique de l'algèbre des séries		(indicateur d')	130
entières formelles	77	EULÉRIEN (développement)	110
intérieure d'une algèbre de Lie	500	EXTÉRIEUR (produit) :	
d'une algèbre	41	de formes linéaires	264
DÉRIVÉE :		de deux formes multilinéaires alter-	
d'une fraction rationnelle	45	nées	297
d'un polynôme	40	EXTRAITE (matrice)	327
d'une série entière formelle	77		
DÉTERMINANT :		FACTORIALITÉ (permanence de la) :	
de n vecteurs dans une base	274	pour les polynômes	142, 154
d'un endomorphisme	277	pour les séries entières formelles	256
d'une matrice carrée	279	FACTORIEL (anneau)	138
DÉVELOPPEMENT :		FINI :	
de Laplace d'un déterminant	307	(endomorphisme localement)	395
d'un déterminant suivant une co-		(valeur propre d'indice)	397
lonne, ou une ligne	285	FONCTIONNEL (calcul)	415, 497
DIAGONALISABLE :		FONDAMENTAL :	
(composante) d'un endomorphisme .	430	(invariant) d'une matrice	384
(endomorphisme)	404	(polynôme symétrique)	202
(matrice)	446	(théorème) de l'algèbre	61
DIFFÉRENCES FINIES :		(théorème) de l'algèbre linéaire	389
(équation aux)	463	FONTENÉ-ROUCHÉ (théorème de)	351
(opérateur aux)	222	FORMELLE :	
(système d'équations aux)	466	(exponentielle)	82
DIFFÉRENTIEL(LE) :		(exponentielle) d'un endomorphisme .	473
(équation)	470	(logarithme)	83
(forme)	119	(série) du binôme	85
(opérateur)	171	(série entière) à une indéterminée . . .	82
(système d'équations)	472	(série entière) à plusieurs indétermi-	
d'une fraction rationnelle	174	nées	207
d'un polynôme	166, 245	(série entière) à coefficients vecto-	
DIRICHLET (série formelle de)	125	riels	242
DISTINGUE (polynôme)	254		

- GAUSS :
 (décomposition de) d'une matrice carrée 381
 (propriété de) pour un anneau 23
 GÉNÉRALISÉE (série entière formelle) ... 75
 GÉNÉRATEUR d'un idéal 22
 GRAPHE 373
- HADAMARD-FROBENIUS (théorème d') . 375
 HAMILTON-CAYLEY (théorème de) 422
 HANKEL (déterminant de) 121
 HILBERT :
 (polynôme de) 344
 (théorème de permanence de) pour les polynômes 137, 155
 (théorème de permanence de) pour les séries entières formelles 252
 HILBERT-DIRAC (théorème de) 398
 HOMOGÈNE :
 (composante) d'un polynôme 152
 (composante) d'une série entière formelle 211
 (équation linéaire) 334
 (fraction rationnelle) 154
 (polynôme) 152
 (système linéaire) 336
 HYPERBOLIQUE (série entière formelle) . 88
- IMPAIR(E) :
 (polynôme) 12
 (série entière formelle) 74
 INDÉCOMPOSABLE (sous-espace vectoriel) 461
 INDÉTERMINATION (point d') 164
 INDÉTERMINÉE 3, 147
 INDICE d'une valeur propre 397
 INTÉGRITÉ (permanence de l') ... 135, 150
 INVARIANT(S) :
 (facteur) d'une matrice 384
 (système des) d'une permutation ... 183
 INVERSION d'une permutation 187
 IRRÉDUCTIBLE :
 (polynôme) 24
 (sous-espace vectoriel) 454
 ISOBARE (polynôme) 195
- JORDAN :
 (base de) 462
 (endomorphisme de) 457
 (matrice de) 457
 (réduction de) 462
- LAGRANGE :
 (décomposition de) d'un polynôme . 105
 (polynôme d'interpolation de) 340
- LAGRANGE-SYLVESTER (polynôme d'interpolation de) 341
 LAPLACE (développement de) d'un déterminant 307
 LEIBNIZ (formule de) 42
 LIE :
 (algèbre de) 500
 (théorème de) 503
 LIMITÉ (développement) d'une fraction rationnelle 50, 241
 (équation) 334
 (équation aux différences finies) ... 463
 (équation différentielle) 470
 (groupe spécial) 279
 (groupe spécial) de type n 281
 (système) 336
 LOGARITHMIQUE (dérivée) :
 d'une fraction rationnelle 47
 d'une série entière formelle généralisée 81
 LONGUEUR d'un cycle 179
- MACLAURIN (formule de) :
 pour les polynômes 55, 172
 pour les séries entières formelles 80, 218
 MINEUR(E) :
 (déterminant) 284
 (matrice) 284
 MINIMAL (polynôme) d'un endomorphisme 393
 MÖBIUS (fonction de) 129
 MONOGÈNE (sous-espace vectoriel) 453
 MONOME 3
 MULTILINÉAIRE (forme) 296
 MULTIPLE :
 (plus petit commun) 28
 (pôle) 19
 (racine) 13
 (zéro) 19
 MULTIPLICATIVE :
 (décomposition) d'un automorphisme 431
 (fonction arithmétique) 128
 MULTIPLICITÉ d'une valeur propre ... 419
- NEWTON (polynôme de) 199
 NILPOTENT(E) :
 (algèbre de Lie) 501
 (composante) d'un endomorphisme. 430
 (endomorphisme localement) 395
 NORMALISATION (théorème de) 255
 NOYAUX (théorème de décomposition). 391
- OPÉRATION d'un groupe sur un ensemble 177

- ORBITE** 177
ORDRE de multiplicité d'une racine 13

P-ADIQUE (fraction rationnelle) 37
PAIR(E) :
 (polynôme) 12
 (série entière formelle) 74
PARTIEL(LE) :
 (degré) 154
 (dérivée) 168, 176
PARTITIONS (formule des) 93
P. G. C. D. 27
p-LINÉAIRE :
 (application) 258
 (forme) 263
POIDS :
 d'un polynôme 196
 pour un groupe 186
POLE d'une fraction rationnelle ... 19, 164
POLYNÔME :
 à une indéterminée à coefficients dans
 un corps 3
 à une indéterminée à coefficients dans
 un anneau 134
 à plusieurs indéterminées 147
 à coefficients vectoriels 242
POLYNOMIALE :
 (application) 156, 244
 (fonction) 10, 156
P. P. C. M. 28
PREMIERS entre eux dans leur ensemble
 (polynômes) 23
PRIMITIF (polynôme) 142
PRIMITIVE :
 d'une fraction rationnelle 47
 d'un polynôme 44
 d'une série entière formelle généra-
 lisée 81
PRINCIPAL(E) :
 (équation) 353
 (inconnue) 353
 (matrice) 328
 (mineur) 381
 (partie) à l'infini 35
 (partie) relative à un polynôme uni-
 taire irréductible 37
PROPRE :
 (sous-espace) 397
 (valeur) 396
 (vecteur) 397

QUOTIENT :
 d'une division euclidienne 21
 d'une division suivant les puissances
 croissantes 52

RACINE d'un polynôme 12
RAMANUJAN (somme de) 130
RANG :
 d'une matrice 326
 d'un système linéaire 348
RATIONNELLE :
 (application) 162
 (fonction) 17, 161
 (fraction) 8
RÉCIPROQUE (série entière formelle) ... 81
REDONDANTE (équation) 351
REDUITE :
 (forme) d'une fraction rationnelle .. 32
 (forme) d'un élément du corps des
 quotients d'un anneau factoriel .. 141
 (matrice triangulaire supérieure) 447
RÉEL :
 (endomorphisme) 438
 (sous-espace vectoriel) 437
 (vecteur) 437
RÉSIDU :
 d'une forme différentielle rationnelle. 120
 d'une fraction rationnelle 49
RÉSOLUBLE (algèbre de Lie) 502
RESTE :
 d'une division euclidienne 21
 d'une division suivant les puissances
 croissantes 52
RIEMANN (fonction ζ de) 129

SCHWARZ (théorème de) :
 pour les polynômes 171
 pour les séries entières formelles ... 217
SCINDÉ(E) :
 (endomorphisme) 401
 (matrice) 446
 (polynôme) 16
SEMBLABLES (matrices) 445
SEMI-SIMPLE :
 (composante) d'un endomorphisme. 430
 (endomorphisme) 408
SIGNATURE d'une permutation 186
SIMPLE :
 (élément) 59
 (pôle) 19
 (racine) 13
 (zéro) 19
SIMULTANÉE :
 (diagonalisation) 427
 (réduction) 429
 (trigonalisation) 428
SOMMABLE (famille) de séries entières
 formelles 69, 210
SPECTRAL (sous-espace) 397
SPECTRE d'un endomorphisme 396
STOCHASTIQUE (matrice) 490

SUBSTITUABLE (élément) :			U-GÉNÉRATEUR (vecteur)	453
dans une fraction rationnelle ..	16,	161	U-MONOGENE (sous-espace vectoriel) ..	453
dans une série entière formelle		21	UNIMODULAIRE :	
SUPPORT :			(automorphisme)	279
d'un cycle		178	(groupe)	279
d'une suite		3	UNIPOTENTE (composante) d'un auto-	
SYMÉTRIQUE :			morphisme	431
application p -linéaire)		258	UNITAIRE (polynôme)	8
(forme multilinéaire)		319	UNIVERSELLE (propriété) :	
(forme p -linéaire)		263	de l'algèbre des polynômes à une	
(fraction rationnelle)		205	indéterminée	4
(polynôme)		192	de l'algèbre des polynômes à plu-	
(produit) de formes linéaires		264	sieurs indéterminées	148
(produit) de deux formes multilinéai-			de l'algèbre $\mathcal{A}(E)$	320
res symétriques		319	de l'algèbre $\mathcal{M}(E)$	319
SYMÉTRISATION (opérateur de)		262	de l'algèbre $\mathcal{P}(E)$	320
SYMÉTRISÉE d'une application p -linéaire.		262	de l'espace vectoriel $\mathcal{A}_p(E)$	312
			de l'espace vectoriel $\mathcal{M}_p(E)$	311
TAYLOR (formule de) :			de l'espace vectoriel $\mathcal{P}_p(E)$	312
pour les fractions rationnelles .	55,	242	d'une extension complexe	435
pour les polynômes	54, 173,	246	VALUATION :	
pour les séries entières formelles	218,	246	d'une fraction rationnelle en un	
TAYLORIEN (développement) :			point	18, 240
d'une fraction rationnelle		242	d'une fraction rationnelle relative à	
d'un polynôme		165	un polynôme unitaire irréductible .	33
d'une série entière formelle		216	d'un polynôme	5
TENSORIEL (produit) :			d'un polynôme en un point	13
de formes linéaires		264	d'un polynôme relative à un poly-	
de deux formes multilinéaires		295	nôme unitaire irréductible	25
TRACE :			d'une série entière formelle	67, 208
d'un endomorphisme		292	VANDERMONDE :	
d'une matrice carrée		293	(déterminant de)	288
TRANSLATION (opérateur de)		222	(déterminant de) généralisé	289
TRANSPOSITION		178	(fonction de)	187
TRANSVECTION		331	(système linéaire de)	352
(matrice de)		332	VECTORIEL (système linéaire)	356
TRIANGULAIRE (système linéaire)		358		
TRIGONALISABLE :			WARING (formules de)	201
(endomorphisme)		421	WEIERSTRASS (théorème préparatoire	
(matrice)		446	de)	253
TRIGONOMÉTRIQUE (série entière for-				
melle)		90	ZÉRO d'une fraction rationnelle ...	19, 164
TRONCATURE d'une série entière for-				
melle	68,	208		

Cet ouvrage couvre les programmes de mathématiques des classes préparatoires aux grandes écoles et ceux du premier cycle MP des universités.

Néanmoins, l'exposé ne se limite pas strictement à ces programmes. En effet, les auteurs ont tenu à donner une vue d'ensemble sur les sujets traités, sans pour autant négliger les résultats classiques. Ils ont ainsi voulu préparer les études ultérieures et favoriser la formation permanente, compte tenu du renouvellement constant de l'enseignement des sciences mathématiques.

Le texte comprend de nombreux exemples et contre-exemples ; il est accompagné d'exercices très variés, allant des applications pratiques du cours à des compléments théoriques.

Le mode d'exposition adopté a été mis au point après une expérimentation pédagogique portant sur plusieurs années.

L. CHAMBADAL, né à Paris en 1935, ancien élève de l'Ecole Normale Supérieure est professeur dans les classes préparatoires aux grandes écoles scientifiques ; il est auteur de nombreux manuels d'enseignement.

J.-L. OVAERT, né à Roubaix en 1934, ancien élève de l'Ecole Normale Supérieure est chargé d'enseignement à la faculté des sciences de Nancy et professeur à l'école des mines de Nancy.