

MATHÉMATIQUES à l'Université

Cours et exercices corrigés

Collection dirigée par
Charles-Michel Marle
Philippe Pilibossian

Éléments de théorie des anneaux

Anneaux commutatifs

 *niveau L3*

Josette Calais





MATHÉMATIQUES À L'UNIVERSITÉ

Collection dirigée par Charles-Michel MARLE et Philippe PILIBOSSIAN

niveau L3

ÉLÉMENTS DE THÉORIE DES ANNEAUX

Anneaux commutatifs



Josette CALAIS

Professeur émérite à l'Université de Reims-Champagne-Ardenne



- * *L'algèbre discrète de la transformée de Fourier*, G. Peyré, 2004.
- * *Algèbre et théorie des nombres – cryptographie, primalité*, S. Al Fakir, 2003.
- * *Algèbre et théorie des nombres – théorie de Galois, codes, géométrie et arithmétique*, S. Al Fakir, 2004.
- * *Algèbre fondamentale – Arithmétique*, G. Gras et M.-N. Gras, 2004.
- * *Algèbre linéaire*, R. Goblot, 2005.
- * *Algèbre linéaire*, F. Bories-Longuet, 2000.
- * *Algèbre linéaire numérique – cours et exercices*, G. Allaire et S. M. Kaber, 2002.
- * *Analyse complexe et distributions*, A. Yger, 2001.
- * *Analyse fonctionnelle – exercices et problèmes corrigés*, B. Maury, 2004.
- * *Calcul différentiel*, G. Christol, A. Cot et Ch.-M. Marle, 1997.
- * *Cours d'algèbre*, R. Elkik, 2002.
- * *Cours de calcul formel – algorithmes fondamentaux*, Ph. Saux Picart, 1999.
- * *Cours de calcul formel – corps finis, systèmes polynomiaux, applications*, Ph. Saux Picart et E. Rannou, 2002.
- * *Distributions – espaces de Sobolev, applications*, M.-Th. Lacroix-Sonrier, 1999.
- * *Éléments d'algèbre commutative*, J. Briançon et Ph. Maisonobe, 2004.
- * *Éléments d'analyse convexe et variationnelle*, D. Azé, 1997.
- * *Éléments de géométrie*, A. Yger et A. Hénaut, 2004.
- * *Éléments de théorie des anneaux – anneaux commutatifs*, J. Calais, 2006.
- * *Éléments d'intégration et d'analyse fonctionnelle*, A. El Kacimi Alaoui, 1999.
- * *Équations aux dérivées partielles et leurs approximations*, B. Lucquin, 2004.
- * *Extensions de corps – théorie de Galois*, J. Calais, 2006.
- * *Géométrie différentielle avec 80 figures*, C. Doss-Bachelet, J.-P. Françoise et Cl. Piquet, 2000.
- * *Les Groupes finis et leurs représentations*, G. Rauch, 2000.
- * *Initiation à la topologie générale*, D. Lehmann, 2004.
- * *Intégrales curvilignes et de surface*, M. Lofficiel et D. Tanré, 2006.
- * *Intégration et théorie de la mesure – une approche géométrique*, P. Krée, 1997.
- * *Une introduction à la géométrie projective*, D. Lehmann, 2003.
- * *Introduction à Scilab – exercices pratiques corrigés d'algèbre linéaire*, G. Allaire et S. M. Kaber, 2002.
- * *Logique, ensemble, catégories – le point de vue constructif*, P. Ageron, 2000.
- * *Méthodes d'approximation, équations différentielles, applications Scilab*, S. Guerre-Delabrière et M. Postel, 2004.
- * *Méthodes numériques directes de l'algèbre matricielle*, Cl. Brezinski et M. Redivo-Zaglia, 2005.
- * *Méthodes numériques itératives – algèbre linéaire et non linéaire*, Cl. Brezinski et M. Redivo-Zaglia, 2006.
- * *Précis d'analyse réelle – topologie, calcul différentiel, méthodes d'approximation, vol. 1*, V. Komornik, 2001.
- * *Précis d'analyse réelle – analyse fonctionnelle, intégrale de Lebesgue, espaces fonctionnels, vol. 2*, V. Komornik, 2002.
- * *Probabilités*, M. Brancovan et Th. Jeulin, 2006.
- * *Quelques aspects des mathématiques actuelles*, ouvrage collectif, 1999.
- * *Systèmes dynamiques – une introduction*, Ch.-M. Marle, 2003.
- * *Théorie de Galois*, I. Gozard, 1997.
- * *Topologie*, G. Christol, A. Cot et Ch.-M. Marle, 1997.
- * *La Topologie des espaces métriques*, E. Burroni, 2005.

ISBN 2-7298-2779-X

© Ellipses Édition Marketing S.A., 2006
32, rue Bague 75740 Paris cedex 15



Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L.122-5.2° et 3°a), 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 » (Art. L.122-4). Cette représentation ou reproduction, par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

Présentation de la collection

“Mathématiques à l'Université”

Depuis 1997, cette collection se propose de mettre à la disposition des étudiants de troisième, quatrième et cinquième années d'études supérieures en mathématiques des ouvrages couvrant l'essentiel des programmes actuels des universités françaises. Certains de ces ouvrages pourront être utiles aussi aux étudiants qui préparent le CAPES ou l'Agrégation, ainsi qu'aux élèves des grandes écoles et aux ingénieurs désirant actualiser leurs connaissances.

Nous avons voulu rendre ces livres accessibles à tous : les sujets traités sont présentés de manière simple et progressive, tout en respectant scrupuleusement la rigueur mathématique. Chaque volume comporte, en général, un exposé du cours avec des démonstrations détaillées de tous les résultats essentiels, des énoncés d'exercices ou de problèmes.

Nous sommes heureux d'accueillir dans notre collection l'ouvrage de Madame Josette Calais, Professeur. Il avait été déjà publié en 2002 aux Presses Universitaires de France ; mais cette édition est aujourd'hui introuvable. Aussi avons-nous décidé de le rééditer dans notre collection. Il peut servir d'introduction au nouvel ouvrage sur les extensions de corps et la théorie de Galois, que Madame Calais publie aussi dans cette collection.

L'anneau $\mathbb{Z}$ des entiers rationnels est utilisé par les enfants dès leurs années de collège. C'est dire à quel point la structure d'anneau est fondamentale en mathématiques. Madame Josette Calais en fait dans ce livre une étude approfondie. Après avoir introduit les concepts de base (notion d'idéal, factorisation) et en avoir déduit certaines propriétés fondamentales, elle étudie les importantes constructions utilisant la structure d'anneau : localisation, modules et algèbres sur un anneau, algèbres des polynômes à une ou plusieurs indéterminées et algèbre des séries formelles. Le second volume, qui traite des extensions de corps et de la théorie de Galois, utilisera ces résultats, en particulier les propriétés des polynômes symétriques présentées dans le dernier chapitre. De nombreux exercices permettront au lecteur de mieux se familiariser avec toutes les notions introduites.



Préface

La notion d'anneau fait partie des concepts fondamentaux de l'Algèbre et elle intervient de façon naturelle, en Théorie Algébrique des Nombres et plus encore, en Géométrie Algébrique.

L'appellation *anneau* (*ring*, en langue anglo-saxonne) est probablement due au mathématicien allemand David HILBERT (1862-1943).

Un anneau est un ensemble muni de deux lois de composition internes, dont l'une lui confère une structure de groupe (additif) abélien. Les règles de calcul dans les anneaux dépendent donc, en partie, des propriétés axiomatiques des groupes abéliens ([11]).

Ce livre s'intéresse, principalement, aux anneaux unitaires et *commutatifs*. Cependant, certains exemples d'anneaux *non commutatifs* s'imposent, tels les anneaux de matrices carrées ; d'ailleurs, l'évocation du cas des anneaux non commutatifs permet, parfois, de mettre en évidence l'importance du rôle joué par la commutativité, lorsqu'elle est présente (Cf. Ch. 3).

Un cas particulier très important d'anneau est celui de *corps*. Les corps de nombres classiquement connus, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sont couramment utilisés dans l'ensemble des disciplines scientifiques ; de plus, la structure algébrique de corps, qui est, en particulier à la base de la notion d'espace vectoriel, intervient, à des degrés divers, dans pratiquement tous les domaines des mathématiques.

Une étude plus approfondie des corps et des Extensions de corps, conduisant à la Théorie de Galois, sera faite dans un prochain volume. Mais déjà, dans ce livre, plusieurs propriétés des domaines d'intégrité (Ch. 5) et des polynômes (Ch. 4 et 8) sont préliminaires à l'introduction des Extensions de corps.



Introduction

Ce volume comprend huit chapitres et deux appendices (A et B).

Le premier anneau rencontré par un étudiant scientifique (en 1^{er} cycle ou même plus tôt) est celui des entiers, noté $\mathbb{Z}$; ses propriétés arithmétiques sont rappelées dans l'Appendice A, qu'il est conseillé de lire, avant même d'aborder le chapitre 1, car l'anneau $\mathbb{Z}$ servira de référence, pratiquement tout au long de ce livre.

Les chapitres 1, 2, 5 contiennent les propriétés fondamentales des anneaux unitaires et commutatifs, essentiellement issues du concept d'*idéal* (Ch. 1 et 2) et du principe de *factorisation* (Ch. 5). Ces propriétés conduisent à définir, en particulier, les anneaux dits principaux, noethériens, euclidiens, factoriels (Ch. 2 et 5).

Les notions de *module* et d'*algèbre*, directement liées à celle d'anneau, sont définies au chapitre 3, en vue de la construction des algèbres de polynômes (Ch. 4) et de séries formelles (Ch. 7).

Le chapitre 6 fait naturellement suite au chapitre 5, car la *localisation* des anneaux unitaires, commutatifs généralise la construction du corps des fractions d'un domaine d'intégrité (Ch. 5).

Dans le chapitre 8, nous revenons sur les polynômes à plusieurs indéterminées pour étudier les propriétés des polynômes *symétriques* et certaines de leurs applications (Résultant, Transformations d'équations polynomiales).

Plusieurs résultats de ce dernier chapitre seront exploités dans un prochain livre concernant les Extensions de corps.

L'introduction du Produit Tensoriel de modules et d'algèbres motive l'Appendice B et représente une ouverture en direction de domaines plus élaborés de l'Algèbre, où le Produit Tensoriel est souvent primordial (tel, par exemple, l'Algèbre Homologique).

D'autre part, le Produit Tensoriel est préliminaire au Calcul Tensoriel abondamment employé en Géométrie Différentielle, ainsi qu'en Mécanique classique ou relativiste.

Dans ce livre, le Produit Tensoriel est utilisé dans les chapitres 3 et 6.

Tout au cours de ce volume, pour chaque construction d'un nouvel anneau (resp. module ou algèbre) faite à partir d'un ou plusieurs anneaux (resp. modules ou algèbres) donnés, l'utilisation systématique de la *Propriété Universelle* garantit l'unicité, à un isomorphisme près, du nouvel objet construit, ce qui, mathématiquement, est très important.

Par ailleurs, la considération d'anneaux (tels que les anneaux de polynômes, de séries formelles ou les localisés d'anneaux) construits à partir d'un anneau possédant des propriétés algébriques intéressantes, amène à se poser la question du *transfert* de ces propriétés au nouvel anneau. Ce type de problème sera régulièrement examiné dans les chapitres 2, 5, 6 et 7.



Table des matières

Notations	xv
1 Structure d'anneau	1
1. Notions Fondamentales	1
A. Anneau	1
B. Règles de calculs dans les anneaux	1
C. Eléments inversibles dans un anneau unitaire - Corps	3
D. Premiers exemples d'anneaux et de corps	4
E. Diviseurs de zéro - Anneaux intègres	7
2. Sous-anneaux	8
A. Notion de sous-anneau - Propriétés élémentaires	8
B. Sous-anneau engendré par une partie non vide d'un anneau	9
3. Notions d'idéal à gauche, à droite, bilatère	10
4. Morphismes d'anneaux	11
A. Définitions	11
B. Propriétés des morphismes d'anneaux	11
C. Caractéristique d'un anneau unitaire	13
5. Produit direct d'anneaux	15
A. Produit direct de deux anneaux	15
B. Produit direct d'une famille quelconque d'anneaux	16
C. Propriété universelle du produit direct d'anneaux	17
6. Exercices	17
2 Idéaux d'un anneau	23
1. Idéal engendré par une partie d'un anneau	23
2. Opérations sur les idéaux d'un anneau	24
A. Intersection, réunion d'idéaux	24
B. Somme d'idéaux dans un anneau unitaire	24
C. Produit d'idéaux dans un anneau unitaire	26
D. Propriétés des opérations sur les idéaux	27
3. Anneaux Quotients	28
A. Notion d'anneau quotient	28
B. Propriétés des anneaux quotients	30
C. Idéaux bilatères copremiers (ou étrangers)	33
4. Idéaux premiers - Idéaux maximaux	35
A. Idéaux premiers d'un anneau unitaire et commutatif	36
B. Idéaux maximaux d'un anneau unitaire	38
5. Notion d'anneau local	40
6. Notion d'anneau commutatif noethérien	40
A. Condition maximale - Condition de chaîne ascendante	40
B. Anneau commutatif noethérien	41
7. Nilradical et Radical de Jacobson	43
8. Anneaux booléens	45
9. Exercices	47

3 Modules et Algèbres	53
1. Notion de A -module	53
2. Sous-modules	54
A. Notion de sous-module	54
B. Sous-module engendré par une partie d'un A -module	55
C. Somme de sous-modules	56
3. Morphismes de A -modules	57
4. Modules quotients	59
5. Produit direct et somme directe de A -modules	60
A. Produit direct de A -modules	60
B. Somme directe de A -modules	62
6. Notion de A -module libre	64
7. Suites exactes de A -modules	67
8. A -modules noethériens	69
9. Notion de A -algèbre	70
10. Algèbre des quaternions réels	71
A. La $\mathbb{R}$ -algèbre $\mathbb{H}$	71
B. Calculs dans $\mathbb{H}$	72
11. Exercices	74
4 Algèbres de Polynômes	79
1. Polynômes à une indéterminée sur A	79
A. Construction de l'algèbre des polynômes à une indéterminée sur A	79
B. Propriété universelle de l'anneau $A[X]$	81
C. Propriétés des degrés des polynômes de $A[X]$	82
D. Composition des polynômes	83
E. Fonction polynôme	84
F. Polynômes dérivés	86
2. Polynômes à une indéterminée sur un corps K	87
A. Division euclidienne dans $K[X]$	87
B. Racines d'un polynôme de $K[X]$	89
C. Division suivant les puissances croissantes	92
3. Polynômes à n indéterminées sur A , $n > 1$	93
A. Construction de l'algèbre des polynômes à n indéterminées	93
B. Propriété universelle de l'anneau $A[X_1, \dots, X_n]$, $n > 1$	95
C. Degrés des polynômes de $A[X_1, \dots, X_n]$, $n > 1$	96
D. Fonction polynôme à n indéterminées	97
E. Polynômes sur un anneau noethérien A	98
4. Exercices	99
5 Factorisation dans les domaines d'intégrité	103
1. Corps des fractions d'un domaine d'intégrité	103
A. Construction du corps des fractions d'un D.I.	103
B. Propriétés du corps des fractions d'un D.I.	105
2. Eléments remarquables dans un D.I.	107
A. Diviseurs et unités dans un anneau unitaire, commutatif	107
B. Eléments associés dans un D.I.	107
C. Eléments irréductibles dans un D.I.	109
D. Eléments premiers dans un D.I.	110

3.	Notion de p.g.c.d. dans un D.I.	112
A.	p.g.c.d. de n éléments non nuls dans A , $n \geq 2$	112
B.	Eléments premiers entre eux dans un D.I.	115
C.	Eléments premiers entre eux dans un D.P.	118
4.	Notion de p.p.c.m. dans un D.I.	118
5.	Anneaux euclidiens	123
A.	Notion d'anneau euclidien	123
B.	p.g.c.d. et p.p.c.m. dans un anneau euclidien	127
6.	Anneaux factoriels	129
A.	Notion d'anneau factoriel	129
B.	p.g.c.d. et p.p.c.m. dans un anneau factoriel	132
C.	Anneaux de polynômes sur un anneau factoriel	133
7.	Exercices	138
6	Localisation	147
1.	Localisation par une partie multiplicative de A	147
A.	Notion de partie multiplicative	147
B.	Localisé de A par une partie multiplicative	147
2.	Idéaux de $S^{-1}A$	151
3.	Localisés d'un domaine d'intégrité	155
4.	Localisé d'un A -module	158
A.	Localisé d'un A -module par S	158
B.	Localisé d'un morphisme de A -modules	158
C.	Propriétés des modules localisés	160
5.	Exercices	162
7	Séries Formelles	165
1.	Séries formelles à une indéterminée sur A	165
A.	Algèbre des séries formelles à une indéterminée sur A	165
B.	Notion d'ordre d'une série formelle	166
C.	Notion de famille sommable dans $A[[X]]$	168
D.	Substitution d'une série formelle dans une autre	169
E.	Notion de série formelle dérivée dans $A[[X]]$	170
2.	Eléments inversibles dans l'anneau $A[[X]]$	171
3.	Propriétés de l'anneau $A[[X]]$	172
4.	Séries formelles et fractions rationnelles	176
5.	Structure d'espace métrique de $A[[X]]$	180
A.	Norme et distance dans $A[[X]]$	180
B.	Etude de l'espace métrique $A[[X]]$	181
6.	Séries formelles à n indéterminées sur A , $n > 1$	182
A.	A -algèbre des séries formelles à n indéterminées	182
B.	Propriétés de l'anneau $A[[X_1, \dots, X_n]]$	182
7.	Exercices	183
8	Polynômes symétriques	187
1.	Ordre lexicographique dans $A[X_1, \dots, X_n]$, $n > 1$	187
2.	Polynômes symétriques dans $A[X_1, \dots, X_n]$, $n > 1$	188
A.	Notion de polynôme symétrique	188
B.	Théorème fondamental	190

C.	Recherche pratique du polynôme ϕ connaissant f	192
3.	Formules de Newton	194
4.	Fractions rationnelles symétriques	197
A.	Notion de fraction rationnelle symétrique	197
B.	Applications des fractions rationnelles symétriques	199
5.	Résultant - Discriminant	201
A.	Introduction	201
B.	Résultant de deux polynômes	201
C.	Calcul de $R(f, g)$ en fonction des racines de f et de g	203
D.	Discriminant d'un polynôme	205
6.	Applications	207
A.	Problème général d'élimination	207
B.	Transformation des équations polynômiales	208
7.	Exercices	211
A	Propriétés arithmétiques de $\mathbb{Z}$	219
1.	Rappels	219
2.	Divisibilité dans $\mathbb{Z}$. Notion de nombre premier	219
3.	Division et congruences dans $\mathbb{Z}$	221
A.	Division dans $\mathbb{Z}$	221
B.	Congruences dans $\mathbb{Z}$	221
4.	Factorisation unique dans $\mathbb{Z}$	222
A.	Théorème Fondamental de l'Arithmétique	222
B.	Théorème de Factorisation Unique dans $\mathbb{Z}$	223
C.	Conséquences du Théorème de Factorisation Unique	223
5.	p.g.c.d. et p.p.c.m. dans $\mathbb{Z}$. Théorème de Bezout	224
A.	Notion de p.g.c.d. et p.p.c.m. dans $\mathbb{Z}$	224
B.	Éléments premiers entre eux dans $\mathbb{Z}$. Théorème de Bezout	227
C.	Généralisation	230
B	Produit tensoriel	231
1.	Produit tensoriel de deux A -modules	231
A.	Applications bilinéaires	231
B.	Construction du produit tensoriel de deux A -modules	232
C.	Propriétés du produit tensoriel	235
2.	Produit tensoriel de morphismes de A -modules	238
3.	Produit tensoriel et suites exactes	240
4.	Restriction et extension des scalaires	242
A.	Restriction des scalaires	242
B.	Extension des scalaires	243
5.	Produit tensoriel de A -algèbres	243
	Bibliographie	247
	Index	249

Notations

$\doteq$ signifie : égal, par définition
 X et Y étant deux ensembles,
 $X \setminus Y = \{x \in X; x \notin Y\}$
 $X \times Y = \{(x, y); x \in X, y \in Y\}$
 $\text{card}(X)$ ou $|X|$: cardinal de X
 $\mathbb{N}$ (resp. $\mathbb{N}^*$), 1
 $\mathbb{Z}$ (resp. $\mathbb{Z}^*$), 1
 C_n^k , 2
 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, 4
 $\mathbb{Z}/n\mathbb{Z}$, 7
 $\mathcal{L}_K(E)$, 5
 $M_n(K)$, 5
 $\mathbb{Z}[i]$, 8
 A désignant un anneau,
 U_A , 3
 $Z(A)$, 8
 $\text{car } A$, 14
 S étant une partie de A ,
 $\langle S \rangle$, 9
 $\text{Ann}_S(S)$, $\text{Ann}_d(S)$, 10
 $(S)_g$, $(S)_d$, 23
 Si A et B sont des anneaux,
 $\text{Hom}(A, B)$, 11
 $\text{Im } f$, $\text{Ker } f$, 11
 $\text{End}(A)$, 11
 $\text{Aut}(A)$, 13
 $A_1 \times A_2$, 15
 $\prod_{i \in I} A_i$, 16
 $\sum_{1 \leq i \leq n} I_i$, 24
 $\sum_{\lambda \in \Lambda} I_\lambda$, $\bigoplus_{\lambda \in \Lambda} I_\lambda$, 26
 $\prod_{1 \leq i \leq n} I_i$, 27
 I étant un idéal de A ,
 I^n , 28
 A/I , 29
 $x \equiv y \pmod{I}$, 30
 $\sqrt{I}$, 50
 $\text{Spec}(A)$, 38
 $\mathcal{N}(A)$, $\mathcal{J}(A)$, 43, 44
 Mod_A , ${}_A\text{Mod}$, ${}_A\text{Mod}_B$, 53
 Pour S , partie d'un A -module,
 $\text{Ann}(S)$, 54

$A(S)$, $(S)_A$, 55
 $\sum_{i \in I} N_i$, 56
 $\bigoplus_{i \in I} N_i$, 57
 $\text{End}_A(M)$, 57
 $\text{Hom}_A(M, M')$, 57
 M/N , 59
 $\prod_{i \in I} M_i$, 60
 $\bigoplus_{i \in I} M_i$, 62
 M^I , $M^{(I)}$, M^n , 64
 A^X , A^n , 65
 $F(X)$, 65
 $\mathbb{H}$, 71
 $\text{Tr}(q)$, $N(q)$, 73
 $A[X]$, 80
 Pour $f \in A[X]$,
 $\text{Supp}(f)$, $\deg f$, 80
 $\tilde{f}$, 84
 f' , 86
 $f^{(k)}$, 87
 $A[X_1, X_2, \dots, X_n]$, 94
 D.L. , 103
 $\frac{a}{s}$, 103
 $\text{Fr } A$, 104
 $b|a$, (resp. $b \nmid a$), 107
 $a \sim b$, 107
 D.P. , 111
 $a \wedge b$, 113
 $a \vee b$, 119
 $S^{-1}A$, 148
 A_p , 149
 $\mathbb{D}$, 149
 I_S , 151
 $A[[X]]$, 166
 $\omega(f)$, 166
 $K(X)_0$, 177
 $A((X))$, 184
 $\text{MD}(f)$, 187
 $R(f, g)$, 202
 $\Delta(f)$, 205
 $v_p(n)$, 224
 $\otimes$, 234



Chapitre premier

Structure d'anneau

Les notions de loi de composition interne, de groupe et en particulier de groupe abélien, sont supposées connues, ainsi que leurs propriétés élémentaires ([11]).

1. Notions Fondamentales

A. Anneau

Définition 1.1. On appelle **anneau** tout ensemble non vide A muni de deux lois de composition internes, généralement notées l'une additivement, l'autre multiplicativement, vérifiant les trois axiomes suivants :

(A_1) : $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0 .

(A_2) : La multiplication est associative : quels que soient x, y, z , dans A ,

$$x(yz) = (xy)z.$$

(A_3) : La multiplication est distributive à droite et à gauche par rapport à l'addition : quels que soient x, y, z , dans A ,

$$(x + y)z = xz + yz \quad \text{et} \quad x(y + z) = xy + xz.$$

Cas particuliers : A étant un anneau,

a) A est dit **nul**, si A est réduit à $\{0\}$.

b) A est dit **unitaire**, s'il possède un élément neutre pour la multiplication, appelé **élément unité** de A et noté 1_A ou 1 , s'il n'y a pas d'ambiguïté.

c) A est dit **commutatif**, si la multiplication de A est commutative.

Dans toute la suite, on note $\mathbb{N}$ l'ensemble des **entiers naturels** :

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

et $\mathbb{Z}$ l'ensemble des entiers positifs, négatifs ou nuls, que nous appellerons **ensemble des entiers rationnels** (on dit aussi **entiers relatifs**). On pose

$$\mathbb{N}^* = \mathbb{N} \setminus \{0\} \quad \text{et} \quad \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}.$$

On suppose connues les propriétés de l'addition et de la multiplication des entiers rationnels, impliquant que $\mathbb{Z}$ est un **anneau unitaire, commutatif** ([42]).

Les propriétés arithmétiques de l'anneau $\mathbb{Z}$ sont traitées dans l'Appendice A de ce livre.

B. Règles de calculs dans les anneaux

Ces règles résultent des propriétés élémentaires des lois de composition internes, ainsi que des axiomes (A_1) , (A_2) , (A_3) .

Proposition 1.2. *Tout anneau A vérifie les propriétés suivantes :*

1) Pour tout $x \in A$, $0x = x0 = 0$.

2) Quels que soient x, y dans A :

$$(-x)y = x(-y) = -xy.$$

3) Quels que soient x, y dans A et n dans $\mathbb{Z}$:

$$(nx)y = n(xy) = x(ny).$$

4) Quels que soient m et n dans $\mathbb{N}^*$, x_i et y_j dans A , avec $1 \leq i \leq m$ et

$1 \leq j \leq n$:

$$\left(\sum_{1 \leq i \leq m} x_i \right) \left(\sum_{1 \leq j \leq n} y_j \right) = \sum_{(i,j)} x_i y_j.$$

5) Quels que soient $x \in A$ et $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$:

$$x^{m+n} = x^m x^n = x^n x^m \quad \text{et} \quad (x^m)^n = x^{mn}.$$

Preuve :

1) En utilisant l'axiome (A_3) et la règle de simplification dans le groupe $(A, +)$, on obtient :

$$(0+0)x = 0x + 0x \implies 0x = 0x + 0x \implies 0x = 0.$$

On montre de même que $x0 = 0$.

2) D'après 1), on peut écrire

$$0 = (x-x)y = xy + (-x)y, \quad \text{d'où} \quad (-x)y = -xy.$$

$$0 = x(y-y) = xy + x(-y), \quad \text{d'où} \quad x(-y) = -xy.$$

3) Si $n = 0$, le résultat découle de 1); si $n > 0$, la distributivité à gauche et à droite de la multiplication par rapport à l'addition implique :

$$(nx)y = n(xy) \quad \text{et} \quad x(ny) = n(xy).$$

Si $n < 0$, on pose $n = -n'$, avec $n' > 0$; alors $nx = (-n')x = -(n'x)$ implique

$$(nx)y = -(n'x)y = -(n'xy) = (-n')xy, \quad \text{d'où} \quad (nx)y = n(xy).$$

On obtient de même $x(ny) = n(xy)$.

4) est conséquence de l'axiome (A_3) .

5) est conséquence de l'axiome (A_2) . □

Remarque 1.3. :

a) Pour $n \in \mathbb{Z}$ et x, y dans A , on pourra écrire nxy à la place de $n(xy)$.

b) Dans un anneau A unitaire, non nul, on a nécessairement $1_A \neq 0$.

Un anneau unitaire quelconque sera, par convention, supposé non nul.

c) Dans tout anneau unitaire A , pour tout $x \in A \setminus \{0\}$, on pose $x^0 = 1_A$.

Proposition 1.4. *A étant un anneau unitaire, commutatif, quels que soient x, y dans A et n dans $\mathbb{N}^*$, on a*

$$(x+y)^n = \sum_{0 \leq k \leq n} C_n^k x^k y^{n-k}, \tag{1.1}$$

$$\text{où} \quad C_n^k = \frac{n(n-1) \dots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!},$$

avec la convention : $0! = 1$.

La relation (1.1) est appelée **formule du binôme**.

Preuve : Notons B_n la relation (1.1) écrite pour x et y donnés dans A et n fixé dans $\mathbb{N}^*$. La formule B_n se démontre par récurrence sur n .

Pour $n = 1$, B_1 s'écrit : $x + y = y + x$; B_1 est vérifiée, puisque $(A, +)$ est un groupe abélien. Supposons $n > 1$ et B_{n-1} vérifiée; calculons $(x + y)^n$.

$$\begin{aligned}(x + y)^n &= (x + y)^{n-1}(x + y) \\ &= \left(\sum_{0 \leq j \leq n-1} C_{n-1}^j x^j y^{n-1-j} \right) (x + y) \\ &= \sum_{0 \leq j \leq n-1} C_{n-1}^j x^{j+1} y^{n-1-j} + \sum_{0 \leq j \leq n-1} C_{n-1}^j x^j y^{n-j}.\end{aligned}$$

En posant : $k = j + 1$, on peut écrire :

$$\sum_{0 \leq j \leq n-1} C_{n-1}^j x^{j+1} y^{n-1-j} = \sum_{1 \leq k \leq n} C_{n-1}^{k-1} x^k y^{n-k}.$$

On obtient alors :

$$(x + y)^n = C_n^n x^n + \sum_{1 \leq k \leq n-1} (C_{n-1}^{k-1} + C_{n-1}^k) x^k y^{n-k} + C_{n-1}^0 y^n,$$

d'où la relation B_n , compte tenu des égalités (à vérifier) :

$$C_{n-1}^{n-1} = C_n^n = 1, \quad C_n^0 = C_{n-1}^0 = 1, \quad C_{n-1}^{k-1} + C_{n-1}^k = C_n^k. \quad \square$$

Remarque 1.5. Soit A un anneau unitaire, non nécessairement commutatif.

a) Quel que soit $n \in \mathbb{N}^*$, on peut écrire la formule du binôme B_n , pour deux éléments x et y de A , si et seulement si $xy = yx$ (autrement dit, si x et y commutent).

b) Pour tout $x \in A$ et tout $n \in \mathbb{N}^*$,

$$(x + 1)^n = \sum_{0 \leq k \leq n} C_n^k x^k, \quad (1.2)$$

$$\text{d'où } x = 1 \implies \sum_{0 \leq k \leq n} C_n^k = 2^n \quad (1.3)$$

$$\text{et } x = -1 \implies \sum_{0 \leq k \leq n} (-1)^k C_n^k = 0. \quad (1.4)$$

C. Éléments inversibles dans un anneau unitaire - Corps

Soit A un anneau unitaire, non nécessairement commutatif. Si un élément non nul x de A possède, dans A , un inverse à gauche x' et un inverse à droite x'' , alors $x' = x''$. En effet :

$$(x'x = 1 \text{ et } xx'' = 1) \implies x'(xx'') = x' = (x'x)x'' = x''.$$

On dit alors que x est **inversible** dans A et l'élément $x' = x''$ est l'**inverse** de x dans A ; il est généralement noté x^{-1} .

Définition 1.6. :

a) Un anneau unitaire, non nécessairement commutatif, dans lequel tout élément non nul est inversible est appelé : **anneau à division** ou **corps gauche**.

b) Un anneau unitaire, commutatif dans lequel tout élément non nul est inversible est appelé **corps commutatif**.

Remarque 1.7. :

a) Tout corps, gauche ou commutatif, a au moins deux éléments 0 et 1.

b) Dans toute la suite, un corps commutatif sera appelé un **corps**.

Notations : Pour tout anneau non nul A , on pose $A^* = A \setminus \{0\}$.

Pour tout anneau unitaire A , on notera U_A l'ensemble des éléments inversibles de A , qui sont aussi appelés les **unités** de A .

Remarque 1.8. Dans tout anneau unitaire A , on a $U_A \neq \emptyset$, car 1 et -1 sont dans U_A .

Proposition 1.9. Dans tout anneau unitaire A , U_A est un groupe, relativement à la multiplication de A , appelé **groupe des éléments inversibles de A** , ou **groupe des unités de A** .

Preuve : D'après la remarque précédente, on a $U_A \neq \emptyset$ et $1 \in U_A$.

D'autre part, pour x et y dans U_A ,

$$y^{-1}x^{-1}xy = 1 \implies (xy)^{-1} = y^{-1}x^{-1}; \text{ d'où, } (x, y) \in U_A \times U_A \implies xy \in U_A;$$

$$x^{-1}x = 1 \implies (x^{-1})^{-1} = x, \text{ donc } x \in U_A \implies x^{-1} \in U_A,$$

d'où le résultat énoncé. $\square$

Remarque 1.10. :

a) Le groupe U_A est abélien si et seulement si l'anneau A est commutatif.

b) Pour l'anneau des entiers $\mathbb{Z}$, on a $U_{\mathbb{Z}} = \{-1, 1\}$.

c) Si K est un corps, gauche ou commutatif, alors $U_K = K^* (= K \setminus \{0\})$.

D. Premiers exemples d'anneaux et de corps

Exemple 1.11. Anneaux et corps de nombres 1) On a rappelé plus haut que, muni des opérations usuelles d'addition et de multiplication, l'ensemble $\mathbb{Z}$ des entiers rationnels est un anneau unitaire, commutatif.

2) On suppose connues ([42]) la construction et les propriétés élémentaires des corps commutatifs $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ des nombres, respectivement, **rationnels**, **réels** et **complexes**, tels que :

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Exemple 1.12. Anneau des classes de congruences modulo n

La construction de l'anneau $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo un entier $n \in \mathbb{N}$ est faite dans l'Appendice A de ce livre. Pour $n > 0$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n . On peut supposer $n > 1$ et en adoptant les notations définies dans l'Appendice A, on écrit

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

D'autre part, on rappelle ([11], Ch. III) que le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et qu'un élément $\bar{k}$ est un générateur de ce groupe si et seulement si k est premier avec n (Ecriture symbolique : $k \wedge n = 1$; Cf. App. A, Déf. 0.27.).

Le cardinal de l'ensemble de ces générateurs est donc égal au nombre d'entiers k tels que $1 \leq k \leq n-1$ et $k \wedge n = 1$; ce nombre est noté $\varphi(n)$; la fonction numérique φ est appelée **Fonction d'Euler** ([47]).

Le Théorème de Bezout (App. A, Th. 0.24.) permet alors de démontrer le résultat suivant.

Proposition 1.13. Pour $n > 1$ dans $\mathbb{N}$, le groupe G_n des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est formé par l'ensemble des générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$; donc G_n est un groupe multiplicatif abélien d'ordre $\varphi(n)$.

Preuve : Compte tenu de la définition du groupe G_n , on a

$$\begin{aligned} \bar{k} \in G_n &\iff \exists \bar{k}' \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \bar{k}\bar{k}' = \bar{1} \\ &\iff \exists k' \in \mathbb{Z} \text{ tel que } (kk' - 1) \in n\mathbb{Z} \\ &\iff \exists (k', q) \in \mathbb{Z} \times \mathbb{Z} \text{ tel que } kk' - nq = 1. \end{aligned}$$

D'après le Théorème de Bezout,

$$kk' - nq = 1 \iff k \wedge n = 1,$$

donc $\bar{k} \in G_n$ si et seulement si $k \wedge n = 1$, d'où le résultat énoncé. $\square$

Corollaire 1.14. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Preuve : D'après la proposition 1.13., $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si tout entier k tel que $1 \leq k \leq p-1$ est premier avec p ; ce qui équivaut à dire que p est un nombre premier (App. A, Déf. 0.5.). $\square$

Exemple 1.15. Anneau des endomorphismes d'un groupe abélien

Soit $\text{End } G$ l'ensemble des endomorphismes d'un groupe abélien $(G, +)$. L'application

$$\begin{aligned} \text{End } G \times \text{End } G &\longrightarrow \text{End } G \\ (f, g) &\longmapsto f + g, \end{aligned}$$

telle que

$$\forall x \in G, (f + g)(x) = f(x) + g(x),$$

définit une loi de composition interne dans $\text{End } G$.

On vérifie que $\text{End } G$ est alors un groupe additif abélien dont l'élément neutre est l'endomorphisme nul de G .

En considérant la loi $\circ$ de composition des endomorphismes de G , comme une multiplication dans $\text{End } G$ on montre que $(\text{End } G, +, \circ)$ est un anneau unitaire, en général non commutatif (id_G est l'élément unité).

Le groupe des éléments inversibles de cet anneau est le groupe des automorphismes de $(G, +)$.

Exemple 1.16. Les exemples décrits ci-dessous supposent connues les notions et propriétés élémentaires de l'Algèbre Linéaire.

1) **Anneau des endomorphismes d'un espace vectoriel**

E étant un espace vectoriel sur un corps K , on note $\mathcal{L}_K(E)$ l'ensemble des endomorphismes K -linéaires de E . Comme dans l'exemple 1.15., on définit une addition dans $\mathcal{L}_K(E)$ par l'application :

$$\begin{aligned} \mathcal{L}_K(E) \times \mathcal{L}_K(E) &\longrightarrow \mathcal{L}_K(E) \\ (f, g) &\longmapsto f + g, \end{aligned}$$

telle que

$$\forall x \in E, (f + g)(x) = f(x) + g(x).$$

$(\mathcal{L}_K(E), +)$ est alors un groupe additif abélien, dont l'élément neutre est l'endomorphisme nul de E .

D'autre part, la composition des K -endomorphismes de E , notée $\circ$, définit une seconde loi de composition interne dans $\mathcal{L}_K(E)$, admettant id_E comme élément unité et telle que $(\mathcal{L}_K(E), +, \circ)$ est un anneau unitaire, non commutatif en général.

Le groupe des éléments inversibles de cet anneau est le groupe $GL_K(E)$ des automorphismes K -linéaires de E .

2) **Anneaux de matrices carrées sur un corps**

Soit $n \in \mathbb{N}^*$ et $M_n(K)$ l'ensemble des matrices carrées d'ordre n sur un corps K ; muni de l'addition et de la multiplication des matrices, $M_n(K)$ est un anneau unitaire, non commutatif en général; l'élément unité étant la matrice carrée unité I_n .

Le groupe des unités de l'anneau $M_n(K)$ est le groupe $GL_n(K)$ des matrices inversibles de $M_n(K)$.

Exemple 1.17. Corps gauche des quaternions dans $M_2(\mathbb{C})$

Dans l'anneau $M_2(\mathbb{C})$ des matrices carrées d'ordre 2 sur le corps des nombres complexes $\mathbb{C}$, on considère

$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} ; (x, y) \in \mathbb{C} \times \mathbb{C} \right\},$$

où $\bar{x}$ et $\bar{y}$ sont, respectivement, les imaginaires conjugués de x et y dans $\mathbb{C}$.

Connaissant les règles de calcul dans $\mathbb{C}$ et dans $M_2(\mathbb{C})$, on vérifie que $\mathbb{H}$ est un sous-anneau unitaire, non commutatif de $M_2(\mathbb{C})$.

D'autre part, pour toute matrice

$$A = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \text{ non nulle dans } \mathbb{H}, \text{ on a}$$

$$\det(A) = x\bar{x} + y\bar{y} = |x|^2 + |y|^2 \neq 0,$$

donc A est inversible dans $M_2(\mathbb{C})$. Montrons que $A^{-1} \in \mathbb{H}$.

On rappelle (voir un cours d'Algèbre Linéaire) que

$$A^{-1} = \Delta^{-1} \tilde{A},$$

où $\Delta = \det(A)$ et $\tilde{A}$ est la matrice adjointe de A , c'est-à-dire, la transposée de la matrice des cofacteurs des éléments du déterminant de A , donc

$$\tilde{A} = \begin{pmatrix} \bar{x} & -y \\ \bar{y} & x \end{pmatrix} \text{ et } A^{-1} = \begin{pmatrix} \Delta^{-1}\bar{x} & -\Delta^{-1}y \\ \Delta^{-1}\bar{y} & \Delta^{-1}x \end{pmatrix}.$$

 **Mensa**
 $\Delta^{-1} \in \mathbb{R}$, par suite $A^{-1} \in \mathbb{H}$.

On en conclut que $\mathbb{H}$ est un corps gauche ou anneau à division (Déf. 1.6.).

Une étude détaillée de ce corps gauche, appelé corps des quaternions, sera faite au Chapitre 3.

Exemple 1.18. Soit E un ensemble non vide et A un anneau. On note A^E l'ensemble des applications de E dans A et on vérifie facilement que A^E est muni d'une structure d'anneau, grâce aux deux lois de composition internes définies par :

$$\begin{aligned} A^E \times A^E &\longrightarrow A^E \\ (f, g) &\longmapsto f + g \\ (f, g) &\longmapsto fg \end{aligned}$$

telles que, quels que soit $x \in E$,

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (fg)(x) = f(x)g(x).$$

L'élément neutre pour l'addition est l'application nulle de E dans A .

On vérifie que :

a) A unitaire $\implies A^E$ unitaire.

L'élément unité de A^E est alors l'application ε telle que, pour tout $x \in E$, $\varepsilon(x) = 1$.

b) A commutatif $\implies A^E$ commutatif.

Cas particulier : si l'on considère l'intervalle fermé $[0, 1]$ de $\mathbb{R}$, d'après ce qui précède, $\mathbb{R}^{[0,1]}$ est un anneau unitaire et commutatif.

E. Diviseurs de zéro - Anneaux intègres

Définition 1.19. Dans un anneau A , un élément x est un **diviseur de zéro à gauche** (resp. à droite), si $x \neq 0$ et s'il existe $y \neq 0$ dans A tel que $xy = 0$ (resp. $yx = 0$).

Dans un anneau commutatif on parlera seulement de "diviseur de zéro".

Exemple : Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ et $\bar{3}$ sont des diviseurs de zéro.

Remarque 1.20. :

a) Si un anneau A , non commutatif, n'a pas de diviseur de zéro à gauche, il n'a pas non plus de diviseur de zéro à droite (et inversement).

En effet, si x est un diviseur de zéro à droite dans A , alors il existe $y \neq 0$ dans A , tel que $yx = 0$; par suite y est un diviseur de zéro à gauche dans A .

b) Pour un élément $x \neq 0$ d'un anneau unitaire A , on a :

$$x \text{ inversible} \implies x \text{ non diviseur de zéro.}$$

En effet, $xy = 0$, avec $y \neq 0$ dans A , implique

$$x^{-1}(xy) = 0 = (x^{-1}x)y = y, \quad \text{d'où une contradiction.}$$

Conclusion : un corps, gauche ou commutatif, n'a pas de diviseur de zéro.

Définition 1.21. :

a) Un anneau est dit **intègre** s'il est non nul et sans diviseur de zéro.

b) On appellera **domaine d'intégrité** tout anneau unitaire, commutatif intègre.

Remarque 1.22. Pour x et y dans un anneau intègre, on a :

$$xy = 0 \implies x = 0 \quad \text{ou} \quad y = 0.$$

Exemple 1.23. :

1) Tout corps (gauche ou commutatif) est intègre.

Tout corps commutatif est un domaine d'intégrité.

2) $\mathbb{Z}$ est un domaine d'intégrité.

3) $\mathbb{Z}/n\mathbb{Z}$ est un domaine d'intégrité si et seulement si n est un nombre premier et dans ce cas, on sait que $\mathbb{Z}/n\mathbb{Z}$ est un corps (Cor. 1.14.).

En effet, pour tout entier k divisant n et tel que $1 < k < n$, $\bar{k}$ est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$; on en déduit que :

$$\mathbb{Z}/n\mathbb{Z} \text{ non intègre} \iff n > 1 \text{ et } n \text{ non premier.}$$

Proposition 1.24. Tout domaine d'intégrité fini est un corps.

Preuve : Soit A un domaine d'intégrité fini.

Si $\text{card}(A) = 2$, $A = \{0, 1\}$; A est un corps.

Supposons $\text{card}(A) = n > 2$ et posons : $A = \{0, 1, a_3, \dots, a_n\}$.

Soit $a_i \in A$, tel que $3 \leq i \leq n$; considérons :

$$a_i A = \{0, a_i, a_i a_3, \dots, a_i a_n\}.$$

$$(3 \leq i \leq n) \implies (a_i \neq 0 \text{ et } a_i \neq 1).$$

A étant intègre, on a $a_i a_j \neq 0$ quel que soit j ($3 \leq j \leq n$) et de plus, pour $3 \leq j \leq n$ et $3 \leq k \leq n$,

$$a_i a_j = a_i a_k \implies a_i(a_j - a_k) = 0 \implies a_j = a_k,$$

c'est-à-dire que $a_i A$ contient n éléments distincts, d'où $a_i A = A$.

On en déduit qu'il existe j ($3 \leq j \leq n$), tel que $a_i a_j = 1$.

Ainsi tout élément non nul de A est inversible, donc A est un corps. □

Remarque 1.25. On peut noter que la commutativité de A n'intervient pas dans la démonstration précédente. Dans le Volume 2 (Extensions de corps), nous démontrerons le résultat suivant (Théorème de Wedderburn) :

"Tout anneau à division fini est un corps commutatif".

Définition 1.26. Dans un anneau A , un élément x est dit **nilpotent**, s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

Exemple : dans l'anneau de matrices $M_2(\mathbb{R})$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Remarque 1.27. Un élément nilpotent non nul est nécessairement un diviseur de zéro dans A .

Définition 1.28. Dans un anneau A , un élément x est dit **idempotent**, si $x^2 = x$.

Exemple : dans l'anneau $M_2(\mathbb{R})$, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ est idempotente.

2. Sous-anneaux

A. Notion de sous-anneau - Propriétés élémentaires

Définition 1.29. A étant un anneau, une partie *non vide* B de A est un **sous-anneau** de A , si :

- i) B est un sous-groupe de $(A, +)$;
- ii) B est stable pour la multiplication de A ; c'est-à-dire que pour x et y dans A , on a :

$$(x, y) \in B \times B \implies xy \in B.$$

Remarque 1.30. D'après la définition 1.29., pour démontrer qu'une partie *non vide* B de A est un sous-anneau de A , il suffit de vérifier que pour x et y dans A , on a :

$$(x, y) \in B \times B \implies (x - y) \in B \quad \text{et} \quad xy \in B.$$

Exemple 1.31. :

1) Dans tout anneau non nul A , (0) et A sont des sous-anneaux.

2) Pour tout entier $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ et tout sous-anneau de $\mathbb{Z}$ s'écrit sous cette forme, de façon unique.

En effet, $n\mathbb{Z}$ est stable pour la multiplication des entiers et d'autre part, pour tout sous-groupe H de $(\mathbb{Z}, +)$ il existe un unique $n \in \mathbb{N}$, tel que $H = n\mathbb{Z}$ ([11], p. 31).

3) $A = \{a + b\sqrt{2} ; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$
est un sous-anneau du corps $\mathbb{R}$ des nombres réels, noté $\mathbb{Z}[\sqrt{2}]$.

4) $A = \{a + ib ; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$,
où i est le nombre complexe tel que $i^2 = -1$, est un sous-anneau du corps $\mathbb{C}$, noté $\mathbb{Z}[i]$ et appelé **anneau des entiers de Gauss**.

5) L'anneau $\mathbb{R}^{[0,1]}$ défini dans l'exemple 1.18. contient plusieurs sous-anneaux intéressants en Analyse, en particulier : l'anneau des fonctions réelles bornées (resp. continues, continûment différentiables) sur l'intervalle $[0, 1]$.

Définition 1.32. A étant un anneau, on appelle **centre** de A , l'ensemble :

$$Z(A) = \{x \in A ; ax = xa, \forall a \in A\}.$$

Proposition 1.33. Pour tout anneau A , $Z(A)$ est un sous-anneau de A et

$$Z(A) \neq A \iff A \text{ non commutatif.}$$

Vérification laissée au lecteur.

Remarque 1.34. :

a) Un sous-anneau B d'un anneau unitaire A ne contient pas nécessairement l'élément unité 1_A . Par exemple, pour tout entier $n > 1$, $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ ne contenant pas 1.

b) Un sous-anneau B d'un anneau unitaire A peut être unitaire et tel que $1_B \neq 1_A$ (Voir Ex. 8, Chap. 1).

c) Etant donné un anneau unitaire A , nous conviendrons d'appeler **sous-anneau unitaire** de A , tout sous-anneau de A contenant 1_A .

d) Tout sous-anneau d'un corps gauche ou commutatif est intègre.

Proposition 1.35. Dans tout anneau A , l'intersection d'une famille quelconque de sous-anneaux de A est un sous-anneau de A .

Vérification laissée au lecteur.

Remarque 1.36. En général, la réunion d'une famille de sous-anneaux de A n'est pas un sous-anneau de A .

Par exemple, dans l'anneau $\mathbb{Z}$, $3\mathbb{Z} \cup 5\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$, puisque ce n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

On a cependant la propriété suivante :

Proposition 1.37. A étant un anneau, si $\{A_i\}_{i \in I}$ est une famille de sous-anneaux de A totalement ordonnée par l'inclusion, alors $\bigcup_{i \in I} A_i$ est un sous-anneau de A .

Même démonstration que dans le cas des groupes ([11], p. 31).

B. Sous-anneau engendré par une partie non vide d'un anneau

Définition 1.38. Soit S une partie non vide d'un anneau A ; notons $\mathcal{B}_S$ l'ensemble des sous-anneaux de A contenant S et posons :

$$\langle S \rangle = \bigcap_{B \in \mathcal{B}_S} B.$$

$\langle S \rangle$ est un sous-anneau de A (Prop. 1.35.) appelé **sous-anneau de A engendré par S** .

Remarque 1.39. Dans l'ensemble des sous-anneaux de A ordonné par l'inclusion, $\langle S \rangle$ est le plus petit sous-anneau de A contenant S .

Proposition 1.40. S étant une partie non vide d'un anneau A , on a :

$$\langle S \rangle = \left\{ \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} x_{i_1} \dots x_{i_n} ; n \in \mathbb{N}^*, x_{i_j} \in S \text{ ou } -x_{i_j} \in S, \forall j (1 \leq j \leq n) \right\}.$$

Principe de la démonstration :

i) Désignons par S' le second membre de la relation ci-dessus ; on remarque que $S \subseteq S'$.

ii) On démontre que S' est un sous-anneau de A ; on en déduit que S' appartient à l'ensemble $\mathcal{B}_S$ des sous-anneaux de A contenant S , d'où

$$\langle S \rangle \subseteq S'.$$

D'autre part, tout sous-anneau de A , contenant S , contient nécessairement tous les éléments de S' ; par suite $S' = \langle S \rangle$.

Exemple 1.41. L'anneau des entiers de Gauss, $\mathbb{Z}[i]$, est le sous-anneau de $\mathbb{C}$ engendré par $\{i\}$.

3. Notions d'idéal à gauche, à droite, bilatère

Définition 1.42. Soit A un anneau.

a) Une partie non vide L de A est un **idéal à gauche** de A , si

- i) L est un sous-groupe de $(A, +)$;
- ii) Pour tout $x \in L$ et tout $a \in A$, $ax \in L$.

b) Une partie non vide R de A est un **idéal à droite** de A , si

- i) R est un sous-groupe de $(A, +)$;
- ii) Pour tout $x \in R$ et tout $a \in A$, $xa \in R$.

c) Une partie non vide I de A est un **idéal bilatère** de A , si I est à la fois un idéal à gauche et un idéal à droite de A .

Remarque 1.43. :

a) Tout idéal d'un anneau A est un sous-anneau de A .

b) Dans un anneau commutatif, tout idéal est bilatère.

Exemple 1.44. :

1) Dans tout anneau non nul A , (0) et A sont des idéaux bilatères de A .

2) Les idéaux de l'anneau $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$ (App. A).

3) Soit S une partie non vide d'un anneau A . On pose :

$$Ann_g(S) = \{a \in A ; ax = 0, \forall x \in S\}.$$

$$Ann_d(S) = \{a \in A ; xa = 0, \forall x \in S\}.$$

$Ann_g(S)$ (resp. $Ann_d(S)$) est appelé l'**annulateur à gauche** (resp. **à droite**) de S dans A .

On vérifie que, quelle que soit la partie non vide S de A , $Ann_g(S)$ (resp. $Ann_d(S)$) est un idéal à gauche (resp. à droite) de A .

Si l'anneau A est commutatif, on appelle **annulateur** d'une partie non vide S de A , l'idéal noté $Ann(S)$ tel que :

$$Ann(S) = Ann_g(S) = Ann_d(S).$$

Définition 1.45. J étant un idéal à gauche (resp. à droite ou bilatère) d'un anneau A , on dira que J est un idéal à gauche (resp. à droite ou bilatère) **propre** de A , si $J \neq A$.

Remarque 1.46. :

a) Dans tout anneau non nul, (0) est un idéal propre.

b) Dans un anneau unitaire A , pour tout $x \in A \setminus \{0\}$, l'idéal $Ann_g(x)$ (resp. $Ann_d(x)$) est un idéal à gauche (resp. à droite) propre de A et

$$Ann_g(x) = (0) \iff x \text{ est non diviseur de zéro à droite dans } A.$$

$$Ann_d(x) = (0) \iff x \text{ est non diviseur de zéro à gauche dans } A.$$

Proposition 1.47. Soit A un anneau unitaire. Si J est un idéal à gauche (à droite, ou bilatère) de A , alors les conditions suivantes sont équivalentes :

- 1) $J \neq A$.
- 2) $1 \notin J$.
- 3) $J \cap U_A = \emptyset$.

Preuve : On suppose J idéal à gauche de A .

1) $\implies$ 2) : Si $1 \in J$, alors, quel que soit $a \in A$, $a1 = a$ appartient à J , d'où $J = A$, ce qui contredit l'hypothèse 1).

2) $\implies$ 3) : Supposons $x \in J \cap U_A$; alors, $x^{-1}x = 1 \implies 1 \in J$, ce qui est contraire à l'hypothèse 2).

3) $\implies$ 1) : L'hypothèse 3) implique $1 \notin J$; d'où $J \neq A$. $\square$

Corollaire 1.48. *Un corps (gauche ou commutatif) K n'a pas d'autre idéal que (0) et K .*

Ce résultat découle du 3) de la proposition 1.47., puisque $U_K = K^*$.

Les propriétés des idéaux d'un anneau seront étudiées dans le Chapitre 2.

4. Morphismes d'anneaux

A. Définitions

Définition 1.49. A et B étant deux anneaux, une application f de A dans B est un **morphisme d'anneaux** si

- i) f est un morphisme de groupes de $(A, +)$ dans $(B, +)$.
- ii) $f(xy) = f(x)f(y)$, quels que soient x et y dans A .

On notera $\text{Hom}(A, B)$ l'ensemble des morphismes d'un anneau A dans un anneau B .

Un morphisme d'anneaux est aussi appelé un **homomorphisme** d'anneaux.

Un morphisme d'un anneau A dans lui-même est appelé un **endomorphisme** d'anneau.

L'ensemble des endomorphismes d'un anneau A sera noté $\text{End}(A)$.

Remarque 1.50. Si A et B sont deux anneaux unitaires, $f \in \text{Hom}(A, B)$ n'implique pas nécessairement $f(1_A) = 1_B$ (Ex. 5, Ch. 1), ce qui justifie la définition suivante :

Définition 1.51. A et B étant deux anneaux unitaires, on dira qu'une application f de A dans B est un **morphisme d'anneaux unitaires**, si

$$f \in \text{Hom}(A, B) \quad \text{et} \quad f(1_A) = 1_B.$$

B. Propriétés des morphismes d'anneaux

Définition 1.52. Soit A et B deux anneaux et $f \in \text{Hom}(A, B)$; alors,

$f(A) = \{f(x) ; x \in A\}$ est appelé **image de f** et noté **Im f** ,

$f^{-1}(0) = \{x \in A ; f(x) = 0\}$ est appelé **noyau de f** et noté **Ker f** .

Proposition 1.53. *Compte tenu des hypothèses et des notations de la définition 1.52., on a*

1) A' sous-anneau de $A \implies f(A')$ sous-anneau de B .

En particulier, Im f est un sous-anneau de B .

2) Si A est unitaire, alors Im f est un anneau unitaire dont l'élément unité est $f(1_A)$; de plus, si x est inversible dans A , alors $f(x)$ est inversible dans Im f et $(f(x))^{-1} = f(x^{-1})$.

3) B' sous-anneau de $B \implies f^{-1}(B')$ sous-anneau de A .

4) Si J est un idéal à gauche (resp. à droite, bilatère) de B , alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite, bilatère) de A .

En particulier, Ker f est un idéal bilatère de A .

5) $\forall n \in \mathbb{Z}, \quad \forall x \in A, \quad f(nx) = nf(x)$.

6) $\forall n \in \mathbb{N}, \quad \forall x \in A, \quad f(x^n) = (f(x))^n$.

Vérification laissée au lecteur.

Remarque 1.54. Si L est un idéal à gauche de A , alors $f(L)$ est un sous-anneau de B , mais n'est pas en général, un idéal à gauche de B . Cependant, $f(L)$ est un idéal à gauche dans l'anneau $\text{Im} f$.

La même remarque est valable pour un idéal à droite ou bilatère de A .

Définition 1.55. Un anneau B est dit **image homomorphe** d'un anneau A , s'il existe un morphisme *surjectif* de A sur B .

Remarque 1.56. A et B étant deux anneaux, soit $f \in \text{Hom}(A, B)$.

a) Si A est unitaire et si f est *surjectif*, alors d'après le 2) de la proposition 1.53., B est unitaire et $1_B = f(1_A)$; donc f est nécessairement un morphisme d'anneaux unitaires.

b) $f \in \text{Hom}(A, B)$ implique que f est un morphisme de groupes de $(A, +)$ dans $(B, +)$, par suite, f est *injectif* si et seulement si $\text{Ker} f = (0)$.

Exemple 1.57. :

1) Soit A' un sous-anneau d'un anneau A ; alors l'injection canonique

$$\begin{aligned} i : A' &\longrightarrow A \\ x &\longmapsto x. \end{aligned}$$

est un morphisme injectif d'anneaux.

2) A et B étant deux anneaux, l'application

$$\begin{aligned} A &\longrightarrow B \\ x &\longmapsto 0. \end{aligned}$$

est un morphisme d'anneaux, appelé **morphisme nul** et noté 0 .

Pour $f \in \text{Hom}(A, B)$, on a : $f = 0 \iff \text{Ker} f = A$.

3) Pour $n > 1$ dans $\mathbb{N}$, la surjection canonique de $\mathbb{Z}$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (Exemple 1.12.) :

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto \bar{x}. \end{aligned}$$

est un morphisme surjectif d'anneaux unitaires tel que $\text{Ker} \pi = n\mathbb{Z}$.

Proposition 1.58. Soit K un corps (gauche ou commutatif) et A un anneau; alors tout morphisme non nul de K dans A est injectif.

Preuve : Soit $f \in \text{Hom}(K, A)$, $f \neq 0$, donc $\text{Ker} f \neq K$. D'après le corollaire 1.48., K n'a pas d'autre idéal que (0) et K , d'où nécessairement $\text{Ker} f = (0)$, donc f est injectif (Rem. 1.56., b)). $\square$

Corollaire 1.59. Soit K un corps (gauche ou commutatif) et A un anneau unitaire; alors tout morphisme d'anneaux unitaires de K dans A est injectif.

Preuve : Rappelons qu'un anneau unitaire quelconque est supposé non nul; par suite, si $f \in \text{Hom}(K, A)$, alors $f(1_K) = 1_A$ implique $f \neq 0$, donc f est injectif, d'après la proposition 1.58. $\square$

Proposition 1.60. Soit trois anneaux A, A', A'' , alors

$$(f \in \text{Hom}(A, A') \text{ et } g \in \text{Hom}(A', A'')) \implies g \circ f \in \text{Hom}(A, A'').$$

De plus, si les trois anneaux sont unitaires et si f et g sont des morphismes d'anneaux unitaires, alors $g \circ f$ est un morphisme d'anneaux unitaires.

Vérification laissée au lecteur.

Définition 1.61. Une application f d'un anneau A dans un anneau B est un **isomorphisme** d'anneaux, si $f \in \text{Hom}(A, B)$ et s'il existe $g \in \text{Hom}(B, A)$ tel que :

$$g \circ f = \text{id}_A \quad \text{et} \quad f \circ g = \text{id}_B.$$

Proposition 1.62. Soit deux anneaux A et B ,

1) f étant une application de A dans B , alors

f isomorphisme de A sur $B \iff f \in \text{Hom}(A, B)$ et f bijectif.

2) f isomorphisme de A sur $B \implies f^{-1}$ isomorphisme de B sur A .

La méthode de démonstration est semblable à celle utilisée dans le cas des morphismes de groupes ([11], Prop. 1.66.).

Définition 1.63. :

a) Deux anneaux A et B sont dits **isomorphes**, s'il existe un isomorphisme d'anneaux de l'un sur l'autre ; dans ce cas, on écrit : $A \simeq B$.

b) Un isomorphisme de A sur lui-même est appelé un **automorphisme** de A . L'ensemble des automorphismes d'un anneau A est noté $\text{Aut}(A)$.

Proposition 1.64. Pour tout anneau A , $\text{Aut}(A)$ est un groupe relativement à la loi $\circ$ de composition des morphismes.

Preuve : Des propositions 1.60. et 1.62., on déduit que $\text{Aut}(A)$ est un sous-groupe du groupe symétrique $(S_A, \circ)$ formé par les bijections de A sur lui-même. $\square$

Exemple 1.65. Soit $\mathcal{L}_K(E)$ l'anneau des endomorphismes d'un K -espace vectoriel E de dimension finie n et $M_n(K)$ l'anneau des matrices carrées d'ordre n sur K (Exemple 1.16.) ; on suppose $n \geq 1$.

A toute base $b = \{e_1, e_2, \dots, e_n\}$ de E sur K , on peut associer l'application

$$\begin{aligned} M_b : \mathcal{L}_K(E) &\longrightarrow M_n(K) \\ u &\longmapsto M_b(u), \end{aligned}$$

où $M_b(u)$ est la matrice de l'endomorphisme u dans la base b , c'est-à-dire la matrice carrée d'ordre n , dont les colonnes sont respectivement formées par les composantes, dans la base b , des vecteurs $u(e_1), u(e_2), \dots, u(e_n)$.

On démontre en Algèbre Linéaire que, pour toute base b de E , M_b est un **isomorphisme** d'anneaux unitaires.

C. Caractéristique d'un anneau unitaire

Proposition 1.66. A étant un anneau unitaire, il n'existe qu'un seul morphisme d'anneaux unitaires de l'anneau des entiers $\mathbb{Z}$ dans A . Si l'on note ϕ ce morphisme, alors $\phi(n) = n1_A$, quel que soit $n \in \mathbb{Z}$.

En effet, d'après le 5) de la proposition 1.53. :

$$\phi(1) = 1_A \implies \phi(n) = n1_A, \quad \forall n \in \mathbb{Z}.$$

ϕ sera appelé le **morphisme canonique** de $\mathbb{Z}$ dans A .

Proposition 1.67. Soit A un anneau unitaire.

1) Pour tout n dans $\mathbb{Z}$, $n1_A$ appartient au centre de A (Déf. 1.32.).

2) Pour n dans $\mathbb{Z}$: $n1_A = 0 \iff (nx = 0, \forall x \in A)$.

Autrement dit, $\text{Ker } \phi = \{n \in \mathbb{Z} ; nx = 0, \forall x \in A\}$, ϕ étant le morphisme canonique de $\mathbb{Z}$ dans A .

Preuve :

1) D'après le 3) de la proposition 1.2., pour tout $x \in A$:

$$(n1_A)x = n(1_Ax) = n(x1_A) = x(n1_A).$$

2) Il est immédiat que : $(nx = 0, \forall x \in A) \implies n1_A = 0$.

Réciproquement, si $n \in \mathbb{Z}$ et $n1_A = 0$, alors :

$$\forall x \in A, (n1_A)x = n(1_Ax) = nx = 0. \quad \square$$

Rappel : Pour tout idéal I de l'anneau $\mathbb{Z}$, il existe un unique $k \in \mathbb{N}$ tel que $I = k\mathbb{Z}$; d'autre part, le noyau d'un morphisme d'anneaux est un idéal bilatère (Prop. 1.53.), d'où la définition suivante :

Définition 1.68. A étant un anneau unitaire et ϕ le morphisme canonique de $\mathbb{Z}$ dans A , on appelle **caractéristique** de A , l'unique entier $k \in \mathbb{N}$ tel que $\text{Ker } \phi = k\mathbb{Z}$. On écrit alors : $\text{car } A = k$.

Remarque 1.69. De la notion de caractéristique d'un anneau unitaire, on déduit les relations suivantes, dans lesquelles n est un entier :

$$\text{car } A = 0 \iff \{(nx = 0, \forall x \in A) \iff n = 0\} \quad (1.5)$$

$$\text{car } A = k > 0 \iff \{(nx = 0, \forall x \in A) \iff n \in k\mathbb{Z}\}. \quad (1.6)$$

$$\text{car } A = k > 0 \iff k \triangleq \inf\{n \in \mathbb{N}^* ; nx = 0, \forall x \in A\}. \quad (1.7)$$

Exemple 1.70. :

1) L'anneau $\mathbb{Z}$, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0.

2) Pour $n > 1$ dans $\mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n .

En particulier, si $p > 1$ est un nombre premier (App. A, Déf. 0.5.), le corps $\mathbb{Z}/p\mathbb{Z}$ (Cor. 1.14.) est de caractéristique p .

Remarque 1.71. A étant un anneau unitaire, si B est un sous-anneau unitaire de A , c'est-à-dire que $1_A \in B$, alors

$$\text{car } B = \text{car } A.$$

Proposition 1.72. Soit p un nombre premier, alors dans tout anneau A , unitaire, commutatif et de caractéristique p , on a, quel que soit $(x, y) \in A \times A$,

$$(x+y)^p = x^p + y^p \quad \text{et} \quad (x-y)^p = x^p + (-1)^p y^p. \quad (1.8)$$

Preuve : D'après la formule du binôme (Prop. 1.4.), on a

$$(x+y)^p = \sum_{0 \leq k \leq p} C_p^k x^k y^{p-k} \quad \text{et} \quad (x-y)^p = \sum_{0 \leq k \leq p} (-1)^{p-k} C_p^k x^k y^{p-k},$$

avec

$$C_p^k = \frac{p!}{k!(p-k)!}, \quad \forall k (0 \leq k \leq p).$$

Par suite, $C_p^0 = C_p^p = 1$ et p divise C_p^k dans $\mathbb{Z}$, pour tout $k (0 < k < p)$; d'où les relations (1.8), puisque p est la caractéristique de A .

On remarque que si $p = 2$, on a $-1 = 1$ et les relations (1.8) sont alors identiques. $\square$

Remarque 1.73. Les relations (1.5) et (1.7) permettent de définir la notion de *caractéristique* pour un anneau non nul A , non nécessairement unitaire :

A est dit **de caractéristique 0**, si $\{(nx = 0, \forall x \in A) \implies n = 0\}$.

A est dit **de caractéristique non nulle**, s'il existe $n \in \mathbb{N}^*$ tel que $nx = 0$, pour tout x dans A . L'entier $k = \inf \{n \in \mathbb{N}^* ; nx = 0, \forall x \in A\}$ est alors appelé la **caractéristique** de A .

5. Produit direct d'anneaux

A. Produit direct de deux anneaux

A_1 et A_2 étant deux anneaux, on considère l'ensemble produit direct

$$A = A_1 \times A_2 = \{(x_1, x_2) ; x_1 \in A_1, x_2 \in A_2\}.$$

On vérifie que A est muni d'une structure d'anneau, grâce à l'addition et à la multiplication respectivement définies par les applications suivantes :

$$\begin{aligned} A \times A &\longrightarrow A \\ ((x_1, x_2), (y_1, y_2)) &\longmapsto (x_1 + y_1, x_2 + y_2). \\ ((x_1, x_2), (y_1, y_2)) &\longmapsto (x_1 y_1, x_2 y_2). \end{aligned}$$

Définition 1.74. L'anneau $A_1 \times A_2$ est appelé **anneau produit direct** des anneaux A_1 et A_2 .

Remarque 1.75. Compte tenu des notations ci-dessus,

a) $A_1 \times A_2$ est unitaire $\iff A_1$ et A_2 sont unitaires.

$(1_{A_1}, 1_{A_2})$ est alors l'élément unité de l'anneau $A_1 \times A_2$.

b) $A_1 \times A_2$ est commutatif $\iff A_1$ et A_2 sont commutatifs.

Remarque 1.76. L'anneau produit direct de deux anneaux n'est jamais intègre. En particulier, l'anneau produit direct de deux corps n'est jamais un corps.

En effet, A_1 et A_2 étant deux anneaux non nuls, soit $x_1 \neq 0$ dans A_1 et $y_2 \neq 0$ dans A_2 ; alors $(x_1, 0)(0, y_2) = (0, 0)$, donc $A_1 \times A_2$ n'est pas intègre.

En particulier, si K_1 et K_2 sont deux corps dont les éléments unités sont, respectivement, 1_{K_1} et 1_{K_2} , alors l'anneau $K_1 \times K_2$ n'est pas intègre, car

$$(1_{K_1}, 0)(0, 1_{K_2}) = (0, 0).$$

Définition 1.77. Au produit direct de deux anneaux A_1 et A_2 , on associe deux couples d'applications :

a) les **projections canoniques** p_1 et p_2 , telles que :

$$\begin{aligned} p_1 : A_1 \times A_2 &\longrightarrow A_1 & \text{et} & & p_2 : A_1 \times A_2 &\longrightarrow A_2 \\ (x_1, x_2) &\longmapsto x_1 & & & (x_1, x_2) &\longmapsto x_2. \end{aligned}$$

b) les **injections canoniques** q_1 et q_2 , telles que :

$$\begin{aligned} q_1 : A_1 &\longrightarrow A_1 \times A_2 & \text{et} & & q_2 : A_2 &\longrightarrow A_1 \times A_2 \\ x_1 &\longmapsto (x_1, 0) & & & x_2 &\longmapsto (0, x_2). \end{aligned}$$

Proposition 1.78. (à vérifier par le lecteur)

1) p_1 et p_2 sont des morphismes surjectifs d'anneaux.

De plus, si les anneaux A_1 et A_2 sont unitaires, alors p_1 et p_2 sont des morphismes d'anneaux unitaires.

2) q_1 et q_2 sont des morphismes injectifs d'anneaux.

3) $p_1 \circ q_1 = id_{A_1}$, $p_2 \circ q_2 = id_{A_2}$.

4) Les restrictions surjectives de q_1 et q_2 , c'est-à-dire les applications :

$$\begin{aligned} A_1 &\longrightarrow A_1 \times (0) = Im q_1 & \text{et} & & A_2 &\longrightarrow (0) \times A_2 = Im q_2 \\ x_1 &\longmapsto (x_1, 0) & & & x_2 &\longmapsto (0, x_2) \end{aligned}$$

sont des isomorphismes d'anneaux ; par suite, l'anneau $A_1 \times A_2$ contient au moins un sous-anneau isomorphe à A_1 et un sous-anneau isomorphe à A_2 .

5) Pour $x = (x_1, x_2) \in A_1 \times A_2$, on peut écrire :

$$x = (p_1(x), p_2(x)) \quad (1.9)$$

$$\text{et } x = q_1(x_1) + q_2(x_2). \quad (1.10)$$

B. Produit direct d'une famille quelconque d'anneaux

Soit I un ensemble non vide, quelconque et $\{A_i\}_{i \in I}$ une famille d'anneaux indexée par I . Comme dans le cas $I = \{1, 2\}$ considéré ci-dessus, on munit

$$A = \prod_{i \in I} A_i = \{(x_i)_{i \in I} ; x_i \in A_i, \forall i \in I\}$$

d'une addition et d'une multiplication, grâce aux applications :

$$\begin{aligned} A \times A &\longrightarrow A \\ ((x_i)_{i \in I}, (y_i)_{i \in I}) &\longmapsto (x_i + y_i)_{i \in I} \\ ((x_i)_{i \in I}, (y_i)_{i \in I}) &\longmapsto (x_i y_i)_{i \in I}. \end{aligned}$$

On vérifie que, relativement à ces deux lois de composition, A est un anneau.

Définition 1.79. L'anneau $A = \prod_{i \in I} A_i$ est appelé **anneau produit direct** des anneaux A_i , $i \in I$.

Pour tout $j \in I$, on définit :

a) la **projection canonique** :

$$\begin{aligned} p_j : \prod_{i \in I} A_i &\longrightarrow A_j \\ (x_i)_{i \in I} &\longmapsto x_j. \end{aligned}$$

b) l'**injection canonique** :

$$q_j : A_j \longrightarrow \prod_{i \in I} A_i,$$

telle que pour tout $x_j \in A_j$, $q_j(x_j) = (x_i)_{i \in I}$, où $x_i = 0$, si $i \neq j$.

Remarque 1.80. Pour tout $i \in I$, la projection (resp. l'injection) canonique p_i (resp. q_i) est un morphisme surjectif (resp. injectif) d'anneaux.

Comme dans la proposition 1.78., pour tout $i \in I$, on a

$$p_i \circ q_i = id_{A_i}, \quad Im q_i \simeq A_i \quad \text{et} \quad \forall x \in \prod_{i \in I} A_i, \quad x = (p_i(x))_{i \in I}.$$

Cette dernière relation généralise le relation (1.9). Par contre, la relation (1.10) ne peut être généralisée que dans le cas où l'ensemble non vide I est fini, puisque dans le groupe $(A, +)$, seule la somme d'un nombre fini d'éléments a un sens. Ainsi pour $I = \{1, 2, \dots, n\}$, $n \in \mathbb{N}^*$ et $x = (x_1, x_2, \dots, x_n) \in \prod_{1 \leq i \leq n} A_i$, on a

$$x = \sum_{1 \leq i \leq n} q_i(x_i). \quad (1.11)$$

C. Propriété universelle du produit direct d'anneaux

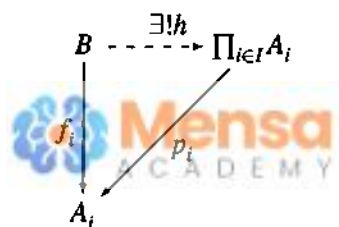
Théorème 1.81. Soit I un ensemble non vide, $\{A_i\}_{i \in I}$ une famille d'anneaux et $\{p_i\}_{i \in I}$ la famille des projections canoniques associées à l'anneau produit direct $\prod_{i \in I} A_i$.

Etant donné un anneau B , alors quelle que soit la famille $\{f_i\}_{i \in I}$ de morphismes d'anneaux telle que, pour tout $i \in I$, $f_i \in \text{Hom}(B, A_i)$, il existe un unique morphisme $h \in \text{Hom}(B, \prod_{i \in I} A_i)$ vérifiant :

$$p_i \circ h = f_i, \text{ quel que soit } i \in I.$$

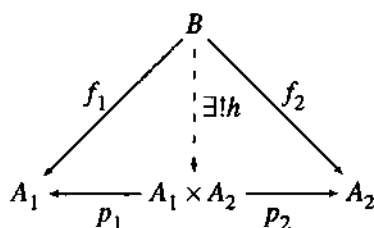
La démonstration de ce résultat se fait exactement comme dans le cas des groupes ([11], Th. 1.91.).

Remarque 1.82. La propriété universelle (Th. 1.81.) exprime que pour tout $i \in I$, le diagramme suivant commute :



$$\text{et } p_i \circ h = f_i, \forall i \in I \iff h(x) = (f_i(x))_{i \in I}, \forall x \in B.$$

Dans le cas où $I = \{1, 2\}$, la propriété universelle se traduit par le diagramme commutatif :



$$\text{donc } p_1 \circ h = f_1, p_2 \circ h = f_2 \quad \text{et} \quad h(x) = (f_1(x), f_2(x)), \quad \forall x \in B.$$

6. Exercices

- 1) Soit G un groupe additif abélien, non réduit à $\{0\}$. On définit dans G une multiplication par l'application :

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\longmapsto 0. \end{aligned}$$

Vérifier que G est alors muni d'une structure d'anneau.
Cet anneau est-il commutatif ? est-il unitaire ?

- 2) Soit A un anneau unitaire, commutatif et $a_1, a_2, \dots, a_s$ des éléments de A , $s \geq 2$ dans $\mathbb{N}$.
Démontrer que pour tout entier $n \geq 2$, on a :

$$(a_1 + a_2 + \dots + a_s)^n = \sum \frac{n!}{i_1! i_2! \dots i_s!} a_1^{i_1} a_2^{i_2} \dots a_s^{i_s},$$

où la somme $\sum$ est prise pour tous les s -uplets $(i_1, i_2, \dots, i_s) \in \mathbb{N}^s$ tels que $i_1 + i_2 + \dots + i_s = n$
(Faire une récurrence sur s).

- 3) On pose :

$$\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\},$$

$$\mathbb{Q}[i\sqrt{5}] = \{p + iq\sqrt{5}; (p, q) \in \mathbb{Q} \times \mathbb{Q}\},$$

où $i^2 = -1$ dans le corps des nombres complexes $\mathbb{C}$.

Vérifier que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau unitaire de $\mathbb{C}$ et que $\mathbb{Q}[i\sqrt{5}]$ est un sous-corps de $\mathbb{C}$.

- 4) Soit deux anneaux A, B et $f \in \text{Hom}(A, B)$. On suppose A unitaire, B intègre et $f \neq 0$. Démontrer que $f(1_A)$ est élément unité de B .

- 5) *Plongement d'un anneau non nul et non nécessairement unitaire A dans un anneau unitaire B .*

1°) On suppose A de caractéristique 0. On considère le groupe additif abélien :

$$B = A \oplus \mathbb{Z}.$$

On rappelle ([11], Ch. VIII) que $B = \{(a, m); a \in A, m \in \mathbb{Z}\}$

et que l'addition dans B est telle que :

$$(a, m) + (b, n) = (a + b, m + n), \quad \forall ((a, m), (b, n)) \in B \times B.$$

On définit dans B , une "multiplication" par l'application :

$$\begin{aligned} B \times B &\longrightarrow B \\ ((a, m), (b, n)) &\longmapsto (ab + na + mb, mn). \end{aligned}$$

- Prouver que B est ainsi muni d'une structure d'anneau unitaire, de caractéristique 0.

- Montrer que B est commutatif, si et seulement si A est commutatif.

- Vérifier que

$$\begin{aligned} f : A &\longrightarrow B \\ a &\longmapsto (a, 0) \end{aligned}$$

est un "plongement" de A dans B , c'est-à-dire un morphisme injectif d'anneaux.

2°) On suppose A de caractéristique $k \neq 0$. On considère le groupe additif abélien

$$B = A \oplus \mathbb{Z}/k\mathbb{Z}.$$

On note $\overline{m}$ la classe modulo $k\mathbb{Z}$ d'un entier $m \in \mathbb{Z}$.

- Démontrer que la correspondance :

$$\begin{aligned} \mu : B \times B &\longrightarrow B \\ ((a, \overline{m}), (b, \overline{n})) &\longmapsto (ab + na + mb, \overline{mn}) \end{aligned}$$

définit une loi de composition interne dans B , que l'on appellera "multiplication". Il faut vérifier que

$$(\overline{m'} = \overline{m} \text{ et } \overline{n'} = \overline{n}) \implies \mu((a, \overline{m'}), (b, \overline{n'})) = \mu((a, \overline{m}), (b, \overline{n})).$$

- Montrer que B est alors muni d'une structure d'anneau unitaire, de caractéristique k et qu'il existe, comme dans le 1°, un plongement de l'anneau A dans l'anneau B .

3°) f désignant le plongement de A dans B (défini dans le 1°) ou le 2°), vérifier que si A est unitaire, on a $f(1_A) \neq 1_B$; autrement dit f n'est pas un morphisme d'anneaux unitaires (Déf. 1.51.).

6) Soit $\mathbb{Z}$ l'anneau des entiers.

1°) On note $\text{End}(\mathbb{Z}, +)$ l'anneau des endomorphismes du groupe additif abélien $(\mathbb{Z}, +)$ (Exemple 1.15.).

A tout $k \in \mathbb{Z}$, on associe l'application

$$\begin{aligned} f_k : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto kx \end{aligned}$$

a) Vérifier que $f_k \in \text{End}(\mathbb{Z}, +)$.

b) Montrer que quel que soit $g \in \text{End}(\mathbb{Z}, +)$, il existe un unique $k \in \mathbb{Z}$ tel que $g = f_k$.

c) Démontrer que l'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \text{End}(\mathbb{Z}, +) \\ k &\longmapsto f_k \end{aligned}$$

est un isomorphisme d'anneaux unitaires.

2°) Pour $n > 1$ dans $\mathbb{Z}$, on considère l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n (Exemple 1.12), ainsi que l'anneau $\text{End}(\mathbb{Z}/n\mathbb{Z}, +)$ des endomorphismes du groupe abélien $(\mathbb{Z}/n\mathbb{Z}, +)$.

A tout $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$, on associe la correspondance



$$\begin{aligned} f_{\bar{k}} : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \bar{x} &\longmapsto \bar{k}\bar{x} \end{aligned}$$

a) Démontrer que $f_{\bar{k}}$ est une application, c'est-à-dire est indépendante du représentant de l'élément $\bar{k}$ et prouver que $f_{\bar{k}} \in \text{End}(\mathbb{Z}/n\mathbb{Z}, +)$.

b) Montrer que

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \text{End}(\mathbb{Z}/n\mathbb{Z}, +) \\ \bar{k} &\longmapsto f_{\bar{k}} \end{aligned}$$

est un isomorphisme d'anneaux unitaires.

3°) A étant un anneau unitaire quelconque, on considère l'anneau $\text{End}(A, +)$ des endomorphismes du groupe abélien $(A, +)$.

A tout $a \in A$, on associe l'application

$$\begin{aligned} f_a : A &\longrightarrow A \\ x &\longmapsto ax. \end{aligned}$$

a) Vérifier que $f_a \in \text{End}(A, +)$.

b) Montrer que

$$\begin{aligned} f : A &\longrightarrow \text{End}(A, +) \\ a &\longmapsto f_a \end{aligned}$$

est un morphisme injectif d'anneaux unitaires.

Quelle conclusion générale peut-on en déduire ?

- 7) On considère l'anneau $M_2(\mathbb{R})$ des matrices carrées d'ordre 2 sur le corps des nombres réels $\mathbb{R}$. On pose :

$$A = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} ; (x, y) \in \mathbb{R} \times \mathbb{R} \right\},$$

$$B = \left\{ \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} ; x \in \mathbb{R} \right\} \quad \text{et} \quad C = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} ; x \in \mathbb{R} \right\}.$$

1°) Vérifier que A, B, C sont des sous-anneaux de $M_2(\mathbb{R})$.

Sont-ils commutatifs ? Sont-ils unitaires ? (préciser, le cas échéant, l'élément unité).

2°) Montrer que l'anneau A a une infinité d'éléments unités à gauche et aucun élément unité à droite.

3°) Prouver que B et C sont des corps isomorphes à $\mathbb{R}$.

- 8) Dans l'anneau $M_2(\mathbb{Q})$ des matrices carrées d'ordre 2 sur le corps des nombres rationnels $\mathbb{Q}$, on considère l'ensemble, noté $M_2(\mathbb{Z})$, des matrices à coefficients dans l'anneau des entiers $\mathbb{Z}$.

1°) Vérifier que $M_2(\mathbb{Z})$ est un sous-anneau unitaire de $M_2(\mathbb{Q})$.

2°) Pour tout $n \in \mathbb{Z}$, on pose $M(n) = \begin{pmatrix} n & 0 \\ 2n & 0 \end{pmatrix}$.

-Montrer que $A = \{M(n) ; n \in \mathbb{Z}\}$ est un sous-anneau de $M_2(\mathbb{Z})$, isomorphe à $\mathbb{Z}$ (ne contenant pas la matrice unité de $M_2(\mathbb{Z})$).

-Trouver d'autres sous-anneaux de $M_2(\mathbb{Z})$, isomorphes à $\mathbb{Z}$.

- 9) A étant un anneau non nul et $\mathbb{Q}$ le corps des nombres rationnels, soit f et g deux morphismes (d'anneaux) non nuls de $\mathbb{Q}$ dans A .

On note respectivement, $f|_{\mathbb{Z}}$ et $g|_{\mathbb{Z}}$ les restrictions de f et g à l'anneau des entiers $\mathbb{Z}$.

Démontrer que

$$f|_{\mathbb{Z}} = g|_{\mathbb{Z}} \implies f = g.$$

- 10) Soit A un anneau non nul ; on suppose que pour tout $a \neq 0$ dans A , il existe un unique $b \in A$ tel que

$$a = aba.$$

Démontrer les propriétés suivantes :

i) A est intègre.

ii) Pour a et b dans A : $a = aba \implies b = bab$.

iii) A est unitaire.

iv) A est un anneau à division (ou corps gauche).

- 11) Soit $Z(A)$ le centre d'un anneau non nul A (Déf. 1.32.). On suppose que pour tout $x \in A$, on a : $(x^2 - x) \in Z(A)$.

Prouver que, quel que soit $(x, y) \in A \times A$, on a $(xy + yx) \in Z(A)$.

En déduire que l'anneau A est commutatif.

- 12) A étant un anneau non nul, vérifier les propriétés suivantes.

1°) Si x est un élément non nul et *idempotent* de A (Déf. 1.28.), alors x n'est pas *nilpotent* dans A (Déf. 1.26.).

2°) Si A est unitaire et intègre, alors 0 et 1 sont les seuls éléments idempotents de A .

13) Soit A un anneau unitaire, *commutatif*.

1°) Montrer que pour a et b dans A on a :

$$(a \text{ et } b \text{ nilpotents}) \implies a + b \text{ nilpotent.}$$

2°) En considérant, dans l'anneau de matrices $M_2(\mathbb{R})$, les éléments :

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix},$$

montrer que la propriété du 1°) n'est plus vraie dans un anneau *non commutatif*.

14) Dans l'anneau $\mathbb{R}^{[0,1]}$ (Exemple 1.18.), on considère le sous-anneau A des fonctions réelles *continues* sur $[0, 1]$ (Exemple 1.31., 5)).

1°) Soit f et g dans A , tels que :

$$f(x) = \begin{cases} 0 & \text{si } 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \text{si } \frac{1}{2} < x \leq 1 \end{cases}, \quad g(x) = \begin{cases} -x + \frac{1}{2} & \text{si } 0 \leq x \leq \frac{1}{2} \\ 0 & \text{si } \frac{1}{2} < x \leq 1. \end{cases}$$

Montrer que f et g sont des diviseurs de 0 dans A .

2°) Démontrer qu'un élément $h \in A$ est un diviseur de 0 dans A , si et seulement si l'ensemble des $x \in [0, 1]$, tels que $h(x) = 0$, contient un intervalle ouvert.

3°) Déterminer les éléments *idempotents*, les éléments *nilpotents* et les éléments *inversibles* de A .

15) Soit E un ensemble non vide et $S = \mathcal{P}(E)$, l'ensemble des parties de E .

Pour A et B dans S , on pose $A \setminus B = \{a \in A; a \notin B\}$.

On définit, dans S , deux lois de composition internes, notées respectivement additivement et multiplicativement, telles que :

$$\begin{aligned} S \times S &: \longrightarrow S \\ (A, B) &\longmapsto A + B := (A \setminus B) \cup (B \setminus A) \\ (A, B) &\longmapsto AB := A \cap B. \end{aligned}$$

1°) Montrer que S est ainsi muni d'une structure d'anneau commutatif et unitaire ; préciser l'élément neutre de l'addition et l'élément unité.

Vérifier que l'anneau S est de caractéristique 2 et que tout élément de S est idempotent.

S est appelé l'**anneau de Boole** des parties de E .

2°) On suppose l'ensemble E de *cardinal infini*. Soit $T = \mathcal{F}(E)$, l'ensemble des parties *finies* de E .

a) Montrer que T est un sous-anneau de S .

b) Vérifier que T n'est pas unitaire et que tout élément "non nul" de T est un diviseur de zéro dans T .

c) Prouver que dans l'anneau S , tout élément "non nul" et différent de l'élément unité est un diviseur de zéro.

16) Soit A, B deux anneaux et f une application de A dans B .

1°) On dit que f est un **monomorphisme d'anneaux** de A dans B , si $f \in \text{Hom}(A, B)$ et si pour tout anneau R , on a :

$$(u \text{ et } v \text{ dans } \text{Hom}(R, A) \quad \text{et} \quad f \circ u = f \circ v) \implies u = v.$$

a) Montrer que si un morphisme $f \in \text{Hom}(A, B)$ est *injectif*, alors c'est un monomorphisme de A dans B .

b) Réciproquement, on suppose que f est un monomorphisme d'anneaux de A dans B . Soit x et x' dans A , vérifiant : $f(x) = f(x')$.

En utilisant les morphismes d'anneaux u et v de $\mathbb{Z}$ dans A , tels que :

$$u : n \longmapsto x^n \quad \text{et} \quad v : n \longmapsto x'^n,$$

démontrer que f est injectif.

2°) On dit qu'une application f est un **épimorphisme d'anneaux** de A dans B , si $f \in \text{Hom}(A, B)$ et si pour tout anneau R , on a :

$$(u \text{ et } v \text{ dans } \text{Hom}(B, R) \quad \text{et} \quad u \circ f = v \circ f) \implies u = v.$$

a) Prouver que si $f \in \text{Hom}(A, B)$ est *surjectif*, alors c'est un épimorphisme de A dans B .

b) Soit j l'injection canonique de $\mathbb{Z}$ dans $\mathbb{Q}$ et R un *domaine d'intégrité* (Déf. 1.21.). Soit u et v deux morphismes d'anneaux unitaires de $\mathbb{Q}$ dans R tels que : $u \circ j = v \circ j$.

Démontrer que j est un épimorphisme de $\mathbb{Z}$ dans $\mathbb{Q}$.

Quelle conclusion peut-on tirer des résultats ci-dessus ? (Conclusion que l'on pourra comparer à celle obtenue dans le cas des morphismes de groupes (Cf. [11], Prop. 1.80)).



Chapitre 2

Idéaux d'un anneau

La notion d'idéal à gauche (resp. à droite, bilatère) a été introduite dans le Chapitre 1 (Déf.1.42.).

1. Idéal engendré par une partie d'un anneau

Définition 2.1. Soit S une partie **non vide** d'un anneau A . On appelle **idéal à gauche** de A **engendré par S** , l'intersection de tous les idéaux à gauche de A contenant S . On définit de même l'**idéal à droite** (resp. **bilatère**) de A engendré par S .

On notera, respectivement, $(S)_g, (S)_d$ et (S) les idéaux à gauche, à droite et bilatère de A , engendrés par S .

Remarque 2.2. D'après la définition (2.1.), $(S)_g$ (resp. $(S)_d, (S)$) est (relativement à l'inclusion) le plus petit idéal à gauche (resp. à droite, bilatère) de A contenant S .

Proposition 2.3. Soit A un anneau unitaire et S une partie non vide de A , alors :

$$(S)_g = \{ \sum_{1 \leq i \leq m} a_i x_i ; m \in \mathbb{N}^*, \forall i (1 \leq i \leq m), a_i \in A, x_i \in S \}$$

$$(S)_d = \{ \sum_{1 \leq i \leq m} x_i a_i ; m \in \mathbb{N}^*, \forall i (1 \leq i \leq m), a_i \in A, x_i \in S \}$$

$$(S) = \{ \sum_{1 \leq i \leq m} a_i x_i b_i ; m \in \mathbb{N}^*, \forall i (1 \leq i \leq m), (a_i, b_i) \in A \times A, x_i \in S \}.$$

Preuve : Démontrons, par exemple, la première égalité ; désignons par L son second membre. On vérifie aisément que L est un idéal à gauche de A et que $S \subseteq L$; or, $(S)_g$ est le plus petit idéal à gauche de A contenant S , d'où : $(S)_g \subseteq L$.

D'autre part, tout idéal à gauche de A contenant S , contient nécessairement tous les éléments de L , on a donc $L \subseteq (S)_g$ et par suite $(S)_g = L$. □

Remarque 2.4. L'anneau A étant unitaire, si $S = \{x_1, x_2, \dots, x_n\}$, $n \in \mathbb{N}^*$, alors,

$$(S)_g = \{ \sum_{1 \leq i \leq n} a_i x_i ; \forall i (1 \leq i \leq n), a_i \in A \};$$

les éléments des idéaux $(S)_d$ et (S) s'écrivent de façon analogue.

Cas particulier : $S = \{x\}$, où $x \in A$:

$$(x)_g = \{ax ; a \in A\} \text{ est noté : } Ax$$

$$(x)_d = \{xa ; a \in A\} \text{ est noté : } xA$$

$$(x) = \{ \sum_{1 \leq i \leq m} a_i x b_i ; m \in \mathbb{N}^*, \forall i (1 \leq i \leq m), (a_i, b_i) \in A \times A \}.$$

Définition 2.5. Soit I un idéal à gauche (resp. à droite, bilatère) d'un anneau A ,

a) I est dit **principal** s'il est engendré par un seul élément.

b) I est dit **de type fini** s'il est engendré par un nombre fini d'éléments.

Remarque 2.6. :

a) Dans tout anneau unitaire A , les idéaux bilatères (0) et A sont principaux (*l'idéal A est engendré par 1_A*).

b) Dans l'anneau $\mathbb{Z}$, tout idéal est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$, donc tout idéal est principal (Cf. App. A).

Définition 2.7. : a) On appellera **anneau principal**, tout anneau unitaire, commutatif, dans lequel tout idéal est principal.

b) On appellera **domaine principal**, tout domaine d'intégrité (Déf. 1.21) dans lequel tout idéal est principal.

$\mathbb{Z}$ est le premier exemple de domaine principal (Cf. App. A).

Remarque 2.8. Dans certains ouvrages, ce que nous appelons *domaine principal* est appelé *anneau principal*.

2. Opérations sur les idéaux d'un anneau

A. Intersection, réunion d'idéaux

Proposition 2.9. Soit $\{I_\lambda\}_{\lambda \in \Lambda}$ une famille non vide d'idéaux à gauche (resp. à droite, bilatères) d'un anneau A , alors $I = \bigcap_{\lambda \in \Lambda} I_\lambda$ est un idéal à gauche (resp. à droite, bilatère) de A .

Vérification laissée au lecteur.

Remarque 2.10. Les hypothèses étant celles de la proposition précédente, $\bigcup_{\lambda \in \Lambda} I_\lambda$ n'est pas, en général, un idéal à gauche (resp. à droite, bilatère) de A (Rem. 1.36.). On a cependant le résultat suivant :

Proposition 2.11. Si dans un anneau A , $\{I_\lambda\}_{\lambda \in \Lambda}$ est une famille non vide d'idéaux à gauche (resp. à droite, bilatères) totalement ordonnée par l'inclusion, alors $\bigcup_{\lambda \in \Lambda} I_\lambda$ est un idéal à gauche (resp. à droite, bilatère) de A .

La preuve est la même que pour les sous-anneaux (Prop. 1.37.).

B. Somme d'idéaux dans un anneau unitaire

1. Cas d'une famille finie d'idéaux

Soit $\{I_i\}_{1 \leq i \leq n}$, $n \in \mathbb{N}^*$, une famille finie d'idéaux à gauche (resp. à droite, bilatères) d'un anneau A . On pose

$$\sum_{1 \leq i \leq n} I_i = \{ \sum_{1 \leq i \leq n} x_i ; \forall i (1 \leq i \leq n), x_i \in I_i \}. \quad (2.1)$$

On vérifie facilement que $\sum_{1 \leq i \leq n} I_i$ est un idéal à gauche (resp. à droite, bilatère) de A .

Définition 2.12. L'idéal $\sum_{1 \leq i \leq n} I_i$ défini par la rel. (2.1) est appelé **somme des idéaux à gauche** (resp. à droite, bilatères) I_i , $(1 \leq i \leq n)$.

On pourra écrire $\sum_{1 \leq i \leq n} I_i = I_1 + I_2 + \dots + I_n$.

Proposition 2.13. Soit $\{I_i\}_{1 \leq i \leq n}$ une famille finie d'idéaux à gauche (resp. à droite, bilatères) d'un anneau unitaire A ; $\sum_{1 \leq i \leq n} I_i$ est alors l'idéal à gauche (resp. à droite, bilatère) de A engendré par $\bigcup_{1 \leq i \leq n} I_i$.

Preuve : Démontrons la propriété dans le cas des idéaux à gauche et supposons $n = 2$. Notons $(I_1 \cup I_2)$ l'idéal à gauche de A , engendré par $I_1 \cup I_2$.

$$I_1 + I_2 = \{x_1 + x_2; x_1 \in I_1, x_2 \in I_2\} \text{ implique}$$

$$I_1 + I_2 \subseteq (I_1 \cup I_2). \quad (2.2)$$

$$(I_1 \cup I_2) = \{\sum_{1 \leq j \leq m} a_j x_j; m \in \mathbb{N}^*, \forall j (1 \leq j \leq m), a_j \in A, x_j \in I_1 \cup I_2\}.$$

Dans l'expression ci-dessus m décrit $\mathbb{N}^*$, par suite, tout $z \in (I_1 \cup I_2)$ peut s'écrire sous la forme :

$$z = \sum_{1 \leq j \leq m_1} a_j x_j + \sum_{1 \leq k \leq m_2} b_k x_k, \text{ où}$$

$$\forall m \in \mathbb{N}^*, (m_1, m_2) \in \mathbb{N}^* \times \mathbb{N}^*, 1 \leq m_1 \leq m, 1 \leq m_2 \leq m, \text{ et}$$

$$\forall j (1 \leq j \leq m_1), a_j \in A, x_j \in I_1, \quad \forall k (1 \leq k \leq m_2), b_k \in A, x_k \in I_2.$$

On en déduit que $z = z_1 + z_2$, où $z_1 \in I_1$ et $z_2 \in I_2$, d'où

$$(I_1 \cup I_2) \subseteq I_1 + I_2; \quad (2.3)$$

Les inclusions (2.2) et (2.3) impliquent $I_1 + I_2 = (I_1 \cup I_2)$.

Pour $n \geq 2$, on démontre la propriété par récurrence sur n . □

Remarque 2.14. Les hypothèses étant celles de la proposition 2.13., quelque que soit $j (1 \leq j \leq n)$, on a

$$I_j \subseteq \sum_{1 \leq i \leq n} I_i.$$

2. Cas d'une famille quelconque d'idéaux

Soit A un anneau unitaire et $\{I_\lambda\}_{\lambda \in \Lambda}$ une famille d'idéaux à gauche (resp. à droite, bilatères) de A , Λ étant un ensemble non vide quelconque, donc éventuellement infini. On définit l'ensemble

$$\sum_{\lambda \in \Lambda} I_\lambda = \{\sum_{1 \leq j \leq m} x_{\lambda_j}; m \in \mathbb{N}^*, \forall j (1 \leq j \leq m), \lambda_j \in \Lambda, x_{\lambda_j} \in I_{\lambda_j}\}.$$

La proposition 2.13. se généralise comme suit :

Proposition 2.15. *Compte-tenu des hypothèses ci-dessus, $\sum_{\lambda \in \Lambda} I_\lambda$ est l'idéal à gauche (resp. à droite, bilatère) de A engendré par $\bigcup_{\lambda \in \Lambda} I_\lambda$; il est appelé somme des idéaux à gauche (resp. à droite, bilatères) $I_\lambda, \lambda \in \Lambda$.*

Remarque 2.16. Avec les notations précédentes :

a) Pour tout $\mu \in \Lambda$, on a $I_\mu \subseteq \sum_{\lambda \in \Lambda} I_\lambda$.

b) Si Λ est de cardinal infini, alors $x \in \sum_{\lambda \in \Lambda} I_\lambda$ si et seulement si il existe une partie finie $\{\lambda_j; 1 \leq j \leq m\}$ de $\Lambda, m \in \mathbb{N}^*$, telle que $x \in \sum_{1 \leq j \leq m} I_{\lambda_j}$.

On pourra cependant écrire, d'une façon générale,

$$x = \sum_{\lambda \in \Lambda} x_\lambda,$$

où il est entendu que les $x_\lambda \in I_\lambda$ sont "presque tous nuls", c'est-à-dire "nuls, sauf un nombre fini d'entre eux".

3. Somme directe d'idéaux

Définition 2.17. $\{I_\lambda\}_{\lambda \in \Lambda}$ étant une famille non vide d'idéaux à gauche (resp. à droite, bilatères) d'un anneau unitaire A , on dit que $\sum_{\lambda \in \Lambda} I_\lambda$ est **somme directe** des $I_\lambda, \lambda \in \Lambda$, si tout $x \in \sum_{\lambda \in \Lambda} I_\lambda$ s'écrit de façon unique

$$x = \sum_{1 \leq j \leq m} x_{\lambda_j}, \text{ où } m \in \mathbb{N}^*, \forall j (1 \leq j \leq m), \lambda_j \in \Lambda \text{ et } x_{\lambda_j} \in I_{\lambda_j}.$$

Dans ce cas $\sum_{\lambda \in \Lambda} I_\lambda$ est noté $\bigoplus_{\lambda \in \Lambda} I_\lambda$.

Proposition 2.18. Les hypothèses étant celles de la définition 2.17., les conditions suivantes sont équivalentes :

- 1) La somme $\sum_{\lambda \in \Lambda} I_\lambda$ est directe.
- 2) $\sum_{\lambda \in \Lambda} x_\lambda = 0 \implies \forall \lambda \in \Lambda, x_\lambda = 0$.
- 3) $\forall \mu \in \Lambda, I_\mu \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} I_\lambda = (0)$.

Preuve :

1) $\implies$ 2) : Si la somme $\sum_{\lambda \in \Lambda} I_\lambda$ est directe, alors 0 s'écrit de façon unique, $\sum_{\lambda \in \Lambda} x_\lambda$, d'où $x_\lambda = 0$, quel que soit $\lambda \in \Lambda$.

2) $\implies$ 3) : Soit $x \in I_\mu \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} I_\lambda$; si $x \neq 0$, on peut écrire

$$x = x_\mu = \sum_{1 \leq j \leq m} x_{\lambda_j}, \text{ où } m \in \mathbb{N}^* \text{ et } \forall j (1 \leq j \leq m), \lambda_j \in \Lambda \setminus \{\mu\};$$

par suite, $x_\mu - \sum_{1 \leq j \leq m} x_{\lambda_j} = 0$. L'hypothèse 2) implique alors : $x_\mu = 0$, donc $x = 0$.

3) $\implies$ 1) : Supposons $x \in \sum_{\lambda \in \Lambda} I_\lambda$ tel que

$$x = \sum_{\lambda \in \Lambda} x_\lambda = \sum_{\lambda \in \Lambda} y_\lambda, \quad (2.4)$$

où les x_λ et les y_λ sont presque tous nuls dans I_λ .

S'il existe $\mu \in \Lambda$ tel que $x_\mu \neq y_\mu$, on obtient, à partir des égalités (2.4) :

$$x_\mu - y_\mu = \sum_{\lambda \in \Lambda \setminus \{\mu\}} (y_\lambda - x_\lambda);$$

l'hypothèse 3) implique alors $x_\mu - y_\mu = 0$, d'où une contradiction. On en conclut que dans (2.4), quel que soit $\lambda \in \Lambda, x_\lambda = y_\lambda$. $\square$

C. Produit d'idéaux dans un anneau unitaire

1. Cas de deux idéaux

Définition 2.19. Soit I_1, I_2 deux idéaux à gauche (resp. à droite, bilatères) d'un anneau unitaire A . L'idéal à gauche (resp. à droite, bilatère) engendré par l'ensemble

$$S = \{x_1 x_2; x_1 \in I_1, x_2 \in I_2\}$$

est noté $I_1 I_2$ et appelé **produit des idéaux** à gauche (resp. à droite, bilatères) I_1 et I_2 (pris dans cet ordre).

Proposition 2.20. Avec les hypothèses de la définition 2.19., on a

$$x \in I_1 I_2 \iff x = \sum_{\text{finie}} x_{i_1} x_{i_2}; x_{i_1} \in I_1, x_{i_2} \in I_2. \quad (2.5)$$

La relation (2.5) se déduit de la prop. 2.3.; elle exprime que $x \in I_1 I_2$ si et seulement s'il existe deux parties finies non vides N_1, N_2 de $\mathbb{N}$ telles que

$$x = \sum_{(i_1, i_2) \in N_1 \times N_2} x_{i_1} x_{i_2}, \text{ où } \forall (i_1, i_2) \in N_1 \times N_2, x_{i_1} \in I_1, x_{i_2} \in I_2.$$

Proposition 2.21. Dans un anneau unitaire A :

- 1) L_1, L_2 idéaux à gauche $\implies L_1 L_2 \subseteq L_2$ et $L_2 L_1 \subseteq L_1$.
- 2) R_1, R_2 idéaux à droite $\implies R_1 R_2 \subseteq R_1$ et $R_2 R_1 \subseteq R_2$.
- 3) I_1, I_2 idéaux bilatères $\implies I_1 I_2 \subseteq I_1 \cap I_2$ et $I_2 I_1 \subseteq I_1 \cap I_2$.

Preuve : Dans le cas des idéaux à gauche par exemple, $L_1 L_2$ est engendré par l'ensemble S des produits $x_1 x_2$, où $x_1 \in L_1$ et $x_2 \in L_2$; or, L_2 est un idéal à gauche de A , d'où $S \subseteq L_2$; par suite $L_1 L_2 \subseteq L_2$.

On a de même $L_2 L_1 \subseteq L_1$. □

2. Cas d'un nombre fini quelconque d'idéaux

La définition 2.19., ainsi que les propositions 2.20. et 2.21. se généralisent, de façon naturelle, à un nombre fini quelconque n d'idéaux à gauche (resp. à droite, bilatères) d'un anneau unitaire A .

Si l'on considère, par exemple, une famille finie $L_1, L_2, \dots, L_n$, d'idéaux à gauche de A , alors l'idéal à gauche engendré par l'ensemble

$$S = \{x_1 x_2 \cdots x_n; \forall i (1 \leq i \leq n), x_i \in L_i\}$$

est noté $L_1 L_2 \cdots L_n$ et appelé **produit des idéaux à gauche** $L_1, L_2, \dots, L_n$ (pris dans cet ordre). On a :

$$L_1 L_2 \cdots L_n = \{\sum_{\text{finie}} x_{i_1} x_{i_2} \cdots x_{i_n}; \forall j (1 \leq j \leq n), x_{i_j} \in L_j\}$$

et $L_1 L_2 \cdots L_n \subseteq L_2 L_3 \cdots L_n \subseteq \cdots \subseteq L_n$.

En particulier, si I est un idéal à gauche (resp. à droite, bilatère) de A , pour tout $n \in \mathbb{N}$, on note I^n l'idéal à gauche (resp. à droite, bilatère) de A engendré par l'ensemble

$$S = \{x_1 x_2 \cdots x_n; \forall i (1 \leq i \leq n), x_i \in I\}.$$

On a $I^1 = I$ et $\forall n \in \mathbb{N}^*, I^n \subseteq I$.

D. Propriétés des opérations sur les idéaux

Désignons par $\mathcal{J}_g$ (resp. $\mathcal{J}_d, \mathcal{J}$) l'ensemble des idéaux à gauche (resp. à droite, bilatères) d'un anneau unitaire A .

L'étude faite dans les paragraphes précédents montre que l'intersection, la somme et le produit des idéaux définissent des lois de composition dans les ensembles $\mathcal{J}_g, \mathcal{J}_d, \mathcal{J}$; ces lois vérifient les propriétés suivantes :

Proposition 2.22. A étant un anneau unitaire, quels que soient I, J, K , dans $\mathcal{J}_g$ (resp. $\mathcal{J}_d, \mathcal{J}$), on a

- 1) $I \cap J = J \cap I$ et $I + J = J + I$.
- 2) $I \cap (J \cap K) = (I \cap J) \cap K$.
- 3) $I + (J + K) = (I + J) + K$.
- 4) $I(JK) = (IJ)K$.
- 5) $I(J + K) = IJ + IK$ et $(I + J)K = IK + JK$.

Démonstration proposée en exercice (n°3, Ch. 2).

Remarque 2.23. :

a) La proposition 2.22. exprime que dans $\mathcal{J}_g$ (resp. $\mathcal{J}_d, \mathcal{J}$), les opérations "intersection" et "somme" sont *commutatives* [Cf. 1)] et *associatives* [Cf. 2) et 3)]; le "produit" est *associatif* [Cf. 4)] et *distributif* à droite et à gauche par rapport à la "somme" [Cf. 5)].

Le "produit" des idéaux n'est commutatif que si l'anneau A est commutatif.

b) L'associativité du produit des idéaux implique que pour tout idéal à gauche, à droite ou bilatère, I de A et tout $n > 1$ dans $\mathbb{N}$, l'idéal I^n est défini inductivement par

$$I^n = II^{n-1} = I^{n-1}I.$$

Proposition 2.24. *A étant un anneau unitaire, pour $x \in A$, notons respectivement Ax , xA et (x) , les idéaux à gauche, à droite et bilatère engendrés par x , on a alors, quels que soient x et y dans A :*

$$Axy \subseteq Ax Ay; \quad xyA \subseteq xAyA; \quad (xy) \subseteq (x)(y). \quad (2.6)$$

$$(xy) = (x)(y) \iff A \text{ est commutatif.} \quad (2.7)$$

Preuve : L'anneau A étant unitaire, on a $xy \in Ax Ay$ et $xy \in xAyA$, d'où les inclusions (2.6). Si l'anneau A est commutatif, alors tout $z \in (x)(y)$ s'écrit $z = axby$, où $(a, b) \in A \times A$, d'où $z = abxy \in (xy)$.

Si l'anneau A n'est pas commutatif, un élément de l'idéal bilatère $(x)(y)$ n'appartient pas nécessairement à l'idéal bilatère (xy) (voir un exemple dans $M_2(\mathbb{C})$); on en déduit l'équivalence (2.7). $\square$

3. Anneaux Quotients

A. Notion d'anneau quotient

On suppose connues la propriété de compatibilité d'une relation d'équivalence avec une loi de composition, ainsi que la notion de loi de composition quotient ([11], p. 80).

Proposition 2.25. *A étant un anneau, soit I un sous-groupe du groupe $(A, +)$; alors, la relation d'équivalence $\mathcal{R}_I$, associée à I dans le groupe abélien $(A, +)$, est compatible avec la multiplication de l'anneau A , si et seulement si I est un idéal bilatère de A .*

Preuve : On rappelle ([11], Ch. II) que la relation d'équivalence $\mathcal{R}_I$ est définie dans A par

$$x \mathcal{R}_I y \iff (x - y) \in I \quad (2.8)$$

et qu'elle est compatible avec l'addition de l'anneau A .

Si I est un idéal bilatère de A , alors

$$(x - x') \in I \text{ et } (y - y') \in I \implies xy - x'y' = [x(y - y') + (x - x')y'] \in I;$$

par suite, $\mathcal{R}_I$ est compatible avec la multiplication de l'anneau A .

Réciproquement, supposons la relation $\mathcal{R}_I$ compatible avec la multiplication de A et montrons que le sous-groupe I de $(A, +)$ est alors un idéal bilatère de l'anneau A . Quels que soient $x \in I$ et $a \in A$, on peut écrire :

$$a \mathcal{R}_I a \text{ et } (x + x) \mathcal{R}_I x.$$

En appliquant l'hypothèse, on obtient :

$$a(x + x) - ax = ax \in I \text{ et } (x + x)a - xa = xa \in I,$$

donc I est un idéal bilatère de A . $\square$

Sachant que dans le groupe abélien $(A, +)$, toute relation d'équivalence compatible avec l'addition est du type $\mathcal{R}_I$, où I est un sous-groupe de $(A, +)$ (Cf. [11], Ch. II), la proposition 2.25. implique :

Corollaire 2.26. *Dans un anneau A , toute relation d'équivalence compatible avec l'addition et la multiplication est du type $\mathcal{R}_I$, où I est un idéal bilatère de A .*

En conséquence, pour tout idéal bilatère I d'un anneau A , on peut définir dans l'ensemble quotient $A/I = A/\mathcal{R}_I$ une *structure d'anneau*, induite par celle de A .

Désignons par $\bar{x}$ la classe d'équivalence "modulo I " (c'est-à-dire modulo $\mathcal{R}_I$) d'un élément quelconque x de A ; $\bar{x} = x + I = \{x + a; a \in I\}$ et

$$A/I = A/\mathcal{R}_I = \{\bar{x}; x \in A\}.$$

La compatibilité de la relation d'équivalence $\mathcal{R}_I$ avec les deux lois de composition internes de A implique que les correspondances :

$$\begin{aligned} A/I \times A/I &\longrightarrow A/I & \text{et} & & A/I \times A/I &\longrightarrow A/I \\ (\bar{x}, \bar{y}) &\longmapsto \overline{x+y} & & & (\bar{x}, \bar{y}) &\longmapsto \overline{xy} \end{aligned}$$

sont des applications définissant dans A/I une addition et une multiplication, telles que :

$$\bar{x} + \bar{y} = \overline{x+y} \quad \text{et} \quad \bar{x} \bar{y} = \overline{xy}. \quad (2.9)$$

On vérifie que, muni de ces deux opérations, A/I est un anneau.

Définition 2.27. L'anneau A/I , défini ci-dessus, est appelé **anneau quotient** de l'anneau A par l'idéal bilatère I .

Remarque 2.28. I étant un idéal bilatère d'un anneau A , on vérifie facilement les propriétés suivantes :

- a) Si A est commutatif, tout idéal de A est bilatère et tout anneau quotient de A est commutatif.
- b) Si A est unitaire et si $I \neq A$, alors A/I est un anneau unitaire dont l'élément unité est $\bar{1}$, 1 étant l'élément unité de A .
- c) La surjection canonique

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ x &\longmapsto \bar{x} \end{aligned}$$

est un morphisme surjectif d'anneaux et si A est unitaire, π est un morphisme d'anneaux unitaires.

- d) Si $I = (0)$, $A/(0)$ s'identifie à A , car pour tout $a \in A$, on peut écrire $\pi(a) = a$. Si $I = A$, A/A est l'anneau nul, car quel que soit $a \in A$, $\pi(a) = \bar{0}$.

Premier exemple d'anneau quotient : $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}$ (Exemple 1.12.).

Pour $n > 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est commutatif, unitaire et fini, de cardinal n (Voir App. A). On peut écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

où, pour tout $k \in \mathbb{Z}$, $\bar{k}$ est la classe de k modulo n .

Proposition 2.29. Si I est une partie non vide d'un anneau A , alors I est un idéal bilatère de A si et seulement s'il existe un anneau A' et un morphisme d'anneaux f de A dans A' tel que $\text{Ker } f = I$.

Preuve : Si A' est un anneau et $f \in \text{Hom}(A, A')$, on sait que $\text{Ker } f$ est un idéal bilatère de A (Prop. 1.53.). Inversement, si I est un idéal bilatère de A , en prenant $A' = A/I$, on a $I = \text{Ker } \pi$, où π est le morphisme canonique $A \longrightarrow A/I$. $\square$

Remarque 2.30. :

a) Le résultat de la proposition 2.29 montre que dans un anneau, les *idéaux bilatères* jouent un rôle analogue à celui des *sous-groupes normaux* dans un groupe ([11], Ch. IV).

b) La relation d'équivalence $\mathcal{R}_I$, associée à un idéal bilatère I d'un anneau A , est appelée **relation d'équivalence modulo I** . Pour x et y dans A , tels que $x \mathcal{R}_I y$, on dit que : *x est équivalent à y , modulo I* , et on écrit

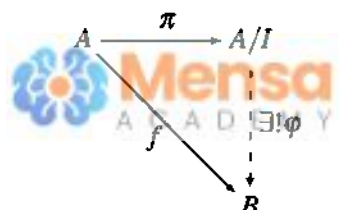
$$x \equiv y \pmod{I}.$$

B. Propriétés des anneaux quotients**1. Propriété universelle de l'anneau quotient**

Théorème 2.31. Soit I un idéal bilatère d'un anneau A et π le morphisme canonique : $A \longrightarrow A/I$; alors, quels que soient l'anneau B et $f \in \text{Hom}(A, B)$ tel que $I \subseteq \text{Ker } f$, il existe un unique morphisme $\varphi \in \text{Hom}(A/I, B)$ tel que

$$\varphi \circ \pi = f.$$

La méthode de démonstration de cette propriété est exactement la même que celle utilisée dans le cas des groupes quotients ([11], Ch. IV); elle est ici proposée en exercice, (n°4, Ch. 2). Le résultat s'exprime par la commutativité du diagramme suivant :



c'est-à-dire : $\forall x \in A, \quad \varphi(\pi(x)) = f(x).$

Corollaire 2.32. Les hypothèses étant celles du théorème 2.31.,

a) f surjectif $\implies \varphi$ surjectif.

b) $I = \text{Ker } f \implies \varphi$ injectif.

c) (f surjectif et $I = \text{Ker } f$) $\implies \varphi$ isomorphisme.

Vérification laissée au lecteur.

Remarque 2.33. Comme dans le cas des groupes, la "propriété universelle" énoncée dans le théorème 2.31. est une propriété du couple $(A/I, \pi)$.

Théorème 2.34. Premier théorème d'isomorphisme

Pour tout morphisme f d'un anneau A dans un anneau B , on a

$$\text{Im } f \simeq A/\text{Ker } f \quad (\text{isomorphisme d'anneaux}).$$

Preuve : On considère la restriction surjective f_1 de f , définie par

$$\begin{aligned} f_1 : A &\longrightarrow \text{Im } f \\ x &\longmapsto f_1(x) = f(x). \end{aligned}$$

$\text{Ker} f_1 = \text{Ker} f$ donc (Th. 2.31.), il existe un unique morphisme $\varphi \in \text{Hom}(A/\text{Ker} f, \text{Im} f)$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\text{Ker} f \\ & \searrow f_1 & \downarrow \exists! \varphi \\ & & \text{Im} f \end{array}$$

c'est-à-dire que $\varphi \circ \pi = f_1$; alors

$(\text{Im} f_1 = \text{Im} f) \implies \varphi$ surjectif et $(\text{Ker} f_1 = \text{Ker} f) \implies \varphi$ injectif,
par suite, φ est un isomorphisme de $A/\text{Ker} f$ sur $\text{Im} f$ et
 $\forall \bar{x} = \pi(x) \in A/\text{Ker} f, \quad \varphi(\bar{x}) = f(x).$ □

2. Sous-anneaux et idéaux d'un anneau quotient

Théorème 2.35. Soit I un idéal bilatère d'un anneau A et π le morphisme canonique : $A \longrightarrow A/I$.

1) Tout sous-anneau (resp. idéal à gauche, à droite ou bilatère) de A/I est l'image par π d'un unique sous-anneau (resp. idéal à gauche, à droite ou bilatère) contenant I . Plus précisément, si $\bar{J}$ est un sous-anneau (resp. idéal à gauche, à droite ou bilatère) de A/I ,
 $\bar{J} = \pi(J)$, où $J = \pi^{-1}(\bar{J}) \supseteq I$; ainsi $\bar{J} = J/I$.

2) Si J_1 est un sous-anneau (resp. idéal à gauche, à droite ou bilatère) de A tel que $I \not\subseteq J_1$, alors $I + J_1$ est le plus petit sous-anneau (resp. idéal à gauche, à droite ou bilatère) de A contenant I et $\pi(J_1) = (I + J_1)/I$.

La démonstration du théorème 2.35. est la même que celle faite dans le cas des sous-groupes d'un groupe quotient ([11], Ch. IV); elle est proposée ici en exercice (n°4, Ch. 2).

Exemple 2.36. Pour $n \geq 2$ dans $\mathbb{N}$, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$, tels que k divise n dans $\mathbb{N}$; ce sont aussi les seuls sous-anneaux de $\mathbb{Z}/n\mathbb{Z}$.

3. Deuxième et troisième théorèmes d'isomorphisme

Lemme 2.37. Soit deux anneaux A et A' et deux idéaux bilatères I dans A et I' dans A' ; alors, pour tout morphisme $f \in \text{Hom}(A, A')$ tel que $f(I) \subseteq I'$, il existe un unique morphisme $\bar{f} \in \text{Hom}(A/I, A'/I')$ tel que

$$\bar{f} \circ \pi = \pi' \circ f,$$

où π et π' sont les surjections canoniques $A \longrightarrow A/I$ et $A' \longrightarrow A'/I'$.

Preuve :

$$f(I) \subseteq I' \iff I \subseteq f^{-1}(I');$$

d'autre part, on vérifie que $\text{Ker}(\pi' \circ f) = f^{-1}(I')$.

D'après le théorème 2.31., la condition $I \subseteq \text{Ker}(\pi' \circ f)$ implique l'existence d'un unique

morphisme d'anneaux $\bar{f} \in \text{Hom}(A/I, A'/I')$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \pi \downarrow & & \downarrow \pi' \\ A/I & \xrightarrow{\exists! \bar{f}} & A'/I' \end{array}$$

donc $\bar{f} \circ \pi = \pi' \circ f$. □

Remarque 2.38. Comme conséquences du corollaire 2.32., on a :

a) Si $\pi' \circ f$ est surjectif, alors $\bar{f}$ est surjectif.

On notera que $\pi' \circ f$ peut être surjectif, sans que f le soit (voir Th. 2.39.).

b) Si $\text{Ker}(\pi' \circ f) = I$ ($\iff f^{-1}(I') = I$), alors $\bar{f}$ est injectif.

Théorème 2.39. Deuxième théorème d'isomorphisme

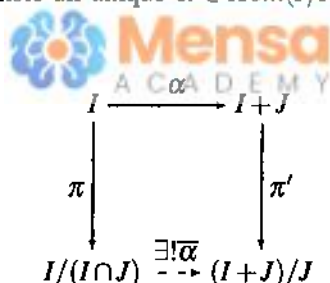
Quels que soient les idéaux bilatères I et J d'un anneau A , on a :

$$I/(I \cap J) \simeq (I+J)/J \quad (\text{isomorphisme d'anneaux}).$$

Preuve : Soit α l'injection canonique de I dans $I+J$; alors,

$$\alpha(I \cap J) = I \cap J \subseteq J;$$

d'après le lemme 2.37., il existe un unique $\bar{\alpha} \in \text{Hom}(I/(I \cap J), (I+J)/J)$ tel que le diagramme suivant



$$\begin{array}{ccc} I & \xrightarrow{\alpha} & I+J \\ \pi \downarrow & & \downarrow \pi' \\ I/(I \cap J) & \xrightarrow{\exists! \bar{\alpha}} & (I+J)/J \end{array}$$

commute : $\bar{\alpha} \circ \pi = \pi' \circ \alpha$, où π et π' sont les surjections canoniques.

$$\pi' \circ \alpha(I) = \pi'(I) = (I+J)/J,$$

donc $\pi' \circ \alpha$ est surjectif (bien que α ne le soit pas) ; on en déduit que $\bar{\alpha}$ est surjectif (Rem. 2.38., a)). D'autre part, $\alpha^{-1}(J) = I \cap J$, donc $\bar{\alpha}$ est injectif (Rem. 2.38., b)) ; par suite $\bar{\alpha}$ est un isomorphisme. □

Remarque 2.40. :

a) Les hypothèses du théorème 2.39. impliquent aussi :

$$J/(I \cap J) \simeq (I+J)/I.$$

b) Si la somme $I+J$ est directe, on a $I \cap J = (0)$, d'où

$$J \simeq (I \oplus J)/I \quad \text{et} \quad I \simeq (I \oplus J)/J.$$

Théorème 2.41. Troisième théorème d'isomorphisme

Quels que soient les idéaux bilatères I et J d'un anneau A tels que $I \subseteq J$, on a

$$A/J \simeq (A/I)/(J/I) \quad (\text{isomorphisme d'anneaux}).$$

Preuve : Soit σ la surjection canonique $A \longrightarrow A/I$.

$$I \subseteq J \implies \sigma(J) = J/I.$$

Il existe alors un unique morphisme $\bar{\sigma} \in \text{Hom}(A/J, (A/I)/(J/I))$ tel que le diagramme suivant commute (Lemme 2.37)

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A/I \\ \pi \downarrow & & \downarrow \pi' \\ A/J & \xrightarrow{\exists! \bar{\sigma}} & (A/I)/(J/I) \end{array}$$

donc, $\bar{\sigma} \circ \pi = \pi' \circ \sigma$, où π et π' sont les surjections canoniques.

$$\begin{aligned} \pi' \circ \sigma \text{ surjectif} &\implies \bar{\sigma} \text{ surjectif,} \\ \text{Ker}(\pi' \circ \sigma) = J &\implies \bar{\sigma} \text{ injectif;} \end{aligned}$$

donc $\bar{\sigma}$ est un isomorphisme. □

C. Idéaux bilatères copremiers (ou étrangers)

1. Idéaux bilatères copremiers dans un anneau unitaire

Définition 2.42. A étant un anneau unitaire, deux idéaux bilatères I et J de A sont dits **copremiers** (ou **étrangers**), si

$$I + J = A.$$

Remarque 2.43. Deux idéaux non nuls $m\mathbb{Z}$ et $n\mathbb{Z}$ sont **copremiers** dans $\mathbb{Z}$, si et seulement si m et n sont premiers entre eux (App. A, Prop. A.28.).

Lemme 2.44. Soit $\{I_j\}_{1 \leq j \leq n}$, $n \geq 2$ dans $\mathbb{N}$, une famille finie d'idéaux bilatères d'un anneau unitaire A ; alors les idéaux I_j , $1 \leq j \leq n$, sont deux à deux copremiers si et seulement si, pour tout j ($1 \leq j \leq n$),

$$A = I_j + \bigcap_{1 \leq k \leq n, k \neq j} I_k. \quad (2.10)$$

Preuve :

a) Supposons les idéaux bilatères I_j , $1 \leq j \leq n$, deux à deux copremiers; quel que soit (j, k) , $j \neq k$ dans $\{1, 2, \dots, n\}$, on a

$$A = I_j + I_k.$$

Si $n = 2$, la relation (2.10) est vérifiée. Pour $n \geq 3$, on raisonne par récurrence sur n . L'anneau A est unitaire, donc en tant qu'idéal bilatère de lui-même, il vérifie : $A^2 = A$.

L'hypothèse de récurrence permet d'écrire :

$$A = I_1 + \bigcap_{2 \leq k \leq n-1} I_k;$$

par suite, $A = A^2 = (I_1 + \bigcap_{2 \leq k \leq n-1} I_k)(I_1 + I_n)$.

$$\begin{aligned} (I_1 + \bigcap_{2 \leq k \leq n-1} I_k)(I_1 + I_n) &\subseteq I_1 + (\bigcap_{2 \leq k \leq n-1} I_k)I_n \\ &\subseteq I_1 + (\bigcap_{2 \leq k \leq n-1} I_k) \cap I_n; \end{aligned}$$

d'où $A = I_1 + \bigcap_{2 \leq k \leq n} I_k$. On a ainsi prouvé la Rel. (2.10) pour $j = 1$, on la démontrait de même pour tout j ($1 < j \leq n$).

b) Réciproquement, si la relation (2.10) est vérifiée quel que soit j , ($1 \leq j \leq n$), alors pour tout couple (j, l) tel que $j \neq l$ dans $\{1, 2, \dots, n\}$:

$$A = I_j + \bigcap_{1 \leq k \leq n, k \neq j} I_k \subseteq I_j + I_l$$

implique $A = I_j + I_l$, donc les I_j , ($1 \leq j \leq n$), sont deux à deux copremiers. $\square$

Proposition 2.45. Soit $\{I_j\}_{1 \leq j \leq n}$, $n \geq 2$ dans $\mathbb{N}$, une famille finie d'idéaux bilatères d'un anneau unitaire A , deux à deux copremiers; alors, quels que soient les éléments $a_1, a_2, \dots, a_n$ de A , il existe un élément $b \in A$ tel que :

$$\forall j (1 \leq j \leq n), \quad b \equiv a_j \pmod{I_j}. \quad (2.11)$$

De plus, si $c \in A$ vérifie la même propriété que b , alors

$$c \equiv b \pmod{\bigcap_{1 \leq j \leq n} I_j}.$$

Preuve : D'après la relation (2.10) du lemme 2.44., quel que soit j ($1 \leq j \leq n$), il existe $x_j \in I_j$ et $b_j \in \bigcap_{k \neq j} I_k$, ($1 \leq k \leq n$), tel que

$$\begin{aligned} a_j &= x_j + b_j, \\ \text{donc } b_j &\equiv a_j \pmod{I_j}, \\ \text{et } b_j &\equiv 0 \pmod{I_k}, \quad \forall k \neq j. \end{aligned}$$

Par suite, en posant $b = b_1 + b_2 + \dots + b_n$, on obtient

$$\begin{aligned} \forall j (1 \leq j \leq n), \quad b &\equiv a_j \pmod{I_j}. \\ \text{Si } c \in A \text{ est tel que } \forall j (1 \leq j \leq n), \quad c &\equiv a_j \pmod{I_j}, \\ \text{alors, } \forall j (1 \leq j \leq n), \quad b &\equiv c \pmod{I_j}, \\ \text{d'où } b &\equiv c \pmod{\bigcap_{1 \leq j \leq n} I_j}. \end{aligned}$$

$\square$

Proposition 2.46. Soit $\{I_j\}_{1 \leq j \leq n}$ une famille finie d'idéaux bilatères d'un anneau unitaire A , ($n \geq 2$ dans $\mathbb{N}$). On considère l'application

$$\begin{aligned} \theta : A &\longrightarrow \prod_{1 \leq j \leq n} A/I_j \\ a &\longmapsto (\pi_j(a))_{1 \leq j \leq n} \end{aligned}$$

où, pour tout j ($1 \leq j \leq n$), π_j est la surjection canonique $A \longrightarrow A/I_j$;

$$\begin{aligned} \theta \text{ surjectif} &\iff I_1, I_2, \dots, I_n \text{ deux à deux copremiers.} \\ \theta \text{ injectif} &\iff \bigcap_{1 \leq j \leq n} I_j = 0. \end{aligned}$$

Preuve :

a) Supposons les idéaux bilatères I_j , $1 \leq j \leq n$, deux à deux copremiers. Soit $(\pi_j(a_j))_{1 \leq j \leq n}$ un élément quelconque du produit direct $\prod_{1 \leq j \leq n} A/I_j$. D'après la Prop. 2.45., il existe $b \in A$ tel que :

$$\forall j (1 \leq j \leq n), \quad \pi_j(b) = \pi_j(a_j), \quad \text{d'où } (\pi_j(a_j))_{1 \leq j \leq n} = (\pi_j(b))_{1 \leq j \leq n} = \theta(b),$$

donc θ est surjectif.

Réciproquement, si θ est surjectif, il existe, en particulier, $b \in A$ tel que :

$$\theta(b) = (\pi_j(b))_{1 \leq j \leq n} = (\bar{1}, \bar{0}, \dots, \bar{0});$$

$$\text{donc } b \equiv 1 \pmod{I_1} \text{ et } \forall k (2 \leq k \leq n), b \equiv 0 \pmod{I_k}.$$

Par suite il existe $x_1 \in I_1$ tel que $b - 1 = x_1$; d'autre part, $b \in \bigcap_{2 \leq k \leq n} I_k$ d'où :

$$b - x_1 = 1 \implies I_1 + \bigcap_{2 \leq k \leq n} I_k = A.$$

La relation (2.10) est donc vérifiée par les idéaux $\{I_j\}_{1 \leq j \leq n}$, pour $j = 1$ et on montrerait de même, qu'elle l'est pour tout j ($1 < j \leq n$); les idéaux I_j , $1 \leq j \leq n$, sont alors deux à deux coprimiers.

b) La définition de θ , implique $\text{Ker } \theta = \bigcap_{1 \leq j \leq n} I_j$, d'où le résultat énoncé. $\square$

2. Cas de l'anneau $\mathbb{Z}$

Théorème 2.47. Théorème des restes chinois

Etant donné m et n premiers entre eux dans $\mathbb{Z}^*$, pour tout couple d'entiers $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, il existe $x \in \mathbb{Z}$ tel que

$$x \equiv a \pmod{m} \text{ et } x \equiv b \pmod{n}.$$

De plus, si $y \in \mathbb{Z}$ vérifie la même propriété que x , alors

$$y \equiv x \pmod{mn}.$$

Preuve : Il suffit d'appliquer la proposition 2.45. dans le cas des idéaux $m\mathbb{Z}$ et $n\mathbb{Z}$, sachant que m et n sont premiers entre eux si et seulement si $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$ (App. A, Prop. A.28.) $\square$

Une autre démonstration de ce théorème sera proposée en exercice (n° 6, Ch. 5).

Proposition 2.48. Théorème des restes chinois généralisé

Soit $m_1, m_2, \dots, m_n$, des entiers deux à deux premiers entre eux dans $\mathbb{Z}^*$, $n \geq 2$ dans $\mathbb{N}$; alors quels que soient $a_1, a_2, \dots, a_n$ dans $\mathbb{Z}$, il existe $x \in \mathbb{Z}$ tel que

$$\forall i (1 \leq i \leq n), \quad x \equiv a_i \pmod{m_i}.$$

De plus, si $y \in \mathbb{Z}$ vérifie la même propriété que x , alors

$$y \equiv x \pmod{\prod_{1 \leq i \leq n} m_i}.$$

Ce résultat se déduit des propositions 2.45. et A.28., App. A.

4. Idéaux premiers - Idéaux maximaux

Remarques préliminaires : Soit I un idéal bilatère d'un anneau unitaire A et π la surjection canonique $A \rightarrow A/I$.

a) On sait que si x est inversible dans A , alors $\pi(x)$ est inversible dans A/I ; mais la réciproque est fautive. En effet, $\mathbb{Z}$ n'est pas un corps, cependant, pour tout nombre premier p , $\mathbb{Z}/p\mathbb{Z}$ est un corps (Cor.1.14.).

b) Si x est non diviseur de zéro dans A , on n'a pas nécessairement $\pi(x)$ non diviseur de zéro dans A/I .

En effet, $\mathbb{Z}$ est un anneau intègre, mais, pour tout entier $n > 1$ et non premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Dans ce qui suit, nous allons caractériser les idéaux I d'un anneau unitaire et commutatif A , pour lesquels A/I est intègre ou A/I est un corps.

A. Idéaux premiers d'un anneau unitaire et commutatif

Proposition 2.49. Pour un idéal propre P d'un anneau unitaire commutatif A , les deux conditions suivantes sont équivalentes :

- 1) $((x, y) \in A \times A \text{ et } xy \in P) \implies x \in P \text{ ou } y \in P$.
- 2) $(I \text{ et } J \text{ idéaux de } A \text{ et } IJ \subseteq P) \implies I \subseteq P \text{ ou } J \subseteq P$.

Preuve :

1) $\implies$ 2) : I et J étant deux idéaux de A , supposons $IJ \subseteq P$ et $I \not\subseteq P$; il existe alors $x \in I$ tel que $x \notin P$. D'autre part, quel que soit $y \in J$, on a $xy \in IJ$, donc $xy \in P$ et, par hypothèse, $(xy \in P \text{ et } x \notin P) \implies y \in P$, d'où $J \subseteq P$.

2) $\implies$ 1) : Supposons x et y dans A tels que $xy \in P$ et $x \notin P$.

Soit (x) et (y) les idéaux de A , respectivement engendrés par x et y . La commutativité de l'anneau A implique $(xy) = (x)(y)$ (Prop. 2.24.) ; par suite,

$$xy \in P \implies (x)(y) \subseteq P; \text{ d'autre part, } x \notin P \implies (x) \not\subseteq P,$$

alors compte tenu de l'hypothèse 2) on obtient :

$$((x)(y) \subseteq P \text{ et } (x) \not\subseteq P) \implies (y) \subseteq P, \text{ donc } y \in P. \quad \square$$

Définition 2.50. Dans un anneau unitaire et commutatif A , un idéal P est dit **premier**, si

i) P est un idéal propre de A .

ii) P vérifie l'une des conditions équivalentes de la proposition 2.49.

Remarque 2.51. Dans un anneau unitaire, non commutatif A , on peut définir une notion d'idéal bilatère premier :

Un idéal bilatère propre de A est dit *premier*, si

$$(I \text{ et } J \text{ idéaux de } A \text{ et } IJ \subseteq P) \implies I \subseteq P \text{ ou } J \subseteq P.$$

A n'étant pas commutatif, cette condition n'est plus équivalente à la condition 1) de la proposition 2.49., car en général (Prop. 2.24.),

$$xy \in P \not\implies (x)(y) \subseteq P.$$

Théorème 2.52. Dans un anneau unitaire commutatif A ,

$$I \text{ est un idéal premier} \iff A/I \text{ est un domaine d'intégrité.}$$

Preuve : Supposons I premier ; alors

$$I \neq A \implies A/I \text{ non nul.}$$

A/I est un anneau unitaire commutatif, montrons qu'il est intègre.

Notons $\bar{x}$ la classe modulo I d'un élément x de A . Soit $\bar{x}, \bar{y}$ dans A/I , tels que $\bar{x}\bar{y} = \bar{0}$.

$$\bar{x}\bar{y} = \bar{0} \iff \overline{xy} = \bar{0} \iff xy \in I.$$

$$I \text{ étant premier : } xy \in I \implies x \in I \text{ ou } y \in I;$$

$$\text{par suite : } \bar{x}\bar{y} = \bar{0} \implies \bar{x} = \bar{0} \text{ ou } \bar{y} = \bar{0}, \text{ donc } A/I \text{ est intègre.}$$

On en conclut que A/I est un domaine d'intégrité.

Réciproquement, on suppose que l'anneau A/I est un domaine d'intégrité ; nécessairement, A/I est non nul, donc I est un idéal propre de A . Soit x et y dans A tels que $xy \in I$.

$$\text{Dans } A/I : \bar{x}\bar{y} = \bar{0} \implies \bar{x} = \bar{0} \text{ ou } \bar{y} = \bar{0};$$

$$\text{par suite : } xy \in I \implies x \in I \text{ ou } y \in I,$$

donc I est premier. □

Corollaire 2.53. Si A est un anneau unitaire et commutatif, alors A est intègre si et seulement si (0) est un idéal premier.

Exemple 2.54. On sait que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $n = 0$ ou n est un nombre premier ; on en déduit que les idéaux premiers de $\mathbb{Z}$ sont (0) et les $p\mathbb{Z}$, pour p premier.

Proposition 2.55. Soit A un anneau unitaire commutatif, P un idéal premier de A et $n \geq 2$ dans $\mathbb{N}$.

- 1) Pour des éléments $x_1, x_2, \dots, x_n$ de A , on a

$$x_1 x_2 \cdots x_n \in P \implies \exists i (1 \leq i \leq n) \text{ tel que } x_i \in P.$$
- 2) Pour des idéaux $I_1, I_2, \dots, I_n$ de A :

$$I_1 I_2 \cdots I_n \subseteq P \implies \exists i (1 \leq i \leq n) \text{ tel que } I_i \subseteq P.$$

Preuve : Démontrons la propriété 1) ; supposons

$$x_1 x_2 \cdots x_n = x_1 (x_2 \cdots x_n) \in P.$$

L'idéal P étant premier, on a $x_1 \in P$ ou $x_2 \cdots x_n \in P$.

Si $x_1 \in P$, la propriété est démontrée.

Si $x_1 \notin P$, on réitère le raisonnement précédent à partir de $x_2 \cdots x_n$ et de proche en proche, on en déduit qu'il existe nécessairement i ($1 \leq i \leq n$) tel que $x_i \in P$.

Par le même processus, on démontre la propriété 2). □

Corollaire 2.56. P étant un idéal premier d'un anneau unitaire commutatif A , pour tout $n \in \mathbb{N}^*$:

- 1) $(x \in A \text{ et } x^n \in P) \implies x \in P.$
- 2) $(I \text{ idéal de } A \text{ et } I^n \subseteq P) \implies I \subseteq P.$

Proposition 2.57. Soit $f \in \text{Hom}(A, B)$, un morphisme d'anneaux unitaires commutatifs.

- 1) Quel que soit l'idéal premier Q de B , $f^{-1}(Q)$ est un idéal premier de A contenant $\text{Ker} f$.
- 2) Dans le cas où f est surjectif, quel que soit l'idéal premier P de A contenant $\text{Ker} f$, $f(P)$ est un idéal premier de B .

Preuve :

- 1) Q étant un idéal de B , on sait que $f^{-1}(Q)$ est un idéal de A , contenant $\text{Ker} f$, car $0 \in Q$. Il reste à vérifier que

$$Q \text{ premier dans } B \implies f^{-1}(Q) \text{ premier dans } A.$$

Soit $xy \in f^{-1}(Q)$; alors, $f(xy) = f(x)f(y) \in Q$ et

$$\begin{aligned} ((f(x)f(y) \in Q \text{ et } Q \text{ premier}) \implies f(x) \in Q \text{ ou } f(y) \in Q \\ \text{donc, } xy \in f^{-1}(Q) \implies x \in f^{-1}(Q) \text{ ou } y \in f^{-1}(Q). \end{aligned}$$

- 2) Si f est surjectif et P est un idéal premier de A contenant $\text{Ker} f$, alors $f(P)$ est un idéal de $B = \text{Im} f$ (Rem. 1.54.). Montrons que $f(P)$ est premier.

Soit $f(x)$ et $f(x')$ dans B tels que $f(x)f(x') \in f(P)$. Il existe alors $a \in P$, tel que

$$\begin{aligned} f(xx') = f(x)f(x') = f(a); \quad \text{par suite,} \\ ((xx' - a) \in \text{Ker} f, \text{Ker} f \subseteq P \text{ et } a \in P) \implies xx' \in P. \end{aligned}$$

On en déduit que $x \in P$ ou $x' \in P$, d'où :

$$f(x)f(x') \in f(P) \implies f(x) \in f(P) \text{ ou } f(x') \in f(P),$$

donc $f(P)$ est un idéal premier de B . □

Corollaire 2.58. Soit I un idéal propre d'un anneau unitaire commutatif A . Notons π la surjection canonique : $A \rightarrow A/I$; alors, $\bar{P}$ est un idéal premier de l'anneau A/I si et seulement si $\pi^{-1}(\bar{P})$ est un idéal premier de A contenant I .

Ce résultat est une conséquence directe de la proposition précédente, puisque π est un morphisme surjectif et $\text{Ker } \pi = I$.

Définition 2.59. L'ensemble des idéaux premiers d'un anneau unitaire, commutatif A est appelé le **Spectre** de A ou plus précisément, le **Spectre premier** de A et noté $\text{Spec}(A)$.

B. Idéaux maximaux d'un anneau unitaire

1. Notion d'idéal maximal

Définition 2.60. I est un idéal bilatère **maximal** d'un anneau A , si

i) I est un idéal bilatère *propre* de A .

ii) $(J \text{ idéal bilatère de } A \text{ et } I \subseteq J \subseteq A) \implies J = I \text{ ou } J = A$.

On définit, de la même façon, un idéal à gauche (resp. à droite) **maximal** de A .

Remarque 2.61. La définition 2.60. exprime qu'un idéal bilatère I d'un anneau A est **maximal**, si c'est un élément *maximal* dans l'ensemble des idéaux bilatères *propres* de A , ordonné par l'inclusion.

La même remarque peut être faite pour les idéaux maximaux à gauche, ou à droite de A .

Théorème 2.62. Dans un anneau unitaire et commutatif A , on a :

$$I \text{ est un idéal maximal} \iff A/I \text{ est un corps.}$$

Preuve : Si A/I est un corps, on a nécessairement $I \neq A$. D'autre part, supposons J idéal de A tel que $I \subsetneq J$; alors J/I est un idéal non nul du corps A/I , donc $J/I = A/I$, (Cor. 1.48.). Par suite $J = A$, donc I est un idéal maximal de A .

Réciproquement, soit I un idéal maximal de A , alors A/I est non nul et c'est un anneau unitaire commutatif; la maximalité de I implique que A/I n'a pas d'autre idéal que (0) et A/I , donc A/I est un corps (Cor. 1.48.). $\square$

Remarque 2.63. Dans tout corps K , (0) est le seul idéal maximal.

Corollaire 2.64. Pour un idéal I d'un anneau unitaire commutatif A , on a
 $I \text{ maximal} \implies I \text{ premier.}$

Ce résultat se déduit des théorèmes 2.52. et 2.62., puisque

$$A/I \text{ est un corps} \implies A/I \text{ est intègre.}$$

Remarque 2.65. La réciproque du corollaire 2.64. est fautive.

Par exemple, dans $\mathbb{Z}$, (0) est un idéal premier qui n'est pas maximal.

On a cependant le résultat suivant :

Théorème 2.66. Dans un domaine principal (Déf. 2.7.) tout idéal premier non nul est maximal.

Preuve : Soit I un idéal premier non nul d'un domaine principal A . Il existe $a \neq 0$ dans A , tel que $I = aA$.

Supposons J idéal de A tel que $I \subsetneq J$; il existe alors b non nul dans A tel que $J = bA$ et $b \notin I$.

$$aA \subsetneq bA \implies \exists x \in A \text{ tel que } a = bx.$$

$$(bx \in aA, aA \text{ idéal premier et } b \notin aA) \implies x \in aA.$$

On en déduit qu'il existe y non nul dans A tel que $x = ay$, d'où $a = bay$. L'anneau A étant commutatif, unitaire et intègre, on a

$$a = bay \implies a(1 - by) = 0 \implies by = 1.$$

b est donc inversible dans A , d'où $J = bA = A$ (Prop. 1.47.).

On en conclut que l'idéal $I = aA$ est maximal dans A . $\square$

Remarque 2.67. $\mathbb{Z}$ étant un domaine principal, les idéaux maximaux de $\mathbb{Z}$, sont les $p\mathbb{Z}$, pour tous les nombres premiers p .

2. Existence des idéaux maximaux dans un anneau unitaire

Le résultat fondamental de ce paragraphe est le suivant :

Théorème 2.68. *Tout anneau unitaire a au moins un idéal bilatère (resp. à gauche, à droite) maximal.*

Nous rappelons, ci-dessous, la notion d'ensemble inductif et l'Axiome de Zorn ([11], p.162) qui seront utilisés dans la preuve du théorème 2.68.

Définition 2.69. Un ensemble E , non vide et partiellement ordonné, est dit **inductif**, si tout sous-ensemble non vide et *totale*ment ordonné de E a un majorant dans E .

Axiome de Zorn : *Tout ensemble non vide, partiellement ordonné et inductif, a au moins un élément maximal.*

Preuve du théorème 2.68. : Soit A un anneau unitaire.

Notons $\mathcal{B}$ l'ensemble des idéaux bilatères *propres* de A . On a $(0) \in \mathcal{B}$, donc $\mathcal{B} \neq \emptyset$ et $\mathcal{B}$ est partiellement ordonné par l'inclusion.

Soit $\{I_\lambda\}_{\lambda \in \Lambda}$ une famille d'éléments de $\mathcal{B}$, totalement ordonnée par l'inclusion. On sait que dans ce cas, $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ est un idéal bilatère de A (Prop. 2.11.). De plus, par hypothèse, pour tout $\lambda \in \Lambda$, I_λ est un idéal propre de A , par suite

$$(\forall \lambda \in \Lambda, 1 \notin I_\lambda) \implies 1 \notin I.$$

On en déduit que I est un idéal propre de A , donc $I \in \mathcal{B}$; ainsi $\mathcal{B}$ est inductif, car I est un majorant de la famille $\{I_\lambda\}_{\lambda \in \Lambda}$. En vertu de l'Axiome de Zorn, on en conclut qu'il existe au moins un idéal bilatère maximal dans A .

On prouve, de la même façon, l'existence d'un idéal à gauche (resp. à droite) maximal, dans l'anneau unitaire A . □

Corollaire 2.70. *Tout anneau unitaire commutatif A a au moins une image homomorphe (Déf. 1.55.) qui est un corps.*

En effet, A a au moins un idéal maximal M ; le morphisme canonique : $A \longrightarrow A/M$ est surjectif et A/M est un corps (Th. 2.62.).

Corollaire 2.71. *Dans un anneau unitaire A , tout idéal bilatère propre I est contenu dans un idéal bilatère maximal de A .*

Preuve : $I \neq A \implies A/I \neq 0$. L'anneau A/I est unitaire, donc d'après le théorème 2.68., il existe un idéal bilatère maximal $\overline{M}$ dans A/I . On en déduit qu'il existe un unique idéal bilatère M de A , tel que (Th. 2.35.)

$$I \subseteq M \text{ et } \pi(M) = \overline{M} = M/I,$$

où π est la surjection canonique de A sur A/I .

Vérifions que M est un idéal bilatère maximal de A . Soit J un idéal bilatère de A tel que

$$I \subseteq M \subseteq J \subseteq A.$$

Dans A/I , on a : $M/I \subseteq J/I \subseteq A/I$.

La maximalité de $\overline{M} = M/I$ dans A/I implique alors

$J/I = M/I$ ou $J/I = A/I$; donc $J = M$ ou $J = A$. □

Corollaire 2.72. Dans un anneau unitaire commutatif,

- a) tout idéal propre est contenu dans un idéal maximal.
- b) tout élément non inversible est contenu dans un idéal maximal.

La propriété a) est justifiée par le corollaire 2.71. ; la propriété b) s'en déduit immédiatement, puisque qu'un élément non inversible engendre un idéal propre.

5. Notion d'anneau local

Définition 2.73. On appellera **anneau local** tout anneau unitaire commutatif n'ayant qu'un seul idéal maximal.

Remarque 2.74. D'après la remarque 2.63., tout corps (commutatif) est un anneau local, mais nous rencontrerons plus loin des exemples d'anneaux locaux qui ne sont pas des corps.

Proposition 2.75. Si $\mathcal{M}$ est l'unique idéal maximal d'un anneau local, alors $\mathcal{M}$ est l'ensemble des éléments non inversibles de A .

Preuve : Tout élément non inversible de A est dans $\mathcal{M}$ (Cor. 2.72.). Inversement, si $x \in \mathcal{M}$, alors l'idéal principal (x) est inclus dans $\mathcal{M}$, c'est donc un idéal propre de A , d'où x non inversible (Prop. 1.47.). $\square$

Remarque 2.76. En général, dans un anneau unitaire commutatif, l'ensemble des éléments non inversibles ne forme pas un idéal. Par exemple, dans $\mathbb{Z}$, l'ensemble $\mathbb{Z} \setminus \{-1, 1\}$ des éléments non inversibles n'est pas un idéal.

Théorème 2.77. Un anneau unitaire commutatif A est local si et seulement si l'ensemble de ses éléments non inversibles forme un idéal de A ; c'est alors l'unique idéal maximal de A .

Preuve : Désignons par (C) la condition :

"Dans A , l'ensemble des éléments non inversibles forme un idéal."

D'après la proposition 2.75., tout anneau local satisfait à la condition (C).

Réciproquement, supposons la condition (C) vérifiée par A et notons I , l'idéal de A formé par les éléments non inversibles. On remarque que I est nécessairement un idéal propre de A (Prop. 1.47.). Si l'on suppose I non maximal, alors d'après le corollaire 2.72., il existe un idéal maximal M de A tel que

$$I \subsetneq M \subsetneq A.$$

Par suite, il existe $x \in M$ tel que $x \notin I$; or,

$$x \in M \implies x \text{ non inversible} \implies x \in I;$$

d'où une contradiction. En conclusion, I est maximal et c'est l'unique idéal maximal de A , puisqu'il contient tous les éléments non inversibles de A . $\square$

Définition 2.78. Si $\mathcal{M}$ est l'unique idéal maximal d'un anneau local A , le corps $A/\mathcal{M}$ est appelé le **corps résiduel** de A .

6. Notion d'anneau commutatif noethérien

A. Condition maximale - Condition de chaîne ascendante

Définition 2.79. Soit E un ensemble non vide, partiellement ordonné.

a) On dit que E vérifie la **condition maximale** (C.M.), si tout sous-ensemble non vide de E contient au moins un élément maximal.

b) On dit que E vérifie la **condition de chaîne ascendante** (C.C.A.) si toute suite strictement croissante d'éléments de E :

$$x_1 < x_2 < \dots < x_n < x_{n+1} < \dots \quad \text{est finie.} \quad (2.12)$$

autrement dit, si toute suite croissante d'éléments de E :

$$x_1 \leq x_2 \leq \dots \leq x_n \leq x_{n+1} \leq \dots \quad \text{est stationnaire.} \quad (2.13)$$

On rappelle qu'une suite telle que (2.13), est *stationnaire* s'il existe un entier $l \geq 1$ tel que $x_n = x_l$, quel que soit $n \geq l$.

Proposition 2.80. Dans un ensemble partiellement ordonné la condition maximale est équivalente à la condition de chaîne ascendante.

Preuve : Soit E un ensemble non vide partiellement ordonné.

1°) Supposons la C.M. vérifiée ; soit

$$x_1 < x_2 < \dots < x_n < x_{n+1} < \dots$$

une suite strictement croissante dans E . Posons :

$$X = \{x_1, x_2, \dots, x_n, \dots\}.$$

X est un sous-ensemble non vide de E ; la condition C.M. implique qu'il contient au moins un élément maximal ; celui-ci est nécessairement un plus grand élément, car les éléments de X forment une suite strictement croissante. On en conclut que la suite des $x_n, n \in \mathbb{N}^*$, est finie, donc la C.C.A. est vérifiée.

2°) On suppose que E vérifie la C.C.A., mais ne vérifie pas la C.M. ; il existe alors une partie non vide X de E ne contenant pas d'élément maximal.

Soit $x_1 \in X$, x_1 n'étant pas maximal dans X , il existe $x_2 \in X$ tel que $x_1 < x_2$.

L'élément x_2 n'étant pas maximal dans X , il existe $x_3 \in X$ tel que $x_2 < x_3$, d'où :

$$x_1 < x_2 < x_3.$$

On peut ainsi construire une suite strictement croissante infinie d'éléments de E , ce qui contredit la C.C.A. ; on en conclut que nécessairement la C.M. est vérifiée dans E . $\square$

B. Anneau commutatif noethérien

Définition 2.81. Un anneau unitaire commutatif est dit **noethérien**, si l'ensemble de ses idéaux, partiellement ordonné par l'inclusion, vérifie la C.C.A. (équivalente à la C.M.).

Théorème 2.82. Un anneau unitaire commutatif A est noethérien si et seulement si tout idéal de A est de type fini (Déf. 2.5.).

Preuve : Supposons A noethérien. Soit I un idéal de A ; si $I = (0)$ ou $I = A$, alors I est principal, donc de type fini. Dans ce qui suit, I sera un idéal propre, non nul, de A .

Notons $\mathcal{J}$, l'ensemble des idéaux J de A tels que :

$$J \text{ est de type fini et } J \subseteq I.$$

On a $\mathcal{J} \neq \emptyset$, car $(0) \in \mathcal{J}$. A étant noethérien, l'ensemble des idéaux de A vérifie la C.M., donc il existe un élément maximal J_0 dans $\mathcal{J}$.

Supposons $J_0 \neq I$, donc $J_0 \subsetneq I$, il existe alors $x \in I$, tel que $x \notin J_0$.

L'idéal J_0 étant de type fini, soit $\{a_1, a_2, \dots, a_r\}$ une famille génératrice finie de J_0 , $r \in \mathbb{N}^*$.

Notons J l'idéal de A engendré par $\{a_1, a_2, \dots, a_r, x\}$; on a alors :

$$J \in \mathcal{J} \text{ et } J_0 \subsetneq J \subseteq I,$$

ce qui contredit la maximalité de J_0 dans $\mathcal{J}$. Par suite, $J_0 = I$, donc I est de type fini.

Réciproquement, soit A un anneau unitaire, commutatif, dans lequel tout idéal est de type fini ; montrons qu'il vérifie la C.C.A. Si

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots \quad (2.14)$$

est une chaîne strictement croissante d'idéaux de A , alors $I = \bigcup_{n \in \mathbb{N}} I_n$ est un idéal de A (Prop. 2.11.). Supposons I engendré par $\{a_1, a_2, \dots, a_r\}$, $r \in \mathbb{N}^*$.

Quel que soit i ($1 \leq i \leq r$), il existe $n_i \in \mathbb{N}$, tel que $a_i \in I_{n_i}$. Soit $m = \sup\{n_i; 1 \leq i \leq r\}$; pour tout i ($1 \leq i \leq r$), on a $I_{n_i} \subseteq I_m$, d'où $\{a_1, a_2, \dots, a_r\} \subseteq I_m$ et par suite, $I \subseteq I_m$.

Mais $I = \bigcup_{n \in \mathbb{N}} I_n$ implique $I_m \subseteq I$, donc $I = I_m$; ainsi la chaîne (2.14) est finie et A est noethérien. $\square$

Remarque 2.83. :

a) Tout corps (commutatif) K est noethérien, puisque l'ensemble des idéaux de K est réduit à $\{(0), K\}$.

b) Tout anneau principal est noethérien, en particulier, l'anneau $\mathbb{Z}$ est noethérien.

Des exemples d'anneaux noethériens non principaux apparaîtront dans les chapitres suivants.

Proposition 2.84. *Un anneau unitaire et commutatif A est noethérien si et seulement si, quel que soit l'idéal propre I de A , A/I est noethérien.*

Preuve : Supposons A noethérien. Soit I un idéal propre de A et

$$\overline{J}_1 \subsetneq \overline{J}_2 \subsetneq \cdots \subsetneq \overline{J}_n \subsetneq \overline{J}_{n+1} \subsetneq \cdots \quad (2.15)$$

une chaîne strictement croissante d'idéaux de l'anneau unitaire et commutatif A/I . Pour tout $n \in \mathbb{N}^*$, posons $J_n = \pi^{-1}(\overline{J}_n)$, où π est le morphisme canonique de A sur A/I ; alors

$$I \subseteq J_1 \subsetneq J_2 \subsetneq \cdots \subsetneq J_n \subsetneq J_{n+1} \subsetneq \cdots$$

est une chaîne croissante d'idéaux de A , donc elle est stationnaire. Par suite, la chaîne (2.15) est finie, d'où A/I noethérien.

Réciproquement, si quel que soit l'idéal $I \neq A$, A/I est noethérien, alors $A = A/(0)$ est noethérien. $\square$

Théorème 2.85. *Un anneau unitaire et commutatif A est noethérien si et seulement si tout idéal premier de A est de type fini.*

Preuve : Si A est noethérien, alors (Th. 2.82.) tout idéal premier est de type fini ; démontrons la réciproque.

Tout idéal premier de A étant, par hypothèse, de type fini, supposons A non noethérien ; l'ensemble X des idéaux de A qui ne sont pas de type fini est alors non vide ; de plus X est partiellement ordonné par l'inclusion. On vérifie alors facilement que X est inductif (Déf. 2.69.) et l'Axiome de Zorn implique l'existence d'au moins un élément maximal P dans X (voir la preuve du Th. 2.68.).

Compte tenu des hypothèses, P n'est pas un idéal premier, donc il existe a, b dans A tels que $ab \in P$, $a \notin P$, $b \notin P$.

On a $P \subsetneq P + (a)$, $P \subsetneq P + (b)$ et P maximal dans X , par suite les idéaux $P + (a)$ et $P + (b)$ ne sont pas dans X , donc sont de type fini.

Soit $\{x_i + ay_i\}_{1 \leq i \leq n}$ une famille génératrice finie de l'idéal $P + (a)$; $n \in \mathbb{N}^*$ et pour tout i ($1 \leq i \leq n$), $x_i \in P$, $y_i \in A$.

Soit $J := \{z \in A; az \in P\}$; on a $P \subset J$ et on vérifie que J est un idéal de A ; alors,

$$(P \subset J \text{ et } ab \in P) \implies b \in J \implies P + (b) \subset J.$$

On en déduit que $J \notin X$, donc J est un idéal de type fini. Supposons J engendré par $\{z_1, z_2, \dots, z_r\}$, $r \in \mathbb{N}^*$ et démontrons que l'ensemble $\{x_1, \dots, x_n, az_1, \dots, az_r\}$ engendre l'idéal P .

Soit $p \in P$, a fortiori $p \in P + (a)$, d'où

$$p = \sum_{1 \leq i \leq n} \alpha_i (x_i + ay_i), \text{ où } \forall i (1 \leq i \leq n), \alpha_i \in A;$$

$$p = \sum_{1 \leq i \leq n} \alpha_i x_i + a (\sum_{1 \leq i \leq n} \alpha_i y_i) \implies a (\sum_{1 \leq i \leq n} \alpha_i y_i) \in P,$$

alors, $\sum_{1 \leq i \leq n} \alpha_i y_i \in J$, donc il existe des $\beta_j \in A$, $1 \leq j \leq r$, tels que

$$p = \sum_{1 \leq i \leq n} \alpha_i x_i + \sum_{1 \leq j \leq r} \beta_j (az_j).$$

Ainsi P est de type fini, ce qui contredit le fait que $P \in X$. On en conclut que A est noethérien. $\square$

7. Nilradical et Radical de Jacobson

Dans tout ce paragraphe, on ne considère que des anneaux **commutatifs, unitaires**.

Proposition 2.86. Dans un anneau commutatif, unitaire A , l'ensemble $\mathcal{N}$ des éléments nilpotents forme un idéal de A et l'anneau $A/\mathcal{N}$ n'a pas d'élément nilpotent non nul (Déf. 1.26.).

Preuve : Par définition, $\mathcal{N} = \{x \in A; \exists n \in \mathbb{N}^* \text{ tel que } x^n = 0\}$.

$\mathcal{N}$ n'est pas vide, car $0 \in \mathcal{N}$. Soit x, y dans $\mathcal{N}$; il existe m et n dans $\mathbb{N}^*$ tels que $x^m = 0$ et $y^n = 0$, alors

$$(-x)^m = (-1)^m x^m = 0 \quad \text{et} \quad (x+y)^{m+n} = \sum_{0 \leq p \leq m+n} C_{m+n}^p x^p y^{m+n-p} = 0$$

et quel que soit $a \in A$, $(ax)^m = a^m x^m = 0$. Par suite, $\mathcal{N}$ est un idéal de A .

Notons $\bar{x}$, la classe modulo $\mathcal{N}$ d'un élément x de A . Supposons $\bar{x}$ nilpotent dans $A/\mathcal{N}$; il existe $m \in \mathbb{N}^*$ tel que $\bar{x}^m = \bar{0}$; alors

$$\bar{x}^m = \bar{0} \iff \overline{x^m} = \bar{0} \iff x^m \in \mathcal{N}.$$

$$x^m \in \mathcal{N} \iff \exists p \in \mathbb{N}^* \text{ tel que } (x^m)^p = x^{mp} = 0$$

$$\text{et } x^{mp} = 0 \implies x \in \mathcal{N}, \text{ d'où } \bar{x} = \bar{0}.$$

Ainsi $A/\mathcal{N}$ n'a pas d'élément nilpotent non nul. $\square$

Définition 2.87. Dans un anneau unitaire commutatif A , l'idéal $\mathcal{N}$ formé par l'ensemble des éléments nilpotents est appelé le **nilradical** de A .

Théorème 2.88. Le nilradical $\mathcal{N}$ d'un anneau unitaire commutatif A est l'intersection de tous les idéaux premiers de A .

Preuve : On rappelle que l'ensemble des idéaux premiers de A est noté $\text{Spec}(A)$ (Déf. 2.59.).

a) Soit $x \in \mathcal{N}$; il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$. Or, quel que soit $P \in \text{Spec}(A)$, $0 \in P$ implique $x^n \in P$ et par suite $x \in P$ (Cor. 2.56.), d'où

$$x \in \mathcal{N} \implies x \in \bigcap_{P \in \text{Spec}(A)} P. \quad (2.16)$$

b) Démontrons que si $x \notin N$, alors $x \notin \bigcap_{P \in \text{Spec}(A)} P$.

Étant donné $x \in A \setminus N$, considérons l'ensemble X des idéaux I de A tels que : quel que soit $n \in \mathbb{N}^*$, $x^n \notin I$.

L'ensemble X est non vide, car $(0) \in X$; d'autre part X est partiellement ordonné par l'inclusion, on montre alors (voir la preuve du Th. 2.68.) que X est un ensemble *inductif* (Déf. 2.69.). On en déduit, en appliquant l'*Axiome de Zorn*, qu'il existe un élément *maximal* dans X , que nous noterons P_0 .

Montrons que P_0 est un idéal *premier* de A . Soit a et b dans $A \setminus P_0$; on a

$$P_0 \subsetneq P_0 + (a) \quad \text{et} \quad P_0 \subsetneq P_0 + (b),$$

donc les idéaux $P_0 + (a)$ et $P_0 + (b)$ n'appartiennent pas à l'ensemble X . On en déduit qu'il existe m et n dans $\mathbb{N}^*$ tels que

$$x^m \in P_0 + (a) \quad \text{et} \quad x^n \in P_0 + (b);$$

alors $x^{m+n} \in P_0 + (ab)$; par suite, $P_0 + (ab)$ n'appartient pas à X , donc $ab \notin P_0$. Ainsi P_0 est un idéal premier tel que $x \notin P_0$, d'où $x \notin \bigcap_{P \in \text{Spec}(A)} P$.

Compte tenu de l'implication (2.16) ci-dessus, on en conclut que

$$N = \bigcap_{P \in \mathcal{P}} P. \quad \square$$

Remarque 2.89. Si A est un domaine d'intégrité, alors son nilradical est nul, car (0) étant un idéal premier, $\bigcap_{P \in \text{Spec}(A)} P = (0)$; mais la réciproque est fautive.

En effet, si N est le nilradical d'un anneau unitaire commutatif A , d'après la proposition 2.86., le nilradical de l'anneau A/N est nul; cependant A/N n'est pas nécessairement intègre, car l'idéal N n'est pas nécessairement premier.

Définition 2.90. Soit A un anneau unitaire commutatif, on appelle **radical de Jacobson** de A , l'intersection des idéaux maximaux de A .

Nous désignerons par $\mathcal{J}(A)$ ce radical.

Les éléments de $\mathcal{J}(A)$ sont caractérisés par la propriété suivante :

Proposition 2.91. A étant un anneau unitaire commutatif, si U_A désigne l'ensemble de ses éléments inversibles, alors

$$x \in \mathcal{J}(A) \iff \forall y \in A, (1 - xy) \in U_A.$$

Preuve :

a) Supposons $x \in \mathcal{J}(A)$ et $y \in A$ tels que $(1 - xy) \notin U_A$. Le corollaire 2.72. implique l'existence d'un idéal maximal M de A contenant $1 - xy$ et d'après la définition de $\mathcal{J}(A)$,

$$x \in \mathcal{J}(A) \implies xy \in \mathcal{J}(A) \implies xy \in M.$$

$$[(1 - xy) \in M \text{ et } xy \in M] \implies 1 \in M,$$

ce qui est impossible; donc $(1 - xy) \in U_A$.

b) Soit $x \in A \setminus \mathcal{J}(A)$; il existe alors un idéal maximal M de A tel que $x \notin M$. On en déduit que $M + (x) = A$.

Par suite, il existe $a \in M$ et $y \in A$ tels que $a + xy = 1$; mais $(1 - xy) \in M$ implique $(1 - xy) \notin U_A$, d'où le résultat énoncé. $\square$

Corollaire 2.92. Dans tout anneau unitaire, commutatif A , on a

$$N(A) \subseteq \mathcal{J}(A),$$

où $N(A)$ désigne le nilradical de A .

Preuve : Quel que soit $x \in N(A) \setminus \{0\}$, il existe un entier $n > 1$ tel que $x^n = 0$; on en déduit que $1 - x$ est inversible dans A . En effet,

$$(1 - x)(1 + x + x^2 + \dots + x^{n-1}) = 1 - x^n = 1.$$

Par suite, $\mathcal{N}(A)$ étant un idéal de A ,

$$\forall x \in \mathcal{N}(A), \forall y \in A, (1 - xy) \in U_A;$$

d'où $\mathcal{N}(A) \subseteq \mathcal{J}(A)$, d'après la proposition 2.91. $\square$

Définition 2.93. Dans un anneau unitaire, commutatif A , on dit qu'un idéal I est un **nil-idéal** si tous les éléments de I sont nilpotents.

Remarque 2.94. La définition du nilradical de A et le corollaire 2.92. impliquent que pour tout nil-idéal I de A , on a $I \subseteq \mathcal{N}(A) \subseteq \mathcal{J}(A)$.

8. Anneaux booléens

Définition 2.95. On appelle **anneau booléen**, tout anneau unitaire dans lequel tout élément est *idempotent* (Déf. 1.28.).

Remarque 2.96. :

a) La définition 2.95. implique que tout sous-anneau unitaire d'un anneau booléen est un anneau booléen.

b) L'anneau de Boole $\mathcal{P}(E)$, des parties d'un ensemble non vide E , étudié dans l'Exercice 15, Chap. 1, est un anneau booléen, qui joue un rôle fondamental, puisque nous montrerons dans ce paragraphe, que tout anneau booléen est *isomorphe à un sous-anneau* d'un anneau de Boole du type $\mathcal{P}(E)$.

Proposition 2.97. Si B est un anneau booléen, alors

1) B est de caractéristique 2.

2) B est commutatif.

3) Tout $x \in B \setminus \{0, 1\}$ est un diviseur de zéro dans B . M Y

4) Tout idéal premier P de B est maximal et B/P est un corps à deux éléments.

Preuve :

1) B étant un anneau booléen, B est unitaire, donc $B \neq (0)$ et pour tout $x \in B$, on a $x^2 = x$; alors pour tout $x \neq 0$ dans B , on a

$$(x+x)^2 = x+x = 2x \implies 4x^2 = 4x = 2x \implies 2x = 0,$$

d'où car $B = 2$. Par suite, pour tout $x \in B$, on a $x = -x$.

2) Soit x et y non nuls dans B ;

$$(x^2 = x, y^2 = y, (x+y)^2 = x+y) \implies xy + yx = 0;$$

$$\text{alors } yx = -yx \implies xy - yx = 0,$$

donc B est anneau commutatif.

3) Pour $x \in B$, $x^2 = x \iff x(x-1) = 0$;

par suite, $x \neq 0$ et $x \neq 1$ implique : x diviseur de zéro dans B .

4) Soit P un idéal premier de B ; l'anneau quotient B/P est alors *intègre* (Th. 2.52.).

Pour tout $x \in B$, notons $\bar{x}$, la classe de x modulo P ;

$$(x(x-1) = 0, \text{ dans } B) \implies (\bar{x}(\bar{x}-\bar{1}) = \bar{0}, \text{ dans } B/P),$$

d'où $\bar{x} = \bar{0}$ ou $\bar{x} = \bar{1}$.

On en déduit que B/P est un domaine d'intégrité à deux éléments, c'est donc un *corps isomorphe à $\mathbb{Z}/2\mathbb{Z}$* (Prop. 1.24., Cor. 1.14.), par suite l'idéal P est maximal (Th. 2.62.). $\square$

Remarque 2.98. :

a) Le corps $\mathbb{Z}/2\mathbb{Z}$ est un cas particulier d'anneau booléen.

b) Les notations étant celles de la Prop. 2.97, la condition : $x^2 = x$, pour tout $x \in B$ implique *qu'un anneau booléen n'a pas d'élément nilpotent non nul* (Déf. 1.26.). On en déduit que le **nilradical de B est nul** (Déf. 2.87.).

Proposition 2.99. *Un anneau B est booléen si et seulement si il est isomorphe à un sous-anneau unitaire d'un produit direct de corps tous isomorphes à $\mathbb{Z}/2\mathbb{Z}$.*

Preuve : Soit $A = \prod_{i \in I} A_i$, où I est un ensemble non vide tel que pour tout $i \in I$, $A_i \simeq \mathbb{Z}/2\mathbb{Z}$; alors tout élément de A est idempotent, donc A est un anneau booléen et tout sous-anneau unitaire de A est booléen (Rem. 2.96.).

Réciproquement, soit B un anneau booléen. Compte tenu de la remarque 2.98., a), supposons $B \not\simeq \mathbb{Z}/2\mathbb{Z}$.

Soit $\{P_j\}_{j \in J}$ la famille des idéaux premiers de B ; B étant un anneau unitaire, cette famille est non vide (Th. 2.68., Cor. 2.64.). Pour tout $j \in J$, notons π_j la surjection canonique $B \rightarrow B/P_j$ et considérons

$$\begin{aligned}\theta : B &\longrightarrow \prod_{j \in J} B/P_j \\ x &\longmapsto (\pi_j(x))_{j \in J}.\end{aligned}$$

θ est un morphisme d'anneaux unitaires et $\text{Ker } \theta = \bigcap_{j \in J} P_j$. On en déduit que $\text{Ker } \theta$ est le nilradical $\mathcal{N}(B)$ de l'anneau B (Th. 2.88.); or $\mathcal{N}(B) = (0)$ (Rem. 2.98., b)), ce qui entraîne $B \simeq \text{Im } \theta$. Ainsi B est isomorphe à un sous-anneau de $\prod_{j \in J} B/P_j$, où pour tout $j \in J$, $B/P_j \simeq \mathbb{Z}/2\mathbb{Z}$ (Prop. 2.97.).

On remarque que si B n'a qu'un seul idéal maximal, alors d'après ce qui précède, celui-ci est nul; dans ce cas on a $B \simeq \mathbb{Z}/2\mathbb{Z}$. $\square$

Théorème 2.100. *Tout anneau booléen est isomorphe à un sous-anneau de l'anneau de Boole des parties d'un ensemble non vide.*

Preuve : Soit B un anneau booléen. Considérons, comme ci-dessus, la famille des idéaux premiers de B et en reprenant les mêmes notations que dans la démonstration précédente, posons

$$E := \{\pi_j\}_{j \in J} \quad \text{et} \quad \forall x \in B, E_x := \{\pi_j \in E; \pi_j(x) \neq \bar{0}\}.$$

Montrons que $E_x = \emptyset \iff x = 0$. En effet, quel que soit $j \in J$, π_j est un morphisme d'anneaux, donc $\pi_j(0) = \bar{0}$ et d'après ce qui précède,

$$(\forall j \in J, \pi_j(x) = \bar{0}) \implies x \in \bigcap_{j \in J} P_j = (0).$$

D'autre part, quel que soit $j \in J$, on a $\pi_j(B) = B/P_j \simeq \mathbb{Z}/2\mathbb{Z}$, donc il existe $x \in B$ tel que $\pi_j(x) \neq \bar{0}$. On en conclut que

$$E = \bigcup_{x \in B} E_x.$$

Vérifions l'injectivité de l'application

$$\begin{aligned}\phi : B &\longrightarrow \mathcal{P}(E) \\ x &\longmapsto E_x.\end{aligned}$$

Supposons $E_x = E_y$, non vide; alors, quel que soit π_j dans E_x , on a $\pi_j(x) = \pi_j(y) = \bar{1}$, d'où

$$\forall \pi_j \in E_x, (x - y) \in P_j = \text{Ker } \pi_j.$$

De plus, pour tout $\pi_j \in E \setminus E_x$, $\pi_j(x) = \pi_j(y) = \bar{0}$, par suite

$$(x - y) \in \bigcap_{j \in J} P_j = (0), \quad \text{donc } x = y.$$

Vérifions que ϕ est un morphisme d'anneaux unitaires de B dans l'anneau de Boole $\mathcal{P}(E)$ (Cf. Ex.15, Ch.1). On a

$$E_0 = \emptyset \iff \phi(0) = 0 \quad \text{dans l'anneau } \mathcal{P}(E)$$

$$E_1 = E \iff \phi(1) = 1 \quad \text{dans l'anneau } \mathcal{P}(E).$$

D'autre part, pour tout $j \in J$, B/P_j est un corps à deux éléments, donc pour x et y dans B , $\pi_j(xy) = \pi_j(x)\pi_j(y)$ implique

$$\pi_j(xy) = \bar{1} \iff \pi_j(x) = \bar{1} \text{ et } \pi_j(y) = \bar{1}.$$

On en déduit que : $E_{xy} = E_x \cap E_y$, ce qui équivaut à

$$\phi(xy) = \phi(x)\phi(y) \text{ dans l'anneau } \mathcal{P}(E).$$

De même $\pi_j(x+y) = \pi_j(x) + \pi_j(y)$, implique

$$\pi_j(x+y) = \bar{1} \iff \{(\pi_j(x) = \bar{1}, \pi_j(y) = \bar{0}) \text{ ou } (\pi_j(x) = \bar{0}, \pi_j(y) = \bar{1})\};$$

ainsi, $E_{x+y} = (E_x \setminus E_y) \cup (E_y \setminus E_x)$ est équivalent à

$$\phi(x+y) = \phi(x) + \phi(y) \text{ dans l'anneau } \mathcal{P}(E).$$

L'injectivité du morphisme ϕ implique $B \simeq \text{Im } \phi$, donc B est isomorphe à un sous-anneau de l'anneau de Boole $\mathcal{P}(E)$. $\square$

Théorème 2.101. *Tout anneau booléen fini B est isomorphe à l'anneau de Boole $\mathcal{P}(E)$ d'un certain ensemble fini E et il existe un entier $k > 0$ tel que $\text{card}(B) = 2^k$.*

Preuve : B étant un anneau booléen fini, soit $\{P_i\}_{1 \leq i \leq k}$ la famille, nécessairement finie, de ses idéaux premiers.

Démontrons que B est isomorphe à l'anneau $\prod_{1 \leq i \leq k} B/P_i$. Comme dans la preuve de la proposition 2.99., on considère le morphisme

$$\begin{aligned} \theta : B &\longrightarrow \prod_{1 \leq i \leq k} B/P_i \\ x &\longmapsto (\pi_i(x))_{1 \leq i \leq k}. \end{aligned}$$

On sait que θ est *injectif* et que tout P_i , $1 \leq i \leq k$, est un idéal *maximal* de B tel que $\text{card}(B/P_i) = 2$ (Prop. 2.97. et 2.99.).

Si $k > 1$ dans $\mathbb{N}$, on suppose naturellement que pour $i \neq j$, on a $P_i \neq P_j$; alors, pour tout couple (i, j) , $1 \leq i \leq k$, $1 \leq j \leq k$,

$$i \neq j \implies P_i + P_j = B.$$

Les idéaux P_i , $1 \leq i \leq k$, sont donc *deux à deux coprimiers* (Déf. 2.42.).

Le morphisme θ est alors *surjectif* (Prop. 2.46.), par suite θ est un isomorphisme, d'où

$$\text{card}(B) = \text{card}(\prod_{1 \leq i \leq k} B/P_i) = 2^k.$$

D'autre part, posons, comme dans la preuve du théorème précédent

$$E := \{\pi_i\}_{1 \leq i \leq k}.$$

E est un ensemble fini de cardinal k , alors $\text{card}(\mathcal{P}(E)) = 2^k$ ([15], t.1), par suite le morphisme d'anneaux

$$\begin{aligned} \phi : B &\longrightarrow \mathcal{P}(E) \\ x &\longmapsto E_x, \end{aligned}$$

qui est *injectif*, d'après la preuve du théorème 2.100., est ici *bijectif*, puisque B et $\mathcal{P}(E)$ sont des ensembles finis de même cardinal ([2]); d'où $B \simeq \mathcal{P}(E)$. $\square$

9. Exercices

1) Soit I un idéal à droite d'un anneau A . On pose

$$J = \{x \in A; ax = 0, \forall a \in I\}.$$

Montrer que J est un idéal bilatère de A .

- 2) Dans l'anneau $M_2(\mathbb{R})$ des matrices carrées d'ordre 2 sur le corps des nombres réels $\mathbb{R}$, on pose

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} ; (x, y) \in \mathbb{R} \times \mathbb{R} \right\} \quad ; \quad L = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} ; (x, y) \in \mathbb{R} \times \mathbb{R} \right\} ;$$

$$S = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} ; x, y, z \text{ dans } \mathbb{R} \right\}.$$

Montrer que dans l'anneau $M_2(\mathbb{R})$:

R est un idéal à droite ; L est un idéal à gauche ;

S est un sous-anneau qui n'est ni un idéal à droite, ni un idéal à gauche.

- 3) 1°) Démontrer les propriétés des opérations sur les idéaux d'un anneau, énoncées dans la proposition 2.22.

2°) Soit $n > 1$ dans $\mathbb{N}$ et $\{I_i\}_{1 \leq i \leq n}$ une famille d'idéaux bilatères d'un anneau A . On pose $S = \sum_{1 \leq i \leq n} I_i$. Montrer que la somme S est *directe* (Déf. 2.17.) si et seulement si S est isomorphe au *produit direct* des anneaux I_i , $1 \leq i \leq n$ (Déf. 1.79.).

- 4) Démontrer les théorèmes 2.31 et 2.35 (Voir [11], Ch.IV).

- 5) Soit A un anneau unitaire ; on note $Z(A)$ son centre (Déf. 1.32.).

On suppose qu'il existe dans A un élément non nul e tel que $e \neq 1$, $e^2 = e$, et $e \in Z(A)$. On dira que e est un *idempotent central* de A .

1°) Vérifier que $1 - e$ est aussi un idempotent central non nul de A .

Montrer que eA et $(1 - e)A$ sont des idéaux bilatères de A tels que

$$A = eA \oplus (1 - e)A.$$

2°) Soit $I \neq (0)$ un idéal bilatère *propre* de A .

Démontrer que les trois conditions suivantes sont équivalentes :

i) Il existe un idéal bilatère J de A tel que

$$A = I \oplus J.$$

ii) I est un anneau unitaire, d'élément unité $e \neq 1$.

iii) $I = eA$, où $e \neq 1$ est un idempotent central de A .

- 6) Soit A un anneau unitaire et commutatif. On suppose que A contient un idéal *maximal* M tel que

$$1 + M := \{1 + x ; x \in M\} \subseteq U_A,$$

où U_A est le groupe des éléments inversibles de A .

Prouver que A est un anneau *local* (Déf. 2.73.).

- 7) Soit A un *domaine d'intégrité* et U_A le groupe de ses éléments inversibles. Pour tout $x \in A$, on note (x) l'idéal de A engendré par x .

1°) Vérifier que : $(x) = (y) \iff \exists u \in U_A \text{ tel que } y = ux$.

2°) On suppose que (x) et (y) sont des idéaux *premiers*, *non nuls* de A .

Montrer que : $(x) \subseteq (y) \implies (x) = (y)$.

- 8) Soit A un anneau unitaire, commutatif, dans lequel on suppose que tout idéal *propre* est *premier*. Le but de cet exercice est de prouver que A est un corps.

1°) Vérifier que A est intègre.

2°) On suppose $A \setminus U_A \neq \{0\}$, U_A étant le groupe des éléments inversibles de A . Démontrer que quel que soit $x \neq 0$ dans $A \setminus U_A$, on a

$$(x) = A \setminus U_A,$$

où (x) est l'idéal de A engendré par x .

En déduire que A est un corps (Utiliser l'exercice 7 précédent).

9) Soit B un anneau booléen (Déf. 2.95.).

Démontrer que tout idéal de type fini de B est principal.

(Faire une récurrence sur le nombre n de générateurs d'un idéal de type fini, en considérant d'abord le cas $n = 2$).

10) Soit A un anneau unitaire et commutatif. On dira qu'une partie non vide S de A est une *partie multiplicative* de A , si

i) $1 \in S$ et $0 \notin S$;

ii) $(a, b) \in S \times S \implies ab \in S$.

1°) Soit P un idéal propre de A . Démontrer que $S \setminus P$ est une partie multiplicative de A si et seulement si P est un idéal premier de A .

2°) Soit S une partie multiplicative de A . On désigne par $\mathcal{S}$ l'ensemble des idéaux I de A tels que $S \cap I = \emptyset$. L'ensemble $\mathcal{S}$ étant ordonné par l'inclusion,

i) Justifier l'existence d'un élément maximal dans $\mathcal{S}$.

ii) Démontrer que tout élément maximal dans $\mathcal{S}$ est un idéal premier de A .

11) Dans un anneau unitaire, commutatif, A , on dira qu'une partie multiplicative S (Cf. exercice 10 précédent) est *saturée*, si quel que soit $x \in S$, on a

$$(y \in A^* \text{ et } y|x) \implies y \in S.$$

1°) Vérifier que dans A , l'ensemble, noté S_0 , des non-diviseurs de zéro est une partie multiplicative saturée.

2°) Soit S une partie multiplicative saturée de A .

a) Montrer que : $x \in A \setminus S \implies (x) \cap S = \emptyset$, où (x) est l'idéal de A engendré par x .

b) Pour $x \in A \setminus S$, on note $\mathcal{S}_x$ l'ensemble des idéaux I de A pour lesquels,

$$x \in I \text{ et } I \cap S = \emptyset.$$

- Montrer que $\mathcal{S}_x$, ordonné par l'inclusion, admet au moins un élément maximal, que l'on notera P_x .

- Prouver que P_x est un idéal premier de A .

3°) Utiliser les résultats précédents pour démontrer que les conditions suivantes sont équivalentes :

i) S est une partie multiplicative saturée de A .

ii) $A \setminus S$ est la réunion (ensembliste) d'une famille d'idéaux premiers de A .

4°) a) Quelle est la plus petite partie multiplicative saturée de A contenant l'élément unité de A ?

b) U_A étant l'ensemble des éléments inversibles de A , démontrer que $A \setminus U_A$ est la réunion de tous les idéaux maximaux de A .

12) Soit A un anneau unitaire, commutatif et $n \in \mathbb{N}^*$.

1°) Soit $\{I_i\}_{1 \leq i \leq n}$ une famille finie d'idéaux de A et P un idéal premier tel que $\bigcap_{1 \leq i \leq n} I_i \subseteq P$.

- Prouver qu'il existe i ($1 \leq i \leq n$) tel que $I_i \subseteq P$.

- En déduire que si $P = \bigcap_{1 \leq i \leq n} I_i$, alors il existe i ($1 \leq i \leq n$) tel que $P = I_i$.

2°) Soit $\{P_i\}_{1 \leq i \leq n}$ une famille finie d'idéaux premiers de A et I un idéal de A tel que $I \subseteq \bigcup_{1 \leq i \leq n} P_i$.

Démontrer qu'il existe $i (1 \leq i \leq n)$ tel que $I \subseteq P_i$.

- 13) Soit A et B deux anneaux unitaires, commutatifs et f un morphisme d'anneaux unitaires de A dans B .

1°) Soit I un idéal de A ; on rappelle que $f(I)$ n'est pas, en général, un idéal de B . L'idéal de B engendré par $f(I)$ est appelé *extension de I par f* ; on le notera I^e . Comment s'écrivent les éléments de I^e ?

2°) Soit j l'injection canonique de $\mathbb{Z}$ dans $\mathbb{Q}$. Si P est un idéal premier non nul de $\mathbb{Z}$, quel est l'idéal P^e , extension de P par j ?

En déduire, qu'en général, l'extension I^e d'un idéal premier I de A par un morphisme $f \in \text{Hom}(A, B)$ n'est pas un idéal premier de B .

- 14) Pour tout idéal I d'un anneau unitaire, commutatif, A , on pose

$$\sqrt{I} := \{x \in A; \exists n \in \mathbb{N}^*, x^n \in I\}.$$

1°) Montrer que $\sqrt{I}$ est un idéal de A , contenant I .

L'idéal $\sqrt{I}$ est appelé le *radical* de I .

2°) Soit π la surjection canonique $A \rightarrow A/I$.

$N(A/I)$ désignant le *nilradical* de l'anneau A/I (Déf. 2.87.), vérifier que

$$\sqrt{I} = \pi^{-1}(N(A/I)).$$

3°) Quels sont les idéaux $\sqrt{0}$ et $\sqrt{A}$? En déduire que dans A , $\sqrt{I}$ est un idéal propre si et seulement si I est un idéal propre.

4°) Soit $f \in \text{Hom}(A, B)$ un morphisme d'anneaux unitaires. Comme dans l'exercice 13 précédent, on note I^e , l'extension par f d'un idéal I de A . Démontrer que

$$(\sqrt{I})^e \subseteq \sqrt{I^e}.$$

- 15) Dans un anneau unitaire, commutatif A , un idéal Q est dit **primaire** si

i) $Q \neq A$;

ii) $\forall (x, y) \in A \times A, (xy \in Q, y \notin Q) \implies \exists n \in \mathbb{N}^*, x^n \in Q$.

1°) Vérifier que dans A , tout idéal premier est primaire.

2°) La notion de radical d'un idéal ayant été définie dans l'exercice 14 ci-dessus, prouver que si P est un idéal premier de A , alors, quel que soit $m \in \mathbb{N}^*$, $\sqrt{P^m} = P$.

3°) Démontrer que si Q est un idéal primaire de A , alors $\sqrt{Q}$ est un idéal premier de A et c'est le plus petit idéal premier de A contenant Q (La réciproque est fautive; voir exercice 5, Ch. 4).

4°) Déterminer tous les idéaux primaires de l'anneau $\mathbb{Z}$.

5°) Démontrer qu'un idéal Q de A est primaire si et seulement si $Q \neq A$ et tout diviseur de zéro dans A/Q est nilpotent.

6°) a) Soit M un idéal maximal de l'anneau A et soit $x \in A \setminus M$. Prouver qu'il existe $z \in A$ tel que $(xz - 1) \in M$ (Considérer l'anneau quotient A/M).

b) Soit I un idéal de A tel que $\sqrt{I}$ est un idéal maximal de A . On note $\bar{x}$ la classe modulo I d'un élément x de A .

Montrer, à l'aide du résultat a) ci-dessus, que dans l'anneau A/I ,

$$\bar{x} \neq \bar{0} \implies \bar{x} \text{ nilpotent ou inversible.}$$

En déduire, en utilisant la question 5°), que dans A

$$\sqrt{I} \text{ idéal maximal} \implies I \text{ idéal primaire.}$$

- 16) Dans un anneau unitaire, commutatif A , un idéal J sera dit **irréductible** si quels que soient les idéaux J_1, J_2 ,

$$J = J_1 \cap J_2 \implies J = J_1 \text{ ou } J = J_2.$$

1°) Vérifier que pour un idéal J de A

$$J, \text{ idéal irréductible dans } A \iff (\bar{0}), \text{ idéal irréductible dans } A/J.$$

En déduire que tout idéal maximal de A est irréductible.

2°) On suppose l'anneau A *noethérien*.

Le but de cette question est de prouver que tout idéal *propre* de A est l'intersection d'un nombre fini d'idéaux irréductibles de A .

On suppose qu'il n'en est pas ainsi, c'est-à-dire que l'ensemble, noté Σ , des idéaux *propres* de A qui ne sont pas intersection d'un nombre fini d'idéaux irréductibles est non vide.

Justifier l'existence d'un élément maximal I_0 dans l'ensemble Σ , ordonné par l'inclusion.

Démontrer qu'il existe des idéaux I_1 et I_2 de A tels que $I_0 = I_1 \cap I_2$.

En déduire une contradiction et conclure.

3°) On suppose, comme dans la question précédente, A *noethérien*.

En utilisant le 5°) de l'exercice 15 précédent, ainsi que le résultat de la question 1°) ci-dessus, démontrer que pour un idéal propre J de A , on a

$$J \text{ irréductible} \implies J \text{ primaire.}$$

Indication : étant donné $\bar{x}$ et $\bar{y}$ dans A/J tels que $\bar{x}\bar{y} = \bar{0}$ et $\bar{y} \neq \bar{0}$, on démontrera, en considérant la chaîne croissante d'idéaux de A/J

$$\text{Ann } \bar{x} \subseteq \text{Ann } \bar{x}^2 \subseteq \dots,$$

qu'il existe $n \in \mathbb{N}^*$ pour lequel $(\bar{y}) \cap (\bar{x}^n) = (\bar{0})$.

En conclure que, dans un anneau commutatif, noethérien, tout idéal propre est intersection d'un nombre fini d'idéaux *primaires*.



17) 1°) Soit E un ensemble non vide et partiellement ordonné.

On dit que E vérifie la *condition minimale* (C.m.), si tout sous-ensemble non vide de E contient un élément minimal.

On dit que E vérifie la *condition de chaîne descendante* (C.C.D.), si toute suite strictement décroissante (resp. décroissante) d'éléments de E est finie (resp. stationnaire).

Démontrer que les conditions (C.m.) et (C.C.D.) sont équivalentes.

2°) On dit qu'un anneau unitaire, commutatif est *artinien*, si l'ensemble de ses idéaux, partiellement ordonné par l'inclusion, vérifie la C.m. (équivalente à la C.C.D.).

a) Vérifier que tout corps est un anneau artinien.

b) Montrer que l'anneau des entiers, $\mathbb{Z}$, n'est pas artinien (alors que $\mathbb{Z}$ est noethérien, car principal).

Indication : considérer la chaîne strictement décroissante des idéaux de $\mathbb{Z}$, de la forme $2^n \mathbb{Z}$, pour $n \in \mathbb{N}$.

N.B. : On peut démontrer que tout anneau commutatif artinien est noethérien ([35]).

3°) Prouver qu'un anneau unitaire, commutatif, A , est artinien si et seulement si, pour tout idéal propre I de A , l'anneau quotient A/I est artinien.

4°) Montrer que tout domaine d'intégrité artinien, A , est un corps.

Indication : pour a non nul dans A , considérer la chaîne décroissante des idéaux principaux (a^n) , $n \in \mathbb{N}$.

5°) A étant un anneau commutatif artinien, soit $\mathcal{J}(A)$ son radical de Jacobson (Déf. 2.90.). On pose $J := \mathcal{J}(A)$.

Le but de cette question est de prouver que l'idéal J est nilpotent, c'est-à-dire qu'il existe un entier $m > 0$ tel que $J^m = (0)$.

a) En considérant la chaîne décroissante des idéaux J^n , pour $n \in \mathbb{N}$, justifier l'existence de $m \in \mathbb{N}^*$ tel que, quel que soit l'entier $n \geq m$, on ait $J^n = J^m$.

b) On suppose $J^m \neq (0)$, montrer qu'alors, l'ensemble, noté X , des idéaux I de A tels que $I \subseteq J^m$ et $I J^m \neq (0)$ est non vide et contient un élément minimal, que l'on notera I_0 . Prouver $I_0 = (0)$; en conclure que $J^m = (0)$.

18) *Spectre d'un anneau unitaire, commutatif ; Topologie de Zariski.*

Cet exercice suppose connues les notions élémentaires de Topologie Générale.

Soit A un anneau unitaire, commutatif. On rappelle que le *spectre* de A est l'ensemble des idéaux premiers de A , noté $\text{Spec}(A)$ (Déf. 2.59.). Pour toute partie non vide E de A , on pose

$$V(E) = \{P \in \text{Spec}(A) ; E \subseteq P\} \quad \text{et} \quad D(E) = \text{Spec}(A) \setminus V(E).$$

Si $E = \{x\}$, où $x \in A$, on écrira $V(E) = V(x)$ et $D(E) = D(x)$.

1°) a) Quels sont les ensembles $V(0)$ et $V(1)$?

Pour toute partie non vide E de A , on note I_E l'idéal de A engendré par E . Prouver que

$$V(E) = V(I_E) = V(\sqrt{I_E}),$$

où $\sqrt{I_E}$ est le radical de l'idéal I_E (Cf. Exercice 14, ci-dessus).

b) Si $\{E_i\}_{i \in I}$ est une famille non vide de parties de A , prouver que

$$V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} V(E_i).$$

c) Démontrer que, quels que soient les idéaux I et J de A , on a

$$V(I \cap J) = V(IJ) = V(I) \cup V(J).$$

2°) Montrer que les ensembles $V(E)$, pour E décrivant l'ensemble des parties non vides de A , vérifient les axiomes des *fermés* d'un espace topologique.

En conclure que $\text{Spec}(A)$ est ainsi muni d'une topologie, qui est appelée **Topologie de Zariski**, dont les *ouverts* sont les $D(E)$, pour E décrivant l'ensemble des parties non vides de A .

3°) Démontrer que pour toute partie non vide E de A , on a

$$D(E) = \bigcup_{x \in E} D(x).$$

En déduire, pour tout $P \in \text{Spec}(A)$, un système fondamental de voisinages (Cf. [17]).

Chapitre 3

Modules et Algèbres

Dans tout ce chapitre, A désigne un anneau unitaire.

1. Notion de A-module

Définition 3.1. A étant un anneau unitaire, on appelle **A-module à gauche**, tout ensemble non vide M muni

a) d'une loi de composition interne notée, en général, additivement et telle que $(M, +)$ est un groupe abélien ;

b) d'une loi de composition externe à opérateurs dans l'anneau A :

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, x) &\longmapsto ax \end{aligned}$$

vérifiant les conditions suivantes :

- i) $\forall x \in M, \forall (a, b) \in A \times A, (a + b)x = ax + bx.$
- ii) $\forall x \in M, \forall (a, b) \in A \times A, a(bx) = (ab)x$, noté abx .
- iii) $\forall (x, y) \in M \times M, \forall a \in A, a(x + y) = ax + ay.$
- iv) $\forall x \in M, 1x = x$ (1 étant l'élément unité de A).

On définit de même un **A-module à droite** (la loi de composition externe est définie sur $M \times A$).

Définition 3.2. A et B étant deux anneaux unitaires, on dira que M est un **A-B-bimodule**, si M est à la fois un A-module à gauche et un B-module à droite vérifiant la condition

$$\forall x \in M, \forall (a, b) \in A \times B, (ax)b = a(bx), \text{ noté } axb.$$

Notations : Compte tenu des définitions précédentes, on pourra écrire $M \in_A \text{Mod}$ (resp. $M \in \text{Mod}_A, M \in_A \text{Mod}_B$) pour exprimer que M est un A-module à gauche (resp. A-module à droite, A-B-bimodule).

Dans toute la suite, les propriétés générales seront énoncées et démontrées dans le cas des A-modules à gauche.

Exemple 3.3. :

1) Tout anneau unitaire A est un A-module à gauche et à droite. On notera ${}_A A$ (resp. A_A) le A-module à gauche (resp. à droite) A .

2) Tout groupe abélien $(G, +)$ est un $\mathbb{Z}$ -module à gauche ; par suite,

Tout anneau unitaire A est un $\mathbb{Z}$ -module à gauche.

Tout A-module à gauche est un $\mathbb{Z}$ -module à gauche.

3) Si K est un corps, tout K -espace vectoriel est un K -module à gauche (la loi de composition externe étant généralement notée à gauche).

Définition 3.4. Soit S une partie non vide d'un A -module à gauche M . On appelle **annulateur de S** , l'ensemble :

$$\text{Ann}(S) = \{a \in A ; \forall x \in S, ax = 0\}.$$

Proposition 3.5. Etant donné $M \in {}_A \text{Mod}$, pour toute partie non vide, S de M , $\text{Ann}(S)$ est un idéal à gauche de A .

Preuve : On a $\text{Ann}(S) \neq \emptyset$, car $0 \in \text{Ann}(S)$ et quels que soient a, a' dans $\text{Ann}(S)$, x dans S ,
 $(ax = 0 \text{ et } a'x = 0) \implies (a - a')x = 0 \implies (a - a') \in \text{Ann}(S)$.

D'autre part, quels que soient $a \in \text{Ann}(S)$, $b \in A$ et $x \in S$,
 $ax = 0 \implies bax = 0 \implies ba \in \text{Ann}(S)$,

par suite, $\text{Ann}(S)$ est un idéal à gauche de A . □

2. Sous-modules

A. Notion de sous-module

Définition 3.6. M étant un A -module à gauche, une partie non vide N de M est un **sous-module** (plus précisément, un **sous- A -module**) de M , si

- i) N est un sous groupe de $(M, +)$;
- ii) Pour tout $x \in N$ et tout $a \in A$, $ax \in N$.

Exemple 3.7. :

- 1) Dans tout A -module M , (0) et M sont des sous-modules de M .
- 2) Les sous-modules du A -module à gauche ${}_A A$ (resp. à droite A_A) sont les idéaux à gauche (resp. à droite) de l'anneau A .

Proposition 3.8. : Propriétés élémentaires des sous-modules

Soit $\{N_i\}_{i \in I}$ une famille non vide de sous-modules d'un A -module M ; alors, $\bigcap_{i \in I} N_i$ est un sous-module de M .

Par contre, $\bigcup_{i \in I} N_i$ n'est pas, en général, un sous-module de M .

Cependant, si la famille $\{N_i\}_{i \in I}$ est totalement ordonnée par l'inclusion, alors $\bigcup_{i \in I} N_i$ est un sous-module de M .

Démonstrations analogues à celles des Propositions 1.35. et 1.37.

Proposition 3.9. Soit $M \in {}_A \text{Mod}$, alors pour tout sous-module N de M , $\text{Ann}(N)$ est un idéal bilatère de A .

Preuve : On sait que $\text{Ann}(N)$ est un idéal à gauche de A (Prop. 3.5.). De plus, N étant un sous-module de M , quels que soient $a \in \text{Ann}(N)$, $b \in A$ et $x \in N$,

$$bx \in N \implies a(bx) = 0 = (ab)x \implies ab \in \text{Ann}(N);$$

donc $\text{Ann}(N)$ est un idéal bilatère de A . □

Définition 3.10. Un A -module à gauche M est dit **fidèle**, si $\text{Ann}(M) = (0)$.

Exemple 3.11. :

- 1) Si K est un corps, tout K -espace vectoriel est un K -module fidèle.
- 2) Si A est un anneau unitaire, alors ${}_A A$ (resp. A_A) est un A -module à gauche (resp. à droite) fidèle.

Proposition 3.12. Soit M un A -module à gauche. Notons $\bar{A}$ l'anneau unitaire, commutatif $A/\text{Ann}(M)$; alors M est un $\bar{A}$ -module à gauche fidèle.

Preuve : Montrons que la correspondance

$$\begin{aligned}\bar{A} \times M &\longrightarrow M \\ (\bar{a}, x) &\longmapsto ax\end{aligned}$$

est une application. En effet, supposons $\bar{a} = \bar{b}$ dans $\bar{A}$,

$$\begin{aligned}\bar{a} = \bar{b} &\iff (a - b) \in \text{Ann}(M) \iff \forall x \in M, (a - b)x = 0, \\ &\iff \forall x \in M, ax = bx.\end{aligned}$$

Par suite, on peut définir sur M , une loi de composition externe à opérateurs dans $\bar{A}$ telle que

$$\forall x \in M, \forall \bar{a} \in \bar{A}, \bar{a}x = ax$$

et on vérifie que M est ainsi un $\bar{A}$ -module à gauche. De plus,

$$\begin{aligned}\forall x \in M, \bar{a}x = 0 &\iff \forall x \in M, ax = 0 \\ &\iff a \in \text{Ann}(M) \iff \bar{a} = \bar{0},\end{aligned}$$

donc M est un $\bar{A}$ -module à gauche fidèle. □

B. Sous-module engendré par une partie d'un A-module

Définition 3.13. Soit S une partie non vide d'un A -module M . On appelle **sous-module** (ou **sous-A-module**) de M **engendré par** S , l'intersection de tous les sous-modules de M contenant S ; c'est donc *le plus petit sous-module de M contenant S .*

Si M est un A -module à gauche (resp. à droite), on notera ${}_A(S)$ (resp. $(S)_A$) le sous-module de M engendré par S .

Proposition 3.14. *Compte tenu des notations ci-dessus,*

$${}_A(S) = \left\{ \sum_{1 \leq i \leq n} a_i x_i ; n \in \mathbb{N}^*, \forall i (1 \leq i \leq n), a_i \in A, x_i \in S \right\}. \quad (3.1)$$

Démonstration laissée au lecteur (Voir preuve de la Prop. 1.40.).

Définition 3.15. Si M est un A -module à gauche et $x_1, x_2, \dots, x_n$ sont des éléments de M ($n \in \mathbb{N}^*$), on appelle **combinaison linéaire sur A des x_i** , ($1 \leq i \leq n$), tout élément $x \in M$ de la forme

$$x = \sum_{1 \leq i \leq n} a_i x_i, \text{ où } \forall i (1 \leq i \leq n), a_i \in A.$$

Remarque 3.16. La relation (3.1) montre que ${}_A(S)$ est l'ensemble des combinaisons linéaires sur A de toutes les parties finies (non vides) de S .

Définition 3.17. Une partie non vide S d'un A -module à gauche M est une **partie génératrice** de M , si ${}_A(S) = M$.

On dit aussi, dans ce cas, que S *engendre le A-module M* ou que S *est un ensemble de générateurs de M .*

Définition 3.18. M étant un A -module à gauche,

a) M est dit **de type fini**, s'il possède une partie génératrice finie.

Dans ce cas, si $S = \{x_1, x_2, \dots, x_n\}$ engendre M , alors

$$x \in M \iff x = \sum_{1 \leq i \leq n} a_i x_i, \text{ où } \forall i (1 \leq i \leq n), a_i \in A.$$

b) M est dit **monogène**, s'il est engendré par un seul élément x ; alors

$$M = Ax = \{ax; a \in A\}.$$

C. Somme de sous-modules

On définit la notion de *somme de sous-modules* d'un A-module, comme on a défini la notion de *somme d'idéaux* d'un anneau, dans le Chapitre 2.

1. Cas d'une famille finie de sous-modules

Soit $\{N_i\}_{1 \leq i \leq n}$, $n \in \mathbb{N}^*$, une famille finie de sous-modules d'un A-module M . On pose

$$\sum_{1 \leq i \leq n} N_i = \{\sum_{1 \leq i \leq n} x_i ; \forall i (1 \leq i \leq n), x_i \in N_i\}.$$

On vérifie que $\sum_{1 \leq i \leq n} N_i$ est un sous-module de M .

Définition 3.19. Avec les hypothèses ci-dessus, le sous-module $\sum_{1 \leq i \leq n} N_i$ de M est appelé **somme des sous-modules** N_i , $1 \leq i \leq n$.

Comme dans le cas des idéaux d'un anneau (Prop. 2.13.), on démontre le résultat suivant.

Proposition 3.20. Etant donné une famille finie $\{N_i\}_{1 \leq i \leq n}$ de sous-modules d'un A-module M , $\sum_{1 \leq i \leq n} N_i$ est le sous-module de M engendré par $\bigcup_{1 \leq i \leq n} N_i$.

2. Cas d'une famille quelconque de sous-modules

Etant donnée une famille non vide quelconque, $\{N_i\}_{i \in I}$, de sous-modules d'un A-module M , on note $\sum_{i \in I} N_i$ l'ensemble suivant

$$\{\sum_{1 \leq j \leq m} x_{i_j} ; m \in \mathbb{N}^*, \{i_j\}_{1 \leq j \leq m} \subseteq I, \forall j (1 \leq j \leq m), x_{i_j} \in N_{i_j}\}.$$

Proposition 3.21. Avec les hypothèses ci-dessus, $\sum_{i \in I} N_i$ est un sous-module de M , appelé **somme des sous-modules** N_i ($i \in I$) et c'est le sous-module de M engendré par $\bigcup_{i \in I} N_i$.

Même justification que dans le cas des idéaux (Prop. 2.15.).

Remarque 3.22. Compte tenu des notations et résultats précédents,

a) Pour tout $j \in I$, N_j est un sous-module de $\sum_{i \in I} N_i$.

b) L'expression des éléments de $\sum_{i \in I} N_i$ montre que si l'ensemble I est de cardinal infini, alors $x \in \sum_{i \in I} N_i$ si et seulement s'il existe une partie finie $\{i_1, i_2, \dots, i_m\}$ de I telle que $x \in \sum_{1 \leq j \leq m} N_{i_j}$. On pourra cependant écrire

$$x = \sum_{i \in I} x_i, \text{ où, pour tout } i \in I, x_i \in N_i,$$

les x_i étant "presque tous nuls" (c'est-à-dire "nuls sauf un nombre fini d'entre eux"), car tout $x \in \sum_{i \in I} N_i$ est une somme finie d'éléments de $\bigcup_{i \in I} N_i$.

3. Somme directe de sous-modules

Définition 3.23. Etant donné une famille non vide quelconque $\{N_i\}_{i \in I}$ de sous-modules d'un A-module M , on dit que la somme $\sum_{i \in I} N_i$ est **directe** si tout $x \in \sum_{i \in I} N_i$ s'écrit de façon unique

$$x = \sum_{1 \leq j \leq m} x_{i_j}, \text{ où } m \in \mathbb{N}^* \text{ et } \forall j (1 \leq j \leq m), i_j \in I, x_{i_j} \in N_{i_j}.$$

Dans ce cas la somme $\sum_{i \in I} N_i$ est notée $\bigoplus_{i \in I} N_i$.

Le résultat qui suit se démontre comme dans le cas des idéaux (Prop. 2.18.).

Proposition 3.24. Les notations étant celles de la définition 3.23., les conditions suivantes sont équivalentes :

- 1) La somme des sous-modules N_i , pour $i \in I$, est directe.
- 2) $(\sum_{i \in I} x_i = 0 \text{ dans } \sum_{i \in I} N_i) \implies x_i = 0, \forall i \in I$.
- 3) $\forall j \in I, N_j \cap \sum_{i \in I \setminus \{j\}} N_i = (0)$.

Définition 3.25. Soit M un A-module à gauche,

- a) Deux sous-modules N_1 et N_2 de M sont dits **supplémentaires** dans M , si $M = N_1 \oplus N_2$.
- b) Un sous-module N de M est dit **facteur direct** dans M , s'il existe un sous-module N' de M tel que $M = N \oplus N'$.

Remarque 3.26. :

- a) Avec les notations précédentes :

$$M = N_1 \oplus N_2 \iff M = N_1 + N_2 \text{ et } N_1 \cap N_2 = (0).$$

- b) Si $M = \bigoplus_{i \in I} N_i$, où $\{N_i\}_{i \in I}$ est une famille non vide de sous-modules de M , alors pour tout $j \in I$, N_j est facteur direct dans M .

En effet, le groupe $(M, +)$ étant abélien, le 3) de la proposition 3.24., implique

$$M = N_j \oplus \left(\bigoplus_{i \in I \setminus \{j\}} N_i \right).$$

- c) Un sous-module N d'un A-module M n'est pas, en général, un facteur direct dans M . On sait cependant que dans un K-espace vectoriel, tout sous-espace vectoriel a un supplémentaire, donc est facteur direct.

3. Morphismes de A-modules



Définition 3.27. Soient M et M' deux A-modules à gauche ; une application $f : M \longrightarrow M'$ est un **morphisme de A-modules** si

- i) f est un morphisme de groupes de $(M, +)$ dans $(M', +)$.
- ii) $\forall x \in M, \forall a \in A, f(ax) = af(x)$.

On note $\text{Hom}_A(M, M')$ l'ensemble des morphismes (on dit aussi *homomorphismes*) de M dans M' .

Un morphisme d'un A-module M dans lui-même est appelé **endomorphisme** (ou plus précisément **A-endomorphisme**) de M .

On note $\text{End}_A(M)$ l'ensemble des endomorphismes d'un A-module M .

Exemple 3.28. :

- 1) Si N est un sous-module d'un A-module M , alors l'injection canonique, $i : N \longrightarrow M$, telle que pour tout $x \in N, i(x) = x$, est un morphisme de A-modules.
- 2) M et M' étant deux A-modules, l'application

$$\begin{aligned} M &\longrightarrow M' \\ x &\longmapsto 0 \end{aligned}$$

est un morphisme de A-modules, appelé **morphisme nul** et noté 0.

Définition 3.29. Pour $f \in \text{Hom}_A(M, M')$,

$f(M) := \{f(x); x \in M\}$ est appelé **image** de f et noté **Im f**.

$f^{-1}(0) := \{x \in M; f(x) = 0\}$ est appelé **noyau** de f et noté **Ker f**.

Propriétés élémentaires (à vérifier par le lecteur) :

Avec les notations de la définition précédente :

1) N sous-module de $M \implies f(N)$ sous-module de M' .

En particulier, $Im f$ est un sous-module de M' .

2) N' sous-module de $M' \implies f^{-1}(N')$ sous-module de M .

En particulier, $Ker f$ est un sous-module de M .

3) (f surjectif $\iff Im f = M$) et (f injectif $\iff Ker f = (0)$).

4) Composition des morphismes :

$$\{f \in Hom_A(M, M') \text{ et } g \in Hom_A(M', M'')\} \implies g \circ f \in Hom_A(M, M'').$$

Proposition 3.30. Pour deux A -modules à gauche M et M' ,

1) $Hom_A(M, M')$ est un groupe additif abélien.

2) Si l'anneau A est commutatif, alors $Hom_A(M, M')$ est un A -module à gauche.

Preuve :

1) On définit une addition dans $Hom_A(M, M')$ telle que pour tout couple (f, f') de morphismes de A -modules de M dans M' , on ait

$$\forall x \in M, (f + f')(x) = f(x) + f'(x).$$

On vérifie que $(Hom_A(M, M'), +)$ est alors, un groupe additif abélien.

2) Lorsque l'anneau A est commutatif, montrons que le groupe abélien $(Hom_A(M, M'), +)$ peut être muni d'une structure de A -module à gauche.

Pour $a \in A$ et $f \in Hom_A(M, M')$ considérons l'application

$$af : M \longrightarrow M' \text{ telle que pour tout } x \in M, af(x) = a(f(x)).$$

Vérifions que $af \in Hom_A(M, M')$. On a

$$\forall (x, y) \in M \times M, af(x+y) = a(f(x+y)) = a(f(x) + f(y)) = a(f(x)) + a(f(y)),$$

$$\text{d'où } af(x+y) = af(x) + af(y).$$

D'autre part,

$$\forall b \in A, \forall x \in M, af(bx) = a(bf(x)) = abf(x).$$

La commutativité de l'anneau A implique :

$$abf(x) = b(af(x)), \text{ d'où } af(bx) = b(af(x)).$$

L'application :

$$A \times Hom_A(M, M') \longrightarrow Hom_A(M, M')$$

$$(a, f) \longmapsto af$$

définit alors, sur le groupe abélien $(Hom_A(M, M'), +)$, une loi de composition externe à opérateurs dans A , satisfaisant aux conditions de la définition 3.1. (à vérifier); ainsi $Hom_A(M, M')$ est un A -module à gauche. $\square$

Définition 3.31. Pour deux A -modules M et M' , une application f de M dans M' est un **isomorphisme** de A -modules, si $f \in Hom_A(M, M')$ et s'il existe $g \in Hom_A(M', M)$ tel que

$$g \circ f = id_M \text{ et } f \circ g = id_{M'}. \quad (3.2)$$

Remarque 3.32. Les relations (3.2) impliquent qu'un isomorphisme de A -modules, f , est une application *bijective* et $g = f^{-1}$.

Proposition 3.33. Soit deux A -modules M et M' ,

1) f étant une application de M dans M' , alors

f isomorphisme de M sur $M' \iff f \in Hom_A(M, M')$ et f bijectif.

2) f isomorphisme M sur $M' \implies f^{-1}$ isomorphisme de M' sur M .

La preuve est analogue à celle faite dans le cas des groupes ([11], p.45) et des anneaux (Prop. 1.62.).

Définition 3.34. :

- a) Deux A -modules M et M' sont dits **isomorphes** (ou **A-isomorphes**) s'il existe un isomorphisme de A -modules de l'un sur l'autre ; on écrit alors, symboliquement, $M \simeq M'$.
 b) Un isomorphisme d'un A -module M sur lui-même est appelé un **automorphisme** de M ; l'ensemble de ces automorphismes est noté $\text{Aut}_A(M)$.

Proposition 3.35. Pour un A -module M , $\text{Aut}_A(M)$ est un groupe par rapport à la loi $\circ$ de composition des morphismes.

Même justification que dans le cas des anneaux (Prop. 1.64.).

Remarque 3.36. Si A est un corps K et $M := E$ est un K -espace vectoriel, alors le groupe $\text{Aut}_K(E)$ est le **groupe linéaire** de E , généralement noté $GL_K(E)$, ou simplement $GL(E)$, s'il n'y a pas d'ambiguïté possible.

4. Modules quotients

A étant un anneau unitaire quelconque, soit M un A -module à gauche et N un sous-module de M .

On sait que $(N, +)$ est un sous-groupe du groupe abélien $(M, +)$; on montre alors facilement que la relation d'équivalence $\mathcal{R}_N$, définie dans M par

$$x \mathcal{R}_N y \iff (x - y) \in N,$$

est compatible avec la loi de composition externe à opérateurs dans A , c'est-à-dire que pour x et y dans M ,

$$\forall a \in A, \quad x \mathcal{R}_N y \implies ax \mathcal{R}_N ay. \quad (3.3)$$

On note $\bar{x}$ la classe d'équivalence modulo $\mathcal{R}_N$ (on dit aussi, modulo N) d'un élément x de M .

De (3.3) on déduit que le groupe abélien quotient $(M/N, +)$ peut être muni d'une loi de composition externe à opérateurs dans A , définie par

$$\begin{aligned} A \times M/N &\longrightarrow M/N \\ (a, \bar{x}) &\longmapsto \overline{ax}. \end{aligned}$$

En effet, d'après (3.3), quels que soient $a \in A, \bar{x}$ et $\bar{x}'$ dans M/N , on a

$$\bar{x} = \bar{x}' \implies \overline{ax} = \overline{ax'}.$$

On peut donc poser, dans M/N , $a\bar{x} = \overline{ax}$.

On vérifie alors que M/N est muni d'une structure de A -module à gauche induite par celle de M .

Définition 3.37. Le A -module à gauche M/N , défini ci-dessus, est appelé **A-module quotient** du A -module M par le sous-module N .

Remarque 3.38. :

- a) Pour un idéal à gauche L d'un anneau unitaire A , le A -module à gauche quotient de ${}_A A$ par L sera noté A/L .

On pourra considérer de même, le A -module à droite, A/R , quotient de A_A par un idéal à droite R .

- b) Pour tout A -module quotient M/N , l'application

$$\pi : M \longrightarrow M/N \quad \text{telle que} \quad \pi(x) = \bar{x}$$

est un morphisme surjectif de A -modules, appelé **surjection canonique**.

On démontre que le couple $(M/N, \pi)$ satisfait à une *propriété universelle*, semblable à celle vue dans le cas des groupes quotients et des anneaux quotients (Th. 2.31.), dont on déduit les théorèmes d'isomorphisme classiques.

Nous ne ferons, ici, qu'énoncer ces théorèmes, leurs démonstrations étant analogues à celles des théorèmes 2.31., 2.34., 2.39. et 2.41.

Théorème 3.39. Propriété universelle du couple $(M/N, \pi)$

Quels que soient le A -module P et le morphisme $f \in \text{Hom}_A(M, P)$ pour lequel $N \subseteq \text{Ker } f$, il existe un unique morphisme $\varphi \in \text{Hom}_A(M/N, P)$ tel que $\varphi \circ \pi = f$.

Le théorème se traduit par la commutativité du diagramme suivant

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/N \\ & \searrow f & \downarrow \exists! \varphi \\ & & P \end{array}$$

Théorème 3.40. Premier théorème d'isomorphisme

Pour tout morphisme de A -module, $f \in \text{Hom}_A(M, M')$, on a

$$\text{Im } f \simeq M / \text{Ker } f \quad (\text{isomorphisme de } A\text{-modules}).$$

Théorème 3.41. Deuxième théorème d'isomorphisme

Quels que soient les sous-modules N_1 et N_2 d'un A -module M , on a

$$(N_1 + N_2) / N_2 \simeq N_1 / (N_1 \cap N_2) \quad (\text{isomorphisme de } A\text{-modules}).$$

Corollaire 3.42. Pour un A -module M et deux sous-modules N, N' , on a

$$M = N \oplus N' \implies M/N \simeq N' \text{ et } M/N' \simeq N \quad (\text{isom. de } A\text{-modules}).$$

Preuve : L'hypothèse du corollaire implique $N \cap N' = (0)$; le résultat découle alors immédiatement du deuxième théorème d'isomorphisme. $\square$

Théorème 3.43. Troisième théorème d'isomorphisme

Quels que soient les sous-modules N et N' d'un A -module M tels que $N' \subseteq N$, on a

$$M/N \simeq (M/N') / (N/N') \quad (\text{isomorphisme de } A\text{-modules}).$$

5. Produit direct et somme directe de A -modules

A. Produit direct de A -modules

Soit $\{M_i\}_{i \in I}$ une famille non vide de A -modules à gauche. On considère le groupe abélien $(P, +)$, produit direct des groupes abéliens $(M_i, +)$, $i \in I$:

$$P = \prod_{i \in I} M_i = \{(x_i)_{i \in I} ; x_i \in M_i, \forall i \in I\}.$$

L'addition dans P est telle que : $(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}$
(Cf. [11], Ch. I et VIII).

Une loi de composition externe, à opérateurs dans A , est définie sur P par

$$\begin{aligned} A \times P &\longrightarrow P \\ (a, (x_i)_{i \in I}) &\longmapsto (ax_i)_{i \in I}. \end{aligned}$$

La structure de A -module à gauche de chaque M_i , $i \in I$, induit alors une structure de A -module à gauche sur P .

Définition 3.44. Le A-module à gauche $P = \prod_{i \in I} M_i$ est appelé **produit direct** des A-modules $M_i, i \in I$.

Si I est fini et $I = \{1, 2, \dots, n\}$, on écrit

$$P = \prod_{1 \leq i \leq n} M_i = M_1 \times M_2 \times \dots \times M_n.$$

Définition 3.45. Morphismes canoniques associés au produit direct.

Quel que soit l'ensemble non vide I , on définit, pour tout $j \in I$,

a) la **projection canonique** :

$$p_j : \prod_{i \in I} M_i \longrightarrow M_j \quad \text{telle que} \quad p_j((x_i)_{i \in I}) = x_j.$$

b) l'**injection canonique** :

$$q_j : M_j \longrightarrow \prod_{i \in I} M_i \quad \text{telle que} \quad q_j(x_j) = (x_i)_{i \in I}, \text{ où } x_i = 0, \text{ si } i \neq j.$$

Pour tout $j \in I$, p_j (resp. q_j) est un morphisme *surjectif* (resp. *injectif*) de A-modules et
 $i \neq j \implies q_i \circ p_j = 0; \quad p_j \circ q_j = id_{M_j}; \quad Im q_j \simeq M_j;$

$$\forall x \in \prod_{i \in I} M_i, \quad x = (p_i(x))_{i \in I}.$$

Si I est fini et $I = \{1, 2, \dots, n\}$, alors

$$x = (x_i)_{1 \leq i \leq n} \in \prod_{1 \leq i \leq n} M_i \implies x = \sum_{1 \leq i \leq n} q_i(x_i) = \sum_{1 \leq i \leq n} (q_i \circ p_i)(x).$$

Théorème 3.46. Propriété universelle du couple $(\prod_{i \in I} M_i, \{p_i\}_{i \in I})$.

Quels que soient le A-module à gauche N et la famille de morphismes $\{f_i\}_{i \in I}$ telle que pour tout $i \in I$, $f_i \in Hom_A(N, M_i)$, il existe un unique morphisme $g \in Hom_A(N, \prod_{i \in I} M_i)$ vérifiant :

$$\forall i \in I, p_i \circ g = f_i.$$

Cette propriété est semblable à celle déjà vue dans le cas du produit direct d'anneaux (Th. 1.81.) ; elle exprime que, pour tout $i \in I$, le diagramme suivant commute

$$\begin{array}{ccc} N & \xrightarrow{\exists! g} & \prod_{i \in I} M_i \\ f_i \downarrow & \nearrow p_i & \\ M_i & & \end{array}$$

Du théorème 3.46., on déduit les corollaires suivants (démonstrations proposées en exercice : n° 1, Ch. 3).

Corollaire 3.47. Les hypothèses et les notations étant celles du théorème 3.46., l'application

$$\begin{aligned} \phi : Hom_A(N, \prod_{i \in I} M_i) &\longrightarrow \prod_{i \in I} Hom_A(N, M_i) \\ g &\longmapsto (p_i \circ g)_{i \in I} \end{aligned}$$

est un isomorphisme de groupes additifs. Si de plus, l'anneau A est commutatif, alors ϕ est un isomorphisme de A-modules à gauche.

Corollaire 3.48. Etant donné deux familles non vides de A-modules à gauche $\{M_i\}_{i \in I}$ et $\{M'_i\}_{i \in I}$, alors

$$(\forall i \in I, M_i \simeq M'_i) \implies \prod_{i \in I} M_i \simeq \prod_{i \in I} M'_i.$$

B. Somme directe de A-modules

La notion de *somme directe* de A-modules se définit comme celle de somme directe de groupes abéliens ([11], Ch. VIII).

Définition 3.49. Etant donné une famille non vide de A-modules à gauche $\{M_i\}_{i \in I}$, pour tout $x = (x_i)_{i \in I}$ dans le A-module $P = \prod_{i \in I} M_i$, on appelle **support** de x , l'ensemble :

$$\text{supp}(x) = \{i \in I; x_i \neq 0\}.$$

Si $\text{supp}(x)$ est une partie finie de I , on dit que x est à **support fini**.

Posons $M = \{x \in \prod_{i \in I} M_i; x \text{ à support fini}\}$.

Pour $x = 0$, on a $\text{supp}(x) = \emptyset$, donc $0 \in M$ et on vérifie que M est un sous-module de $P = \prod_{i \in I} M_i$.

Définition 3.50. Etant donné une famille non vide de A-modules à gauche $\{M_i\}_{i \in I}$, le sous-module M de $P = \prod_{i \in I} M_i$, défini ci-dessus, est appelé **somme directe des A-modules** $M_i, i \in I$. On écrit

$$M = \bigoplus_{i \in I} M_i.$$

Remarque 3.51. Compte tenu des notations précédentes

a) $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i \iff I$ est fini.

b) Pour toute injection canonique $q_i, i \in I$, $\text{Im } q_i$ est un sous-module de $M = \bigoplus_{i \in I} M_i$. On en déduit que :

$$\sum_{i \in I} \text{Im } q_i \subseteq \bigoplus_{i \in I} M_i.$$

D'autre part, si $x \in M$ et $\text{supp}(x) = \{i_1, i_2, \dots, i_n\}$, alors $x = \sum_{1 \leq j \leq n} q_{i_j}(x_{i_j})$; par suite, $x \in \sum_{i \in I} \text{Im } q_i$.

De plus, la définition des q_i implique que pour tout $j \in I$,

$$\text{Im } q_j \cap \sum_{i \in I \setminus \{j\}} \text{Im } q_i = (0),$$

donc la somme $\sum_{i \in I} \text{Im } q_i$ des sous-modules $\text{Im } q_i$ de $\bigoplus_{i \in I} M_i$ est directe (Déf. 3.50.). On en conclut que

$$\bigoplus_{i \in I} M_i = \bigoplus_{i \in I} \text{Im } q_i. \quad (3.4)$$

On notera que dans le premier membre de l'égalité (3.4), le symbole $\bigoplus$ exprime une somme directe de A-modules et dans le second membre le même symbole exprime une somme directe de sous-modules de $M = \bigoplus_{i \in I} M_i$.

c) Les injections canoniques q_i , pour $i \in I$, associées au *produit direct* des A-modules M_i , pourront aussi être considérées, comme associées à la *somme directe* des M_i .

Théorème 3.52. Propriété universelle du couple $(\bigoplus_{i \in I} M_i, \{q_i\}_{i \in I})$

Quels que soient le A-module à gauche N et la famille de morphismes $\{f_i\}_{i \in I}$ telle que pour tout $i \in I$, $f_i \in \text{Hom}_A(M_i, N)$, il existe un unique morphisme $h \in \text{Hom}_A(\bigoplus_{i \in I} M_i, N)$ vérifiant la condition :

$$\forall i \in I, h \circ q_i = f_i.$$

La preuve est la même que dans le cas de la somme directe de groupes abéliens ([11], Ch. VIII).

Le théorème exprime que, pour tout $i \in I$, le diagramme suivant commute

$$\begin{array}{ccc} M_i & \xrightarrow{q_i} & \bigoplus_{i \in I} M_i \\ & \searrow f_i & \downarrow \exists! h \\ & & N \end{array}$$

donc pour $x \in \bigoplus_{i \in I} M_i$ et $\text{supp}(x) = \{i_1, i_2, \dots, i_n\}$, on a

$$h(x) = h(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = h(\sum_{1 \leq j \leq n} q_{i_j}(x_{i_j})) = \sum_{1 \leq j \leq n} f_{i_j}(x_{i_j}).$$

Dans le cas particulier où $I = \{1, 2\}$, on obtient le diagramme suivant

$$\begin{array}{ccccc} M_1 & \xrightarrow{q_1} & M_1 \oplus M_2 & \xleftarrow{q_2} & M_2 \\ & \searrow f_1 & \vdots \exists! h & \swarrow f_2 & \\ & & N & & \end{array}$$

donc $h \circ q_1 = f_1$, $h \circ q_2 = f_2$ et quel que soit $(x_1, x_2) \in M_1 \oplus M_2$, on a $h(x_1, x_2) = f_1(x_1) + f_2(x_2)$.

Corollaire 3.53. Avec les hypothèses du théorème 3.52., l'application

$$\begin{aligned} \psi : \text{Hom}_A(\bigoplus_{i \in I} M_i, N) &\longrightarrow \prod_{i \in I} \text{Hom}_A(M_i, N) \\ h &\longmapsto (h \circ q_i)_{i \in I} \end{aligned}$$

est un isomorphisme de groupes et lorsque l'anneau A est commutatif, alors ψ est un isomorphisme de A -modules.

Démonstration proposée en exercice (n° 1, Ch. 3).

En conséquences des corollaires 3.47. et 3.53. on obtient :

Proposition 3.54. Pour une famille finie, non vide de A -modules à gauche $\{M_i\}_{1 \leq i \leq n}$, on a les isomorphismes de groupes suivants :

$$\text{Hom}_A(N, \bigoplus_{1 \leq i \leq n} M_i) \simeq \bigoplus_{1 \leq i \leq n} \text{Hom}_A(N, M_i). \quad (3.5)$$

$$\text{Hom}_A(\bigoplus_{i \in I} M_i, N) \simeq \bigoplus_{1 \leq i \leq n} \text{Hom}_A(M_i, N). \quad (3.6)$$

Corollaire 3.55. Pour deux familles finies, non vides de A -modules à gauche $\{M_i\}_{1 \leq i \leq n}$ et $\{N_j\}_{1 \leq j \leq p}$, l'application

$$\begin{aligned} \text{Hom}_A(\bigoplus_{1 \leq i \leq n} M_i, \bigoplus_{1 \leq j \leq p} N_j) &\longrightarrow \bigoplus_{(i,j)} \text{Hom}_A(M_i, N_j) \\ h &\longmapsto (p_j \circ h \circ q_i)_{(i,j)}, \end{aligned}$$

où les q_i sont les injections canoniques associées à $\bigoplus_{1 \leq i \leq n} M_i$ et les p_j sont les projections canoniques associées à $\bigoplus_{1 \leq j \leq p} N_j$, est un isomorphisme de groupes.

Remarque 3.56. Dans la proposition 3.54. et le corollaire 3.55., les isomorphismes de groupes deviennent des isomorphismes de A -modules à gauche, lorsque A est un anneau commutatif.

Proposition 3.57. Soit $\{M_i\}_{i \in I}$ une famille non vide de A -modules à gauche. Pour tout $i \in I$, désignons par N_i , un sous-module de M_i ; alors $\bigoplus_{i \in I} N_i$ est un sous-module de $\bigoplus_{i \in I} M_i$ et le quotient $\bigoplus_{i \in I} M_i / \bigoplus_{i \in I} N_i$ est isomorphe au A -module $\bigoplus_{i \in I} M_i / N_i$.

Preuve : On vérifie facilement que $\bigoplus_{i \in I} N_i$ est un sous-module de $\bigoplus_{i \in I} M_i$.

Quel que soit $i \in I$, notons π_i la surjection canonique : $M_i \rightarrow M_i/N_i$.

Pour tout $(x_i)_{i \in I}$ dans $\bigoplus_{i \in I} M_i$, les x_i étant "presque tous nuls", les $\pi_i(x_i)$ sont aussi "presque tous nuls"; par suite

$$(\pi_i(x_i))_{i \in I} \in \bigoplus_{i \in I} M_i/N_i$$

et on peut considérer l'application

$$\begin{aligned} \pi : \bigoplus_{i \in I} M_i &\longrightarrow \bigoplus_{i \in I} M_i/N_i \\ (x_i)_{i \in I} &\longmapsto (\pi_i(x_i))_{i \in I}. \end{aligned}$$

On vérifie que π est un morphisme de A -modules et sa définition implique sa surjectivité. D'autre part,

$$(x_i)_{i \in I} \in \text{Ker } \pi \iff \forall i \in I, \pi_i(x_i) = 0,$$

donc $\text{Ker } \pi = \bigoplus_{i \in I} N_i$ et d'après le premier théorème d'isomorphisme,

$$\bigoplus_{i \in I} M_i / \bigoplus_{i \in I} N_i \simeq \bigoplus_{i \in I} M_i / N_i. \quad \square$$

Notations : Soit M un A -module et $n \geq 2$ dans $\mathbb{N}$, on note M^n la somme directe de n modules égaux à M , on dit : de n copies de M .

Plus généralement, I étant un ensemble non vide quelconque, si pour tout $i \in I$, M_i est une copie de M , on écrit alors

$$M^I = \prod_{i \in I} M_i \quad \text{et} \quad M^{(I)} = \bigoplus_{i \in I} M_i. \quad (3.7)$$

$M^{(I)}$ est un sous-module de M^I et d'après la remarque 3.51., a),

$$M^{(I)} = M^I \iff I \text{ est un ensemble fini.}$$

On rappelle que deux ensembles sont dits **équipotents** ou de **même cardinal**, s'il existe une bijection de l'un sur l'autre ; lorsque les ensembles sont finis, cela signifie qu'ils ont le même nombre d'éléments.

Définition 3.58. On dit qu'un ensemble est **dénombrable** s'il est équipotent à une partie de $\mathbb{N}$.

En particulier, tout ensemble fini (y compris l'ensemble vide) ou équipotent à $\mathbb{N}$ est dénombrable ; dans ce dernier cas, on dit que l'ensemble est *infini dénombrable*.

Les relations (3.7) montrent que pour des ensembles non vides I et J ,

$$\text{card}(I) = \text{card}(J) \implies M^I = M^J \text{ et } M^{(I)} = M^{(J)}. \quad (3.8)$$

6. Notion de A -module libre

Remarque 3.59. K étant un corps, on sait que tout K -espace vectoriel a une *base*, c'est-à-dire, une partie génératrice et libre sur K .

(Voir un cours d'Algèbre Linéaire).

On rappelle que si E est un K -espace vectoriel, alors $\mathcal{B} = \{e_i\}_{i \in I}$ est une *base* de E si et seulement si tout $x \in E$ s'écrit de *façon unique* :

$$x = \sum_{i \in I} a_i e_i, \text{ où les } a_i \text{ sont "presque tous nuls" dans } K.$$

Définition 3.60. M étant un A -module à gauche, une **partie non vide** $X = \{x_i\}_{i \in I}$, de M est dite **libre sur A** , si pour toute partie finie non vide $\{i_1, i_2, \dots, i_p\}$ de I , on a

$$(\sum_{1 \leq j \leq p} a_j x_{i_j} = 0, \text{ où } \forall j (1 \leq j \leq p), a_j \in A) \implies \forall j (1 \leq j \leq p), a_j = 0.$$

Remarque 3.61. :

a) *Par convention*, on considère la partie vide d'un A-module quelconque, comme une partie libre.

b) D'après la définition 3.60., quel que soit le A-module M , $\{0\}$ n'est pas une partie libre de M .

c) Si X est une partie libre non vide d'un A-module M , alors

$$X' \subseteq X \implies X' \text{ partie libre de } M.$$

Par suite, 0 n'appartient à aucune partie libre de M .

Définition 3.62. Un A-module M est dit **libre** s'il possède une partie génératrice, libre sur A.

Dans ce cas, toute partie libre et génératrice du A-module M est appelée une **base** de M sur A.

Remarque 3.63. :

a) *Par convention*, le A-module (0) est considéré comme *libre*, de base l'ensemble vide.

b) Tout K-espace vectoriel est un K-module libre (Rem. 3.59.).

c) A étant un anneau unitaire, le A-module à gauche ${}_A A$ (resp. à droite A_A) est libre de base $\{1\}$.

d) Si A n'est pas un corps, un A-module n'est pas nécessairement libre.

En particulier tout $\mathbb{Z}$ -module n'est pas libre, puisque qu'un groupe abélien fini, de cardinal $n > 1$, n'est pas un $\mathbb{Z}$ -module libre ([11], Ch. VIII).

Proposition 3.64. Pour un A-module à gauche $M \neq (0)$, les conditions suivantes sont équivalentes :

1) M est libre de base $X = \{x_i\}_{i \in I}$.

2) Tout $x \in M$ s'écrit de façon unique :

$$x = \sum_{i \in I} a_i x_i; \text{ les } a_i \text{ étant "presque tous nuls" dans } A.$$

3) $M \simeq A^{(I)}$ (isomorphisme de A-modules à gauche).

Preuve : L'équivalence des propriétés 1) et 2) est une conséquence directe des définitions 3.60. et 3.62.

La condition 2) équivaut à $M = \bigoplus_{i \in I} Ax_i$; or, pour tout $i \in I$, on a $Ax_i \simeq_A A$, d'où l'équivalence des conditions 2) et 3) (Cf. Cor. 3.48.). $\square$

Corollaire 3.65. M est un A-module à gauche libre de base $\{x_1, x_2, \dots, x_n\}$, $n > 0$, si et seulement si M est isomorphe au A-module à gauche A^n .

Remarque 3.66. :

a) Dans la proposition 3.64., $X = \{x_i\}_{i \in I}$, donc $\text{card}(X) = \text{card}(I)$; d'où $A^{(X)} = A^{(I)}$, d'après la relation (3.8).

On en conclut qu'étant donné un anneau unitaire A et un ensemble X, il existe toujours un A-module libre de base X, défini à un isomorphisme près et que nous noterons ici, $F_{(X)}$.

$$\text{Si } X = \emptyset, F_{\emptyset} = (0); \quad \text{si } X \neq \emptyset, F_{(X)} \simeq A^{(X)}.$$

En particulier, si $\text{card}(X) = n > 0$, dans $\mathbb{N}$, on a $F_{(X)} \simeq A^n$.

b) On rappelle (Voir un cours d'Algèbre Linéaire) qu'un K-espace vectoriel E, ayant une partie génératrice finie, a une base finie et que toutes ses bases ont le même cardinal, appelé *dimension* de E sur K.

Plus généralement, on démontre (Ex. 9, Ch. 3) que si A est un anneau unitaire, commutatif, alors toutes les bases d'un A-module libre F ont le même cardinal (que celui-ci soit fini

ou non); lorsque ce cardinal est fini, il est appelé le **rang** de F ; sinon on dit que F est libre de **rang infini**.

Ce résultat est démontré pour les $\mathbb{Z}$ -modules libres dans ([11], Ch. VIII).

c) Lorsque l'anneau unitaire A n'est pas commutatif, la propriété ci-dessus n'est plus nécessairement vraie, pour les A -modules libres ayant une base finie; c'est-à-dire qu'un tel A -module peut avoir des bases finies n'ayant pas le même cardinal (Ex. 8, Ch. 3).

Théorème 3.67. : Propriété universelle d'un A -module libre

Soit M un A -module à gauche engendré par une partie non vide X . On note α l'injection canonique de X dans M ; alors M est un A -module libre de base X si et seulement si quels que soient le A -module à gauche N et l'application $f : X \rightarrow N$, il existe un unique morphisme $\varphi \in \text{Hom}_A(M, N)$ tel que $\varphi \circ \alpha = f$.

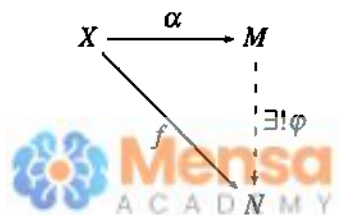
Preuve :

1°) On suppose que M est un A -module libre de base $X \neq \emptyset$. Montrons que le couple (M, α) vérifie la propriété énoncée.

Posons $X = \{x_i\}_{i \in I}$; tout $x \in M$ s'écrit alors de façon unique

$$x = \sum_{i \in I} a_i x_i; \text{ les } a_i \text{ étant "presque tous nuls" dans } A.$$

Dans le diagramme suivant



où le A -module à gauche N et l'application f sont donnés, on définit l'application φ en posant, pour tout $x = \sum_{i \in I} a_i x_i$ dans M :

$$\varphi(x) = \sum_{i \in I} a_i f(x_i).$$

On vérifie que φ est un morphisme de A -modules à gauche et sa définition implique $\varphi \circ \alpha = f$.

De plus, φ est unique. En effet, s'il existe $\varphi' \in \text{Hom}_A(M, N)$ tel que $\varphi' \circ \alpha = f$, alors pour tout $x = \sum_{i \in I} a_i x_i$ dans M , on a

$$\begin{aligned} \varphi'(x) &= \sum_{i \in I} a_i \varphi'(x_i) = \sum_{i \in I} a_i (\varphi' \circ \alpha)(x_i) \\ &= \sum_{i \in I} a_i f(x_i) = \varphi(x), \quad \text{donc } \varphi' = \varphi. \end{aligned}$$

2°) Réciproquement, soit M_1 un A -module à gauche engendré par un ensemble non vide X , tel que, α_1 étant l'injection canonique de X dans M_1 , le couple (M_1, α_1) vérifie la propriété énoncée dans le théorème 3.67.

D'autre part, soit (M, α) le couple formé par un A -module libre de base X et l'injection canonique de X dans M .

Les hypothèses impliquent qu'il existe un unique $\psi \in \text{Hom}_A(M_1, M)$ et un unique $\varphi \in \text{Hom}_A(M, M_1)$ tels que

$$\psi \circ \alpha_1 = \alpha \quad \text{et} \quad \varphi \circ \alpha = \alpha_1$$

$$\text{d'où} \quad \varphi \circ \psi \circ \alpha_1 = \alpha_1 \quad \text{et} \quad \psi \circ \varphi \circ \alpha = \alpha.$$

$$\text{Par suite,} \quad \forall x \in X, \quad \varphi \circ \psi(x) = x \quad \text{et} \quad \psi \circ \varphi(x) = x.$$

$$\text{On en déduit que} \quad \varphi \circ \psi = id_{M_1} \quad \text{et} \quad \psi \circ \varphi = id_M.$$

car φ et ψ sont des morphismes de A-modules, M et M_1 étant engendrés par X . On en conclut que φ et ψ sont des isomorphismes, $\psi = \varphi^{-1}$ et quel que soit $x \in X$, $\psi(x) = x$, donc M_1 est un A-module libre de base X . $\square$

Théorème 3.68. *Tout A-module à gauche M est quotient d'un A-module à gauche libre. Lorsque M est de type fini, alors M est quotient d'un A-module à gauche libre de type fini.*

Preuve : Supposons $M \neq (0)$ et considérons une partie génératrice X de M ; notons j l'injection canonique de X dans M .

Par ailleurs, soit F un A-module libre de base X et α l'injection canonique de X dans F . D'après la propriété universelle vérifiée par le couple (F, α) (Th. 3.67.), il existe un unique morphisme $\varphi \in \text{Hom}_A(F, M)$ tel que le diagramme suivant commute

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & F \\ & \searrow j & \vdots \exists! \varphi \\ & & M \end{array}$$

donc, $\varphi \circ \alpha = j$.

Si $X = \{x_i\}_{i \in I}$, alors tout $x \in M$ s'écrit $x = \sum_{i \in I} a_i x_i$, où les a_i sont "presque tous nuls" dans A .

D'autre part, on a $\forall i \in I, x_i = j(x_i) = \varphi \circ \alpha(x_i)$, donc,

$$x = \sum_{i \in I} a_i (\varphi \circ \alpha)(x_i) = \varphi \left(\sum_{i \in I} a_i \alpha(x_i) \right), \text{ car } \varphi \in \text{Hom}_A(F, M).$$

On en déduit que φ est surjectif, d'où

$$M \simeq F / \text{Ker } \varphi.$$

Si le A-module M est de type fini, engendré par $X = \{x_1, x_2, \dots, x_n\}$, avec $n > 0$ dans $\mathbb{N}$, le raisonnement précédent montre que M est quotient d'un A-module libre F de base X , donc de type fini.

On remarque que dans ce cas, on a $F \simeq A^n$, donc M est isomorphe à un quotient du A-module à gauche A^n . $\square$

7. Suites exactes de A-modules

Définition 3.69. Soit N, M, P trois A-modules à gauche.

Etant donné $f \in \text{Hom}_A(N, M)$, $g \in \text{Hom}_A(M, P)$, on dit que le diagramme

$$N \xrightarrow{f} M \xrightarrow{g} P \quad (3.9)$$

est une suite exacte en M , si $\text{Im } f = \text{Ker } g$.

La notion générale de suite exacte de A-modules est la suivante :

Définition 3.70. Soit I une partie de $\mathbb{N}$ telle que $\text{card}(I) \geq 3$. Etant donné une famille $\{M_i\}_{i \in I}$ de A-modules à gauche et une famille $\{f_i\}_{i \in I}$ de morphismes de A-modules telle que, pour tout $i \in I$, $f_i \in \text{Hom}_A(M_i, M_{i+1})$, on dit que la suite

$$\cdots M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \cdots \quad (3.10)$$

est une **suite exacte** de A -modules si

$$\forall i \in I, \operatorname{Im} f_i = \operatorname{Ker} f_{i+1}.$$

Pour I fini et $I = \{0, 1, \dots, n\}, n \geq 2$ dans $\mathbb{N}$, la suite du type (3.10), est exacte, si

$$\forall i (0 \leq i \leq n-1), \operatorname{Im} f_i = \operatorname{Ker} f_{i+1}.$$

Exemple 3.71. Notons 0 le A -module nul ; alors, pour tout A -module M , les flèches $0 \longrightarrow M$ et $M \longrightarrow 0$ désignent des morphismes nuls.

On en déduit que, N, M, P , étant des A -modules à gauche et f, g des morphismes de A -modules, on a

- 1) $0 \longrightarrow N \xrightarrow{f} M$ est exacte $\iff f$ est injectif.
- 2) $M \xrightarrow{f} P \longrightarrow 0$ est exacte $\iff f$ est surjectif.
- 3) $0 \longrightarrow N \xrightarrow{f} M \longrightarrow 0$ est exacte $\iff f$ est un isomorphisme.
- 4) Compte tenu de ce qui précède

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0 \quad (3.11)$$

est exacte si et seulement si f est injectif, g est surjectif et $\operatorname{Im} f = \operatorname{Ker} g$.

Définition 3.72. Une suite exacte de A -modules, du type (3.11) ci-dessus, est appelée une **suite exacte courte**.

Exemple 3.73. Soit N un sous-module d'un A -module M , alors la suite

$$0 \longrightarrow N \xrightarrow{j} M \xrightarrow{\pi} M/N \longrightarrow 0, \quad (3.12)$$

où j est l'injection canonique et π la surjection canonique, est une suite exacte courte.

Proposition 3.74. Toute suite exacte courte de A -modules à gauche

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

est "isomorphe" à la suite exacte courte suivante

$$0 \longrightarrow \operatorname{Im} f \xrightarrow{j} M \xrightarrow{\pi} M/\operatorname{Im} f \longrightarrow 0.$$

Autrement dit, il existe des isomorphismes de A -modules, $\operatorname{Im} f \xrightarrow{u} N$ et $M/\operatorname{Im} f \xrightarrow{v} P$ tels que le diagramme suivant commute

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Im} f & \xrightarrow{j} & M & \xrightarrow{\pi} & M/\operatorname{Im} f \longrightarrow 0 \\ & & \downarrow u & & \downarrow id_M & & \downarrow v \\ 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P \longrightarrow 0 \end{array} \quad (3.13)$$

donc $f \circ u = j$ et $v \circ \pi = g$.

Preuve : Par hypothèse, f est injectif, g est surjectif et $\operatorname{Im} f = \operatorname{Ker} g$.

Soit f_1 la restriction surjective de f :

$$f_1 : N \longrightarrow \operatorname{Im} f \quad \text{et} \quad \forall x \in N, f_1(x) = f(x).$$

Le morphisme f_1 est surjectif et il est injectif, car f est injectif, donc f_1 est un isomorphisme. On en déduit que $u = f_1^{-1}$ est un isomorphisme de $Im f$ sur N et

$$f \circ u = id_{Im f} \implies f \circ u = j = id_M \circ j.$$

D'autre part, d'après la propriété universelle du module quotient (Th. 3.39.), la condition $Im f = Ker g$ implique l'existence d'un unique morphisme $v \in Hom_A(M/Im f, P)$ tel que le diagramme suivant commute

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/Im f \\ & \searrow g & \downarrow \exists! v \\ & & P \end{array}$$

d'où $v \circ \pi = g = g \circ id_M$. De plus, $Ker g = Im f$ implique v injectif, g surjectif entraîne v surjectif, donc v est un isomorphisme de $M/Im f$ sur P . $\square$

8. A-modules noethériens

Définition 3.75. A étant un anneau unitaire, commutatif, un A -module à gauche (ou à droite) est dit **noethérien** si l'ensemble de ses sous-modules, partiellement ordonné par l'inclusion, vérifie la *condition de chaîne ascendante* (C.C.A.) équivalente à la *condition maximale* (C.M.) (Déf. 2.78.).

Théorème 3.76. Un A -module M est noethérien si et seulement si tout sous-module de M est de type fini.

La méthode de démonstration est la même que dans le cas des anneaux noethériens (Th. 2.82.).

Remarque 3.77. Un anneau unitaire, commutatif A est noethérien si et seulement si le A -module ${}_A A$ (ou A_A) est noethérien.

Proposition 3.78. Soit M un A -module.

a) Si M est noethérien, alors tout sous-module et tout quotient de M est un A -module noethérien.

b) S'il existe un sous-module N de M tel que N et M/N sont des A -modules noethériens, alors M est noethérien.

Preuve :

a) On suppose M noethérien. Soit N un sous-module de M , $N \neq (0)$.

L'ensemble des sous-modules de N est l'ensemble des sous-modules de M contenus dans N , donc tout sous-module de N est de type fini, d'où N noethérien.

Les sous-modules du A -module M/N sont les A -modules quotients N'/N , où N' décrit l'ensemble des sous-modules de M contenant N ; tous les sous-modules N' de M étant de type fini, il en est de même de des sous-modules N'/N , de M/N , qui est donc un A -module noethérien.

b) $N \neq (0)$ et M/N étant, par hypothèse, des A -modules noethériens, considérons une suite croissante de sous-modules de M ,

$$P_0 \subseteq P_1 \subseteq \dots \subseteq P_i \subseteq P_{i+1} \subseteq \dots \quad (3.14)$$

Les ensembles $\{P_i \cap N\}_{i \in \mathbb{N}}$ et $\{(P_i + N)/N\}_{i \in \mathbb{N}}$ forment, respectivement, une suite croissante de sous-modules de N et de M/N , par suite il existe m et m' dans $\mathbb{N}$ tels que

$$n \geq m \implies P_n \cap N = P_{n+1} \cap N. \quad (3.15)$$

$$n \geq m' \implies (P_n + N)/N = (P_{n+1} + N)/N. \quad (3.16)$$

Démontrons que pour tout $n \geq \sup\{m, m'\}$, on a $P_n = P_{n+1}$.

Par hypothèse, on a $P_n \subseteq P_{n+1}$, il suffit de prouver l'inclusion inverse.

Compte tenu des égalités (3.15) et (3.16), le deuxième théorème d'isomorphisme (Th. 3.41.) implique

$$P_n/P_n \cap N = P_{n+1}/P_n \cap N.$$

On en déduit que

$$\forall x \in P_{n+1}, \exists y \in P_n \text{ tel que } (x - y) \in P_n \cap N \subseteq P_n,$$

d'où $x \in P_n$, ce qui entraîne l'égalité $P_n = P_{n+1}$. On en conclut que la chaîne croissante (3.14) est stationnaire, donc M est noethérien. $\square$

Corollaire 3.79. Soit $\{M_i\}_{1 \leq i \leq n}$ une famille finie ($n \in \mathbb{N}^*$) de A -modules à gauche noethériens ; alors le A -module à gauche $M := \bigoplus_{1 \leq i \leq n} M_i$ est noethérien.

Preuve :

Pour $n = 2$, $M = M_1 \oplus M_2$; alors M_1 et $M/M_1 \simeq M_2$ sont noethériens, donc M est noethérien, d'après la proposition 3.78.

Pour $n > 2$, on raisonne par récurrence sur n . $\square$

Corollaire 3.80. Si A est un anneau commutatif, noethérien, alors tout A -module de type fini est noethérien.

Preuve : Soit M un A -module de type fini ; alors M est le quotient d'un A -module libre de type fini (Th. 3.68.), donc M est isomorphe à un quotient de A^n , pour un certain entier $n > 0$.

Par hypothèse ${}_A A$ est noethérien, on en déduit (Cor. 3.79.) que pour tout entier $n > 0$, le A -module $A^n = ({}_A A)^n$ est noethérien et par suite M est noethérien (Prop. 3.78.). $\square$

9. Notion de A -algèbre

Définition 3.81. A étant un anneau unitaire et commutatif, on dit que R est une A -algèbre à gauche si

- i) R est un anneau unitaire (élément unité 1_R) ;
- ii) R est un A -module à gauche ;
- iii) $\forall (x, y) \in R \times R, \forall a \in A, a(xy) = (ax)y = x(ay)$.

On définit de même une A -algèbre à droite. Dans la suite, de façon générale, nous considérerons des A -algèbres à gauche.

Une A -algèbre R est dite **commutative** si l'anneau R est commutatif.

Une A -algèbre R est dite **libre** si le A -module R est libre.

On remarque que si K est un corps, toute K -algèbre est libre.

Exemple 3.82. :

1) Tout anneau unitaire est une $\mathbb{Z}$ -algèbre.

Un anneau unitaire et commutatif A est une A -algèbre à droite et à gauche.

2) Si K est un corps, l'anneau $M_n(K)$ des matrices carrées d'ordre $n > 1$ sur K est une K -algèbre libre, non commutative.

Il en est de même de l'anneau $\text{End}_K(E)$ des endomorphismes d'un K -espace vectoriel E tel que $\dim_K(E) > 1$.

3) Dans le chapitre 4, nous construirons l'algèbre des polynômes à une ou plusieurs indéterminées sur un anneau unitaire commutatif.

4) La $\mathbb{R}$ -algèbre des quaternions fait l'objet du paragraphe 10/ suivant.

5) Au chapitre 7, nous étudierons les algèbres de séries formelles.

Définition 3.83. R étant une A -algèbre, une partie S de R est une **sous-algèbre** (plus précisément, une **sous- A -algèbre**) de R si S est à la fois un sous-anneau unitaire et un sous- A -module de R .

Remarque 3.84. Pour un entier $n > 1$, $n\mathbb{Z}$ n'est pas une sous- $\mathbb{Z}$ -algèbre de $\mathbb{Z}$, car $1 \notin n\mathbb{Z}$.

Définition 3.85. Pour deux A -algèbres R et R' , une application f de R dans R' est un **morphisme de A -algèbres**, si f est à la fois un morphisme d'anneaux unitaires et un morphisme de A -modules.

10. Algèbre des quaternions réels

Dans le Chapitre 1 (Exemple 1.17), nous avons défini l'anneau à division (ou corps gauche) $\mathbb{H}$ des quaternions en tant que sous-anneau de l'anneau $M_2(\mathbb{C})$ des matrices carrées d'ordre 2 sur le corps des nombres complexes. L'étude qui suit montre que $\mathbb{H}$ est une $\mathbb{R}$ -algèbre, d'où l'appellation : *Algèbre des quaternions réels*.

Rappelons que

$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} ; (x, y) \in \mathbb{C} \times \mathbb{C} \right\}. \quad (3.17)$$

A. La $\mathbb{R}$ -algèbre $\mathbb{H}$

Proposition 3.86. Le centre, $Z(\mathbb{H})$, de l'anneau à division $\mathbb{H}$ est isomorphe au corps des nombres réels, $\mathbb{R}$.

Preuve : Soit I la matrice unité de $M_2(\mathbb{C})$; montrons que

$$Z(\mathbb{H}) = \{aI ; a \in \mathbb{R}\}.$$

Il est immédiat que pour tout $a \in \mathbb{R}$, $aI \in Z(\mathbb{H})$.

Réciproquement, si $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in Z(\mathbb{H})$, alors, pour tout $\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \in \mathbb{H}$,

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

donc, quel que soit $(x, y) \in \mathbb{C} \times \mathbb{C}$,

$$ax - b\bar{y} = ax - \bar{b}y, \quad \bar{b}x + a\bar{y} = a\bar{y} + \bar{b}x \quad (3.18)$$

$$ay + b\bar{x} = bx + \bar{a}y, \quad -\bar{b}y + a\bar{x} = -b\bar{y} + a\bar{x}. \quad (3.19)$$

A partir des relations (3.18) et (3.19), on obtient

$$\forall y \in \mathbb{C}, b\bar{y} \in \mathbb{R}, \text{ donc } b \in \mathbb{R} ; \text{ alors,}$$

$$b(x - \bar{x}) = (a - \bar{a})\bar{y} = (a - \bar{a})y, \text{ implique}$$

$$\forall y \in \mathbb{C}, (a - \bar{a})(\bar{y} - y) = 0,$$

d'où $a - \bar{a} = 0$, par suite $a \in \mathbb{R}$ et $b = 0$. L'application

$$\phi : Z(\mathbb{H}) \longrightarrow \mathbb{R} \quad \text{telle que} \quad \phi(aI) = a \quad (3.20)$$

est alors un isomorphisme du sous-anneau $Z(\mathbb{H})$ de $\mathbb{H}$, sur le corps $\mathbb{R}$. $\square$

Théorème 3.87. *Le corps gauche des quaternions, $\mathbb{H}$, est une $\mathbb{R}$ -algèbre de dimension 4.*

Preuve : $M_2(\mathbb{C})$ est une $\mathbb{C}$ -algèbre (Exemple 3.82., 2)), donc a fortiori une $\mathbb{R}$ -algèbre. Dans $M_2(\mathbb{C})$, $\mathbb{H}$ est un sous-anneau unitaire (Exemple 1.17.) et un sous- $\mathbb{R}$ -espace vectoriel (à vérifier) ; on en déduit que $\mathbb{H}$ est une sous- $\mathbb{R}$ -algèbre de $M_2(\mathbb{C})$.

On remarque que $\mathbb{H}$ n'est pas une sous- $\mathbb{C}$ -algèbre de $M_2(\mathbb{C})$, car $\mathbb{H}$ n'est pas un espace vectoriel sur $\mathbb{C}$.

Déterminons la dimension de $\mathbb{H}$ sur $\mathbb{R}$. Notons ici ε , un élément de $\mathbb{C}$ tel que $\varepsilon^2 = -1$. Tout nombre complexe, x , s'écrit alors, de façon unique, $x = a + b\varepsilon$, où $(a, b) \in \mathbb{R} \times \mathbb{R}$. On en déduit que tout élément q de $\mathbb{H}$ s'écrit, de façon unique,

$$q = \begin{pmatrix} a + b\varepsilon & c + d\varepsilon \\ -c + d\varepsilon & a - b\varepsilon \end{pmatrix}, \text{ avec } (a, b, c, d) \in \mathbb{R}^4. \quad (3.21)$$

En identifiant $Z(\mathbb{H})$ à $\mathbb{R}$ par l'isomorphisme (3.20) (donc en écrivant pour tout $a \in \mathbb{R}$, a à la place de aI) et en posant d'autre part,

$$i = \begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \varepsilon \\ \varepsilon & 0 \end{pmatrix},$$

on peut écrire, de façon unique, tout élément $q \in \mathbb{H}$ sous la forme

$$q = a + bi + cj + dk, \quad (a, b, c, d) \in \mathbb{R}^4. \quad (3.22)$$

On en conclut que $\{1, i, j, k\}$ est une base du $\mathbb{R}$ -espace vectoriel $\mathbb{H}$, d'où $\dim_{\mathbb{R}} \mathbb{H} = 4$. Cette base sera dite *canonique*. $\square$

Remarque 3.88. L'identification de $Z(\mathbb{H})$ à $\mathbb{R}$ permet de considérer $\mathbb{R}$ comme un sous-corps de $\mathbb{H}$ et $\mathbb{H}$ comme une algèbre sur son centre.

Le $\mathbb{R}$ -espace vectoriel $\mathbb{H}$ s'écrit $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$.

B. Calculs dans $\mathbb{H}$

Les opérations dans l'anneau $M_2(\mathbb{C})$ impliquent que les éléments $1, i, j, k$, de la base canonique de $\mathbb{H}$ vérifient les relations

$$i^2 = j^2 = k^2 = -1 \quad (3.23)$$

$$ij = -ji = k; \quad jk = -kj = i; \quad ki = -ik = j \quad (3.24)$$

et pour deux quaternions $q = a + bi + cj + dk$, $q' = a' + b'i + c'j + d'k$,

$$\begin{aligned} qq' &= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + ca' + db' - bd')j \\ &\quad + (ad' + da' + bc' - cb')k. \end{aligned} \quad (3.25)$$

Proposition 3.89. $\mathbb{R} \oplus \mathbb{R}i$ est une sous- $\mathbb{R}$ -algèbre de $\mathbb{H}$ isomorphe à $\mathbb{C}$.

Preuve : $\mathbb{R} \oplus \mathbb{R}i$ est un sous- $\mathbb{R}$ -espace vectoriel de $\mathbb{H}$; de plus, pour

$q = a + bi$ et $q' = a' + b'i$ dans $\mathbb{R} \oplus \mathbb{R}i$, on a

$$q + q' = (a + a') + (b + b')i \quad \text{et} \quad qq' = (aa' - bb') + (ab' + ba')i.$$

On en déduit que l'application

$$\begin{aligned} \psi : \mathbb{R} \oplus \mathbb{R}i &\longrightarrow \mathbb{C} \\ a + bi &\longmapsto a + b\varepsilon \end{aligned}$$

est un isomorphisme de $\mathbb{R}$ -algèbres. □

Remarque 3.90. L'isomorphisme ψ , ci-dessus, permet d'identifier $\mathbb{R} \oplus \mathbb{R}i$ à $\mathbb{C}$, donc de considérer $\mathbb{C}$ comme une sous- $\mathbb{R}$ -algèbre de $\mathbb{H}$ et en particulier comme un sous-corps de $\mathbb{H}$.

Définition 3.91. Dans $\mathbb{H}$, le sous- $\mathbb{R}$ -espace vectoriel

$$P := \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

s'appelle le sous-espace des **quaternions purs** de $\mathbb{H}$.

Pour $q = a + bi + cj + dk$ dans $\mathbb{H}$,

a est appelé la **partie réelle** de q et sera noté $\mathcal{R}(q)$;

$bi + cj + dk$ est la partie **quaternion pur** de q qui sera noté $\mathcal{P}(q)$.

Remarque 3.92. D'après la définition précédente, on a $\mathbb{H} = \mathbb{R} \oplus P$, mais on remarque que P n'est pas une sous- $\mathbb{R}$ -algèbre de $\mathbb{H}$, car P n'est pas fermé pour la multiplication des quaternions (Par exemple, $i \in P$, mais $i^2 = -1 \notin P$).

Définition 3.93. Etant donné $q = a + bi + cj + dk$ dans $\mathbb{H}$, on appelle **conjugué** de q , le quaternion noté $\bar{q}$, tel que

$$\bar{q} = a - bi - cj - dk.$$

On vérifie alors facilement les propriétés suivantes.

Proposition 3.94. P désignant le sous-espace des quaternions purs, pour q et q' dans $\mathbb{H}$:

$$1) \bar{\bar{q}} = q; \quad \bar{q} = q \iff q \in \mathbb{R}; \quad \bar{q} = -q \iff q \in P.$$

$$2) q + q' = \bar{q} + \bar{q}'; \quad q q' = \bar{q}' \bar{q}.$$

$$3) q \in P \iff q^2 \leq 0 \text{ dans } \mathbb{R}.$$

Définition 3.95. Quel que soit $q = a + bi + cj + dk$ dans $\mathbb{H}$,

a) $q + \bar{q} = 2a$ est appelé la **trace** de q et noté $Tr(q)$.

b) $q\bar{q} = a^2 + b^2 + c^2 + d^2$ est appelé la **norme** de q et noté $N(q)$.

Remarque 3.96. Pour $q \in \mathbb{H}$,

a) $Tr(q)$ et $N(q)$ sont des nombres réels et $N(q) \geq 0$.

b) $(q \neq 0 \text{ et } N(q) = q\bar{q}) \implies q^{-1} = \bar{q}(N(q))^{-1}$.

c) $(q \in P \iff Tr(q) = 0) \quad \text{et} \quad (q \in \mathbb{H} \implies (q - \bar{q}) \in P).$

d) En écrivant $q = a + bi + cj + dk = \begin{pmatrix} a + b\varepsilon & c + d\varepsilon \\ -c + d\varepsilon & a - b\varepsilon \end{pmatrix}$

on voit que

$Tr(q) = 2a$ est la **trace** de la matrice q et

$N(q) = a^2 + b^2 + c^2 + d^2$ est le **déterminant** de la matrice q .

La remarque d), ci-dessus, permet de justifier les propriétés suivantes (que l'on peut aussi vérifier directement).

Proposition 3.97. *Quels que soient q et q' dans $\mathbb{H}$,*

1) $Tr(qq') = Tr(q'q)$, d'où $\forall s \in \mathbb{H} \setminus \{0\}$, $Tr(sq s^{-1}) = Tr(q)$.

2) $N(qq') = N(q)N(q')$ et pour $q \neq 0$, $N(q^{-1}) = (N(q))^{-1}$.

Remarque 3.98. :

a) On peut vérifier que l'application

$$N : \mathbb{H} \longrightarrow \mathbb{R} \\ q \longmapsto N(q) = q\bar{q}$$

est une forme quadratique définie positive sur le $\mathbb{R}$ -espace vectoriel $\mathbb{H}$, qui est ainsi muni d'une structure d'espace euclidien ; la norme euclidienne qui lui est associée est telle que

$$\forall q \in \mathbb{H}, \|q\| = \sqrt{N(q)} = \sqrt{q\bar{q}}.$$

b) On pourra montrer que $G := \{1, -1, i, -i, j, -j, k, -k\}$ est un sous-groupe du groupe multiplicatif $\mathbb{H}^* = \mathbb{H} \setminus \{0\}$; G est isomorphe au groupe à 8 éléments, appelé *groupe des quaternions* et noté Q_8 dans ([11], p.27).

c) Nous avons choisi d'introduire la $\mathbb{R}$ -algèbre $\mathbb{H}$, comme sous-algèbre de $M_2(\mathbb{C})$ pour des raisons de commodité, mais ce n'est pas de cette façon, qu'en 1843, le mathématicien anglais, William HAMILTON eut le mérite de mettre en évidence (après bien des années de recherches) ce *premier exemple de corps non commutatif*.

La méthode inspirée par les travaux de W. HAMILTON consiste à considérer, dans l'espace vectoriel $\mathbb{R}^4$, la base canonique notée $\{1, i, j, k\}$ et à munir $\mathbb{R}^4$ d'une multiplication (interne), qui sera définie par bilinéarité, à partir des relations (3.23) et (3.24). Il est alors nécessaire de vérifier l'associativité de cette multiplication, ce qui est un peu fastidieux (Voir [8]).

11. Exercices

1 Démontrer les corollaires 3.47., 3.48. et 3.53.

2) Soit $M \in {}_A \text{Mod}$, A étant un anneau unitaire, commutatif. Soit $x \in M \setminus \{0\}$ et $I := \text{Ann } x$. On suppose que l'idéal I est maximal parmi les annulateurs des éléments non nuls de M , montrer qu'alors, I est un idéal premier de A .

3) Dans la $\mathbb{R}$ -algèbre $M_4(\mathbb{R})$ des matrices carrées d'ordre 4 sur $\mathbb{R}$, on considère l'ensemble H des matrices de la forme

$$M(x_0, x_1, x_2, x_3) = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & -x_3 & x_2 \\ -x_2 & x_3 & x_0 & -x_1 \\ -x_3 & -x_2 & x_1 & x_0 \end{pmatrix}; \quad (x_0, x_1, x_2, x_3) \in \mathbb{R}^4.$$

On note I la matrice unité de $M_4(\mathbb{R})$ et on pose

$$E_1 = M(0, 1, 0, 0), E_2 = M(0, 0, 1, 0), E_3 = M(0, 0, 0, 1).$$

Exprimer $M(x_0, x_1, x_2, x_3)$ en fonction de I, E_1, E_2, E_3 .

Démontrer que H est une sous- $\mathbb{R}$ -algèbre de $M_4(\mathbb{R})$, isomorphe à la $\mathbb{R}$ -algèbre des quaternions $\mathbb{H}$.

- 4) $\mathbb{H}$ étant la $\mathbb{R}$ -algèbre des quaternions, pour tout $q \in \mathbb{H}$, $N(q)$ et $Tr(q)$ désignent la norme et la trace de q (Déf. 3.95.).

1°) a) Si $\mathcal{R}(q)$ et $\mathcal{P}(q)$ sont, respectivement, la partie réelle et la partie quaternion pur de q , vérifier que

$$\mathcal{R}(q) = \frac{1}{2}Tr(q) \quad \text{et} \quad \mathcal{P}(q) = \frac{1}{2}(q - \bar{q}).$$

b) Montrer que quel que soit $q \in \mathbb{H}$, on a

$$q^2 - Tr(q)q + N(q) = 0.$$

2°) $\{1, i, j, k\}$ étant la base canonique de $\mathbb{H}$ sur $\mathbb{R}$, on pose

$$\mathbb{H}_{\mathbb{Q}} = \{q = a + bi + cj + dk; (a, b, c, d) \in \mathbb{Q}^4\}.$$

a) Montrer que $\mathbb{H}_{\mathbb{Q}}$ est un sous-corps gauche de $\mathbb{H}$, mais n'est pas une sous- $\mathbb{R}$ -algèbre de $\mathbb{H}$.

b) On note J l'ensemble des quaternions $q = a + bi + cj + dk$, tels que :

- soit a, b, c, d sont dans $\mathbb{Z}$,

- soit a, b, c, d sont de la forme $\frac{2n+1}{2}$, où $n \in \mathbb{Z}$.

Prouver que J est un sous-anneau unitaire de $\mathbb{H}_{\mathbb{Q}}$.

Vérifier que pour tout $q \in J$, $Tr(q)$ et $N(q)$ appartiennent à $\mathbb{Z}$.

J est-il un sous-corps gauche de $\mathbb{H}_{\mathbb{Q}}$?

- 5) Endomorphismes idempotents d'un A -module, l'anneau A étant unitaire, commutatif.

Soit $M \in {}_A \text{Mod}$ et $\varepsilon \in \text{End}_A(M)$. On dit que ε est idempotent si c'est un élément idempotent de l'anneau $\text{End}_A(M)$, c'est-à-dire si $\varepsilon^2 = \varepsilon$ (Déf. 1.28.).

Si $\varepsilon_1, \varepsilon_2$ sont des endomorphismes idempotents de M , on dit qu'ils sont orthogonaux, si $\varepsilon_1 \circ \varepsilon_2 = \varepsilon_2 \circ \varepsilon_1 = 0$.

Etant donné ε idempotent dans $\text{End}_A(M)$, vérifier les propriétés suivantes :

a) $\text{id}_M - \varepsilon$ est idempotent dans $\text{End}_A(M)$.

b) ε et $(\text{id}_M - \varepsilon)$ sont orthogonaux.

c) $\text{Im}(\text{id}_M - \varepsilon) = \text{Ker } \varepsilon$; $\text{Ker}(\text{id}_M - \varepsilon) = \text{Im } \varepsilon$.

d) $M = \text{Im } \varepsilon \oplus \text{Ker } \varepsilon$.

- 6) L'anneau A étant unitaire, commutatif, soit M un A -module à gauche, de type fini ; on note $\{x_1, x_2, \dots, x_n\}$, $n \geq 1$, une famille génératrice minimale de M ; c'est-à-dire que toute famille génératrice finie de M est de cardinal supérieur ou égal à n . Pour tout idéal I de A , on pose

$$IM = \{\sum_{1 \leq i \leq n} a_i x_i; n \in \mathbb{N}^*, \forall i (1 \leq i \leq n), a_i \in I\}.$$

1°) Vérifier que IM est un sous-module de M .

2°) Soit $\mathcal{J}(A)$ le radical de Jacobson de A (Déf. 2. 90.).

On suppose qu'il existe un idéal I de A tel que $I \subseteq \mathcal{J}(A)$ et $IM = M$; démontrer que cette hypothèse implique $M = (0)$.

Indication : Si $M \neq (0)$, montrer qu'il existe des a_i non tous nuls dans I , $2 \leq i \leq n$, tels que

$$x_1 = \sum_{2 \leq i \leq n} a_i x_i.$$

3°) Etant donné un sous-module N de M , on suppose qu'il existe un idéal I de A tel que

$$I \subseteq \mathcal{J}(A) \text{ et } M = IM + N.$$

Prouver que $M = N$ (Appliquer le résultat du 2°) au module M/N).

4°) On suppose que A est un anneau local. L'unique idéal maximal de A étant noté $\mathcal{M}$, soit $K = A/\mathcal{M}$ le corps résiduel de A .

a) Montrer que le module quotient $M/(\mathcal{M}M)$ est muni, de façon naturelle, d'une structure de K -espace vectoriel de dimension finie.

b) Pour tout $x \in M$, on note $\bar{x}$ la classe de x modulo $\mathcal{M}M$.

Soit $\{y_1, \dots, y_p\}$, $p \in \mathbb{N}^*$, une famille d'éléments de M telle que $\{\bar{y}_1, \dots, \bar{y}_p\}$ soit une base du K -espace vectoriel $M/(\mathcal{M}M)$. En désignant par N le sous-module de M engendré par les y_j , $1 \leq j \leq p$, démontrer que $M = N$.

7) I désignant un ensemble non vide, soit $\{M_i\}_{i \in I}$ une famille de A -modules à gauche (A anneau unitaire, commutatif).

Démontrer que pour $M \in {}_A \text{Mod}$, on a

$$M \simeq \bigoplus_{i \in I} M_i$$

si et seulement si il existe deux familles de morphismes de A -modules $\{f_i\}_{i \in I}$ et $\{g_i\}_{i \in I}$ vérifiant les trois conditions suivantes :

a) Pour tout $i \in I$,

$$f_i \in \text{Hom}_A(M_i, M), \quad g_i \in \text{Hom}_A(M, M_i) \quad \text{et} \quad g_i \circ f_i = \text{id}_{M_i}.$$

b) ($k \neq i$ dans I) $\implies g_k \circ f_i = 0$.

c) Quel que soit $x \in M$, les $g_i(x)$, pour $i \in I$, sont "presque tous nuls" et $x = \sum_{i \in I} (f_i \circ g_i)(x)$.

8) K étant un corps, soit E un K -espace vectoriel ayant une base infinie dénombrable, $\{e_n\}_{n \in \mathbb{N}}$. ($K[X]$ est un exemple d'un tel espace vectoriel).

Soit $A := \text{End}_K(E)$; A est un anneau unitaire, non commutatif, dont l'élément unité est $1_A = \text{id}_E$.

Le A -module à gauche ${}_A A$ est libre de base $\{1_A\}$ (Rem. 3.66., c)), donc est de type fini.

Le but de cet exercice est la mise en évidence d'une base du A -module ${}_A A$ formée de deux éléments; on justifiera ainsi la remarque 3.66, c).

On considère dans A les éléments u_1 et u_2 tels que pour tout $n \in \mathbb{N}$,

$$\begin{aligned} u_1(e_{2n}) &= e_n & u_2(e_{2n}) &= 0 \\ u_1(e_{2n+1}) &= 0 & u_2(e_{2n+1}) &= e_n. \end{aligned}$$

Trouver deux éléments v_1 et v_2 de A tels que

$$v_1 u_1 + v_2 u_2 = \text{id}_E.$$

En déduire que $\{u_1, u_2\}$ est une base du A -module à gauche ${}_A A$.

9) Le but de cet exercice est de prouver que lorsqu'un anneau unitaire A est commutatif, alors toutes les bases d'un A -module à gauche libre F sont de même cardinal (que celui-ci soit fini ou non).

La méthode de démonstration proposée utilise les notions de restriction et extension des scalaires définies dans l'Appendice B.

On rappelle que si K est un corps, alors toutes les bases d'un K -espace vectoriel sont de même cardinal (que celui-ci soit fini ou non).

1°) A étant un anneau unitaire, commutatif, justifier l'existence d'au moins un corps K tel qu'il existe un morphisme surjectif d'anneaux unitaires, de A sur K (Cf. Cor. 2.70.)

2°) Soit K un corps tel qu'il existe un morphisme surjectif $\rho \in \text{Hom}(A, K)$.

a) Vérifier que l'application

$$\begin{aligned} A \times K &\longrightarrow K \\ (a, k) &\longmapsto \rho(a)k \end{aligned}$$

permet de définir une structure de A -module à gauche sur K (Cf. Restriction des scalaires).

b) Soit F un A -module à gauche libre; on considère le K -espace vectoriel $K \otimes_A F$ obtenu à partir de F , par extension des scalaires.

Montrer que si $\{x_i\}_{i \in I}$ est une base de F sur A , alors $\{1 \otimes x_i\}_{i \in I}$ est une base du K -espace vectoriel $K \otimes_A F$.

En conclure que toutes les bases de F sur A ont le même cardinal.

- 10) A désigne un anneau unitaire et les A -modules considérés sont des A -modules à gauche. On dit qu'un A -module M est **simple** s'il est *non nul* et si ses seuls sous-modules sont (0) et M .

1°) Montrer qu'un A -module $M \neq (0)$ est simple si et seulement s'il est engendré par chacun de ses éléments non nuls, c'est-à-dire :

$$\forall x \in M \setminus \{0\}, M = Ax = \{ax; a \in A\}.$$

En déduire que le A -module à gauche ${}_A A$ (resp. à droite A_A) est simple si et seulement si A est un anneau à division (ou corps gauche) (Déf. 1.6.).

2°) Démontrer que les trois conditions suivantes, où M, M', M'' désignent des A -modules à gauche, sont équivalentes.

i) M est un A -module simple.

ii) $\forall M', (f \in \text{Hom}_A(M, M') \text{ et } f \neq 0) \implies f \text{ surjectif.}$

iii) $\forall M'', (f \in \text{Hom}_A(M'', M) \text{ et } f \neq 0) \implies f \text{ injectif.}$

3°) On suppose que M est un A -module simple.

Montrer que tout $f \in \text{End}_A(M) \setminus \{0\}$ est un automorphisme de M ; en déduire que $\text{End}_A(M)$ est un anneau à division.





Chapitre 4

Algèbres de Polynômes

Dans tout ce chapitre, A désigne un anneau unitaire et commutatif.

1. Polynômes à une indéterminée sur A

A. Construction de l'algèbre des polynômes à une indéterminée sur A

1°) $\mathbb{N}$ étant l'ensemble des entiers naturels, on considère le A -module à gauche, *libre*, $A^{(\mathbb{N})}$ (Déf. 3.60.) ; on a

$$f \in A^{(\mathbb{N})} \iff f = (a_i)_{i \in \mathbb{N}}, \text{ les } a_i \text{ étant "presque tous nuls" dans } A.$$

Etant donné f et g dans $A^{(\mathbb{N})}$ tels que, $f = (a_i)_{i \in \mathbb{N}}$, $g = (b_i)_{i \in \mathbb{N}}$,

$$\text{on pose } fg := (c_n)_{n \in \mathbb{N}}, \text{ où } c_n = \sum_{0 \leq i \leq n} a_i b_{n-i}.$$

f et g étant à support fini (Déf. 3.49.), il en est de même de fg ; par suite l'application $(f, g) \mapsto fg$ définit une loi de composition interne dans $A^{(\mathbb{N})}$, appelée "multiplication". L'anneau A étant unitaire et commutatif, on vérifiera que cette multiplication est commutative, associative, distributive par rapport à l'addition du groupe abélien $A^{(\mathbb{N})}$ et que l'élément $(1, 0, 0, \dots)$ est élément unité.

$A^{(\mathbb{N})}$ est ainsi un anneau unitaire et commutatif.

De plus, la structure de A -module à gauche de $A^{(\mathbb{N})}$ implique que quels que soient $\alpha \in A$, f et g dans $A^{(\mathbb{N})}$:

$$\alpha(fg) = (\alpha f)g = f(\alpha g).$$

Le A -module à gauche $A^{(\mathbb{N})}$ étant libre, on en conclut que $A^{(\mathbb{N})}$ est une **A -algèbre libre et commutative**.

2°) Soit $\{e_i\}_{i \in \mathbb{N}}$ la base canonique du A -module libre $A^{(\mathbb{N})}$:

$$e_0 = (1, 0, 0, \dots), e_1 = (0, 1, 0, 0, \dots)$$

et d'une façon générale, $e_i = (\alpha_n)_{n \in \mathbb{N}}$, où $\alpha_i = 1$ et $\alpha_n = 0, \forall n \neq i$.

La définition de la multiplication de l'anneau $A^{(\mathbb{N})}$ implique que

$$\forall (i, j) \in \mathbb{N} \times \mathbb{N}, e_i e_j = e_{i+j}, \text{ d'où } e_i = e_1^i, \forall i \in \mathbb{N}^*;$$

de plus $e_0 = e_1^0$, car e_1 est non nul et e_0 est l'élément unité de l'anneau $A^{(\mathbb{N})}$.

Par suite, tout $f = (a_i)_{i \in \mathbb{N}}$ dans $A^{(\mathbb{N})}$ s'écrit de façon unique,

$$f = \sum_{i \in \mathbb{N}} a_i e_1^i, \text{ les } a_i \text{ étant "presque tous nuls" dans } A.$$

Plus précisément, pour f non nul, le support de f , c'est-à-dire l'ensemble

$$\text{supp}(f) = \{i \in \mathbb{N} ; a_i \neq 0\},$$

est une partie finie, non vide de $\mathbb{N}$, donc il existe un plus grand élément n dans $\text{supp}(f)$ tel que, nécessairement,

$$f = \sum_{0 \leq i \leq n} a_i e_i^1, \text{ avec } a_n \neq 0 \text{ dans } A. \quad (4.1)$$

Définition 4.1. Pour tout f non nul dans $A^{(\mathbb{N})}$, l'entier n , plus grand élément de $\text{supp}(f)$, est appelé le **degré** de f ; on écrira $\deg f = n$.

Par convention, l'élément nul de $A^{(\mathbb{N})}$, noté 0, est de degré strictement inférieur à celui de tout $f \neq 0$; ce degré sera symboliquement noté $-\infty$.

3°) *Changement de notation* Posons $X = e_1$; d'après (4.1), tout f de degré $n \geq 0$ dans $A^{(\mathbb{N})}$, s'écrit, de façon unique,

$$f = \sum_{0 \leq i \leq n} a_i X^i, \text{ avec } a_n \neq 0 \text{ dans } A. \quad (4.2)$$

Définition 4.2. Notations

a) L'élément $e_1 = (0, 1, 0, \dots)$ de $A^{(\mathbb{N})}$, noté maintenant X , est appelé **indéterminée**.

b) Un élément quelconque f de $A^{(\mathbb{N})}$ est alors appelé un **polynôme à une indéterminée** sur A , écrit sous la forme (4.2) il pourra être noté $f(X)$.

L'élément 0 de $A^{(\mathbb{N})}$ est le **polynôme nul**.

c) L'algèbre $A^{(\mathbb{N})}$ est appelée **Algèbre des polynômes à une indéterminée** sur A .

X désignant l'indéterminée, cette algèbre sera désormais notée $A[X]$.

Remarque 4.3. :

a) D'après ce qui précède, pour deux polynômes f et g de $A[X]$ tels que $f = \sum_{0 \leq i \leq n} a_i X^i$, $g = \sum_{0 \leq i \leq m} b_i X^i$, on a

$$f = g \iff (n = m \text{ et } \forall i (0 \leq i \leq n), a_i = b_i).$$

b) Un polynôme f est de degré 0, dans $A[X]$, si et seulement si

$f = a_0 X^0 = a_0$, avec $a_0 \neq 0$ dans A ; le cas $a_0 = 0$ correspond au polynôme nul de degré $-\infty$. On en déduit que l'application

$$\begin{aligned} \mu : A &\longrightarrow A[X] \\ a &\longmapsto aX^0 \end{aligned}$$

est un morphisme injectif de A -algèbres, qui permet d'identifier A à la sous-algèbre $\text{Im } \mu$ de $A[X]$, en écrivant a à la place de aX^0 . En particulier les éléments 0 et 1 de A s'identifient, respectivement, au polynôme nul et à l'élément unité de $A[X]$.

En conclusion de l'étude précédente, on obtient l'assertion suivante.

Proposition 4.4. *A étant un anneau unitaire et commutatif, l'algèbre $A[X]$ des polynômes à une indéterminée sur A est une A -algèbre libre et commutative, contenant A comme sous-algèbre, et dont une base est l'ensemble $\{X^i; i \in \mathbb{N}\}$.*

Remarque 4.5. :

a) La construction de l'algèbre $A[X]$, que nous avons donnée, montre que cette algèbre est indépendante du choix de la lettre X qui désigne l'indéterminée; ainsi les algèbres $A[X]$ et $A[Y]$ sont isomorphes par

$$\begin{aligned} A[X] &\longrightarrow A[Y] \\ f(X) &\longmapsto f(Y). \end{aligned}$$

Ce résultat sera confirmé plus loin (Cor. 4.7.).

b) Si K est un corps, l'algèbre $K[X]$ est un K -espace vectoriel de dimension infinie dénombrable (Déf. 3.58.), puisque $\{X^i; i \in \mathbb{N}\}$ est une base de $K[X]$.

B. Propriété universelle de l'anneau $A[X]$ **Théorème 4.6. Propriété universelle**

Etant donné deux anneaux unitaires, commutatifs A et B , un morphisme d'anneaux unitaires φ de A dans B et un élément $\alpha \in B$, il existe un unique morphisme d'anneaux unitaires, Φ , de $A[X]$ dans B tel que

$$\Phi|_A = \varphi \quad \text{et} \quad \Phi(X) = \alpha.$$

Preuve :

a) Supposons l'existence de Φ ; alors nécessairement,

$$\Phi(\sum_{0 \leq i \leq n} a_i X^i) = \sum_{0 \leq i \leq n} \varphi(a_i) \alpha^i,$$

d'où l'unicité de Φ .

b) Démontrons l'existence de Φ . Pour tout polynôme $\sum_{0 \leq i \leq n} a_i X^i \in A[X]$, posons

$$\Phi(\sum_{0 \leq i \leq n} a_i X^i) := \sum_{0 \leq i \leq n} \varphi(a_i) \alpha^i.$$

Si des polynômes $\sum_{0 \leq i \leq n} a_i X^i$ et $\sum_{0 \leq i \leq p} b_i X^i$ sont tels que $0 \leq p \leq n$, alors, en posant $b_{p+k} = 0$ pour tout k ($1 \leq k \leq n-p$), on peut écrire

$$\begin{aligned} \Phi\left(\sum_{0 \leq i \leq n} a_i X^i + \sum_{0 \leq i \leq p} b_i X^i\right) &= \Phi\left(\sum_{0 \leq i \leq n} (a_i + b_i) X^i\right) = \sum_{0 \leq i \leq n} \varphi(a_i + b_i) \alpha^i \\ &= \sum_{0 \leq i \leq n} \varphi(a_i) \alpha^i + \sum_{0 \leq i \leq p} \varphi(b_i) \alpha^i \\ &= \Phi\left(\sum_{0 \leq i \leq n} a_i X^i\right) + \Phi\left(\sum_{0 \leq i \leq p} b_i X^i\right). \\ \Phi\left(\left(\sum_{0 \leq i \leq n} a_i X^i\right)\left(\sum_{0 \leq j \leq p} b_j X^j\right)\right) &= \Phi\left(\sum_{(i,j)} a_i b_j X^{i+j}\right), \quad 1 \leq i \leq n, \quad 1 \leq j \leq p, \\ &= \sum_{(i,j)} \varphi(a_i) \varphi(b_j) \alpha^{i+j}, \quad 1 \leq i \leq n, \quad 1 \leq j \leq p, \\ &= \Phi\left(\sum_{0 \leq i \leq n} a_i X^i\right) \Phi\left(\sum_{0 \leq j \leq p} b_j X^j\right). \end{aligned}$$

De plus $\Phi(1) = 1$, donc Φ est un morphisme d'anneaux unitaires, tel que $\Phi|_A = \varphi$ et $\Phi(X) = \alpha$. $\square$

Corollaire 4.7. Les A -algèbres $A[X]$ et $A[Y]$ sont canoniquement isomorphes par l'application

$$\begin{aligned} \Phi : A[X] &\longrightarrow A[Y] \\ f(X) &\longmapsto f(Y). \end{aligned}$$

Preuve : On applique le théorème 4.6., en prenant $B = A[Y]$ et pour morphisme φ , l'injection canonique : $A \longrightarrow A[Y]$; il existe alors un unique morphisme Φ de $A[X]$ dans $A[Y]$ tel que

$$\Phi|_A = \text{id} \quad \text{et} \quad \Phi(X) = Y.$$

On en déduit que, pour tout $f(X) \in A[X]$, on a $\Phi(f(X)) = f(Y)$, donc Φ est un morphisme surjectif; de plus,

$$\Phi(\sum_{0 \leq i \leq n} a_i X^i) = 0 \iff \sum_{0 \leq i \leq n} a_i Y^i = 0 \quad (4.3)$$

$$\iff a_i = 0, \forall i (0 \leq i \leq n) \quad (4.4)$$

$$\iff \sum_{0 \leq i \leq n} a_i X^i = 0, \quad (4.5)$$

d'où Φ injectif ; par suite Φ est un isomorphisme d'anneaux unitaires. D'autre part, quels que soient $\alpha \in A$ et $f(X) = \sum_{0 \leq i \leq n} a_i X^i$ dans $A[X]$,

$$\begin{aligned}\Phi(\alpha f(X)) &= \Phi(\sum_{0 \leq i \leq n} \alpha a_i X^i) = \sum_{0 \leq i \leq n} \alpha a_i Y^i \\ &= \alpha \sum_{0 \leq i \leq n} a_i Y^i \\ &= \alpha \Phi(f(X)).\end{aligned}$$

On en conclut que Φ est un isomorphisme de A -algèbres de $A[X]$ sur $A[Y]$. □

Corollaire 4.8. Soit A et B deux anneaux unitaires, commutatifs. Etant donné un morphisme d'anneaux unitaires φ de A dans B , il existe un unique morphisme d'anneaux unitaires $\hat{\varphi} \in \text{Hom}(A[X], B[X])$ tel que

$$\hat{\varphi}|_A = \varphi \quad \text{et} \quad \hat{\varphi}(X) = X.$$

$$\text{De plus,} \quad \varphi \text{ injectif} \implies \hat{\varphi} \text{ injectif,}$$

$$\varphi \text{ surjectif} \implies \hat{\varphi} \text{ surjectif,}$$

$$\text{d'où} \quad \varphi \text{ isomorphisme} \implies \hat{\varphi} \text{ isomorphisme.}$$

Preuve : La propriété universelle de l'anneau $A[X]$ (Th. 4.6.) implique l'existence et l'unicité du morphisme d'anneaux unitaires $\hat{\varphi}$ de $A[X]$ dans $B[X]$ tel que

$$\hat{\varphi}(\sum_{0 \leq i \leq n} a_i X^i) = \sum_{0 \leq i \leq n} \varphi(a_i) X^i.$$

Si φ est injectif, alors

$$\begin{aligned}\hat{\varphi}(\sum_{0 \leq i \leq n} a_i X^i) = 0 &\iff \sum_{0 \leq i \leq n} \varphi(a_i) X^i = 0 \\ &\iff \varphi(a_i) = 0, \forall i (0 \leq i \leq n) \\ &\iff a_i = 0, \forall i (0 \leq i \leq n), \quad \text{d'où} \quad \hat{\varphi} \text{ injectif.}\end{aligned}$$

Supposons φ surjectif et soit $\sum_{0 \leq i \leq n} b_i X^i$ dans $B[X]$. Pour tout $i (0 \leq i \leq n)$, il existe $a_i \in A$ tel que $\varphi(a_i) = b_i$, par suite

$$\sum_{0 \leq i \leq n} b_i X^i = \sum_{0 \leq i \leq n} \varphi(a_i) X^i = \hat{\varphi}(\sum_{0 \leq i \leq n} a_i X^i), \quad \text{d'où} \quad \hat{\varphi} \text{ surjectif.} \quad \square$$

Exemple 4.9. Pour $n > 1$ dans $\mathbb{N}$, soit π la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. D'après le corollaire 4.8, π induit le morphisme d'anneaux unitaires

$$\begin{aligned}\hat{\pi} : \mathbb{Z}[X] &\longrightarrow (\mathbb{Z}/n\mathbb{Z})[X] \\ \sum_{0 \leq i \leq n} a_i X^i &\longmapsto \sum_{0 \leq i \leq n} \pi(a_i) X^i.\end{aligned}$$

C. Propriétés des degrés des polynômes de $A[X]$

1. Vocabulaire associé aux polynômes de $A[X]$

Définition 4.10. Soit f un polynôme non nul de $A[X]$, de degré n :

$$f = \sum_{0 \leq i \leq n} a_i X^i, \quad \text{avec } a_n \neq 0.$$

a) Les éléments a_i de A sont appelés les **coefficients** du polynôme f .

a_n s'appelle le **coefficient directeur** de f et le polynôme f est dit **unitaire**, si $a_n = 1$.

b) Si $f = a_n X^n, n > 0$, f est appelé **monôme** de degré n .

c) Si $f = a_0$, on dit que f est un **polynôme constant**.

d) Si $\deg f = n > 0$, le coefficient a_0 s'appelle le **terme constant** de f .

Lorsque $a_0 = 0$, on dit parfois (par abus de langage), que le polynôme $f \neq 0$ est "sans terme constant".

2. Propriétés des degrés des polynômes de $A[X]$

Proposition 4.11. *L'anneau A étant unitaire et commutatif, pour deux polynômes f et g de $A[X]$, on a*

$$1) \deg(f+g) \leq \max(\deg f, \deg g).$$

$$2) \deg fg \leq \deg f + \deg g.$$

3) $\deg fg = \deg f + \deg g$, quels que soient f et g dans $A[X]$, si et seulement si l'anneau A est intègre.

Preuve : On remarque que les trois relations énoncées dans la proposition sont vérifiées, dès que l'un au moins des polynômes f, g est nul ; on suppose donc f et g non nuls. Posons $\deg f = n \geq 0$, $\deg g = p \geq 0$ et

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i, \quad g(X) = \sum_{0 \leq i \leq p} b_i X^i.$$

Supposons $n \geq p \geq 0$; si $n > p$, on écrira :

$$g(X) = \sum_{0 \leq i \leq n} b_i X^i, \text{ avec } b_i = 0, \text{ pour } p+1 \leq i \leq n.$$

$$(f+g)(X) = \sum_{0 \leq i \leq n} (a_i + b_i) X^i \implies \deg(f+g) \leq n = \max(n, p).$$

$$fg(X) = \sum_{0 \leq k \leq n+p} c_k X^k, \text{ où } c_k = \sum_{0 \leq i \leq k} a_i b_{k-i}.$$

Le coefficient directeur du polynôme fg est $c_{n+p} = a_n b_p$, d'où

$$\deg fg \leq n+p = \deg f + \deg g \quad \text{et} \quad \deg fg = n+p \iff a_n b_p \neq 0.$$

Par suite, $\deg fg = \deg f + \deg g$, quels que soient f et g dans $A[X]$, si et seulement si l'anneau A est intègre. $\square$

Corollaire 4.12. *L'anneau $A[X]$ est intègre si et seulement si l'anneau A est intègre ; en particulier, si K est un corps, alors $K[X]$ est intègre.*

Ce résultat est une conséquence immédiate du 3) de la proposition 4.11.

Remarque 4.13. Quel que soit l'anneau unitaire, commutatif A, l'anneau $A[X]$ n'est jamais un corps. En effet, $A[X]$ contient des éléments non nuls et non inversibles, par exemple le monôme X, puisque

$$Xf(X) = 1 \implies 1 + \deg f = 0, \quad \text{ce qui est impossible.}$$

Proposition 4.14. *Si A est un domaine d'intégrité (Déf. 1.21.), alors le groupe $U_{A[X]}$ des unités de l'anneau $A[X]$ est le groupe U_A des unités de A (Cf. Prop. 1.9.).*

Preuve : L'anneau A étant intègre, pour f et g dans $A[X]$,

$$fg = 1 \implies \deg(f) + \deg(g) = 0 \implies \deg(f) = 0 \text{ et } \deg(g) = 0.$$

On en déduit que $f \in U_{A[X]}$ si et seulement si $f \in U_A$. $\square$

D. Composition des polynômes

Définition 4.15. Soit f et g deux polynômes de $A[X]$. On appelle **polynôme composé** de f par g le polynôme noté $f \circ g$ tel que

$$\text{si } f(X) = \sum_{0 \leq i \leq n} a_i X^i, \quad \text{alors} \quad (f \circ g)(X) = \sum_{0 \leq i \leq n} a_i (g(X))^i.$$

Exemple 4.16. Pour $f(X) = 2 + 3X + X^3$ et $g(X) = 2X^2$, dans $\mathbb{Z}[X]$,
 $(f \circ g)(X) = 2 + 6X^2 + 8X^6$.

Remarque 4.17. Le polynôme $f \circ g$ de $A[X]$ est obtenu en substituant $g(X)$ à l'indéterminée X , dans le polynôme $f(X)$. On en déduit que

$$\deg(f \circ g) = (\deg f)(\deg g).$$

Cas particuliers : avec les notations de la définition 4.15.,

a) si f est un polynôme constant, alors

$$(f = a, a \in A) \implies f \circ g = a, \forall g \in A[X].$$

b) si f est de degré $n > 0$ et g est un polynôme constant, alors

$$(g = c, c \in A) \implies f \circ g = f(c) = \sum_{0 \leq i \leq n} a_i c^i;$$

donc $f \circ c$ est un polynôme constant.

Définition 4.18. Etant donné un polynôme $f \in A[X] \setminus A$, on dit qu'un élément $c \in A$ est une **racine** ou un **zéro** du polynôme f , si $f(c) = 0$.

La notion de racine d'un polynôme sera particulièrement importante dans l'étude des polynômes à coefficients dans un corps.

Proposition 4.19. *Quels que soient les polynômes f, g, h dans $A[X]$, on a*

$$f \circ (g \circ h) = (f \circ g) \circ h. \quad (4.6)$$

$$(f + g) \circ h = f \circ h + g \circ h. \quad (4.7)$$

$$f \circ X = X \circ f = f(X). \quad (4.8)$$

Vérification laissée au lecteur.

Remarque 4.20. :

(4.6) exprime l'associativité de la composition des polynômes.

(4.7) exprime que la composition des polynômes est distributive à droite par rapport à l'addition.

(4.8) justifie la notation $f(X)$ pour un polynôme f appartenant à $A[X]$.

La composition des polynômes n'est ni commutative, ni distributive à gauche par rapport à l'addition.

Par exemple dans $\mathbb{Z}[X]$, pour $f = X + 1$, $g = X^2$, $h = X + 2$ on a

$$\begin{aligned} f \circ g &= X^2 + 1 \quad \text{et} \quad g \circ f = (X + 1)^2; \\ h \circ (f + g) &= X^2 + X + 3 \quad \text{et} \quad h \circ f + h \circ g = X^2 + X + 5. \end{aligned}$$

E. Fonction polynôme

Définition 4.21. A étant un anneau unitaire et commutatif, à tout polynôme $f \in A[X]$ tel que $f(X) = \sum_{0 \leq i \leq n} a_i X^i$, on associe l'application

$$\begin{aligned} \tilde{f} : A &\longrightarrow A \\ x &\longmapsto \sum_{0 \leq i \leq n} a_i x^i. \end{aligned}$$

$\tilde{f}$ est la **fonction polynôme associée** à f .

Soit A^A l'anneau des applications de A dans A (Exemple 1.18.). L'anneau A étant supposé unitaire et commutatif, il en est de même de A^A , dont l'élément unité est l'application

$$\begin{aligned}\varepsilon : A &\longrightarrow A \\ x &\longmapsto 1.\end{aligned}$$

De plus, on vérifie que A^A est une A-algèbre, grâce à l'application

$$\begin{aligned}A \times A^A &\longrightarrow A^A \\ (a, \varphi) &\longmapsto a\varphi\end{aligned}$$

telle que $(a\varphi)(x) = a(\varphi(x))$, pour tout x dans A.

Proposition 4.22. Pour un anneau A unitaire et commutatif, l'application

$$\begin{aligned}\theta : A[X] &\longrightarrow A^A \\ f &\longmapsto \tilde{f}\end{aligned}$$

est un morphisme de A-algèbres. L'image de θ est appelée l'algèbre des fonctions polynômes de A dans A. De plus, quels que soient f non constant et g non nul dans $A[X]$, on a

$$\widetilde{f \circ g} = \tilde{f} \circ \tilde{g}. \quad (4.9)$$

Preuve : Soit $f = \sum_{0 \leq i \leq n} a_i X^i$ dans $A[X]$;

$$\forall x \in A, \tilde{f}(x) = \sum_{0 \leq i \leq n} a_i x^i.$$

Si $f = a$, où $a \in A$, alors $\tilde{f}$ est l'application constante telle que $\tilde{f}(x) = a$, pour tout x dans A. En particulier,

$$f = 0 \implies \tilde{f} = 0 \text{ dans } A^A.$$

$$f = 1 \implies \tilde{f} \text{ élément unité de } A^A.$$

D'autre part, on vérifie que quels que soient f, g dans $A[X]$ et $a \in A$, on a

$$\widetilde{f+g} = \tilde{f} + \tilde{g}; \quad \widetilde{fg} = \tilde{f}\tilde{g}; \quad \text{et} \quad \widetilde{af} = a\tilde{f},$$

donc θ est un morphisme de A-algèbres de $A[X]$ dans A^A .

Avec les notations ci-dessus, si f est non constant et $g \neq 0$ dans $A[X]$, alors

$$\forall x \in A, \widetilde{f \circ g}(x) = \sum_{0 \leq i \leq n} a_i (\tilde{g}(x))^i$$

$$\text{d'où} \quad \forall x \in A, \widetilde{f \circ g}(x) = \tilde{f}(\tilde{g}(x)).$$

Par suite, $\widetilde{f \circ g} = \tilde{f} \circ \tilde{g}$, où $\tilde{f} \circ \tilde{g}$ désigne l'application composée de $\tilde{f}$ et $\tilde{g}$ dans A^A . $\square$

Remarque 4.23. :

a) Le morphisme θ n'est pas injectif, en général.

Par exemple, pour $A = \mathbb{Z}/2\mathbb{Z}$ et $f(X) = X^2 + X$, on a $f \neq 0$ dans $A[X]$ et $\tilde{f} = 0$ dans A^A . Nous verrons cependant, que θ est injectif dans le cas où A est un corps infini (Prop. 4.48.).

b) Dans la remarque 4.17., on a vu que pour un polynôme non constant

$f = \sum_{0 \leq i \leq n} a_i X^i$ et un polynôme constant $g = c$, on a

$$f \circ g = f(c) = \sum_{0 \leq i \leq n} a_i c^i = \tilde{f}(c).$$

Ceci autorise à écrire, pour tout $x \in A$, $f(x)$ à la place de $\tilde{f}(x)$, lorsque qu'aucune ambiguïté n'est possible.

F. Polynômes dérivés

1. Notion de polynôme dérivé

Définition 4.24. Soit $f = \sum_{0 \leq i \leq n} a_i X^i$ dans $A[X]$. On appelle **polynôme dérivé** de f , le polynôme, noté f' , défini par :

$$f'(X) = \sum_{0 \leq i \leq n} i a_i X^{i-1}. \quad (4.10)$$

Proposition 4.25. Pour f dans $A[X]$,

$$\deg f = n \implies \deg f' \leq n-1.$$

Preuve : Supposons $f = \sum_{0 \leq i \leq n} a_i X^i$; par définition,

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \dots + 2 a_2 X + a_1. \quad (4.11)$$

Si f est un polynôme constant (éventuellement nul), alors $f' = 0$.

Si $\deg f = n \geq 1$, on a $a_n \neq 0$ dans A , alors

$$(n a_n \neq 0 \implies \deg f' = n-1); \quad (n a_n = 0 \implies \deg f' < n-1).$$

On remarque que $n a_n = 0$ dans les cas suivants :

i) l'anneau A est de caractéristique $k \neq 0$ et k divise n ;

ii) $n (= n1_A)$ et a_n sont des diviseurs de 0 dans A tels que $n a_n = 0$. □

Corollaire 4.26. Si A est un domaine d'intégrité (en particulier, si A est un corps), et si $\text{car } A = 0$, alors pour $f \in A[X]$,

$$\deg f = n \geq 1 \implies \deg f' = n-1.$$

Remarque 4.27. Compte tenu des notations précédentes,

a) Si $\text{car } A = k \neq 0$, alors, dans la relation (4.10) on a $i a_i = 0$, pour tout $i (1 < i \leq n-1)$ tel que k divise i . Par suite, on peut avoir f non constant et $f' = 0$; par exemple,

$$\forall r \in \mathbb{N}^*, f = X^{kr} \implies f' = 0.$$

Plus généralement, $f = \sum_{0 \leq i \leq n} a_i X^{ki} \implies f' = 0$.

b) Si $A = \mathbb{R}$, alors la fonction polynôme $\tilde{f} : \mathbb{R} \rightarrow \mathbb{R}$ est la dérivée de la fonction polynôme $\tilde{f}$, au sens habituel de l'Analyse Réelle.

Proposition 4.28. A étant un anneau unitaire, commutatif quelconque, quels que soient f, g dans $A[X]$ et $a \in A$, on a

$$(f+g)' = f' + g' \quad (4.12)$$

$$(fg)' = f'g + fg' \quad (4.13)$$

$$(af)' = af' \quad (4.14)$$

$$(f \circ g)' = (f' \circ g)g'. \quad (4.15)$$

Preuve : (4.12) et (4.14) se vérifient facilement, nous démontrons les deux autres relations. Soit $f = \sum_{i \in \mathbb{N}} a_i X^i$ et $g = \sum_{j \in \mathbb{N}} b_j X^j$, où les a_i et les b_j sont "presque tous nuls" dans A .

a) Relation (4.13) : $fg(X) = \sum_{k \in \mathbb{N}} c_k X^k$, où $c_k = \sum_{i+j=k} a_i b_j$.

$$(fg(X))' = \sum_{k \in \mathbb{N}^*} k c_k X^{k-1} = \sum_{(i+j) \in \mathbb{N}^*} (i+j) a_i b_j X^{i+j-1}.$$

D'autre part,

$$\begin{aligned}(f'g + fg')(X) &= \left(\sum_{i \in \mathbb{N}^*} ia_i X^{i-1}\right) \left(\sum_{j \in \mathbb{N}} b_j X^j\right) + \left(\sum_{i \in \mathbb{N}} a_i X^i\right) \left(\sum_{j \in \mathbb{N}^*} jb_j X^{j-1}\right) \\ &= \sum_{(i+j) \in \mathbb{N}^*} (i+j)a_i b_j X^{i+j-1},\end{aligned}$$

d'où la relation (4.13).

b) Relation (4.15) : $f = \sum_{i \in \mathbb{N}} a_i X^i \implies f \circ g = \sum_{i \in \mathbb{N}} a_i (g(X))^i$;
les relations (4.12), (4.13) et (4.14) impliquent alors

$$(f \circ g)' = \sum_{i \in \mathbb{N}^*} ia_i (g(X))^{i-1} g'(X) = f'(g(X))g'(X),$$

d'où $(f \circ g)' = (f' \circ g)g'$. □

Remarque 4.29. D'après la proposition 4.28., l'application

$$\begin{aligned}\mathcal{D} : A[X] &\longrightarrow A[X] \\ f &\longmapsto f'\end{aligned}$$

est un endomorphisme de A -modules.

2. Dérivations successives d'un polynôme

Pour tout $k \in \mathbb{N}$, on définit l'endomorphisme du A -module $A[X]$, $\mathcal{D}^k$, par récurrence sur k . On pose :

$$\mathcal{D}^0 = id_{A[X]}; \quad \mathcal{D}^1 = \mathcal{D}; \quad \mathcal{D}^k = \mathcal{D} \circ \mathcal{D}^{k-1}, \quad \forall k > 1.$$

Définition 4.30. Pour tout $f \in A[X]$ et tout $k \in \mathbb{N}$, le polynôme $\mathcal{D}^k(f)$, noté $f^{(k)}$, est appelé **polynôme dérivé $k^{\text{ème}}$** (ou **polynôme dérivé à l'ordre k**) de f .

$$f^{(0)} = f, f^{(1)} = f', f^{(2)}, \dots, f^{(k)}, \dots$$

sont les **polynômes dérivés successifs** du polynôme f .

Remarque 4.31. Compte tenu de la Prop. 4.25. et la Rem. 4.27.,

Si $\text{car} A = 0$ et A est intègre, alors

$$\deg f = n \implies \deg f^{(k)} = n - k, \quad \forall k (0 \leq k \leq n), \text{ d'où } f^{(n+1)} = 0.$$

Si $\text{car} A \neq 0$, alors

$$\deg f = n \implies \deg f^{(k)} \leq n - k, \quad \forall k (0 \leq k \leq n).$$

Proposition 4.32. Si K est un corps et $\text{car} K = 0$, alors quel que soit $f \in K[X]$ tel que $\deg f = n > 0$, on peut écrire :

$$f(X) = \sum_{0 \leq k \leq n} \frac{1}{k!} f^{(k)}(0) X^k, \text{ où } f^{(k)}(0) = \widetilde{f^{(k)}}(0).$$

Démonstration posée en exercice (Ex. 1, Ch. 4).

2. Polynômes à une indéterminée sur un corps K

A. Division euclidienne dans $K[X]$

Théorème 4.33. Quels que soient les polynômes f et g dans $K[X]$ tels que $g \neq 0$, il existe q et r , uniques dans $K[X]$, vérifiant les conditions

$$f = gq + r, \quad \deg r < \deg g. \quad (4.16)$$

Trouver les polynômes q et r c'est effectuer la **division euclidienne** de f par g dans $K[X]$. Les polynômes q et r sont respectivement appelés le **quotient** et le **reste** de cette division.

Preuve :

a) *Unicité de q et r .* Supposons qu'il existe deux couples de polynômes de $K[X]$, (q, r) et (q_1, r_1) , satisfaisant aux conditions (4.16).

$$f = gq + r = gq_1 + r_1 \implies g(q - q_1) = r_1 - r.$$

$K[X]$ est intègre et $g \neq 0$, donc $(q - q_1 \neq 0 \iff r_1 - r \neq 0)$.

$$q - q_1 \neq 0 \implies \deg(g(q - q_1)) = \deg(r_1 - r) \geq \deg g$$

$$(\deg r < \deg g \text{ et } \deg r_1 < \deg g) \implies \deg(r_1 - r) < \deg g,$$

d'où une contradiction, donc $q_1 = q$ et $r_1 = r$.

b) *Existence de q et r .* Posons $\deg f = n$ et $\deg g = m$. L'hypothèse $g \neq 0$ implique $m \geq 0$. On remarque que si $n < m$, alors les conditions (4.16) sont satisfaites avec $q = 0$ et $r = f$. On suppose donc dans la suite $n \geq m \geq 0$.

Ecrivons les polynômes f et g "suivant les puissances décroissantes de X " :

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0,$$

$$g = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0,$$

avec, par hypothèse, $a_n \neq 0$ et $b_m \neq 0$ dans K .

Si $n = m = 0$, alors $f = a_0 \neq 0$ et $g = b_0 \neq 0$ sont des polynômes constants non nuls et dans le corps K on a

$$a_0 = (a_0 b_0^{-1}) b_0 \iff f = a_0 b_0^{-1} g,$$

d'où, dans ce cas, $q = a_0 b_0^{-1}$ et $r = 0$.

Supposons maintenant $n > m \geq 0$ et raisonnons par récurrence sur n . L'hypothèse de récurrence dit que pour tout polynôme f_1 de degré n_1 tel que $n > n_1 \geq m \geq 0$, le quotient et le reste de la division euclidienne de f_1 par g existent ; or on peut écrire

$$f = a_n b_m^{-1} X^{n-m} g + f_1, \text{ où } \deg f_1 \leq n-1 < n.$$

Par suite, il existe des polynômes q_1 et r_1 dans $K[X]$ tels que

$$f_1 = g q_1 + r_1, \quad \deg r_1 < \deg g.$$

On en déduit

$$f = (a_n b_m^{-1} X^{n-m} + q_1) g + r_1, \quad \deg r_1 < \deg g,$$

d'où l'existence de $q = a_n b_m^{-1} X^{n-m} + q_1$ et $r = r_1$. □

Pratique de la division euclidienne dans $K[X]$

La méthode de calcul du quotient et du reste se déduit de la preuve du théorème 4.33. et la disposition pratique de la division est la même que celle utilisée pour la division dans les entiers.

Exemple : Effectuons la division euclidienne, dans $\mathbb{Q}[X]$, du polynôme

$$f = 5X^4 - X^2 + X - 4 \text{ par le polynôme } g = 2X^2 - X + 1.$$

$$\begin{array}{r|l} 5X^4 & -X^2 + X - 4 \\ \underline{5X^4 - \frac{5}{2}X^3 + \frac{5}{4}X^2 - \frac{5}{8}X + \frac{5}{8}} & \\ \frac{5}{2}X^3 - \frac{7}{2}X^2 + X - 4 & \\ \underline{\frac{5}{2}X^3 - \frac{5}{4}X^2 - \frac{1}{4}X - 4} & \\ -\frac{11}{4}X^2 + \frac{5}{4}X & \\ \underline{-\frac{11}{4}X^2 + \frac{11}{8}X + \frac{23}{8}} & \\ \frac{5}{8}X - \frac{23}{8} & \end{array}$$

Le quotient et le reste de la division euclidienne de f par g sont

$$q = \frac{5}{2}X^2 + \frac{5}{4}X - \frac{9}{8} \quad \text{et} \quad r = -\frac{11}{8} - \frac{23}{8}$$

Remarque 4.34. Si le reste de la division euclidienne de f par g est nul, on dit que g **divise** f dans $K[X]$; on écrit symboliquement $g|f$ et d'après la relation (4.16),

$$g|f \implies \deg g \leq \deg f.$$

Corollaire 4.35. Soit $f(X) \in K[X] \setminus K$; alors, pour tout $\alpha \in K$,

a) le reste de la division euclidienne de $f(X)$ par $X - \alpha$ est $f(\alpha)$, d'où

b) $X - \alpha$ divise $f(X)$, dans $K[X]$, si et seulement si α est racine du polynôme $f(X)$ (Déf. 4.18.).

Preuve : On a $f(X) = (X - \alpha)q(X) + r$, avec $r = 0$ ou $\deg r = 0$.

On en déduit que $r = f(\alpha)$, d'où

$$r = 0 \iff (X - \alpha) \text{ divise } f(X) \iff f(\alpha) = 0. \quad \square$$

Théorème 4.36. Si K est un corps, alors $K[X]$ est un domaine principal.

Preuve : On rappelle qu'un domaine principal (Déf. 2.7.) est un domaine d'intégrité (Déf. 1.21.) dans lequel tout idéal est principal.

$K[X]$ est un anneau unitaire, commutatif et intègre (Cor 4.12.) ; il reste à vérifier que tout idéal de $K[X]$ est principal.

Les idéaux (0) et $K[X] = (1)$ sont principaux. Considérons un idéal propre I , non nul dans $K[X]$; alors

$$(f \neq 0 \text{ et } f \in I) \implies \deg f > 0.$$

Soit $E := \{\deg f; f \in I \setminus \{0\}\}$. L'ensemble E est une partie non vide de $\mathbb{N}^*$, donc il existe un plus petit entier k dans E . Soit $p \in I$ tel que $\deg p = k$; pour tout f non nul dans I , on a $\deg f \geq \deg p$. La division euclidienne de f par p donne

$$f = pq + r, \quad \deg r < \deg p;$$

$$\text{alors, } (r = f - pq, f \in I, p \in I) \implies r \in I;$$

or p est un polynôme non nul, de plus petit degré dans I , par suite $\deg r < \deg p$ entraîne $r = 0$ et $f = pq$, d'où $I = (p)$. $\square$

Corollaire 4.37. I étant un idéal non nul de l'anneau $K[X]$, il existe un unique polynôme unitaire qui engendre I .

Preuve : D'après la démonstration du théorème 4.36., tout polynôme p de degré minimal dans $I \setminus \{0\}$ engendre I . Soit $p = \sum_{1 \leq i \leq d} a_i X^i$, où $d = \deg p$, un générateur de l'idéal I . Les hypothèses impliquent $a_d \neq 0, d \geq 1$ et tout polynôme de degré d dans I , engendre l'idéal I . On en déduit que $q = a_d^{-1}p$ est un polynôme unitaire qui engendre I ; montrons qu'il est unique. Supposons q_1 polynôme unitaire tel que $I = (q_1)$; on vérifie alors que

$$((q) = (q_1), d = \deg q_1 = \deg q, q \text{ et } q_1 \text{ unitaires}) \implies q = q_1. \quad \square$$

B. Racines d'un polynôme de $K[X]$

On rappelle (Déf. 4.18.) qu'un élément $\alpha \in K$ est racine d'un polynôme non constant $f \in K[X]$, si $f(\alpha) = 0$.

Remarque 4.38. : Un polynôme non constant $f(X) \in K[X]$ n'a pas nécessairement de racine dans le corps K . Par exemple $X^2 + 1$, dans $\mathbb{R}[X]$, n'a pas de racine dans $\mathbb{R}$. Par contre, les polynômes $X^2 - 1$ et $X^3 - 1$, de $\mathbb{R}[X]$, ont, respectivement, deux racines et une seule racine dans $\mathbb{R}$.

Une conséquence du corollaire 4.35. est le résultat suivant.

Théorème 4.39. *Un polynôme $f(X) \in K[X]$, de degré $n \geq 1$, a au plus n racines distinctes dans K .*

Preuve : On suppose que $f(X)$ a m racines distinctes dans K , notées $\alpha_1, \alpha_2, \dots, \alpha_m$, $m \geq 1$. Montrons, que $\prod_{1 \leq i \leq m} (X - \alpha_i)$ divise $f(X)$ dans $K[X]$.

Par hypothèse, α_1 est racine de $f(X)$, alors $X - \alpha_1$ divise $f(X)$ dans $K[X]$ (Cor. 4.35.), donc il existe $g_1(X)$, non nul dans $K[X]$, tel que

$$f(X) = (X - \alpha_1)g_1(X).$$

En considérant la racine α_2 , on obtient dans le corps K ,

$$f(\alpha_2) = 0 = (\alpha_2 - \alpha_1)g_1(\alpha_2);$$

alors $(\alpha_2 - \alpha_1) \neq 0$ par hypothèse, implique $g_1(\alpha_2) = 0$. On en déduit que $(X - \alpha_2)$ divise $g_1(X)$ dans $K[X]$, d'où l'existence de $g_2(X) \in K[X] \setminus \{0\}$ tel que

$$f(X) = (X - \alpha_1)(X - \alpha_2)g_2(X).$$

En répétant le raisonnement précédent on obtient de proche en proche,

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_{m-1})g_{m-1}(X),$$

où $g_{m-1}(X)$ est non nul dans $K[X]$. Les racines α_i , pour $1 \leq i \leq m$, étant deux à deux distinctes, on a

$$f(\alpha_m) = 0 = \left(\prod_{1 \leq i \leq m-1} (\alpha_m - \alpha_i)\right) g_{m-1}(\alpha_m) \implies g_{m-1}(\alpha_m) = 0.$$

Par suite, il existe $g_m(X) \in K[X] \setminus \{0\}$ vérifiant

$$g_{m-1}(X) = (X - \alpha_m)g_m(X), \quad \text{d'où}$$

$$f(X) = \left(\prod_{1 \leq i \leq m} (X - \alpha_i)\right) g_m(X). \quad (4.17)$$

On a $\deg g_m \geq 0$, donc en comparant des degrés des polynômes des deux membres de l'égalité (4.17), on obtient $m \leq n (= \deg f)$. $\square$

Remarque 4.40. :

a) Si, dans le théorème précédent, on a $m = n$, alors il est immédiat que

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i \implies f(X) = a_n \prod_{1 \leq i \leq n} (X - \alpha_i). \quad (4.18)$$

b) Un polynôme $f(X) \in K[X]$, de degré $n > 1$, qui a des racines dans K , n'a pas nécessairement n racines dans K (Cf. Rem. 4.38.).

Définition 4.41. Soit $f(X) \in K[X]$ et α une racine de f dans K , alors

a) α est une racine **simple** de f , si dans $K[X]$,

$$(X - \alpha) \mid f \quad \text{et} \quad (X - \alpha)^2 \nmid f.$$

b) α est une racine **multiple d'ordre $k > 1$** , si

$$(X - \alpha)^k \mid f \quad \text{et} \quad (X - \alpha)^{k+1} \nmid f.$$

L'entier k est appelé **l'ordre de multiplicité** de la racine α .

Définition 4.42. Un corps K est dit **algébriquement clos**, si tout polynôme non constant de $K[X]$ a au moins une racine dans K .

Remarque 4.43. La notion de *corps algébriquement clos* sera étudiée dans le Volume 2 (Extensions de Corps), où l'on démontrera, en particulier, que le *corps des nombres complexes*, $\mathbb{C}$, est *algébriquement clos*.

Ce résultat, très important, sera admis dans ce Volume 1.

Par contre, le corps des nombres réels, $\mathbb{R}$, n'est pas algébriquement clos, puisque, par exemple, le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$.

Proposition 4.44. Si K est un corps algébriquement clos, alors tout polynôme $f(X)$ de $K[X]$, de degré $n \geq 1$, a n racines dans K , "distinctes ou confondues". Si $\alpha_1, \alpha_2, \dots, \alpha_m$ désignent les racines distinctes de $f(X)$ dans K , on a $m \leq n$, et en notant, pour tout i ($1 \leq i \leq m$), k_i l'ordre de multiplicité de α_i , on peut écrire, dans $K[X]$,

$$f(X) = a \prod_{1 \leq i \leq m} (X - \alpha_i)^{k_i}, \quad \text{où } a \in K^* \text{ et } \sum_{1 \leq i \leq m} k_i = n. \quad (4.19)$$

Preuve : Le corps K étant algébriquement clos, $f(X)$ a au moins une racine $\alpha_1 \in K$, donc il existe $f_1(X) \in K[X]$, tel que

$$f(X) = (X - \alpha_1) f_1(X) \quad \text{et} \quad \deg f_1 = n - 1.$$

Si $n - 1 \geq 1$, le polynôme $f_1(X)$ a au moins une racine $\alpha_2 \in K$, d'où l'existence de $f_2(X) \in K[X]$, tel que

$$f(X) = (X - \alpha_1)(X - \alpha_2) f_2(X) \quad \text{et} \quad \deg f_2 = n - 2.$$

Ainsi, de proche en proche on obtient

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_{n-1}) f_{n-1}(X), \quad \text{où } \deg f_{n-1} = 1.$$

On en déduit qu'il existe $\alpha_n \in K$ et $a \in K \setminus \{0\}$ tels que

$$f_{n-1}(X) = a(X - \alpha_n), \quad \text{d'où, dans } K[X],$$

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n). \quad (4.20)$$

Les racines α_i , $1 \leq i \leq n$, intervenant dans l'égalité (4.20) ne sont pas nécessairement distinctes (c'est-à-dire deux à deux distinctes), nous dirons couramment qu'elles sont "distinctes ou confondues".

Les racines "confondues" sont les racines multiples, chacune d'elles étant comptée un nombre de fois égal à son ordre de multiplicité.

Si les racines distinctes de $f(X)$ sont $\alpha_1, \alpha_2, \dots, \alpha_m$, où $m \leq n$, on obtient la relation (4.19) de l'énoncé en regroupant, dans (4.20), les facteurs correspondant à chacune des racines multiples. La comparaison des degrés des polynômes des deux membres de (4.19) entraîne que $\sum_{1 \leq i \leq m} k_i = n$. $\square$

Exemple 4.45. Les nombres complexes i et $-i$ étant les racines du polynôme $X^2 + 1$, on a, dans $\mathbb{C}[X]$,

$$X^3 - 1 = (X - 1)(X - j)(X - j^2), \quad \text{où } j = \frac{-1 + i\sqrt{3}}{2}.$$

$$X^4 + 2X^2 + 1 = (X^2 + 1)^2 = (X - i)^2(X + i)^2.$$

Définition 4.46. Un polynôme $f(X) \in K[X]$, de degré $n \geq 1$, est dit **scindé sur K** , si, dans $K[X]$, on peut écrire $f(X)$ sous la forme (4.19) (ou de façon équivalente, sous la forme (4.20)), le corps K n'étant pas nécessairement algébriquement clos.

Exemple 4.47. Le corps $\mathbb{R}$ n'est pas algébriquement clos, cependant le polynôme $X^3 + X^2 - 3X - 3$ est scindé sur $\mathbb{R}$, car

$$X^3 + X^2 - 3X - 3 = (X + 1)(X - \sqrt{3})(X + \sqrt{3}).$$

Les résultats précédents (en particulier, le Th. 4.39. et la Prop. 4.44.) conduisent à la conclusion suivante.

Corollaire 4.48. Quel que soit le corps K , un polynôme $f \in K[X]$ tel que $\deg f = n \geq 1$ a au plus n racines, "distinctes ou confondues", dans K .

Proposition 4.49. Si K est un corps infini, alors l'application

$$\theta : K[X] \longrightarrow K^K$$

$$f \longmapsto \tilde{f}$$

est un morphisme injectif de K -algèbres.

Preuve : On sait que θ est un morphisme de K -algèbres (Prop. 4.22.).

Si f est un polynôme constant, il est immédiat que $\tilde{f} = 0$ implique $f = 0$.

Soit $f = \sum_{0 \leq i \leq n} a_i X^i \in K[X]$, tel que $\deg f = n > 0$. L'application

$\tilde{f} : K \rightarrow K$ est telle que $\forall \alpha \in K$, $\tilde{f}(\alpha) = \sum_{0 \leq i \leq n} a_i \alpha^i$, donc

$$\theta(f) = \tilde{f} = 0 \iff \forall \alpha \in K, \sum_{0 \leq i \leq n} a_i \alpha^i = 0. \quad (4.21)$$

Or, d'après le théorème 4.39., tout polynôme de degré $n > 0$ de $K[X]$ a au plus n racines distinctes dans K ; alors, compte tenu de (4.21), si K est infini, nécessairement, $\tilde{f} = 0$ entraîne $f = 0$, donc θ est injectif. $\square$

Remarque 4.50. :

a) La proposition 4.49 implique que $\text{Im } \theta$, c'est-à-dire la K -algèbre des fonctions polynômes de K dans K , est isomorphe à $K[X]$.

b) Le résultat de la proposition 4.49. n'est plus vraie si K est un corps fini (Cf. Rem. 4.23.).

Du théorème 4.39. et de la proposition 4.49. on déduit le résultat suivant.

Corollaire 4.51. Si K est un corps infini, alors pour tout polynôme non nul, $f \in K[X]$, il existe au moins un élément $a \in K$ tel que $f(a) \neq 0$.

C. Division suivant les puissances croissantes

Pour la division euclidienne dans $K[X]$, on écrit les polynômes comme une somme de monômes ordonnés suivant les puissances décroissantes de X ; c'est-à-dire que pour $f(X) \in K[X]$ de degré $n \geq 1$:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0.$$

Nous allons définir, dans ce paragraphe (Th. 4.52.) une division pour laquelle on écrit les polynômes comme une somme de monômes ordonnés suivant les puissances croissantes de X :

$$f(X) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + a_n X^n.$$

Théorème 4.52. Etant donné deux polynômes f et g de $K[X]$ tels que $g(0) \neq 0$ et un entier $k \geq 0$, il existe un unique couple (q_k, r_k) de polynômes de $K[X]$ vérifiant les conditions :

$$f = g q_k + X^{k+1} r_k, \quad \deg q_k \leq k. \quad (4.22)$$

Déterminer q_k et r_k c'est effectuer la division suivant les puissances croissantes, de f par g , à l'ordre k .

Preuve :

a) *Unicité de (q_k, r_k) .* Supposons l'existence de deux couples (q_k, r_k) et (q'_k, r'_k) vérifiant les conditions (4.22) ; on a

$$g(q_k - q'_k) + X^{k+1}(r_k - r'_k) = 0.$$

Alors l'hypothèse $g(0) \neq 0$ implique que X^{k+1} divise $q_k - q'_k$; par suite,

$$\deg(q_k - q'_k) \leq k \implies q_k - q'_k = 0.$$

b) *Existence de (q_k, r_k) .* Posons

$$f = a_0 + \dots + a_n X^n, \quad g = b_0 + \dots + b_m X^m, \quad \text{avec } b_0 \neq 0.$$

Raisonnons par récurrence sur k .

Pour $k = 0$, en prenant $q_0 = b_0^{-1} a_0$, on obtient $f - g q_0 = X r_0$, où

$$\deg(q_0) \leq 0 \text{ et } r_0 \in K[X].$$

Pour $k > 0$, on suppose (q_{k-1}, r_{k-1}) connu tel que

$$f = gq_{k-1} + X^k r_{k-1}, \quad \deg q_{k-1} \leq k-1.$$

La division de r_{k-1} par g , à l'ordre 0, donne

$$r_{k-1} = g\alpha_k + X\rho_k, \text{ où } \alpha_k = b_0^{-1}r_{k-1}(0) \in K, \rho_k \in K[X].$$

On en déduit que $f = g(q_{k-1} + \alpha_k X^k) + X^{k+1}\rho_k$, d'où

$$q_k = q_{k-1} + \alpha_k X^k \text{ et } r_k = \rho_k. \quad \square$$

Exemple 4.53. Effectuons la division à l'ordre 3, de $f = 1 - X - X^3 - X^6$ par $g = 1 - X - X^2$, dans $\mathbb{Q}[X]$.

Pour trouver le quotient q_3 et le reste r_3 , il suffit de suivre la méthode utilisée dans la preuve du Th. 4.52. La disposition pratique est semblable à celle de la division euclidienne.

$$\begin{array}{r} 1 - X \quad -X^3 \quad -X^6 \\ \quad X^2 - X^3 \quad -X^6 \\ \quad \quad \quad + X^4 - X^6 \end{array} \left| \begin{array}{l} 1 - X - X^2 \\ 1 + X^2 \\ \hline \end{array} \right.$$

d'où

$$1 - X - X^3 - X^6 = (1 - X - X^2)(1 + X^2) + X^4(1 - X^2),$$

donc $q_3 = 1 + X^2$ et $r_3 = 1 - X^2$.

Remarque 4.54. La division des polynômes suivant les puissances croissantes sert pour la décomposition des fractions rationnelles en éléments simples (Voir un cours de 1er cycle) et nous l'utiliserons pour le développement en séries formelles des fractions rationnelles (Ch. 7).

3. Polynômes à n indéterminées sur A , $n > 1$

A. Construction de l'algèbre des polynômes à n indéterminées

1°) On généralise la construction faite précédemment, pour $n = 1$.

On considère le A -module à gauche libre $A^{(\mathbb{N}^n)}$ (Cf. Ch. 3); on a

$$f \in A^{(\mathbb{N}^n)} \iff f = (a_i)_{i \in \mathbb{N}^n},$$

où les a_i sont presque tous nuls dans A , chaque indice i étant ici un n -uple d'entiers naturels $(i_1, i_2, \dots, i_n)$.

On définit dans $A^{(\mathbb{N}^n)}$ une multiplication par l'application

$$(f = (a_i)_{i \in \mathbb{N}^n}, g = (b_i)_{i \in \mathbb{N}^n}) \mapsto fg = (c_i)_{i \in \mathbb{N}^n},$$

$$\text{où } c_{(i_1, i_2, \dots, i_n)} = \sum_{j_r + k_r = i_r, 1 \leq r \leq n} a_{(j_1, j_2, \dots, j_n)} b_{(k_1, k_2, \dots, k_n)}.$$

On peut vérifier que $A^{(\mathbb{N}^n)}$ est alors muni d'une structure d'anneau unitaire, commutatif; l'élément unité étant noté 1, on a

$$1 = (a_i)_{i \in \mathbb{N}^n} \text{ où } a_0 = 1 \text{ pour } i = 0 \text{ dans } \mathbb{N}^n \text{ et } a_i = 0, \forall i \neq 0 \text{ dans } \mathbb{N}^n.$$

D'autre part, la structure de A -module à gauche de $A^{(\mathbb{N}^n)}$ étant définie par l'application

$$\begin{aligned} A \times A^{(\mathbb{N}^n)} &\longrightarrow A^{(\mathbb{N}^n)} \\ (\alpha, (a_i)_{i \in \mathbb{N}^n}) &\longmapsto (\alpha a_i)_{i \in \mathbb{N}^n}, \end{aligned}$$

on en déduit que quels que soient $\alpha \in A$, f et g dans $A^{(\mathbb{N}^n)}$:

$$\alpha(fg) = (\alpha f)g = f(\alpha g).$$

Ainsi, $A^{(\mathbb{N}^n)}$ est une **A-algèbre libre et commutative**.

2°) *Changement de notation* L'objet de ce paragraphe est de mettre en évidence une base canonique de l'algèbre $A^{(\mathbb{N}^n)}$.

Quel que soit $p \in \mathbb{N}^*$ tel que $1 \leq p \leq n$, on note X_p l'élément de $A^{(\mathbb{N}^n)}$ pour lequel $X_p = (a_i)_{i \in \mathbb{N}^n}$, avec

$$\begin{cases} a_i = 1, & \text{pour } i = (i_1, i_2, \dots, i_n), \text{ où } i_p = 1 \text{ et } i_l = 0, \text{ pour } l \neq p \\ a_i = 0, & \text{pour tous les autres éléments } i \in \mathbb{N}^n. \end{cases}$$

On a alors, pour $1 \leq p \leq n$ et $1 \leq q \leq n$ dans $\mathbb{N}$, $X_p X_q = (c_i)_{i \in \mathbb{N}^n}$,

$$\begin{cases} c_i = 1, & \text{pour } i = (i_1, i_2, \dots, i_n), \text{ où } i_p = i_q = 1 \text{ et } i_l = 0, \text{ si } l \neq p, l \neq q. \\ c_i = 0, & \text{pour tous les autres éléments } i \in \mathbb{N}^n. \end{cases}$$

On en déduit que quels que soient les entiers p ($1 \leq p \leq n$) et $r \in \mathbb{N}$, on a $X_p^r = (c_i)_{i \in \mathbb{N}^n}$ tel que

$$\begin{cases} c_i = 1, & \text{pour } i = (i_1, i_2, \dots, i_n) \text{ où } i_p = r, i_l = 0, \forall l (l \neq p) \\ c_i = 0, & \text{pour tous les autres éléments } i \in \mathbb{N}^n. \end{cases}$$

En particulier, pour tout entier p ($1 \leq p \leq n$), on a $X_p^0 = 1$ dans $A^{(\mathbb{N}^n)}$. En effet,

$X_p^0 = (c_i)_{i \in \mathbb{N}^n}$, où

$$c_i = 1, \text{ pour } i = 0 \text{ dans } \mathbb{N}^n; \quad c_i = 0, \text{ pour } i \neq 0 \text{ dans } \mathbb{N}^n.$$

Par suite, un élément $(a_i)_{i \in \mathbb{N}^n}$ de l'algèbre $A^{(\mathbb{N}^n)}$ tel que

$a_i \neq 0$, pour $i = (i_1, i_2, \dots, i_n)$ et $a_j = 0$, pour $j \neq i$ dans $\mathbb{N}^n$, s'écrit

$$a_i X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}. \quad (4.23)$$

La structure de A-algèbre libre de $A^{(\mathbb{N}^n)}$ implique alors que tout élément $f = (a_i)_{i \in \mathbb{N}^n}$ de cette algèbre s'écrit de façon unique

$$f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \quad \text{où } i = (i_1, i_2, \dots, i_n) \in \mathbb{N}^n, \quad (4.24)$$

les a_i étant "presque tous nuls" dans A . Autrement dit

$$\{X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}\}_{(i_1, i_2, \dots, i_n) \in \mathbb{N}^n}$$

est une *base* de l'algèbre libre $A^{(\mathbb{N}^n)}$, qui sera dite *canonique*.

Définition 4.55. Compte tenu des notations ci-dessus,

a) Les éléments $X_1, X_2, \dots, X_n$ sont appelés les **indéterminées**.

b) L'algèbre $A^{(\mathbb{N}^n)}$ est alors notée $A[X_1, X_2, \dots, X_n]$ et tout élément de cette algèbre est appelé **polynôme à n indéterminées sur A**; un tel polynôme f pourra aussi être noté $f(X_1, X_2, \dots, X_n)$.

c) Dans $A[X_1, X_2, \dots, X_n]$, un polynôme de la forme

$$a X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \quad a \in A, (i_1, i_2, \dots, i_n) \in \mathbb{N}^n$$

est appelé un **monôme**.

Remarque 4.56. :

a) La notation (4.24) montre que tout $f \neq 0$ dans $A[X_1, X_2, \dots, X_n]$ est une somme de monômes non nuls.

b) L'application

$$\begin{aligned}\mu : A &\longrightarrow A[X_1, X_2, \dots, X_n] \\ a &\longmapsto aX_1^0 X_2^0 \dots X_n^0\end{aligned}$$

est un morphisme injectif de A -algèbres qui permet d'identifier A à la sous-algèbre $Im \mu$ de $A[X_1, X_2, \dots, X_n]$; on écrira a à la place de $aX_1^0 X_2^0 \dots X_n^0$, ainsi

$$A \text{ est une sous-algèbre de } A[X_1, X_2, \dots, X_n].$$

Plus généralement, pour $m \in \mathbb{N}^*$ tel que $1 \leq m \leq n$, l'application

$$\begin{aligned}A[X_1, X_2, \dots, X_m] &\longrightarrow A[X_1, X_2, \dots, X_n] \\ \sum_{i \in \mathbb{N}^m} a_i X_1^{i_1} X_2^{i_2} \dots X_m^{i_m} &\longmapsto \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} X_2^{i_2} \dots X_m^{i_m} X_{m+1}^0 \dots X_n^0,\end{aligned}$$

où $i = (i_1, \dots, i_m) \in \mathbb{N}^m$ et $i = (i_1, \dots, i_m, 0, 0, \dots, 0) \in \mathbb{N}^n$, est un morphisme injectif de A -algèbres permettant d'identifier $A[X_1, X_2, \dots, X_m]$ à une sous-algèbre de $A[X_1, X_2, \dots, X_n]$.

c) La construction de l'algèbre libre et commutative $A[X_1, X_2, \dots, X_n]$, que nous avons donnée, montre que cette algèbre est indépendante du nom donné à chaque indéterminée, ainsi que de l'ordre dans lequel on considère ces indéterminées. Ces propriétés seront confirmées et précisées dans le paragraphe suivant.

B. Propriété universelle de l'anneau $A[X_1, \dots, X_n]$, $n > 1$ **Théorème 4.57. Propriété universelle**

Soit A et B deux anneaux unitaires, commutatifs et φ un morphisme d'anneaux unitaires de A dans B .

Etant donné $\beta_1, \beta_2, \dots, \beta_n$ dans B , il existe un unique morphisme d'anneaux unitaires, Φ , de $A[X_1, X_2, \dots, X_n]$ dans B tel que

$$\Phi|_A = \varphi \quad \text{et} \quad \Phi(X_i) = \beta_i, \quad \forall i (1 \leq i \leq n).$$

Preuve : Les notations sont celles de la relation (4.24).

Supposons l'existence de Φ ; alors on a nécessairement,

$$\Phi(\sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}) = \sum_{i \in \mathbb{N}^n} \varphi(a_i) \beta_1^{i_1} \dots \beta_n^{i_n},$$

d'où l'unicité de Φ .

Existence de Φ : pour $f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}$, où $i = (i_1, \dots, i_n)$, posons

$$\Phi(f) := \sum_{i \in \mathbb{N}^n} \varphi(a_i) \beta_1^{i_1} \dots \beta_n^{i_n}.$$

On vérifie que Φ est un morphisme d'anneaux unitaires satisfaisant aux conditions de l'énoncé, comme dans la preuve du théorème 4.6. $\square$

Corollaire 4.58. On a $A[X_1, X_2] \simeq A[X_1][X_2] \simeq A[X_2][X_1]$

et plus généralement, pour tout $j (1 \leq j \leq n)$:

$$\begin{aligned}A[X_1, \dots, X_n] &\simeq A[X_1, \dots, \hat{X}_j, \dots, X_n][X_j], \text{ où,} \\ \text{pour } j = 1, A[\hat{X}_1, X_2, \dots, X_n] &= A[X_2, \dots, X_n], \\ \text{pour } j > 1, A[X_1, \dots, \hat{X}_j, \dots, X_n] &= A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n].\end{aligned}$$

Preuve : Démontrons la propriété dans le cas $n = 2$ et $j = 2$.

Considérons la suite

$$A \xrightarrow{\mu} A[X_1] \xrightarrow{\mu'} A[X_1][X_2],$$

où μ et μ' sont les injections canoniques. Appliquons le théorème 4.57. aux anneaux A et $B = A[X_1][X_2]$, avec $\varphi = \mu' \circ \mu$; il existe alors un unique morphisme d'anneaux unitaires Φ de $A[X_1, X_2]$ dans $A[X_1][X_2]$ tel que

$$\Phi|_A = \varphi, \quad \Phi(X_1) = X_1, \quad \Phi(X_2) = X_2.$$

Montrons que Φ est un isomorphisme en construisant son inverse.

Soit ψ l'injection canonique de $A[X_1]$ dans $A[X_1, X_2]$; donc pour tout $f \in A[X_1]$, on a $\psi(f) = f$. D'après le Th. 4.6., il existe un unique morphisme d'anneaux unitaires

$$\Psi : A[X_1][X_2] \longrightarrow A[X_1, X_2]$$

tel que $\Psi|_{A[X_1]} = \psi$ et $\Psi(X_2) = X_2$. On vérifie alors que

$$\Psi \circ \Phi = id_{A[X_1, X_2]} \quad \text{et} \quad \Phi \circ \Psi = id_{A[X_1][X_2]},$$

donc Φ est un isomorphisme et $\Phi^{-1} = \Psi$. □

Remarque 4.59. Pour tout j ($1 \leq j \leq n$), le corollaire 4.58. permet d'identifier les anneaux $A[X_1, \dots, X_n]$ et $A[X_1, \dots, \hat{X}_j, \dots, X_n][X_j]$.

Corollaire 4.60. Quel que soit $n \in \mathbb{N}^*$, les A -algèbres $A[X_1, \dots, X_n]$ et $A[Y_1, \dots, Y_n]$ sont canoniquement isomorphes par

$$\begin{aligned} \Phi : A[X_1, \dots, X_n] &\longrightarrow A[Y_1, \dots, Y_n] \\ f(X_1, \dots, X_n) &\longmapsto f(Y_1, \dots, Y_n). \end{aligned}$$

Preuve : Raisonnons par récurrence sur n . La propriété est vraie pour $n = 1$ (Cor. 4.7.); supposons

$$A[X_1, \dots, X_{n-1}] \simeq A[Y_1, \dots, Y_{n-1}].$$

Posons $A' = A[X_1, \dots, X_{n-1}]$, $B' = A[Y_1, \dots, Y_{n-1}]$ et notons ϕ l'isomorphisme de A' sur B' . D'après le corollaire 4.8., ϕ induit un isomorphisme

$$\hat{\phi} : A'[X_n] \longrightarrow B'[X_n]$$

et le corollaire 4.7. implique $B'[X_n] \simeq B'[Y_n]$; par suite $A'[X_n] \simeq B'[Y_n]$.

Or on a $A'[X_n] \simeq A[X_1, \dots, X_n]$ et $B'[Y_n] \simeq A[Y_1, \dots, Y_n]$,

d'où le résultat énoncé. □

C. Degrés des polynômes de $A[X_1, \dots, X_n]$, $n > 1$.

1. Notion de degré partiel

D'après le Cor. 4.58., étant donné j ($1 \leq j \leq n$), tout polynôme $f \in A[X_1, \dots, X_n]$ peut être considéré comme un polynôme à une indéterminée X_j , sur l'anneau $A[X_1, \dots, \hat{X}_j, \dots, X_n]$, d'où la définition suivante.

Définition 4.61. Etant donné un polynôme non nul f dans $A[X_1, \dots, X_n]$, quel que soit j ($1 \leq j \leq n$), on appelle **degré partiel** de f en X_j , le degré de f considéré comme un polynôme à une indéterminée X_j et à coefficients dans l'anneau $A[X_1, \dots, \hat{X}_j, \dots, X_n]$.

Exemple 4.62. Soit $f \in \mathbb{Z}[X_1, X_2]$ tel que $f = X_1^3 X_2 + 2X_1 X_2^2 - X_2 + 3$, alors le degré partiel de f en X_1 est 3 et le degré partiel de f en X_2 est 2.

2. Notion de degré total

Définition 4.63. :

a) On appelle **degré total d'un monôme** non nul de $A[X_1, \dots, X_n]$, la somme de ses degrés partiels en $X_1, \dots, X_n$:

$$\text{degré total de } aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n} = i_1 + i_2 + \dots + i_n.$$

b) On appelle **degré total d'un polynôme** non nul de $A[X_1, \dots, X_n]$ le *maximum des degrés totaux* des monômes dont il est la somme.

Exemple 4.64. Le degré total du polynôme $f = X_1^3 X_2 + 2X_1 X_2^2 - X_2 + 3$, dans $\mathbb{Z}[X_1, X_2]$, est 4.

Par convention, le degré total du polynôme nul est strictement inférieur au degré total de tout polynôme non nul, il est symboliquement noté $-\infty$.

3. Polynômes homogènes dans $A[X_1, \dots, X_n]$, $n > 1$.

Définition 4.65. Un polynôme f non nul, dans $A[X_1, \dots, X_n]$, est dit **homogène de degré** d s'il est une somme de monômes de même degré total $d \geq 0$.

Exemple 4.66. Dans $\mathbb{Z}[X_1, X_2, X_3]$, le polynôme

$$f = 3X_1 X_2^2 X_3 + 2X_1^2 X_2^2 - X_1 X_2 X_3^2$$

est homogène de degré 4.

Définition 4.67. Etant donné un polynôme non nul $f \in A[X_1, \dots, X_n]$ et un entier $d \geq 0$, on appelle **composante homogène de degré d** de f , la somme des monômes de f , de degré d .

Exemple 4.68. Soit $f = X_1 X_2 - 2X_1^2 X_3 + X_2 X_3$ dans $\mathbb{Z}[X_1, X_2, X_3]$.

f a une composante homogène de degré 2 : $X_1 X_2 + X_2 X_3$

et une composante homogène de degré 3 : $-2X_1^2 X_3$.

Pour tout $d \in \mathbb{N} \setminus \{2, 3\}$, la composante homogène de degré d de f est nulle.

Remarque 4.69. Tout polynôme non nul de $A[X_1, \dots, X_n]$ est la somme de ses composantes homogènes.

D. Fonction polynôme à n indéterminées

Soit $f \in A[X_1, \dots, X_n]$ tel que $f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}$, où les a_i sont "presque tous nuls" dans A (Notation (4.24)).

Pour tout $(x_1, \dots, x_n) \in A^n$, on pose

$$f(x_1, \dots, x_n) := \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \dots x_n^{i_n}.$$

Définition 4.70. A étant un anneau unitaire, commutatif, à tout polynôme $f \in A[X_1, \dots, X_n]$, on associe l'application

$$\begin{aligned} \tilde{f} : A^n &\longrightarrow A \\ (x_1, \dots, x_n) &\longmapsto f(x_1, \dots, x_n). \end{aligned}$$

$\tilde{f}$ est la **fonction polynôme associée** à f .

A^{A^n} étant la A -algèbre des applications de A^n dans A , on a $\tilde{f} \in A^{A^n}$.

On montre, comme dans le cas d'une seule indéterminée (Prop. 4.22.), que l'application

$$\begin{aligned}\theta : A[X_1, \dots, X_n] &\longrightarrow A^{A^n} \\ f &\longmapsto \tilde{f}\end{aligned}$$

est un morphisme de A -algèbres, en général non injectif.

L'image de θ est, par définition, l'algèbre des fonctions polynômes à n indéterminées sur A .

Le résultat suivant généralise le corollaire 4.51.

Proposition 4.71. *Si K est un corps infini et $f \in K[X_1, \dots, X_n] \setminus \{0\}$, alors il existe $(a_1, \dots, a_n) \in K^n$ tel que $f(a_1, \dots, a_n) \neq 0$.*

Preuve : On raisonne par récurrence sur n .

Pour $n = 1$, le résultat est connu (Cor. 4.51.).

Pour $n > 1$, on considère $f(X_1, \dots, X_n)$ dans $K[X_1, \dots, X_{n-1}][X_n]$:

$$f(X_1, \dots, X_n) = \sum_{0 \leq i \leq r} B_i X_n^i, \text{ où } \forall i (0 \leq i \leq r), B_i \in K[X_1, \dots, X_{n-1}].$$

On suppose $B_r \neq 0$; l'hypothèse de récurrence entraîne l'existence de

$(a_1, \dots, a_{n-1}) \in K^{n-1}$ tel que $B_r(a_1, \dots, a_{n-1}) \neq 0$.

Le polynôme $f(a_1, \dots, a_{n-1}, X_n)$ est donc non nul dans $K[X_n]$; d'après le corollaire 4.51., il existe $a_n \in K$ tel que $f(a_1, \dots, a_{n-1}, a_n) \neq 0$. $\square$

E. Polynômes sur un anneau noethérien A

Il est entendu que A est un anneau commutatif, noethérien (Déf. 2.81.).

Théorème 4.72. Théorème de Hilbert

Si A est un anneau noethérien, alors pour tout $n \in \mathbb{N}^*$, l'anneau $A[X_1, \dots, X_n]$ est noethérien.

Preuve : Dans A , l'idéal engendré par des éléments $x_1, x_2, \dots, x_k$ sera noté $(x_1, x_2, \dots, x_k)$.

1°) Cas $n = 1$. Pour prouver que

$$A \text{ noethérien} \implies A[X] \text{ noethérien},$$

démontrons la contraposée de cette implication, c'est-à-dire

$$A[X] \text{ non noethérien} \implies A \text{ non noethérien.} \quad (4.25)$$

Si l'anneau $A[X]$ n'est pas noethérien, il contient au moins un idéal propre, non nul I , qui n'est pas de type fini (Th. 2.82.).

Soit $f_1 \in I \setminus (0)$, de degré minimal; l'hypothèse implique $I \neq (f_1)$. On en déduit qu'il existe $f_2 \in I \setminus (f_1)$, que l'on choisit de degré minimal.

Ainsi de proche en proche, pour tout entier $k \geq 1$, on choisit

$$f_{k+1} \in I \setminus (f_1, f_2, \dots, f_k), \text{ de degré minimal.}$$

Posons $n_k = \deg f_k$; le choix des f_k , pour $k \in \mathbb{N}^*$, implique

$$1 \leq n_1 \leq n_2 \leq \dots \leq n_k \leq n_{k+1} \leq \dots$$

D'autre part, pour tout $k \in \mathbb{N}^*$, notons a_k le coefficient directeur (Déf. 4.10.) du polynôme f_k et considérons la chaîne croissante d'idéaux de A :

$$(a_1) \subseteq (a_1, a_2) \subseteq \dots \subseteq (a_1, \dots, a_k) \subseteq (a_1, \dots, a_k, a_{k+1}) \subseteq \dots$$

Si cette chaîne était stationnaire, il existerait un entier $k > 0$ tel que

$$(a_1, \dots, a_k) = (a_1, \dots, a_k, a_{k+1});$$

on pourrait donc écrire dans A ,

$$a_{k+1} = \sum_{1 \leq i \leq k} b_i a_i, \text{ où } \forall i (1 \leq i \leq k), b_i \in A.$$

En posant $g = f_{k+1} - \sum_{1 \leq i \leq k} b_i X^{n_{k+1} - n_i} f_i$; on aurait

$$g \in I \setminus (f_1, f_2, \dots, f_k) \text{ et } \deg g < \deg f_{k+1},$$

ce qui est contraire au choix de f_{k+1} ; d'où la conclusion (4.25).

2°) Pour $n > 1$, on raisonne par récurrence sur n .

Supposons l'anneau $A[X_1, \dots, X_{n-1}]$ noethérien, alors le résultat démontré pour $n = 1$, implique (Cor. 4.58. et Rem. 4.59.)

$$A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n] \text{ noethérien.} \quad \square$$

4. Exercices

1) Démontrer la proposition 4.32.

2) Soit A un anneau unitaire, commutatif.

1°) Pour tout idéal I de A , on note $IA[X]$ l'idéal de l'anneau de polynômes $A[X]$ engendré par I et on désigne, respectivement, par π et σ les surjections canoniques $A \rightarrow A/I$ et $A[X] \rightarrow A[X]/IA[X]$.

Démontrer qu'il existe un unique isomorphisme d'anneaux unitaires ϕ de $A[X]/IA[X]$ sur $(A/I)[X]$ tel que $\phi \circ \sigma = \hat{\pi}$, où $\hat{\pi}$ est le morphisme de $A[X]$ sur $(A/I)[X]$ prolongeant π (Cor. 4.8.).

2°) Étant donné un idéal B de $A[X]$, soit $I := B \cap A$. En utilisant les notations du 1°), on pose $\bar{B} := \sigma(B)$. Prouver que $\bar{B}$ est un idéal de $A[X]/IA[X]$ tel que $\phi(\bar{B}) \cap A/I = (\bar{0})$, où $\bar{0} = \pi(0)$.

3) K étant un corps, soit $g \in K[X] \setminus K$. En utilisant la division euclidienne dans $K[X]$, démontrer que pour tout polynôme $f \in K[X]$, il existe une famille finie de polynômes, $f_0, f_1, \dots, f_r$, uniques dans $K[X]$, tels que

$$\forall i (0 \leq i \leq r), \deg f_i < \deg g \text{ et } f = g^r f_r + g^{r-1} f_{r-1} + \dots + g f_1 + f_0.$$

4) A étant un anneau unitaire, commutatif, soit $p(X) \in A[X] \setminus A$, dont le coefficient directeur est inversible dans A . Le but de l'exercice est alors de prouver que pour tout polynôme $f(X) \in A[X]$, il existe $q(X)$ et $r(X)$ dans $A[X]$ tels que

$$f(X) = p(X)q(X) + r(X), \quad r = 0 \text{ ou } 0 \leq \deg r \leq \deg p. \quad (4.26)$$

On note π la surjection canonique $A[X] \rightarrow A[X]/(p(X))$, où $(p(X))$ désigne l'idéal de $A[X]$ engendré par $p(X)$. On pose $\bar{X} = \pi(X)$.

Pour $f(X) = \sum_{0 \leq i \leq n} b_i X^i$ dans $A[X]$, écrire $\pi(f(X))$ en fonction de $\bar{X}$.

Montrer que pour tout $f(X) \in A[X]$, il existe $r(X) \in A[X]$ tel que

$$f(X) \equiv r(X) \pmod{p(X)} \quad \text{et} \quad (r = 0 \text{ ou } 0 \leq \deg r \leq \deg p).$$

En déduire (4.26).

5) K étant un corps, on pose $A = K[X, Y]$ et on note Q l'idéal de A engendré par X et Y^2 ; on pourra écrire $Q = (X, Y^2)$.

1°) Soit (Y^2) l'idéal de A engendré par Y^2 , démontrer que $A/Q \simeq K[Y]/(Y^2)$ (isomorphisme d'anneaux).

2°) Prouver que tout diviseur de zéro de A/Q est *nilpotent* (Déf. 1.26.).

En déduire que l'idéal Q de A est *primaire* (Ex. 15, Ch. 2) et que $\sqrt{Q}$ (Ex. 14, Ch. 2) est l'idéal de A engendré par X et Y .

3°) On pose $P = \sqrt{Q} = (X, Y)$. Vérifier que $P^2 \subsetneq Q \subsetneq P$.

En déduire qu'un idéal primaire n'est pas nécessairement une puissance de son radical (Ex. 15, Ch. 2).

6) Soit $K[X, Y, Z]$ l'anneau des polynômes à trois indéterminées sur un corps K . On note I l'idéal de $K[X, Y, Z]$ engendré par le polynôme $XY - Z^2$.

On pose $B = K[X, Y, Z]/I$; π étant la surjection canonique de $K[X, Y, Z]$ sur B , pour tout polynôme $f(X, Y, Z) \in K[X, Y, Z]$ on écrira

$$\pi(f(X, Y, Z)) = \overline{f(X, Y, Z)}.$$

1°) Montrer que tout élément de B peut s'exprimer sous la forme

$$f(\overline{X}, \overline{Y}) + g(\overline{X}, \overline{Y})\overline{Z},$$

où f et g sont des polynômes à deux indéterminées sur K .

2°) Soit P l'idéal de B engendré par $\overline{X}$ et $\overline{Z}$.

a) Montrer que l'anneau B/P est isomorphe à $K[Y]$. En déduire que P est un idéal premier de B .

b) Prouver que P n'est pas un idéal *primaire* de B (Ex. 15, Ch. 2). En déduire que, d'une façon générale, pour un idéal I d'un anneau unitaire commutatif :

$$\sqrt{I} \text{ premier} \not\Rightarrow I \text{ primaire.}$$

7) A étant un D.I., quel est le radical de Jacobson (Déf. 2.90.) de l'anneau de polynômes $A[X]$? (Voir Th. 2.91.)

8) 1°) Soit A un anneau unitaire, commutatif, *non intègre*; on note U_A le groupe des éléments inversibles de A .

Etant donné un élément $a \in A$, *nilpotent* non nul (Déf. 1.26.), montrer que pour tout $u \in U_A$, on a $(u - a) \in U_A$.

2°) Vérifier que dans l'anneau $(\mathbb{Z}/8\mathbb{Z})[X]$, le polynôme $3 - 4X + 2X^2$ est inversible.

9) Comme dans l'exercice précédent, on considère un anneau A unitaire, commutatif, *non intègre*. Le but des deux premières questions est de caractériser les éléments *inversibles* de $A[X]$. On note U_A (resp. $U_{A[X]}$) le groupe des unités de A (resp. $A[X]$). Il s'agit de prouver que

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i \in A[X] \setminus \{0\}$$

est inversible dans $A[X]$ si et seulement si les coefficients de f vérifient :

$$a_0 \in U_A \quad \text{et} \quad \forall i (1 \leq i \leq n), a_i \text{ est nilpotent dans } A. \quad (4.27)$$

1°) On suppose que les coefficients $a_i, 0 \leq i \leq n$, vérifient les conditions (4.27). Démontrer que le polynôme $\sum_{1 \leq i \leq n} a_i X^i$ est nilpotent dans $A[X]$

(Voir Ex. 13, Ch. 1).

En déduire que $f(X) \in U_{A[X]}$ (Voir Ex. 8, ci-dessus).

2°) On suppose $f(X) = \sum_{0 \leq i \leq n} a_i X^i \in U_{A[X]}$, $n = \deg f$.

Soit $g(X) = \sum_{0 \leq i \leq p} b_i X^i$ dans $A[X]$ tel que $p = \deg g$ et $fg = 1$.

a) Montrer que $a_0 \in U_A$.

b) En supposant $n \geq 1$, démontrer que $a_n b_p = 0$, $a_n^2 b_{p-1} = 0$ et plus généralement,

$$\forall r (0 \leq r \leq p), a_n^{r+1} b_{p-r} = 0.$$

Prouver alors que a_n est nilpotent dans A . En déduire (Ex. 8, précédent) que

$$f - a_n X^n = \sum_{0 \leq i \leq n-1} a_i X^i \in U_{A[X]}.$$

c) Prouver que pour $1 \leq i \leq n$, tous les coefficients a_i de f sont nilpotents.

3°) Soit $p(X) = \sum_{0 \leq i \leq n} c_i X^i$ un polynôme non nul de $A[X]$, de degré n . D'après le 1°) ci-dessus, si tous les coefficients de $p(X)$ sont nilpotents, alors $p(X)$ est nilpotent dans $A[X]$.

a) Démontrer que $p(X)$ est nilpotent dans $A[X]$ si et seulement si tous ses coefficients sont nilpotents dans A .

(Utiliser le 1°) et pour la réciproque, considérer le polynôme $f = 1 - p(X)$).

b) Soit $\mathcal{N}(A)$ (resp. $\mathcal{N}(A[X])$) le nilradical de A (resp. $A[X]$) (Déf. 2.87.). Montrer que les résultats précédents justifient l'égalité

$$\mathcal{N}(A[X]) = \mathcal{N}(A)[X].$$

4°) Soit $\mathcal{J}(A)$ (resp. $\mathcal{J}(A[X])$) le radical de Jacobson de A (resp. $A[X]$) (Déf. 2.90.).

a) Justifier l'inclusion $\mathcal{N}(A[X]) \subseteq \mathcal{J}(A[X])$.

b) Montrer que pour tout $f(X) \in \mathcal{J}(A[X])$, le polynôme $1 - Xf(X)$ est inversible dans $A[X]$. Prouver alors les relations

$$\mathcal{N}(A[X]) = \mathcal{J}(A[X]) \subseteq \mathcal{J}(A)[X].$$





Chapitre 5

Factorisation dans les domaines d'intégrité

Rappel de notations : Pour un anneau unitaire, commutatif A , on pose : $A^* = A \setminus \{0\}$ et U_A désigne le groupe des éléments inversibles de A , aussi appelés *unités* de A (Rem. 1.7., Prop. 1.9.).

1. Corps des fractions d'un domaine d'intégrité

Rappelons que tout sous-anneau d'un corps est un domaine d'intégrité. Nous verrons dans ce paragraphe qu'inversement, tout domaine d'intégrité est sous-anneau d'un corps. Dans la suite, on utilisera couramment la *notation abrégée* D.I. pour désigner un domaine d'intégrité.

A. Construction du corps des fractions d'un D.I.

Soit A un domaine d'intégrité. On remarque que

$$1 \in A^* \quad \text{et} \quad (s, t) \in A^* \times A^* \implies st \in A^*.$$

On définit dans $A \times A^*$ une relation binaire $\mathcal{R}$ par :

$$(a, s) \mathcal{R} (b, t) \iff at = bs.$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence : il est immédiat que $\mathcal{R}$ est réflexive et symétrique, de plus, quelques que soient $(a, s), (b, t), (c, r)$ dans $A \times A^*$,

$$\begin{aligned} ((a, s) \mathcal{R} (b, t) \iff at = bs) \quad \text{et} \quad ((b, t) \mathcal{R} (c, r) \iff br = ct) \\ \text{impliquent } (ar)t = (cs)t, \text{ d'où } ar = cs, \text{ dans l'anneau intègre } A; \end{aligned}$$

par suite $(a, s) \mathcal{R} (c, r)$, donc $\mathcal{R}$ est transitive.

Définition 5.1. Notation

La classe d'équivalence modulo $\mathcal{R}$ d'un élément $(a, s) \in A \times A^*$ est notée $\frac{a}{s}$ et appelée **fraction**. On pose

$$K = (A \times A^*) / \mathcal{R} = \left\{ \frac{a}{s}; (a, s) \in A \times A^* \right\}.$$

On considère alors les correspondances :

$$\begin{aligned} K \times K &\longrightarrow K \\ (i) \quad \left(\frac{a}{s}, \frac{b}{t} \right) &\longmapsto \frac{at + bs}{st} \\ (ii) \quad \left(\frac{a}{s}, \frac{b}{t} \right) &\longmapsto \frac{ab}{st} \end{aligned}$$

et on vérifie que (i) et (ii) définissent deux applications de $K \times K$ dans K . En effet :

$$\frac{a'}{s'} = \frac{a}{s} \quad \text{et} \quad \frac{b'}{t'} = \frac{b}{t} \iff a's = as' \quad \text{et} \quad b't = bt',$$

d'où $(a't' + b's')st = (at + bs)s't'$ et $a'b'st = abs't'$, par suite

$$\frac{a't' + b's'}{s't'} = \frac{at + bs}{st} \quad \text{et} \quad \frac{a'b'}{s't'} = \frac{ab}{st}.$$

Ainsi K est muni de deux lois de composition internes définies par (i) et (ii), respectivement notées additivement et multiplicativement.

Pour tout couple de fractions $(\frac{a}{s}, \frac{b}{t}) \in K \times K$, on écrira

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{et} \quad \frac{a}{s} \frac{b}{t} = \frac{ab}{st}. \quad (5.1)$$

Les éléments $\frac{0}{1}$ et $\frac{1}{1}$ sont, respectivement, élément neutre pour l'addition et la multiplication dans K ; il est facile de vérifier que ces deux opérations définissent sur K une structure d'anneau unitaire commutatif induite par celle de A . De plus, on a

$$\frac{a}{s} \neq \frac{0}{1} \iff a \neq 0 \text{ dans } A.$$

Par suite, dans K , tout $\frac{a}{s}$ non nul a un inverse $\frac{s}{a}$, donc K est un corps.

L'application $\alpha : A \longrightarrow K$ telle que pour tout $a \in A$, $\alpha(a) = \frac{a}{1}$ est un morphisme d'anneaux unitaires et

$$\alpha(a) = \frac{0}{1} \iff a = 0,$$

donc α est injectif; par suite A est isomorphe au sous-anneau unitaire $Im \alpha$ de K . En général on identifie A à $Im \alpha$ en écrivant a à la place de $\frac{a}{1}$ pour tout a dans A . Grâce à cette identification, on peut dire que A est un sous-anneau unitaire du corps K .

Le morphisme α est alors appelé : *injection canonique* de A dans K .

Définition 5.2. Le corps K , construit ci-dessus, est appelé **corps des fractions** du domaine d'intégrité A ; on écrira $K = Fr A$.

Remarque 5.3. Avec les hypothèses et les notations ci-dessus, étant donné $\frac{a}{s} \in K$, on a

$$\frac{a}{s} = \frac{a}{1} \frac{1}{s} = \alpha(a)(\alpha(s))^{-1}.$$

Mais compte tenu de l'identification de A à son image par α , on a $\alpha(a) = a$ et $\alpha(s) = s$, ce qui permet d'écrire dans K :

$$\frac{a}{s} = as^{-1}.$$

Il est important de noter que s^{-1} n'a de sens, en général, que dans K , car s n'est pas nécessairement inversible dans l'anneau A .

Exemple 5.4. :

- 1) Le corps $\mathbb{Q}$ des nombres rationnels est le corps des fractions de l'anneau des entiers $\mathbb{Z}$.
- 2) Si A est un D.I. (en particulier, si A est un corps), on sait que l'anneau des polynômes $A[X]$ est aussi un D.I. (Cor. 4.12). Dans ce cas, le corps $Fr A[X]$ est appelé **corps des fractions rationnelles à une indéterminée sur A** et est noté $A(X)$.

$$A(X) = \left\{ \frac{f(X)}{g(X)} ; f(X), g(X) \text{ dans } A[X], g(X) \neq 0 \right\}.$$

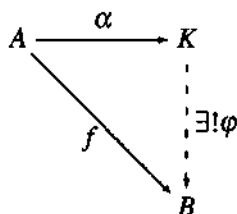
Plus généralement, avec les mêmes hypothèses sur A , $A[X_1, X_2, \dots, X_n]$ est un D.I., quel que soit $n \in \mathbb{N}^*$; on peut donc considérer, pour $n > 1$, $Fr A[X_1, X_2, \dots, X_n]$, appelé **corps des fractions rationnelles à n indéterminées sur A** et noté $A(X_1, X_2, \dots, X_n)$.

B. Propriétés du corps des fractions d'un D.I.**Théorème 5.5. : Propriété universelle**

A étant un D.I., si $K = \text{Fr} A$ et si α est l'injection canonique de A dans K , alors pour tout anneau unitaire, commutatif B et tout morphisme d'anneaux unitaires $f \in \text{Hom}(A, B)$ tel que $f(A^) \subseteq U_B$, il existe un unique $\varphi \in \text{Hom}(K, B)$ vérifiant : $\varphi \circ \alpha = f$.*

Preuve : On rappelle que U_B désigne le groupe des unités de B .

a) Supposons l'existence d'un morphisme φ tel que le diagramme suivant commute



et démontrons qu'alors, il est unique.

$$\varphi \circ \alpha = f \iff \forall a \in A, \varphi\left(\frac{a}{1}\right) = f(a).$$

Soit $\frac{a}{s} \in K$; on peut écrire : $\frac{a}{1} = \frac{a}{s} \frac{s}{1}$.

$$\varphi \in \text{Hom}(K, B) \implies f(a) = \varphi\left(\frac{a}{1}\right) = \varphi\left(\frac{a}{s}\right) \varphi\left(\frac{s}{1}\right)$$

$$f(A^*) \subseteq U_B \implies \varphi\left(\frac{s}{1}\right) = f(s) \in U_B.$$

On en déduit que

$$\forall \frac{a}{s} \in K, \quad \varphi\left(\frac{a}{s}\right) = f(a)(f(s))^{-1}, \quad (5.2)$$

d'où l'unicité de φ .

b) Montrons que la condition : $f(A^*) \subseteq U_B$, entraîne l'existence d'un morphisme $\varphi \in \text{Hom}(K, B)$ tel que $\varphi \circ \alpha = f$. Le résultat précédent conduit à considérer la correspondance :

$$\begin{aligned} \varphi : K &\longrightarrow B \\ \frac{a}{s} &\longmapsto f(a)(f(s))^{-1}. \end{aligned}$$

- Vérifions que φ est une application :

$$\frac{a'}{s'} = \frac{a}{s} \text{ dans } K \iff a's = as' \text{ dans } A;$$

$$a's = as' \implies f(a')f(s) = f(a)f(s'),$$

$$(s, s') \in A^* \times A^* \implies (f(s), f(s')) \in U_B \times U_B,$$

$$\text{d'où : } f(a')(f(s'))^{-1} = f(a)(f(s))^{-1}, \text{ c'est-à-dire :}$$

$$\varphi\left(\frac{a'}{s'}\right) = \varphi\left(\frac{a}{s}\right).$$

- Montrons que l'application φ est un morphisme d'anneaux unitaires.

Pour tout couple $\left(\frac{a}{s}, \frac{b}{t}\right) \in K \times K$, on a

$$\varphi\left(\frac{a}{s} + \frac{b}{t}\right) = \varphi\left(\frac{at + bs}{st}\right) = f(at + bs)(f(st))^{-1}.$$

Mais f est un morphisme d'anneaux unitaires et B est un anneau commutatif, alors,

$$\varphi\left(\frac{a}{s} + \frac{b}{t}\right) = f(a)(f(s))^{-1} + f(b)(f(t))^{-1} = \varphi\left(\frac{a}{s}\right) + \varphi\left(\frac{b}{t}\right).$$

$$\begin{aligned}\varphi\left(\frac{a}{s} \frac{b}{t}\right) &= \varphi\left(\frac{ab}{st}\right) = f(ab)(f(st))^{-1} \\ &= f(a)(f(s))^{-1} f(b)(f(t))^{-1} = \varphi\left(\frac{a}{s}\right) \varphi\left(\frac{b}{t}\right).\end{aligned}$$

D'autre part, $\varphi\left(\frac{1}{1}\right) = f(1)(f(1))^{-1} = 1$ (unité de B).

De plus, $\forall a \in A$, $\varphi\left(\frac{a}{1}\right) = f(a)(f(1))^{-1} = f(a)$, d'où : $\varphi \circ \alpha = f$. $\square$

Remarque 5.6. Avec les hypothèses du théorème précédent :

$$f(A^*) \subseteq U_B \implies f \neq 0;$$

par suite le morphisme $\varphi \in \text{Hom}(K, B)$ est non nul, donc *injectif* puisque K est un corps (Prop. 1.58.).

Corollaire 5.7. :

1) Soit A un D.I. et F un corps. S'il existe un morphisme injectif d'anneaux unitaires de A dans F , alors F contient un sous-corps isomorphe au corps $K = \text{Fr} A$.

2) A étant un D.I., s'il existe un corps K' et un morphisme injectif $\alpha' \in \text{Hom}(A, K')$ tel que le couple (K', α') vérifie la propriété universelle du couple (K, α) (Th. 5.5.), alors il existe un isomorphisme φ de K sur K' tel que $\varphi \circ \alpha = \alpha'$.

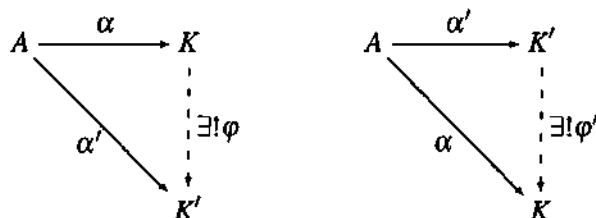
Preuve :

1) Par hypothèse, il existe un morphisme injectif d'anneaux unitaires $f : A \rightarrow F$, donc

$$f(A^*) \subseteq F^*, \text{ où } F^* = F \setminus \{0\} = U_F,$$

puisque F est un corps. D'après le théorème 5.5. et la remarque 5.6., il existe un unique morphisme injectif $\varphi : K \rightarrow F$ tel que $\varphi \circ \alpha = f$, d'où $K \simeq \text{Im } \varphi$; F contient donc un sous-corps isomorphe à K .

2) Compte tenu des hypothèses, l'application du théorème 5.5 aux couples (K, α) et (K', α') , respectivement, donne les deux diagrammes commutatifs suivants :



donc $\varphi \circ \alpha = \alpha'$ et $\varphi' \circ \alpha' = \alpha$.

On en déduit que $\varphi' \circ \varphi \circ \alpha = \alpha$ et $\varphi \circ \varphi' \circ \alpha' = \alpha'$.

La propriété universelle vérifiée par les couples (K, α) et (K', α') implique que nécessairement,

$$\varphi' \circ \varphi = \text{id}_K \quad \text{et} \quad \varphi \circ \varphi' = \text{id}_{K'}.$$

Par suite φ est un isomorphisme et $\varphi^{-1} = \varphi'$. $\square$

Remarque 5.8. :

Le 1) du corollaire 5.7. exprime qu'à un isomorphisme près, le corps des fractions d'un domaine d'intégrité A est "le plus petit corps" contenant A .

Le 2) du corollaire 5.7. exprime l'unicité, à un isomorphisme près, du corps des fractions d'un domaine d'intégrité A .

2. Eléments remarquables dans un D.I.

A. Diviseurs et unités dans un anneau unitaire, commutatif

Dans ce paragraphe, A désigne un anneau unitaire, commutatif.

La notion de divisibilité se définit dans l'anneau A , comme dans l'anneau $\mathbb{Z}$ (Cf. App. A).

Définition 5.9. Etant donné $a \in A$, on dit que $b \in A^*$ **divise** a (ou est un **diviseur** de a) dans A s'il existe $q \in A$ tel que $a = bq$.

Notations : Ce sont les mêmes que celles utilisées dans $\mathbb{Z}$ (Cf. App. A) ; on écrira, $b|a$ (resp. $b \nmid a$) pour exprimer que b divise a (resp. b ne divise pas a) dans A .

Pour tout $a \in A$, on note (a) l'idéal de A engendré par a .

Proposition 5.10. :

1) Pour $(a, b) \in A \times A^*$, on a $b|a \iff (a) \subseteq (b)$.

2) $u \in U_A \iff (u) = A$.

3) $\forall (u, a) \in U_A \times A$, $u|a$.

4) $(u \in U_A \text{ et } v|u \text{ dans } A) \implies v \in U_A$.

Preuve :

1) $b|a \iff \exists q \in A$, $a = bq$, donc

$$b|a \iff a \in (b) \iff (a) \subseteq (b).$$

2) $u \in U_A \iff \exists u^{-1} \in A$, $uu^{-1} = 1$, alors

$$u \in U_A \iff 1 \in (u) \iff (u) = A.$$

3) Quels que soient $a \in A$ et $u \in U_A$, $a = 1a = uu^{-1}a$, donc $u|a$.

4) Soit $u \in U_A$ et $v \in A$ tels que $v|u$; alors $u = vq$, avec $q \in A^*$, d'où

$$1 = uu^{-1} = vqu^{-1} \implies v \in U_A. \quad \square$$

B. Eléments associés dans un D.I.

Définition 5.11. Deux éléments a et b d'un domaine d'intégrité A , sont dits **associés** si $a = b = 0$ ou $((a, b) \in A^* \times A^* \text{ est tel que } (a|b \text{ et } b|a))$.

Notation : On écrira $a \sim b$, pour exprimer que a et b sont *associés* dans un domaine d'intégrité A .

Proposition 5.12. A étant D.I., quels que soient $(a, b) \in A^* \times A^*$,

$$a \sim b \iff \exists u \in U_A, b = ua.$$

$$\iff \exists v \in U_A, a = vb.$$

Preuve : a et b non nuls et $a \sim b$ implique $a|b$ et $b|a$, donc

$$\exists (u, v) \in A^* \times A^*; b = ua \text{ et } a = vb;$$

par suite, $a = vua$, donc $a(1 - vu) = 0$. L'anneau A étant intègre,

$$(a \neq 0 \text{ et } a(1 - vu) = 0) \implies vu = 1,$$

d'où u et v dans U_A .

Réciproquement, si a et b sont non nuls dans A ,

$$(b = ua \text{ et } a = vb, (u, v) \in U_A \times U_A) \implies (a|b, \text{ et } b|a),$$

donc a et b sont associés. □

Remarque 5.13. :

a) Dans l'anneau $\mathbb{Z}$, $U_{\mathbb{Z}} = \{1, -1\}$, donc pour deux entiers m et n , on a

$$m \sim n \iff m = \pm n.$$

b) Dans un corps K , deux éléments non nuls quelconques a, b sont toujours associés, puisque $a = bb^{-1}a$ et $b^{-1}a \in U_K = K^*$.

Proposition 5.14. Soit A un domaine d'intégrité.

1) Dans A^* , la relation de divisibilité est un **préordre**.

2) Dans A , la relation d'association est une relation d'**équivalence** et si l'on note $\tilde{a}$ la classe d'équivalence d'un élément a modulo la relation d'association, alors :

$$\tilde{a} = \tilde{b} \iff (a) = (b),$$

où (a) et (b) sont les idéaux de A , respectivement engendrés par a et b .

3) Dans A^* , la divisibilité est compatible avec la relation d'association et elle induit dans l'ensemble $\tilde{A}^*$ des classes d'équivalence $\tilde{a} \neq \tilde{0}$ une relation d'**ordre**, que l'on appellera encore "divisibilité" et que l'on notera encore symboliquement $|$, telle que

$$\tilde{a} | \tilde{b} \text{ dans } \tilde{A}^* \iff a | b \text{ dans } A.$$

Preuve :

1) On rappelle qu'une relation binaire est un *préordre*, si c'est une relation réflexive et transitive. Dans l'Appendice A, on montre que la divisibilité est une relation de *préordre* dans $\mathbb{Z}^*$ (Rem. 0.4.) ; la même justification est valable pour un D.I. quelconque et d'après la proposition 5.12., la divisibilité n'est ni une relation d'équivalence, ni une relation d'ordre.

2) Dans A on a $0 \sim 0$ (Déf. 5.11.) et pour a non nul, $a = 1a$ implique $a \sim a$; de plus,

$$a \sim b \iff b \sim a.$$

D'autre part, d'après la proposition 5.12., pour a, b, c dans A :

$$(a \sim b \text{ et } b \sim c) \iff (\exists (u, v) \in U_A \times U_A : b = ua, c = vb),$$

$$\text{d'où } (a \sim b \text{ et } b \sim c) \implies c = vua \implies a \sim c, \quad \text{car } vu \in U_A.$$

On en conclut que la relation d'association est réflexive, symétrique, transitive, donc est une relation d'équivalence.

Par ailleurs, pour a et b non nuls dans A ,

$$\tilde{a} = \tilde{b} \iff a \sim b \iff (a|b, \text{ et } b|a).$$

Or, d'après la proposition 5.10. :

$$(a|b \iff (b) \subseteq (a)) \quad \text{et} \quad (b|a \iff (a) \subseteq (b)),$$

$$\text{par suite, } \tilde{a} = \tilde{b} \iff (a) = (b).$$

3) Dire que la divisibilité est compatible avec la relation d'association dans A^* , c'est exprimer que quels que soient a, a', b, b' dans A^* ,

$$(a|b, a' \sim a \text{ et } b' \sim b) \implies a' | b'.$$

$$\text{En effet, } a|b \iff \exists q \in A, b = aq;$$

$$a' \sim a \iff \exists u \in U_A, a = ua';$$

$$b' \sim b \iff \exists v \in U_A, b = vb';$$

alors, $b = aq \implies vb' = ua'q \implies b' = a'ua'q^{-1}$, donc $a' | b'$.

On peut alors considérer dans l'ensemble $\tilde{A}^*$, la relation binaire, notée comme la divisibilité et définie par

$$\tilde{a} | \tilde{b} \text{ dans } \tilde{A}^* \iff a | b \text{ dans } A^*.$$

Cette relation est *réflexive* et *transitive*, puisque la divisibilité dans A^* est un *préordre* ; de plus

$$\begin{aligned} \tilde{a}|\tilde{b} \text{ et } \tilde{b}|\tilde{a} &\iff a|b \text{ et } b|a \text{ dans } A^* \\ &\iff a \sim b \text{ dans } A^* \iff \tilde{a} = \tilde{b}; \end{aligned}$$

ainsi la "divisibilité" considérée dans $\tilde{A}^*$ est *antisymétrique*. On en conclut que c'est une relation d'ordre. $\square$

Exemple 5.15. Dans le cas de l'anneau des entiers $\mathbb{Z}$, pour tout $m \in \mathbb{Z}^*$, $\tilde{m} = \{-m, m\}$, donc $|m|$ est un représentant de la classe d'équivalence $\tilde{m}$. Par suite, $\tilde{\mathbb{Z}}^* = \{\tilde{m}; m \in \mathbb{Z}^*\}$ s'identifie à l'ensemble $\{|m|; m \in \mathbb{Z}^*\} = \mathbb{N}^*$.

C. Éléments irréductibles dans un D.I.

Définition 5.16. Un élément r d'un domaine d'intégrité A est dit **irréductible dans A** si :

- i) $r \notin U_A$,
- ii) $r = ab$ dans $A \implies a \in U_A$ ou $b \in U_A$.

Proposition 5.17. Soit A un D.I., alors :

- 1) 0 n'est pas irréductible dans A .
- 2) r est irréductible dans A si et seulement si

$$r \neq 0, r \notin U_A \text{ et } (r = ab \implies r \sim a \text{ ou } r \sim b). \quad (5.3)$$

- 3) Dans A : $(r \text{ irréductible et } r' \sim r) \implies r' \text{ irréductible}$.

Preuve :

- 1) $0 = 00$ et $0 \notin U_A \implies 0$ non irréductible dans A .
- 2) Soit r irréductible dans A ; compte tenu du résultat ci-dessus, on a $r \neq 0, r \notin U_A$ et $(r = ab \text{ dans } A \implies a \in U_A \text{ ou } b \in U_A)$.

La dernière condition exprime que

$$r = ab \text{ dans } A \implies r \sim b \text{ ou } r \sim a.$$

Réciproquement, soit $r \in A$ satisfaisant aux conditions (5.3). Si $r = ab$ dans A et si $r \sim a$, alors il existe $u \in U_A$ tel que $r = au$. L'anneau A étant intègre,

$$(ab = r = au \text{ et } a \neq 0) \implies b = u.$$

Ainsi, $r \sim a \implies b \in U_A$; de même, $r \sim b \implies a \in U_A$.

On en conclut que r est irréductible dans A (Def. 5.16.).

- 3) Dans A , soit r irréductible et $r' \sim r$. Il existe $u \in U_A$ tel que $r = ur'$; r étant irréductible, on a $r \neq 0$ et $r \notin U_A$, d'où

$$r' \sim r \implies r' \neq 0 \text{ et } r' \notin U_A.$$

Supposons $r' = ab$ dans A ; alors $r = ur' = uab$, par suite,

$$r \text{ irréductible} \implies ua \in U_A \text{ ou } b \in U_A,$$

donc $a \in U_A$ ou $b \in U_A$, d'où r' irréductible dans A . $\square$

Remarque 5.18. Pour un élément r , la propriété d'être irréductible dépend du D.I. dans lequel il est considéré ; en particulier, si A et B sont deux D.I. tels que $A \subset B$, alors un élément $r \in A$ peut être irréductible dans A et non irréductible dans B . Par exemple, 2 est irréductible dans $\mathbb{Z}$ et est une unité dans $\mathbb{Q}$.

Proposition 5.19. A étant un D.I., $r \in A$ est irréductible dans A si et seulement si l'idéal (r) est maximal dans l'ensemble des idéaux principaux, propres de A .

Preuve : Soit r un élément irréductible dans A ; alors

$$r \neq 0 \text{ et } r \notin U_A \implies (r) \neq (0) \text{ et } (r) \neq A.$$

Soit (a) un idéal principal propre de A ; supposons : $(r) \subsetneq (a) \subseteq A$.

D'après les propositions 5.10. et 5.14.,

$$(r) \subsetneq (a) \subseteq A \implies a|r \text{ et } a \nmid r;$$

donc il existe $b \in A^* \setminus U_A$ tel que $r = ab$; alors,

$$r \text{ irréductible, } r = ab \text{ et } b \notin U_A \implies a \in U_A,$$

d'où $(a) = A$. On en conclut que (r) est maximal dans l'ensemble des idéaux principaux, propres de A .

Réciproquement, si un idéal $(r) \neq (0)$ est maximal dans l'ensemble des idéaux principaux, propres de A , on a alors $r \neq 0$ et $r \notin U_A$.

Supposons $r = ab$ dans A ; nécessairement a et b sont non nuls et

$$a|r \implies (r) \subseteq (a) \subseteq A.$$

La maximalité de l'idéal principal (r) implique alors,

soit : $(a) = (r)$, donc $r \sim a$ et par suite $b \in U_A$; soit : $(a) = A$, donc $a \in U_A$.

On en conclut que r est irréductible dans A . □

D. Éléments premiers dans un D.I.

Définition 5.20. Un élément p d'un domaine d'intégrité A est dit **premier** dans A s'il vérifie les conditions :

i) $p \neq 0$, $p \notin U_A$;

ii) $(p|ab \text{ dans } A) \implies p|a \text{ ou } p|b$, dans A .

Proposition 5.21. Dans un domaine d'intégrité A ,

1) $(p \text{ premier et } p' \sim p) \implies p' \text{ premier}$.

2) $p \text{ premier} \implies p \text{ irréductible}$ (mais en général, la réciproque est fausse).

Preuve :

1) Soit p un élément premier dans A ; alors

$$p' \sim p \text{ dans } A \implies \exists u \in U_A; p' = up.$$

Supposons $p'|ab$ dans A^* ; donc il existe $q \in A^*$ tel que $ab = p'q$.

$$ab = p'q \implies ab = upq \implies u^{-1}ab = pq \implies p|(u^{-1}a)b;$$

$$p \text{ premier} \implies p|u^{-1}a \text{ ou } p|b;$$

$$p|u^{-1}a \implies up|a \implies p'|a;$$

$$p|b \implies (\exists m \in A^*; b = pm = u^{-1}upm = p'u^{-1}m) \implies p'|b,$$

d'où : $p'|ab$ implique $(p'|a \text{ ou } p'|b)$, donc p' est premier dans A .

2) Supposons p premier et $p = ab$ dans A^* ;

$$p = ab \implies p|ab \implies p|a \text{ ou } p|b.$$

Si $p \nmid a$, alors $p|b$; donc il existe $q \in A^*$ tel que $b = pq$.

$$p = ab \implies p = apq = paq \implies 1 = aq$$

car A est intègre et $p \neq 0$, donc $a \in U_A$. □

Donnons un contre-exemple montrant qu'en général, dans un D.I.,

p irréductible $\nRightarrow p$ premier.

Soit $A := \mathbb{Z}(i\sqrt{5}) := \{a + ib\sqrt{5}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} \subset \mathbb{C}$.

A est un sous-anneau du corps des nombres complexes $\mathbb{C}$, donc est un D.I.

Vérifions que 3 est irréductible, mais non premier dans A .

Supposons que l'on ait $3 = xy$ dans A ; on en déduit que $9 = |x|^2 |y|^2$.

Si x s'écrit $a + ib\sqrt{5}$ dans A , alors $|x|^2 = a^2 + 5b^2$, donc $|x|^2 \in \mathbb{N}^*$; de même, on a $|y|^2 \in \mathbb{N}^*$, par suite

$$9 = |x|^2 |y|^2 \implies |x|^2 = 1 \text{ ou } |x|^2 = 3 \text{ ou } |x|^2 = 9.$$

$$|x|^2 = 1 \implies (a = 1 \text{ et } b = 0) \implies x \in U_A;$$

$$|x|^2 = 3 \text{ est impossible};$$

$$|x|^2 = 9 \implies |y|^2 = 1 \implies y \in U_A;$$

ainsi, $3 = xy$ dans A implique $x \in U_A$ ou $y \in U_A$, donc 3 est irréductible dans $A = \mathbb{Z}(i\sqrt{5})$.

Montrons que 3 n'est pas premier dans A ; en effet,

$$(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9 \implies 3 \mid (2 + i\sqrt{5})(2 - i\sqrt{5}) \text{ dans } A;$$

cependant, $3 \nmid (2 + i\sqrt{5})$ et $3 \nmid (2 - i\sqrt{5})$ dans A .

Proposition 5.22. Pour un élément p d'un domaine d'intégrité A , on a

1) p premier $\iff (p)$ idéal premier non nul de A .

2) p premier $\iff (p) \neq (0)$ et $A/(p)$ intègre.

Preuve :

1) Soit p un élément premier dans A ; $p \neq 0$ implique $(p) \neq (0)$.

Supposons a, b non nuls dans A tels que $ab \in (p)$, donc $p \mid ab$ dans A ; alors p premier implique : $p \mid a$ ou $p \mid b$, c'est-à-dire, $a \in (p)$ ou $b \in (p)$, ce qui prouve que l'idéal (p) est premier, non nul dans A (Prop. 2.49., Déf. 2.50.).

Supposons (p) idéal premier non nul dans A ; alors pour a et b dans A^* :

$$ab \in (p) \implies a \in (p) \text{ ou } b \in (p);$$

$$\text{autrement dit : } p \mid ab \implies p \mid a \text{ ou } p \mid b,$$

donc p est un élément premier dans A .

2) D'après le théorème 2.52., dans un anneau unitaire, commutatif A , un idéal I est premier si et seulement si l'anneau quotient A/I est intègre et dans ce cas c'est un D.I. ; on en déduit, compte tenu du résultat 1) ci-dessus, qu'un élément p d'un domaine d'intégrité A est premier si et seulement si $(p) \neq (0)$ et $A/(p)$ est intègre. $\square$

Théorème 5.23. Dans un domaine principal (Déf. 2.7.), tout élément irréductible est premier.

Preuve : On sait que dans un D.I., A , tout élément premier est irréductible (Prop. 5.21.), de plus, si r est irréductible, alors l'idéal (r) est maximal dans l'ensemble des idéaux principaux, propres de A (Prop. 5.11.).

On en déduit que si r est irréductible dans un domaine principal A , alors (r) est un idéal maximal donc premier dans A (Cor 2.64.) ; par suite, r est un élément premier dans A (Prop. 5.22.). $\square$

Remarque 5.24. : Nous avons utilisé la notation abrégée D.I. pour désigner un domaine d'intégrité, de même nous désignerons couramment par D.P. un domaine principal.

Exemple 5.25. :

1) On sait que l'anneau des entiers $\mathbb{Z}$ est un D.P. et que les idéaux premiers, non nuls de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$, pour lesquels p est un nombre premier (Exemple 2.54., Déf. A.5.).

Par suite (Th. 5.23.), les éléments irréductibles de $\mathbb{Z}$ sont les éléments $\pm p$, où p est un nombre premier.

2) Lorsque K est un corps, l'anneau de polynômes $K[X]$ est un D.P. (Th. 4.36.). Montrons que, dans $K[X]$, les polynômes du premier degré sont des éléments irréductibles (donc premiers); mais nous verrons plus loin, que ce ne sont pas nécessairement les seuls.

Soit $aX + b$ un polynôme du premier degré dans $K[X]$, alors

$$aX + b = f(X)g(X) \text{ dans } K[X] \implies \deg f = 0 \text{ ou } \deg g = 0,$$

donc $f \in K^*$ ou $g \in K^*$; or $K^* = U_K$, d'où $aX + b$ irréductible dans $K[X]$.

Proposition 5.26. Soit A un D.I. et m, n dans $\mathbb{N}^*$.

1) Si $p, p_1, p_2, \dots, p_n$, sont $n+1$ éléments premiers dans A , alors

$$p | p_1 p_2 \cdots p_n \implies \exists i (1 \leq i \leq n), \quad p \sim p_i.$$

2) Si $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ sont des éléments premiers dans A :

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \implies m = n \text{ et } \exists \sigma \in S_n \mid \forall i (1 \leq i \leq n), p_i \sim q_{\sigma(i)}.$$

S_n désigne le groupe des permutations de $\{1, 2, \dots, n\}$.

Preuve :

1) $p | p_1 p_2 \cdots p_n$ entraîne $p_1 p_2 \cdots p_n \in (p)$; or p étant un élément premier, (p) est un idéal premier de A . Par suite (Prop. 2.55.), il existe $i (1 \leq i \leq n)$ tel que $p_i \in (p)$, donc $p | p_i$.

Supposons $p_i = ap$, avec $a \in A^*$; comme p_i est irréductible dans A et $p \notin U_A$, on a nécessairement $a \in U_A$, d'où $p \sim p_i$.

2) Par hypothèse $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, les $p_i, 1 \leq i \leq n$, et les $q_j, 1 \leq j \leq m$, étant premiers dans A .

Supposons $m \neq n$ et par exemple, $n > m$; alors p_1 étant premier dans A ,

$$p_1 | q_1 q_2 \cdots q_m \implies \exists j_1 (1 \leq j_1 \leq m), \quad p_1 \sim q_{j_1}.$$

Par suite il existe $u_1 \in U_A$ tel que $q_{j_1} = p_1 u_1$ et A étant intègre :

$$p_1 p_2 \cdots p_n = p_1 u_1 (\prod_{1 \leq j \leq m, j \neq j_1} q_j) \implies p_2 \cdots p_n = u_1 (\prod_{1 \leq j \leq m, j \neq j_1} q_j).$$

En répétant le raisonnement pour $i = 2, \dots, m$, on obtient que pour tout $i (1 \leq i \leq m)$, il existe $j_i \in \{1, 2, \dots, m\}$ et $u_i \in U_A$ tels que $q_{j_i} = u_i p_i$. On en déduit :

$$p_{m+1} p_{m+2} \cdots p_n = u_1 u_2 \cdots u_m \in U_A,$$

ce qui implique p_i inversible pour tout $i (m+1 \leq i \leq n)$, d'où une contradiction, puisque tout p_i est premier, par hypothèse. On en conclut que $m = n$ et l'application $i \mapsto j_i$ définit une permutation σ de $\{1, 2, \dots, n\}$ telle que pour tout $i (1 \leq i \leq n)$, $p_i \sim q_{\sigma(i)}$. $\square$

3. Notion de p.g.c.d. dans un D.I.

La notion de p.g.c.d. (plus grand commun diviseur) a été définie dans l'anneau des entiers $\mathbb{Z}$ (Cf. App. A), nous l'étendons ici à un D.I. quelconque.

Dans tout ce qui suit, A désigne un D.I.

A. p.g.c.d. de n éléments non nuls dans $A, n \geq 2$

Définition 5.27. Etant donné n éléments non nuls $a_1, a_2, \dots, a_n$ dans A , on appelle p.g.c.d. des $a_i, 1 \leq i \leq n$, tout élément $d \in A^* = A \setminus \{0\}$ tel que

i) $\forall i (1 \leq i \leq n), d | a_i$;

ii) Pour $c \in A^* : (\forall i (1 \leq i \leq n), c | a_i) \implies c | d$.

Remarque 5.28. Les propriétés qui suivent vont permettre de préciser et de justifier cette notion de *plus grand commun diviseur* et d'évoquer la question de l'existence des p.g.c.d. dans un D.I.

Proposition 5.29. Soit $a_1, a_2, \dots, a_n$ dans A^* .

Si d un p.g.c.d. des a_i , $1 \leq i \leq n$, alors $d' \in A^*$ en est un autre si et seulement si d' est associé à d dans A (Déf. 5.11.).

Preuve : Par hypothèse, d est p.g.c.d. des a_i , $1 \leq i \leq n$.

Supposons $d' \sim d$ dans A^* ; donc il existe $u \in U_A$ tel que $d = d'u$. La condition i) de la définition 5.27. implique que pour tout i ($1 \leq i \leq n$), il existe $a'_i \in A^*$ tel que $a_i = da'_i$; alors

$$\forall i (1 \leq i \leq n), a_i = d'ua'_i \implies d'|a_i.$$

D'autre part, si $c \in A^*$ et si quel que soit i ($1 \leq i \leq n$), c divise a_i , alors c divise d , donc il existe $c' \in A^*$ tel que $d = cc'$ et

$$(cc' = d'u, u \in U_A) \implies d' = cc'u^{-1} \implies c|d'.$$

Par suite d' est p.g.c.d. des a_i , $1 \leq i \leq n$.

Réciproquement, supposons que d' soit un p.g.c.d. des a_i , $1 \leq i \leq n$.

La condition ii) de la définition 5.27. appliquée à d et d' donne :

$d|d'$ et $d'|d$ donc $d' \sim d$. □

Remarque 5.30. :

a) La proposition 5.29. montre que si n éléments non nuls d'un D.I. ont un p.g.c.d., d , celui-ci est défini à une unité multiplicative près. En conséquence, d' est aussi un p.g.c.d. de ces éléments si et seulement si $(d') = (d)$.

Par ailleurs, la définition 5.27. implique que l'idéal (d) est indépendant de l'ordre dans lequel on considère les éléments a_i , $1 \leq i \leq n$.

b) Nous supposons l'entier $n \geq 2$, mais dans le cas particulier d'un seul élément $a \in A^*$, on conviendra que a est un p.g.c.d. de a .

c) **Notation :** Un p.g.c.d. de n éléments $a_1, a_2, \dots, a_n$ sera noté symboliquement

$$a_1 \wedge a_2 \wedge \dots \wedge a_n.$$

Plus précisément, cette notation désignera un représentant de la classe d'équivalence des p.g.c.d. des a_i , $1 \leq i \leq n$, modulo la relation d'association dans A .

Proposition 5.31. : Propriété d'associativité des p.g.c.d.

Soit A un D.I. dans lequel on suppose que quel que soit $n \geq 2$, n éléments non nuls quelconques ont un p.g.c.d.; alors pour a_1, a_2, a_3 dans A^* , on a

$$1) a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge a_3 = a_1 \wedge (a_2 \wedge a_3).$$

$$2) a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge (a_2 \wedge a_3).$$

Preuve :

$$1) \text{ Posons } d = a_1 \wedge a_2 \wedge a_3, \delta = a_1 \wedge a_2 \text{ et } d' = (a_1 \wedge a_2) \wedge a_3 = \delta \wedge a_3.$$

En utilisant les conditions i) et ii) de la définition 5.27, on obtient

$$d|a_1 \text{ et } d|a_2 \implies d|\delta$$

$$d|\delta \text{ et } d|a_3 \implies d|d'.$$

$$(d'|\delta \text{ et } \delta|a_i, i = 1, 2) \implies d'|a_1 \text{ et } d'|a_2.$$

Or $d'|a_3$, par suite, $d'|d$. On en conclut que d' est un p.g.c.d. des a_i , $1 \leq i \leq 3$, d'où

$$a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge a_3.$$

On démontre de même la relation $a_1 \wedge a_2 \wedge a_3 = a_1 \wedge (a_2 \wedge a_3)$.

2) Considérons $d = a_1 \wedge a_2 \wedge a_3$, $\delta = a_1 \wedge a_2$, $\delta' = a_2 \wedge a_3$ et montrons que $d \sim \delta \wedge \delta'$. Posons $\Delta = \delta \wedge \delta'$; alors :

$$\begin{aligned}\Delta|\delta \text{ et } \delta|a_1 &\implies \Delta|a_1, \\ \Delta|\delta' \text{ et } \delta'|a_2 &\implies \Delta|a_2, \\ \Delta|\delta' \text{ et } \delta'|a_3 &\implies \Delta|a_3.\end{aligned}$$

par suite $\Delta|d$. D'autre part, d'après les relations 1) de l'énoncé,

$$d = \delta \wedge a_3 = a_1 \wedge \delta' \implies d|\delta \text{ et } d|\delta' \implies d|\Delta.$$

On en résulte que Δ est un p.g.c.d. des a_i , $1 \leq i \leq 3$. □

Corollaire 5.32. *Quel que soit $n \geq 2$ dans $\mathbb{N}$, n éléments non nuls quelconques d'un domaine d'intégrité A ont un p.g.c.d. dans A si et seulement si deux éléments non nuls quelconques en ont un.*

Ce résultat se déduit de la Prop. 5.31., par récurrence sur n .

Remarque 5.33. Compte tenu du corollaire précédent, nous conviendrons de dire que : **les p.g.c.d. existent dans un domaine d'intégrité A** , si deux éléments non nuls quelconques de A ont un p.g.c.d.

Exemple 5.34. Les p.g.c.d. existent dans $\mathbb{Z}$ (Cf. App. A).

Proposition 5.35. *On suppose que A est un D.I. dans lequel les p.g.c.d. existent ; alors, pour des éléments $a_1, a_2, \dots, a_n$ non nuls dans A , $n \geq 2$, les trois conditions suivantes sont équivalentes :*

- 1) $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$.
- 2) Dans l'ensemble $\tilde{A}^*$ des classes d'équivalence de A^* modulo la relation d'association, partiellement ordonné par la relation de divisibilité (Prop. 5.14.), on a $\tilde{d} = \sup\{\tilde{c} \in \tilde{A} \text{ tels que } \forall i (1 \leq i \leq n), \tilde{c}|\tilde{a}_i\}$.
- 3) (d) est le plus petit idéal principal de A contenant les a_i , $1 \leq i \leq n$.

Preuve : Démontrons la propriété pour $n = 2$. Soit a, b non nuls dans A .

1) $\iff$ 2) : $d = a \wedge b$, alors

$$\begin{aligned}(d|a \text{ et } d|b) \text{ dans } A &\iff (\tilde{d}|\tilde{a} \text{ et } \tilde{d}|\tilde{b}) \text{ dans } \tilde{A}; \\ (c|a \text{ et } c|b \implies c|d) \text{ dans } A &\iff (\tilde{c}|\tilde{a} \text{ et } \tilde{c}|\tilde{b} \implies \tilde{c}|\tilde{d}) \text{ dans } \tilde{A}^*.\end{aligned}$$

On en déduit le résultat énoncé :

$$d = a \wedge b \iff \tilde{d} = \sup\{\tilde{c} \in \tilde{A} \text{ tels que } \tilde{c}|\tilde{a} \text{ et } \tilde{c}|\tilde{b}\}.$$

1) $\iff$ 3) : $d = a \wedge b$, alors

$$\begin{aligned}d|a \text{ et } d|b &\iff a \in (d) \text{ et } b \in (d); \\ (c|a \text{ et } c|b \implies c|d) &\iff (a \in (c) \text{ et } b \in (c) \implies d \in (c)),\end{aligned}$$

donc $(d) \subseteq (c)$.

On en conclut que (d) est le plus petit idéal principal de A contenant a et b . □

Corollaire 5.36. Les hypothèses étant celles de la proposition 5.35., d est p.g.c.d. des a_i , ($1 \leq i \leq n$) si et seulement si (d) est le plus petit idéal principal contenant l'idéal $\sum_{1 \leq i \leq n} (a_i)$.

Preuve : $\sum_{1 \leq i \leq n} (a_i)$ étant l'idéal de A engendré par les a_i , $1 \leq i \leq n$, (Prop. 2.13.), le corollaire 5.36. résulte de l'équivalence des conditions 1) et 3) de la Prop. 5.35. $\square$

Remarque 5.37. :

a) Le 2) de la proposition 5.35. justifie l'appellation plus grand commun diviseur et généralise ce qui a été vu dans le cas de l'anneau $\mathbb{Z}$ (App. A).

b) On sait que dans un ensemble partiellement ordonné, une partie non vide n'a pas nécessairement une borne supérieure, donc a priori, dans un D.I. quelconque, deux éléments non nuls n'ont pas toujours un p.g.c.d..

L'existence des p.g.c.d. dans $\mathbb{Z}$ n'est qu'un cas particulier du résultat plus général suivant.

Proposition 5.38. Dans tout domaine principal A , deux éléments a, b non nuls, quelconques ont un p.g.c.d. et

$$d = a \wedge b \iff (d) = (a) + (b) \quad (5.4)$$

$$d = a \wedge b \implies \exists (u, v) \in A \times A, \quad d = au + bv. \quad (5.5)$$

Preuve : Soit A un D.P. ; étant donné a, b dans A^* , il existe $d \in A^*$ tel que $(a) + (b) = (d)$ et cette relation équivaut à $d = a \wedge b$, d'après le corollaire 5.36.

D'autre part, la relation (5.4) implique (5.5) de façon immédiate. $\square$

Exemple 5.39. Si K est un corps, l'anneau $K[X]$ des polynômes à une indéterminée sur K est un D.P. (Th. 4.36.), donc les p.g.c.d. existent dans $K[X]$.

Remarque 5.40. Nous verrons plus loin, qu'il existe des D.I. qui ne sont pas principaux et dans lesquels les p.g.c.d. existent.

B. Éléments premiers entre eux dans un D.I.

Définition 5.41. Soit A un domaine d'intégrité.

a) Deux éléments non nuls de A sont dits **premiers entre eux** si leurs seuls diviseurs communs sont les unités de A .

b) n éléments non nuls de A ($n > 2$) sont dits **premiers entre eux dans leur ensemble** si leurs seuls diviseurs communs sont les unités de A .

Remarque 5.42. Comme ci-dessus, A désigne un D.I.

a) D'après la définition 5.41., pour deux éléments non nuls a, b de A les conditions suivantes sont équivalentes :

$$i) a \text{ et } b \text{ sont premiers entre eux dans } A. \quad (5.6)$$

$$ii) \forall c \in A^*, (c|a \text{ et } c|b) \implies c \in U_A. \quad (5.7)$$

$$iii) \forall c \in A^*, (c|a \text{ et } c|b) \implies c|1. \quad (5.8)$$

$$iv) a \wedge b = 1. \quad (5.9)$$

De même, pour $n \geq 2$, $a_1, a_2, \dots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$.

On notera cependant, que la notion d'éléments premiers entre eux (Déf. 5.41.) est indépendante de la notion de *p.g.c.d.*.

D'autre part, si n éléments d'un D.I. sont premiers entre eux dans leur ensemble ($n > 2$), ils ne sont pas nécessairement premiers entre eux deux à deux.

Par exemple, dans $\mathbb{Z}$, on a $28 \wedge 20 \wedge 35 = 1$, cependant,

$$28 \wedge 20 = 4, \quad 20 \wedge 35 = 5, \quad 28 \wedge 35 = 7.$$

b) Dans tout domaine d'intégrité A , on a

$$\begin{aligned} (a \in U_A \text{ ou } b \in U_A) &\implies a \wedge b = 1. \\ (\forall b \in A^*, a \wedge b = 1) &\implies a \in U_A. \end{aligned}$$

Proposition 5.43. Soit A un D.I. dans lequel les *p.g.c.d.* existent; alors, quels que soient l'entier $n \geq 2$ et les éléments $a_1, a_2, \dots, a_n$ dans A^* , on a $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$ si et seulement s'il existe des éléments $a'_i \in A^*$ tels que

$$\forall i (1 \leq i \leq n), a_i = da'_i \quad \text{et} \quad a'_1 \wedge a'_2 \wedge \dots \wedge a'_n = 1. \quad (5.10)$$

Preuve : Démontrons la propriété pour $n = 2$; on en déduira le résultat pour $n > 2$, par récurrence sur n , grâce à la Prop. 5.31.

Supposons $d = a \wedge b$ dans A^* , alors

$$d|a \text{ et } d|b \implies \exists a', b' \text{ dans } A^*, \quad a = da', b = db'.$$

Soit $c \in A^*$ tel que $c|a'$ et $c|b'$. On peut donc écrire

$$a' = ca'' \text{ et } b' = cb'', \text{ où } (a'', b'') \in A^* \times A^*.$$

On en déduit : $a = dca''$ et $b = dcb''$; d'où $dc|d$, car $d = a \wedge b$.

Soit $c' \in A^*$ tel que $d = dcc'$; l'anneau A étant intègre :

$$(d(1 - cc')) = 0 \quad \text{et} \quad d \neq 0 \implies 1 = cc';$$

donc $c \in U_A$ et par suite, $a' \wedge b' = 1$.

Réciproquement, supposons a, b, d, a', b' dans A^* tels que

$$a = da', b = db' \quad \text{et} \quad a' \wedge b' = 1.$$

Par hypothèse, a et b ont un *p.g.c.d.* ; posons $\delta = a \wedge b$.

$$(d|a \text{ et } d|b) \implies d|\delta,$$

donc il existe $c \in A^*$ tel que $\delta = dc$.

D'après la première partie de la démonstration, on peut écrire :

$$a = dca'', \quad b = dcb'', \quad \text{avec} \quad a'' \wedge b'' = 1.$$

Or on a $a = da'$ et $b = db'$; on en déduit que $a' = ca''$ et $b' = cb''$, car A est intègre. Par suite

$$a' \wedge b' = 1 \implies c \in U_A,$$

donc $d \sim \delta$; il en résulte que d est un *p.g.c.d.* de a et b . □

Corollaire 5.44. Soit A un D.I. dans lequel les *p.g.c.d.* existent; alors, étant donné un entier $n \geq 2$, et des éléments $a_1, a_2, \dots, a_n$ dans A^* tels que $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$, pour tout $c \in A^*$, on a

$$1) \quad cd = ca_1 \wedge ca_2 \wedge \dots \wedge ca_n.$$

$$2) \quad (a_i = cb_i, \forall i (1 \leq i \leq n)) \implies d = c\delta, \quad \text{où} \quad \delta = b_1 \wedge b_2 \wedge \dots \wedge b_n.$$

Preuve : Comme pour la proposition précédente, il suffit de considérer le cas $n = 2$. Par hypothèse, $d = a_1 \wedge a_2$, donc il existe a'_1, a'_2 non nuls dans A tels que

$$a_1 = da'_1, \quad a_2 = da'_2 \quad \text{et} \quad a'_1 \wedge a'_2 = 1.$$

1) Pour tout $c \in A^*$ on a donc $ca_1 = cda'_1$, $ca_2 = cda'_2$ et la condition : $a'_1 \wedge a'_2 = 1$ implique alors $cd = ca_1 \wedge ca_2$, d'après la Prop. 5.43.

2) $c|a_1$ et $c|a_2 \implies c|d$; donc il existe $\delta \in A^*$ tel que $d = c\delta$, alors

$$cb_1 = a_1 = da'_1 = c\delta a'_1.$$

L'anneau A est intègre et $c \neq 0$, d'où $b_1 = \delta a'_1$. On a de même $b_2 = \delta a'_2$ et comme plus haut, la condition : $a'_1 \wedge a'_2 = 1$ entraîne $\delta = b_1 \wedge b_2$. $\square$

Théorème 5.45. : Théorème de Gauss

A étant un D.I. dans lequel les p.g.c.d. existent ; quels que soient a, b, c dans A^ , on a*
 $(a|bc \text{ et } a \wedge b = 1) \implies a|c$.

Preuve : D'après le 1) du Cor. 5.44., on a

$$a \wedge b = 1 \implies ac \wedge bc = c;$$

par suite, $(a|ac \text{ et } a|bc)$ implique $a|c$. $\square$

Corollaire 5.46. *Soit A un D.I. dans lequel les p.g.c.d. existent. Pour a et b_i , $1 \leq i \leq n$, dans A^* , $n \geq 2$, on a :*

$$(a \wedge b_i = 1, \forall i (1 \leq i \leq n)) \implies a \wedge b_1 b_2 \dots b_n = 1.$$

Preuve : Dans le cas où $b_1 b_2 \dots b_n \in U_A$, la propriété est immédiate, on suppose donc $b_1 b_2 \dots b_n \notin U_A$ et on pose $d = a \wedge b_1 b_2 \dots b_n$. Pour tout i , $1 \leq i \leq n$, soit $c_i := d \wedge b_i$, alors,

$$c_i|d \text{ et } c_i|b_i \implies c_i|a \text{ et } c_i|b_i.$$

Or, par hypothèse, on a $a \wedge b_i = 1$, par suite $c_i \in U_A$, donc, pour tout i , $1 \leq i \leq n$, $d \wedge b_i = 1$. D'après le Théorème de Gauss :

$$d|b_1 b_2 \dots b_n \text{ et } d \wedge b_1 = 1 \implies d|b_2 b_3 \dots b_n$$

$$d|b_2 b_3 \dots b_n \text{ et } d \wedge b_2 = 1 \implies d|b_3 \dots b_n.$$

De proche en proche on aboutit à $d|b_n$, mais $d \wedge b_n = 1$, donc $d \in U_A$. $\square$

Le résultat suivant donne une nouvelle caractérisation des éléments irréductibles d'un D.I.

Proposition 5.47. *A étant un D.I., soit $r \in A^*$ tel que $r \notin U_A$; alors r est irréductible dans A si et seulement si*

$$\forall a \in A^*, (r \nmid a \implies r \wedge a = 1).$$

Preuve : Soit r irréductible dans A et $a \in A^*$ tel que r ne divise pas a . Supposons $c \in A^*$ tel que $c|r$ et $c|a$.

$$c|r \implies \exists c' \in A^* \text{ tel que } r = cc';$$

mais, r étant irréductible dans A , on a $c \in U_A$ ou $c' \in U_A$.

Si $c \notin U_A$, alors $c' \in U_A$, d'où $r \sim c$, donc $r|a$, ce qui est contraire à l'hypothèse ; on en conclut que nécessairement, $c \in U_A$, d'où $r \wedge a = 1$.

Réciproquement, soit $r \in A^* \setminus U_A$ tel que quel que soit $a \in A^*$, la condition $r \nmid a$ implique $r \wedge a = 1$.

Supposons r non irréductible et tel que $r = ab$ dans A^* , avec $a \notin U_A$ et $b \notin U_A$; alors

$$(a|r \text{ et } b \notin U_A) \implies r \nmid a.$$

L'hypothèse implique alors $r \wedge a = 1$; mais $a|r$, ce qui entraîne que $a \in U_A$, d'où une contradiction ; il en résulte que r est irréductible. $\square$

C. Éléments premiers entre eux dans un D.P.

Théorème 5.48. Théorème de Bezout

A étant un domaine principal, pour a et b non nuls dans A , on a

$$a \wedge b = 1 \iff (a) + (b) = A. \quad (5.11)$$

$$a \wedge b = 1 \iff \exists (u, v) \in A \times A, au + bv = 1 \quad (5.12)$$

Preuve : La relation (5.4) de la proposition 5.38 appliquée au cas $d = 1$ donne la relation (5.11). D'autre part on a $(a) + (b) = A$ si et seulement si 1 appartient à l'idéal $(a) + (b)$, d'où la relation (5.12). $\square$

Corollaire 5.49. Généralisation du théorème de Bezout

Pour n éléments non nuls $a_1, a_2, \dots, a_n$ d'un domaine principal $A, n \geq 2$, les conditions suivantes sont équivalentes :

i) $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$;

ii) $\sum_{1 \leq i \leq n} (a_i) = A$;

iii) Il existe $u_i \in A, 1 \leq i \leq n$, tels que $\sum_{1 \leq i \leq n} u_i a_i = 1$.

Vérification laissée au lecteur.

Remarque 5.50. :

a) La relation (5.11) exprime que les idéaux (a) et (b) sont copremiers.

b) La relation (5.12) est généralement appelée **Relation de Bezout** ; elle s'applique, en particulier, dans les domaines principaux $\mathbb{Z}$ (Cf. App.A) et $K[X]$, où K est un corps.

c) Le théorème de Bezout est valable dans tout D.I. dans lequel tout idéal de type fini est principal. (Voir Exercices à la fin du chapitre).

4. Notion de p.p.c.m. dans un D.I.

La notion de *p.p.c.m.* (**plus petit commun multiple**), déjà définie dans l'anneau $\mathbb{Z}$ (Cf. App. A), est étendue ici, au cas d'un D.I. quelconque.

Comme dans le paragraphe précédent, A désigne un D.I.

Définition 5.51. On appelle **p.p.c.m.** de n éléments non nuls $a_1, a_2, \dots, a_n$ de $A, n \geq 2$, tout $m \in A^*$ tel que

i) $\forall i (1 \leq i \leq n), a_i | m$.

ii) Pour $l \in A^* : (\forall i (1 \leq i \leq n), a_i | l) \implies m | l$.

Proposition 5.52. Soit $a_1, a_2, \dots, a_n$ dans $A^*, n \geq 2$.

Si m est un p.p.c.m. des $a_i, 1 \leq i \leq n$, alors $m' \in A^*$ en est un autre si et seulement si m' est associé à m dans A (Déf. 5.11.).

Preuve : Par hypothèse m est un p.p.c.m. des $a_i, 1 \leq i \leq n$.

Supposons $m' \sim m$ dans A ; il existe alors $u \in U_A$ tel que $m = m'u$. D'après la condition i) de la Déf. 5.51., pour tout $i (1 \leq i \leq n)$, il existe $a'_i \in A^*$ tel que $m'u = a_i a'_i$ donc $a_i | m'$.

D'autre part, la condition ii) de la Déf. 5.51 implique que si $l \in A^*$ et si quelque soit $i (1 \leq i \leq n)$ on a $a_i | l$, alors $m | l$, donc il existe $l' \in A^*$ tel que $l = ml'$; par suite

$$l = m'u l' \implies m' | l.$$

On en conclut que m' est un p.p.c.m. des $a_i, 1 \leq i \leq n$.

Réciproquement, si m et m' sont des p.p.c.m. des $a_i, 1 \leq i \leq n$, alors la condition ii) de la Déf. 5.51., appliquée à m et à m' , donne $m' | m$ et $m | m'$, d'où $m' \sim m$. $\square$

Remarque 5.53. :

a) Si dans un domaine d'intégrité A , des éléments non nuls $a_1, a_2, \dots, a_n$, ont un p.p.c.m., alors d'après la définition 5.51., celui-ci est indépendant de l'ordre dans lequel on considère les a_i et la proposition 5.52. montre qu'il est unique à une unité multiplicative près de A .

Notation : Un p.p.c.m. de $a_1, a_2, \dots, a_n$ dans A sera noté symboliquement

$$a_1 \vee a_2 \vee \dots \vee a_n.$$

Cette notation désigne un représentant de la classe d'équivalence d'un p.p.c.m. des a_i , modulo la relation d'association dans A .

b) Dans le cas particulier d'un seul élément $a \in A^*$, on conviendra que tout ua , où $u \in U_A$, est p.p.c.m. de a .

Proposition 5.54. : Propriété d'associativité des p.p.c.m.

Soit A un D.I. dans lequel on suppose que, quel que soit l'entier $n \geq 2$, n éléments non nuls quelconques ont un p.p.c.m.; alors pour a_1, a_2, a_3 dans A^* , on a

$$1) a_1 \vee a_2 \vee a_3 = (a_1 \vee a_2) \vee a_3 = a_1 \vee (a_2 \vee a_3). \quad (5.13)$$

$$2) a_1 \vee a_2 \vee a_3 = (a_1 \vee a_2) \vee (a_2 \vee a_3). \quad (5.14)$$

Preuve :

1) Posons $m = a_1 \vee a_2 \vee a_3$, $\mu = a_1 \vee a_2$ et $m' = \mu \vee a_3$.

En appliquant les conditions i) et ii) de la Déf. 5.51., on obtient :

$$(a_1|m, \text{ et } a_2|m) \implies \mu|m; \quad (\mu|m, \text{ et } a_3|m) \implies m'|m.$$

$$(\text{pour } i = 1, 2, a_i|\mu \text{ et } \mu|m') \implies (a_i|m', \text{ pour } i = 1, 2),$$

donc pour $i = 1, 2, 3$, $a_i|m'$ et par conséquent, $m|m'$.

On en déduit que m' est associé à m , d'où $m' = a_1 \vee a_2 \vee a_3$.

On prouve de même la relation : $a_1 \vee a_2 \vee a_3 = a_1 \vee (a_2 \vee a_3)$.

2) Soit $m = a_1 \vee a_2 \vee a_3$, $\mu = a_1 \vee a_2$, $\mu' = a_2 \vee a_3$; démontrons que m est associé à $\mu \vee \mu'$. Posons $M = \mu \vee \mu'$; alors

$$a_1|\mu \text{ et } \mu|M \implies a_1|M$$

$$a_2|\mu' \text{ et } \mu'|M \implies a_2|M$$

$$a_3|\mu' \text{ et } \mu'|M \implies a_3|M;$$

par suite $m|M$.

D'autre part, d'après la première partie de la démonstration :

$$(m = \mu \vee a_3 = a_1 \vee \mu') \implies \mu|m \text{ et } \mu'|m,$$

d'où $M|m$. On en conclut que $M \sim m$, donc $M = a_1 \vee a_2 \vee a_3$ □

Comme pour les p.g.c.d. (Cor. 5.32.) la proposition 5.54. a pour conséquence directe le résultat suivant.

Corollaire 5.55. Quel que soit $n \geq 2$ dans $\mathbb{N}$, n éléments non nuls quelconques d'un domaine d'intégrité A ont un p.p.c.m. si et seulement si deux éléments non nuls quelconques en ont un.

Remarque 5.56. Nous conviendrons de dire que les p.p.c.m. existent dans un domaine d'intégrité A si et seulement si deux éléments non nuls quelconques de A ont un p.p.c.m..

Exemple 5.57. Les p.p.c.m. existent dans $\mathbb{Z}$ (Cf. App. A).

Proposition 5.58. On suppose que A est un D.I. dans lequel les p.p.c.m. existent ; alors pour n éléments non nuls de A , $n \geq 2$, les conditions suivantes sont équivalentes :

$$1) m = a_1 \vee a_2 \vee \cdots \vee a_n.$$

2) Dans l'ensemble $\tilde{A}$ des classes d'équivalence de A modulo l'association, partiellement ordonné par la relation de divisibilité (Prop. 5.14.), on a

$$\tilde{m} = \inf \{ \tilde{l} \in \tilde{A} \text{ tel que } \forall i (1 \leq i \leq n), \tilde{a}_i | \tilde{l} \}.$$

$$3) (m) = (a_1) \cap (a_2) \cap \cdots \cap (a_n).$$

Preuve : Démontrons la propriété pour $n = 2$, le résultat, pour $n > 2$, s'en déduira par récurrence sur n , grâce à la proposition 5.54. Soit $m = a_1 \vee a_2$.

1) $\iff$ 2) En effet,

$$(a_1 | m \text{ et } a_2 | m) \text{ dans } A \iff (\tilde{a}_1 | \tilde{m} \text{ et } \tilde{a}_2 | \tilde{m}) \text{ dans } \tilde{A};$$

$$(a_1 | l \text{ et } a_2 | l \implies m | l) \text{ dans } A \iff (\tilde{a}_1 | \tilde{l} \text{ et } \tilde{a}_2 | \tilde{l}) \implies \tilde{m} | \tilde{l} \text{ dans } \tilde{A}.$$

La divisibilité étant une relation d'ordre dans $\tilde{A}$, les relations ci-dessus impliquent

$$m = a_1 \vee a_2 \iff \tilde{m} = \inf \{ \tilde{l} \in \tilde{A} ; \tilde{a}_1 | \tilde{l} \text{ et } \tilde{a}_2 | \tilde{l} \},$$

d'où la propriété énoncée.

1) $\iff$ 3) :

$$(a_1 | m \text{ et } a_2 | m) \implies (m) \subseteq (a_1) \cap (a_2).$$

$$l \in (a_1) \cap (a_2) \iff a_1 | l \text{ et } a_2 | l;$$

$$(a_1 | l \text{ et } a_2 | l \implies m | l) \iff (a_1) \cap (a_2) \subseteq (m),$$

d'où le résultat. □

La Prop. 5.58. justifie l'appellation *plus petit commun multiple* et comme dans le cas des p.g.c.d. (Prop. 5.35.), la propriété 2) entraîne que les p.p.c.m. n'existent pas nécessairement dans tout D.I. ; cependant, la propriété 3) implique le résultat suivant :

Corollaire 5.59. A étant un D.I., deux éléments quelconques de A^* ont un p.p.c.m. si et seulement si l'intersection de deux idéaux principaux de A est un idéal principal. En particulier, les p.p.c.m. existent dans tout D.P.

Exemple 5.60. Les p.p.c.m. existent dans $\mathbb{Z}$ (résultat déjà rappelé) et dans $K[X]$, si K est un corps.

Remarque 5.61. Nous rencontrerons plus loin des D.I. non principaux dans lesquels, cependant, les p.p.c.m. existent.

Proposition 5.62. Soit A un D.I. dans lequel les p.p.c.m. existent, alors quels que soient l'entier $n \geq 2$ et les éléments $a_i \in A^*$, $1 \leq i \leq n$, on a

$m = a_1 \vee a_2 \vee \cdots \vee a_n$ si et seulement si il existe des éléments $a'_i \in A^*$ tels que

$$(\forall i (1 \leq i \leq n), m = a_i a'_i) \quad \text{et} \quad a'_1 \wedge a'_2 \wedge \cdots \wedge a'_n = 1. \quad (5.15)$$

Preuve : Démontrons la propriété pour $n = 2$, elle pourra être généralisée au cas $n > 2$, à l'aide de la Prop. 5.31.

Supposons $m = a_1 \vee a_2$; il existe a'_1, a'_2 dans A^* tels que $m = a_i a'_i$, $i = 1, 2$. Soit $c \in A^*$, un diviseur commun aux a'_i , $i = 1, 2$. Posons $a'_i = b_i c$; alors

$$m = a_1 b_1 c = a_2 b_2 c \implies a_1 b_1 = a_2 b_2,$$

car A est intègre et $c \neq 0$. En conséquence :

$(a_1 | a_1 b_1 \text{ et } a_2 | a_1 b_1) \implies m | a_1 b_1$. Or, $m = a_1 b_1 c$ implique $a_1 b_1 | m$. On en déduit que m est associé à $a_1 b_1$ dans A , donc $c \in U_A$. Par suite, a'_1 et a'_2 sont premiers entre eux.

Réciproquement, supposons dans A^* :

$$m = a_1 a'_1 = a_2 a'_2, \text{ avec } a'_1 \wedge a'_2 = 1.$$

Par hypothèse, a_1 et a_2 ont un p.p.c.m. dans A^* ; soit $\mu = a_1 \vee a_2$. Posons $\mu = a_1 x_1 = a_2 x_2$ dans A^* .

$$(a_1 | \mu \text{ et } a_2 | \mu) \implies \mu | m,$$

donc il existe $c \in A^*$ tel que $m = \mu c$, d'où, pour $i = 1, 2$,

$$m = a_i a'_i = a_i x_i c \implies a'_i = x_i c,$$

puisque A est intègre. Ainsi c est un diviseur commun à a'_1 et a'_2 donc par hypothèse, $c \in U_A$, d'où $m \sim \mu$, ce qui entraîne que m est un p.p.c.m. des a_i , $i = 1, 2$. $\square$

Corollaire 5.63. *A étant un D.I. dans lequel les p.p.c.m. existent, soit $a_1, a_2, \dots, a_n$ dans A^* , $n \geq 2$, tels que $m = a_1 \vee a_2 \vee \dots \vee a_n$; alors pour $c \in A^*$, on a*

$$1) cm = ca_1 \vee ca_2 \vee \dots \vee ca_n.$$

$$2) (a_i = cb_i; \forall i, 1 \leq i \leq n, \text{ et } l = b_1 \vee b_2 \vee \dots \vee b_n) \implies cl = m.$$

Preuve :

1) D'après la proposition 5.62., quel que soit i , $1 \leq i \leq n$, on a $m = a_i a'_i$, où les a'_i sont premiers entre eux dans leur ensemble ; on en déduit que pour tout $c \in A^*$, les égalités $cm = ca_i a'_i$, $1 \leq i \leq n$, impliquent

$$cm = ca_1 \vee ca_2 \vee \dots \vee ca_n.$$

2) Compte tenu de la démonstration ci-dessus, les hypothèses impliquent que cl est un p.p.c.m. des cb_i , donc des a_i , pour $1 \leq i \leq n$. $\square$

Proposition 5.64. *Soit A un D.I.*

1) *Si les p.g.c.d. existent dans A et si deux éléments non nuls a, b ont d pour p.g.c.d., alors il existe $m \in A^*$ tel que $m = a \vee b$ et $md = ab$.*

2) *Si les p.p.c.m. existent dans A et si deux éléments non nuls a, b ont m pour p.p.c.m., alors il existe $d \in A^*$ tel que $d = a \wedge b$ et $md = ab$.*

Preuve :

1) On suppose l'existence des p.g.c.d. dans A . Si $d = a \wedge b$, la proposition 5.43. indique qu'il existe a', b' dans A^* tels que

$$a = da', b = db', a' \wedge b' = 1.$$

Posons $m := da'b'$; alors,

$$(m = ab' = ba', \text{ avec } a' \wedge b' = 1) \implies m = a \vee b$$

et la définition de m implique $md = ab$.

2) On suppose l'existence des p.p.c.m. dans A . D'après la proposition 5.62., si $m = a \vee b$, il existe a', b' dans A^* tels que

$$m = aa' = bb', a' \wedge b' = 1.$$

D'autre part, ab étant un multiple commun à a et b , la définition du p.p.c.m. implique $m | ab$. Posons alors $ab = md$ et montrons que d est un p.g.c.d. de a et b . L'anneau A est intègre, donc

$$ab = md = aa'd \implies b = a'd$$

$$ba = md = bb'd \implies a = b'd$$

et la condition $a' \wedge b' = 1$ implique $d = a \wedge b$ (Prop. 5.43). $\square$

Remarque 5.65. La proposition 5.64. montre que dans un D.I., les $p.g.c.d.$ existent si et seulement si les $p.p.c.m.$ existent (Rem. 5.33. et 5.56.).

D'autre part, l'application de la proposition 5.64. au cas où $d = 1$ donne le résultat suivant.

Corollaire 5.66. Soit A un D.I. dans lequel les $p.g.c.d.$ (ou $p.p.c.m.$) existent ; alors pour a et b non nuls dans A , on a

$$a \wedge b = 1 \iff a \vee b = ab.$$

La Prop. 5.64. se généralise de la façon suivante :

Proposition 5.67. A étant un D.I. dans lequel les $p.g.c.d.$ existent, soit $a_1, a_2, \dots, a_n$ des éléments de A^* , $n \geq 2$, tels que

$$d = a_1 \wedge a_2 \wedge \dots \wedge a_n \quad \text{et} \quad \forall i (1 \leq i \leq n), a_i = da'_i.$$

Si les a'_i , $1 \leq i \leq n$, sont deux à deux premiers entre eux, alors il existe un $p.p.c.m.$, des a_i , $1 \leq i \leq n$, m , tel que

$$md^{n-1} = a_1 a_2 \dots a_n.$$

Preuve : La propriété a été démontrée pour $n = 2$ (Prop. 5.64.), supposons $n > 2$. Posons $m = da'_1 a'_2 \dots a'_n$ et montrons que m est un $p.p.c.m.$ des a_i , $1 \leq i \leq n$.

Quel que soit i , $1 \leq i \leq n$,

$$a_i = da'_i \implies a_i | m \quad \text{et} \quad m = a_i b_i, \quad \text{où} \quad b_i = a'_1 \dots a'_{i-1} a'_{i+1} \dots a'_n.$$

Démontrons que les b_i , $1 \leq i \leq n$, sont premiers entre eux dans leur ensemble, sachant que les a'_i sont, par hypothèse, deux à deux premiers entre eux.

Pour $n = 3$, $b_1 = a'_2 a'_3$, $b_2 = a'_1 a'_3$, $b_3 = a'_1 a'_2$.

$$\begin{aligned} b_1 \wedge b_2 \wedge b_3 &= (b_1 \wedge b_2) \wedge b_3 \quad (\text{Prop. 5.31.}) \\ &= a'_3 \wedge a'_1 a'_2 = 1 \end{aligned}$$

Pour $n > 3$, en appliquant les mêmes propriétés que ci-dessus, on obtient :

$$\begin{aligned} b_1 \wedge b_2 \wedge \dots \wedge b_n &= (b_1 \wedge b_2 \wedge \dots \wedge b_{n-1}) \wedge b_n \\ &= a'_n \wedge a'_1 a'_2 \dots a'_{n-1} = 1. \end{aligned}$$

On en déduit (Prop. 5.64.) que $m = a_1 \vee a_2 \vee \dots \vee a_n$ et $(\forall i (1 \leq i \leq n), a_i = da'_i \text{ et } m = da'_1 a'_2 \dots a'_n) \implies md^{n-1} = a_1 a_2 \dots a_n.$ □

Corollaire 5.68. Dans un domaine d'intégrité A , où les $p.g.c.d.$ existent, n éléments non nuls $a_1, a_2, \dots, a_n$, $n \geq 2$, sont deux à deux premiers entre eux si et seulement si

$$a_1 \vee a_2 \vee \dots \vee a_n = a_1 a_2 \dots a_n. \quad (5.16)$$

Ce résultat se déduit de la Prop. 5.67. et généralise le Cor. 5.66.

Remarque 5.69. Pour $n > 2$, la relation (5.16) n'est plus vraie, si les a_i sont seulement premiers entre eux dans leur ensemble.

Par exemple 10, 12, 15 sont premiers entre eux dans leur ensemble et leur $p.p.c.m.$ est 60 $\neq 10 \times 12 \times 15$.

5. Anneaux euclidiens

A. Notion d'anneau euclidien

Définition 5.70. On dit qu'un anneau unitaire, commutatif, A est un **anneau euclidien** si $i) A$ est D.I.

$ii)$ Il existe une application $\delta : A^* \rightarrow \mathbb{N}$ vérifiant les conditions :

(AE_1) : Quel que soit $(a, b) \in A^* \times A^*$, $a|b \implies \delta(a) \leq \delta(b)$.

(AE_2) : Quel que soit $(a, b) \in A \times A^*$, il existe $(q, r) \in A \times A$ tel que

$$a = bq + r, \text{ avec } r = 0 \text{ ou } \delta(r) < \delta(b).$$

L'application δ est appelée **stathme** euclidien.

Remarque 5.71. Les notations sont celles de la définition 5.70.

$a)$ A priori $\delta(0)$ n'est pas défini, mais nous verrons sur des exemples, que dans chaque cas particulier d'anneau euclidien, $\delta(0)$ est en général précisé.

$b)$ Le lecteur vérifiera que la condition (AE_1) est équivalente à la condition $(AE_1)'$: Quel que soit $(a, b) \in A^* \times A^*$, $\delta(a) \leq \delta(ab)$.

La condition $(AE_1)'$ peut donc remplacer la condition (AE_1) dans la définition 5.70.

$c)$ On dit que la condition (AE_2) définit une **division euclidienne** dans A .

Les éléments q et r sont appelés, respectivement, le **quotient** et le **reste** de la division euclidienne de a par b .

On notera que la condition (AE_2) n'impose pas l'unicité du couple (q, r) pour a et b donnés ; cependant, dans certains cas particuliers, le stathme qui définit la structure euclidienne entraîne cette unicité (voir les exemples plus loin).

Proposition 5.72. Dans un anneau euclidien A , de stathme δ , on a

$$u \in U_A \iff \delta(u) = \delta(1).$$

Preuve : Soit $u \in U_A$; en utilisant la condition (AE_1) , on obtient :

$$(1|u \text{ et } u|1) \implies \delta(u) = \delta(1).$$

Réciproquement, supposons $u \in A^*$ tel que $\delta(u) = \delta(1)$. La division euclidienne de 1 par u donne

$$1 = uq + r, \quad r = 0 \text{ ou } \delta(r) < \delta(u);$$

$$\text{mais} \quad (r \neq 0 \text{ et } 1|r) \implies \delta(1) = \delta(u) \leq \delta(r),$$

d'où une contradiction ; par suite $r = 0$, donc u est inversible. □

Exemple 5.73. Le domaine d'intégrité $\mathbb{Z}$ est euclidien relativement au stathme

$$\delta : \mathbb{Z}^* \rightarrow \mathbb{N}$$

$$a \mapsto |a|.$$

Cette propriété est une conséquence de la division définie dans $\mathbb{Z}$ (App. A).

En effet, d'après le Th. A.7., pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|.$$

On remarquera que dans cette division, il y a unicité du couple (q, r) , car on impose à r d'être positif ; mais dans la division euclidienne définie par le stathme $\delta : a \mapsto |a|$, il

n'y a pas unicité du couple (q, r) vérifiant la condition AE_2 . Par exemple, pour $a = 12$ et $b = 5$, on obtient :

$$\begin{aligned} 12 &= 5 \times 2 + 2, \text{ donc } q = 2, r = 2, |2| < |5| \\ \text{ou } 12 &= 5 \times 3 - 3, \text{ donc } q = 3, r = -3, |-3| < |5|. \end{aligned}$$

On notera que dans le cas de l'anneau euclidien $\mathbb{Z}$, on a $\delta(0) = 0$.

Exemple 5.74. Si K est un corps, l'anneau des polynômes à une indéterminée, $K[X]$, est euclidien relativement au stathme

$$\begin{aligned} \delta : K[X] \setminus \{0\} &\longrightarrow \mathbb{N} \\ f &\longmapsto \deg f, \end{aligned}$$

comme le prouve la division qui a été définie au chapitre 4 (Th. 4.33.).

On remarquera qu'il y a unicité du quotient et du reste pour la division euclidienne dans $K[X]$ (Th. 4.33.)

Compte tenu de la convention faite pour le degré du polynôme nul, on peut compléter la définition de δ en posant $\delta(0) = -\infty$.

Exemple 5.75. L'anneau des entiers de Gauss, $\mathbb{Z}[i]$, est un anneau euclidien.

Preuve : On rappelle (Exemple 1.31, 4)) que

$$\mathbb{Z}[i] = \{x + iy; (x, y) \in \mathbb{Z} \times \mathbb{Z}\} \text{ où } i^2 = -1 \text{ dans } \mathbb{C}.$$

$\mathbb{Z}[i]$ est un sous-anneau du corps $\mathbb{C}$, c'est donc un D.I. ; montrons que l'application δ définie ci-dessous satisfait aux conditions $(AE_1)'$ et $(AE_2)'$:

$$\begin{aligned} \delta : \mathbb{Z}[i] &\longrightarrow \mathbb{N} \\ x + iy &\longmapsto x^2 + y^2. \end{aligned}$$

Pour $a = x + iy$ dans $\mathbb{Z}[i]$, $\delta(a)$ est le carré du module du nombre complexe a ; d'où

$$(\delta(a) = 0 \iff a = 0), \quad (a \neq 0 \implies \delta(a) > 0)$$

et pour a et b non nuls dans $\mathbb{Z}[i]$,

$$\delta(ab) = \delta(a)\delta(b) \implies \delta(a) | \delta(ab).$$

La condition $(AE_1)'$ est donc vérifiée.

Définition de la division euclidienne dans $\mathbb{Z}[i]$

Soit $a = x + iy$ et $b = u + iv$ dans $\mathbb{Z}[i]$, $b \neq 0$. Dans le corps $\mathbb{C}$, on a

$$\frac{a}{b} = \frac{x + iy}{u + iv} = p_1 + ip_2,$$

où, a priori, p_1 et p_2 sont dans le corps $\mathbb{Q}$.

1^{er} Cas : $(p_1, p_2) \in \mathbb{Z} \times \mathbb{Z}$, donc $\frac{a}{b} \in \mathbb{Z}[i]$; en posant $q = p_1 + ip_2$ et $r = 0$, on obtient $a = bq$.

2^{ème} Cas : $(p_1, p_2) \notin \mathbb{Z} \times \mathbb{Z}$, c'est-à-dire que l'un au moins des p_i , $i = 1, 2$, est dans $\mathbb{Q} \setminus \mathbb{Z}$. Il existe alors q_1 et q_2 dans $\mathbb{Z}$ tels que

$$|p_1 - q_1| \leq \frac{1}{2} \quad \text{et} \quad |p_2 - q_2| \leq \frac{1}{2}.$$

Posons $q = q_1 + iq_2$ dans $\mathbb{Z}[i]$ et considérons $|\frac{a}{b} - q|$.

$$\begin{aligned} |\frac{a}{b} - q| &= |(p_1 + ip_2) - (q_1 + iq_2)| = |(p_1 - q_1) + i(p_2 - q_2)| \\ (|\frac{a}{b} - q|)^2 &= (p_1 - q_1)^2 + (p_2 - q_2)^2 \leq \frac{1}{2}, \end{aligned}$$

par suite, $|\frac{a}{b} - q| < 1$. Posons $a - bq = r$ dans $\mathbb{Z}[i]$. On est dans le cas où $\frac{a}{b} \notin \mathbb{Z}[i]$, donc $r \neq 0$ et

$$|\frac{r}{b}| = |\frac{a}{b} - q| \leq 1 \implies |r| < |b|,$$

donc $\delta(r) < \delta(b)$. Ainsi δ vérifie la condition (AE_2) .

On en conclut que $\mathbb{Z}[i]$ est un anneau euclidien et la démonstration précédente donne le procédé permettant de trouver le quotient et le reste dans une division euclidienne effectuée dans $\mathbb{Z}[i]$. $\square$

Exemple : effectuons la division euclidienne de $a = 4 + 7i$ par $b = 8 - i$, en utilisant les notations de la démonstration.

$$\begin{aligned} \frac{a}{b} &= \frac{4+7i}{8-i} = \frac{5}{13} + i\frac{12}{13} \implies p_1 = \frac{5}{13} \text{ et } p_2 = \frac{12}{13} \\ |\frac{5}{13} - 0| &< \frac{1}{2} \text{ et } |\frac{12}{13} - 1| < \frac{1}{2} \implies q_1 = 0 \text{ et } q_2 = 1, \end{aligned}$$

d'où $q = i$ et $r = a - bq = 4 + 7i - (8 - i)i = 3 - i$.

Théorème 5.76. *Tout anneau euclidien est un domaine principal.*

Preuve : Soit A un anneau euclidien ; A est donc un D.I., pour montrer que c'est un D.P., il suffit de prouver que tout idéal de A est principal. Les idéaux A et (0) étant principaux, considérons un idéal $I \neq A$ et non nul.

Il existe $a \neq 0$ dans I ; δ étant le stathme euclidien de A , posons

$$\Delta = \{\delta(a) ; a \in I \setminus \{0\}\}.$$

Δ est une partie non vide de $\mathbb{N}$; notons $\delta(a_0)$ le plus petit élément de Δ .

D'autre part, pour tout $a \in I$, il existe q et r dans A tels que

$$a = a_0q + r, \quad r = 0 \text{ ou } \delta(r) < \delta(a_0).$$

Or a et a_0 sont dans I , donc $r \in I$; alors $\delta(a_0)$ étant le plus petit élément de Δ , nécessairement, $r = 0$ et par suite, $a = a_0q$. On en déduit que I est l'idéal principal de A engendré par a_0 . $\square$

Remarque 5.77. La réciproque du théorème 5.76. est fausse, comme le montre l'exemple suivant.

Exemple 5.78. : Pour $\alpha = \frac{1+i\sqrt{19}}{2}$, le sous-anneau de $\mathbb{C}$
 $\mathbb{Z}[\alpha] := \{x + y\alpha ; (x, y) \in \mathbb{Z} \times \mathbb{Z}\}$

est un domaine principal, non euclidien.

Preuve : $\mathbb{Z}[\alpha]$ est un sous-anneau unitaire du corps des nombres complexes $\mathbb{C}$ (à vérifier par le lecteur), c'est donc un D.I..

On a $\alpha + \bar{\alpha} = 1$ et $\alpha\bar{\alpha} = 5$, donc α et $\bar{\alpha}$ sont les racines, dans $\mathbb{C}$, du polynôme à coefficients réels $X^2 - X + 5$. De plus $\bar{\alpha} = 1 - \alpha$, implique $\bar{\alpha} \in \mathbb{Z}[\alpha]$.

On considère, d'autre part,

$$\mathbb{Q}[\alpha] := \{u + v\alpha; (u, v) \in \mathbb{Q} \times \mathbb{Q}\}.$$

$\mathbb{Q}[\alpha]$ est le corps des fractions du domaine d'intégrité $\mathbb{Z}[\alpha]$ (Ex. 2, Ch. 5).

Pour la suite de la démonstration, on pose $A := \mathbb{Z}[\alpha]$. Le module d'un nombre complexe $a \in A$ sera noté $|a|$ et comme d'habitude, $A^* = A \setminus \{0\}$.

Le fait que A est principal résultera des deux lemmes suivants.

Lemme 5.79. *Quel que soit $(a, b) \in A^* \times A$, il existe $(q, r) \in A \times A$ tel que*

$$|r| < |a| \quad \text{et} \quad (b = aq + r \text{ ou } 2b = aq + r).$$

On peut dire que ce lemme définit une *pseudo-division* dans $\mathbb{Z}[\alpha]$.

Preuve : Au couple (a, b) , où a est non nul, on associe $\frac{b}{a}$ dans le corps des fractions de A , c'est-à-dire dans $\mathbb{Q}[\alpha]$, donc

$$\frac{b}{a} = \frac{p}{q} + \frac{p'}{q'} \alpha, \quad \text{où } \left(\frac{p}{q}, \frac{p'}{q'}\right) \in \mathbb{Q} \times \mathbb{Q}.$$

Or tout élément de $\mathbb{Q}$ peut s'écrire $m + m'$, avec $m \in \mathbb{Z}$, $m' \in \mathbb{Q}$ tel que $|m'| \leq \frac{1}{2}$; posons

$$\frac{p}{q} = m + m', \quad \frac{p'}{q'} = n + n',$$

avec m, n entiers et m', n' rationnels tels que $|m'| \leq \frac{1}{2}$ et $|n'| \leq \frac{1}{2}$, alors

$$\frac{b}{a} = (m + m') + (n + n')\alpha.$$

1^{er} cas : $|n'| \leq \frac{1}{3}$, alors

$$|m' + n'\alpha|^2 = (m' + n'\alpha)(m' + n'\bar{\alpha}) \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1.$$

En posant $q = m + n\alpha$ et $r = a(m' + n'\alpha)$, on obtient

$$\frac{b}{a} = q + \frac{r}{a} \quad \text{et} \quad \left|\frac{r}{a}\right| = |m' + n'\alpha| < 1,$$

donc $b = aq + r$ et $|r| < |a|$.

2^{ème} cas : $\frac{1}{3} < |n'| \leq \frac{1}{2}$, alors

$$n' < 0 \implies |2n' + 1| < \frac{1}{3}; \quad n' > 0 \implies |2n' - 1| < \frac{1}{3},$$

d'où $|2n' + \varepsilon| < \frac{1}{3}$, où $\varepsilon = \pm 1$. Écrivons

$$\frac{2b}{a} = 2m + (2n - \varepsilon)\alpha + 2m' + (2n' + \varepsilon)\alpha;$$

$2m' \in \mathbb{Q}$, donc $2m' = u + u'$, avec $u \in \mathbb{Z}$ et $u' \in \mathbb{Q}$ tel que $|u'| \leq \frac{1}{2}$.

En posant

$$q := (2m + u) + (2n - \varepsilon)\alpha, \quad r := a(u' + (2n' + \varepsilon)\alpha),$$

on a $2b = aq + r$ et $|r| < |a|$, car $|u' + (2n' + \varepsilon)\alpha| < \frac{1}{4} + \frac{1}{6} + \frac{5}{9} < 1$. □

Lemme 5.80. *Si $c \in A$ et 2 ne divise pas c , alors il existe s et t dans A tels que $2s + ct = 1$.*

Preuve : Posons $c = \lambda + \mu\alpha$, où λ et μ sont des entiers ; on a alors, $|c|^2 = \lambda^2 + \lambda\mu + 5\mu^2$ et puisque 2 ne divise pas c , λ et μ ne sont pas tous les deux pairs ; par suite $|c|^2$ est impair. Posons $|c|^2 = 2k + 1$ dans $\mathbb{Z}$. En prenant $s = -k$ et $t = \bar{c}$, on obtient : $2s + ct = 1$. □

- Montrons maintenant, que tout idéal de A est principal.

Les idéaux (0) et A sont principaux ; considérons un idéal propre et non nul, I , de A .

Soit $a \in I \setminus \{0\}$ tel que $|a|$ soit minimal (un tel élément existe, car $|a| \in \mathbb{N}^*$). Montrons que a engendre l'idéal I . Etant donné $b \neq 0$ dans I , d'après le lemme 5.79., on a,

soit : $b = aq + r$, avec $(q, r) \in A \times A$ et $|r| < |a|$ ce qui contredit la minimalité de $|a|$; par suite, $r = 0$ donc $b = aq$;

soit : $2b = aq + r$, avec $(q, r) \in A \times A$ et $|r| < |a|$; la minimalité de $|a|$ implique encore $r = 0$, donc $2b = aq$; dans ces conditions,

si 2 divise q dans A , il existe $q' \in A$ tel que $q = 2q'$ d'où $b = aq'$;

si 2 ne divise pas q , d'après le lemme 5.80, il existe s et t dans A tels que $2s + qt = 1$; alors,

$$2b = aq \implies 2bt = aqt \implies 2bt = a(1 - 2s) \implies a = 2(as + bt).$$

On a $(as + bt) \in I$ et $|as + bt| = \frac{|a|}{2} < |a|$, ce qui contredit la minimalité de $|a|$; ce cas est donc impossible.

On en conclut que nécessairement $b \in (a)$, d'où $I = (a)$.

- Démontrons que A n'est pas euclidien.

Soit U_A le groupe des unités de A .

$$z = x + y\alpha \text{ dans } A \implies |z| = x^2 + xy + 5y^2 \in \mathbb{N},$$

$$\text{alors, } z \in U_A \implies |z||z^{-1}| = 1 \implies |z| = 1, \text{ d'où } U_A = \{-1, 1\}.$$

Supposons que A soit euclidien relativement à un stathme δ . Quel que soit $a \in A^* \setminus U_A$, on a (Prop. 5.72.) $\delta(-1) = \delta(1) < \delta(a)$.

On considère $a \in A^* \setminus U_A$ tel que $\delta(a)$ soit minimal; alors pour tout $b \in A$, il existe q et r dans A tels que $b = aq + r$, avec $r = 0$ ou $\delta(r) < \delta(a)$ et

$$\delta(a) \text{ minimal} \implies r = 0 \text{ ou } r \in U_A.$$

Par suite, dans A , a divise b ou $b-1$ ou $b+1$. On en déduit que dans $\mathbb{N}^*$, $|a|^2$ divise $|b|^2$ ou $|b-1|^2$ ou $|b+1|^2$; or,

$$b = 2 \implies |a|^2 \text{ divise } 4 \text{ ou } 1 \text{ ou } 9 \quad \text{et} \quad b = \alpha \implies |a|^2 \text{ divise } 5 \text{ ou } 7;$$

par suite $|a|^2 = 1$, ce qui contredit l'hypothèse $a \notin U_A$; donc A n'est pas euclidien. $\square$

B. p.g.c.d. et p.p.c.m. dans un anneau euclidien

Un anneau euclidien A étant un D.P. (Th. 5.76.), les p.g.c.d. et p.p.c.m. existent dans A et on peut appliquer le théorème de Bezout.

De plus, la division euclidienne conduit à une méthode algorithmique de détermination du p.g.c.d. de deux éléments quelconques de A^* (défini à une unité multiplicative près).

Dans ce qui suit, δ désigne le stathme de l'anneau euclidien considéré.

Algorithme d'Euclide

Soit A est un anneau euclidien; A étant un D.P., la détermination d'un p.g.c.d. de deux éléments non nuls a et b de A revient à trouver un générateur d de l'idéal $(a) + (b)$. (Prop. 5.38.)

Pour a et b donnés, on a $\delta(a) \leq \delta(b)$ ou $\delta(b) \leq \delta(a)$, dans $\mathbb{N}$.

Supposons, par exemple, $\delta(b) \leq \delta(a)$. La division euclidienne de a par b dans A donne :

$$a = bq_1 + r_1, \quad r_1 = 0 \text{ ou } \delta(r_1) < \delta(b).$$

Posons $J_1 = (a) + (b)$ et $J_2 = (b) + (r_1)$ et démontrons que $J_1 = J_2$.

$$a = bq_1 + r_1 \implies a \in J_2 \implies J_1 \subseteq J_2.$$

$$r_1 = a - bq_1 \implies r_1 \in J_1 \implies J_2 \subseteq J_1,$$

d'où l'égalité annoncée.

1^{er} cas : $r_1 = 0$; alors $a = bq_1$, donc $b = a \wedge b$, d'où $(a) + (b) = (b)$.

2^{ème} cas : $r_1 \neq 0$; compte tenu de l'égalité $J_1 = J_2$, on est ramené à déterminer un générateur de $J_2 = (b) + (r_1)$, avec

$$\delta(a) \geq \delta(b) > \delta(r_1).$$

En effectuant la division euclidienne de b par r_1 dans A , on obtient :

$$b = r_1 q_2 + r_2, \quad r_2 = 0 \text{ ou } \delta(r_2) < \delta(r_1).$$

Si $r_2 = 0$, alors $J_1 = J_2 = (r_1)$, donc $r_1 = a \wedge b$.

Si $r_2 \neq 0$, on est ramené à chercher un générateur de

$$J_3 = (r_1) + (r_2) = J_2 = J_1.$$

Comme ci-dessus, on effectue la division euclidienne de r_1 par r_2 et de proche en proche, en réitérant le raisonnement précédent, on aboutit, à la $k^{\text{ème}}$ étape, $k > 2$, aux relations :

$$r_{k-2} = r_{k-1} q_k + r_k; \quad r_k = 0 \text{ ou } \delta(r_k) < \delta(r_{k-1}).$$

Les entiers naturels $\delta(r_k)$ forment une suite strictement décroissante :

$$\delta(b) > \delta(r_1) > \dots > \delta(r_{k-1}) > \delta(r_k) > \dots$$

On en déduit qu'il existe un entier $n \geq 1$ tel que $r_n = 0$, d'où $r_{n-2} = r_{n-1} q_n$; alors,

$$J_n = (r_{n-2}) + (r_{n-1}) = (r_{n-1}) = J_{n-2} = \dots = J_1 \implies r_{n-1} = a \wedge b.$$

Ainsi, le dernier reste non nul, dans la suite algorithmique des divisions euclidiennes effectuées, est un p.g.c.d. de a et b . $\square$

Exemple 5.81. Calcul d'un p.g.c.d. dans l'anneau de Gauss $\mathbb{Z}[i]$.

Déterminons $(4 + 7i) \wedge (8 - i)$. La division euclidienne de $4 + 7i$ par $8 - i$ a été effectuée plus haut (Exemple 5.75.) d'où :

$$4 + 7i = (8 - i)i + 3 - i \implies q_1 = i, r_1 = 3 - i.$$

On obtient ensuite (à vérifier par le lecteur) :

$$8 - i = (3 - i)(2 + i) + 1 - 2i \implies q_2 = 2 + i, r_2 = 1 - 2i.$$

$$3 - i = (1 - 2i)(1 + i) \implies r_3 = 0,$$

par suite $(4 + 7i) \wedge (8 - i) = r_2 = 1 - 2i$.

Remarque 5.82. Si K est un corps, alors l'anneau $K[X]$ est euclidien, par suite il possède des propriétés arithmétiques semblables à celles de $\mathbb{Z}$. On a, en particulier, les résultats suivants (Cf. App. A, Prop. 0.35., 0.36.).

Proposition 5.83. Si K est un corps de caractéristique 0 et si d, m, n sont des entiers strictement positifs, alors

1) $d \mid m$ dans $\mathbb{Z} \iff X^d - 1 \mid X^m - 1$ dans $K[X]$.

2) $d = m \wedge n \iff X^d - 1 = (X^m - 1) \wedge (X^n - 1)$ dans $K[X]$.

En particulier : $m \wedge n = 1 \iff X - 1 = (X^m - 1) \wedge (X^n - 1)$.

Démonstration proposée en exercice (Ex. 5, Ch. 5).

Remarque 5.84. $\mathbb{Z}$ est un anneau euclidien, cependant l'anneau de polynômes $\mathbb{Z}[X]$ n'est pas euclidien, car $\mathbb{Z}[X]$ n'est pas principal. En effet, si $\mathbb{Z}[X]$ était un D.P., le théorème de Bezout y serait applicable, or 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$, mais $1 \notin (2) + (X)$, d'où $(2) + (X) \neq \mathbb{Z}[X]$.

De cet exemple, on déduit que

A anneau euclidien $\nRightarrow A[X]$ anneau euclidien ;

A domaine principal $\nRightarrow A[X]$ domaine principal,

d'où l'importance du résultat suivant.

Théorème 5.85. Pour un anneau unitaire, commutatif A , les conditions suivantes sont équivalentes :

- 1) A est un corps.
- 2) $A[X]$ est un anneau euclidien.
- 3) $A[X]$ est un domaine principal.

Preuve : On a déjà prouvé (Th. 4.33. et 5.76.) que $1) \implies 2) \implies 3)$, il suffit de démontrer que $3) \implies 1)$.

Si $A[X]$ est un D.P., c'est, a fortiori, un D.I., par suite l'anneau unitaire, commutatif A est aussi un D.I. Considérons l'application

$$\gamma : A[X] \longrightarrow A \\ \sum_{1 \leq i \leq n} a_i X_i \longmapsto a_0.$$

On vérifie que γ est un morphisme surjectif d'anneaux unitaires ; on a

$$\text{Ker } \gamma = \{ \sum_{1 \leq i \leq n} a_i X_i \in A[X] ; a_0 = 0 \} \neq (0) \quad \text{et} \quad A \simeq A[X] / \text{Ker } \gamma.$$

A intègre implique $A[X] / \text{Ker } \gamma$ intègre, par suite $\text{Ker } \gamma$ est un idéal premier, non nul de $A[X]$ (Th. 2.52.). Mais $A[X]$ est, par hypothèse, un D.P., donc $\text{Ker } \gamma$ est un idéal maximal de $A[X]$ (Th. 2.65.).

On en conclut que $\frac{A[X]}{\text{Ker } \gamma}$ est un corps (Th. 2.61.), donc A est un corps. $\square$

Remarque 5.86. K étant un corps, on sait que $K[X]$ n'est pas un corps ; il en résulte que $K[X, Y] = K[X][Y]$ n'est pas principal et plus généralement, quel que soit $n \geq 2$, $K[X_1, X_2, \dots, X_n]$ n'est pas un D.P..

6. Anneaux factoriels

A. Notion d'anneau factoriel

Définition 5.87. Un anneau A est un **anneau factoriel** si

i) A est un D.I.

ii) A vérifie les deux conditions suivantes :

(AF_1) : Tout $a \in A^* \setminus U_A$ s'écrit sous la forme : $a = r_1 r_2 \cdots r_n$, où $n \in \mathbb{N}^*$ et pour tout $i (1 \leq i \leq n)$, r_i est irréductible dans A .

(AF_2) : Si $a = r_1 r_2 \cdots r_n = r'_1 r'_2 \cdots r'_p$, où les r_i et r'_j sont irréductibles dans A , quels que soient $i, 1 \leq i \leq n$, et $j, 1 \leq j \leq p$, alors,

$n = p$ et il existe une permutation $\sigma \in S_n$ telle que, pour tout $i (1 \leq i \leq n)$, r_i est associé à $r'_{\sigma(i)}$ dans A .

Exemple 5.88. Le premier exemple d'anneau factoriel est $\mathbb{Z}$ (Cf. App.A).

Théorème 5.89. A étant un D.I., alors A est un anneau factoriel si et seulement si il vérifie la condition (AF_1) et la condition

$(AF_2)'$: Tout élément irréductible de A est premier.

Preuve : A étant un D.I., il faut prouver l'équivalence logique suivante :

$$(AF_1) \text{ et } (AF_2) \iff (AF_1) \text{ et } (AF_2)'.$$

1°) $(AF_1) \text{ et } (AF_2) \implies (AF_1) \text{ et } (AF_2)'$.

Soit r un élément irréductible dans A ; on a donc $r \neq 0$ et $r \notin U_A$.

Pour montrer que r est premier, supposons $r|ab$ dans A^* ; alors il existe $x \neq 0$ tel que $ab = rx$. D'après la condition (AF_1) , a, b, x s'écrivent,

$$a = a_1 a_2 \cdots a_m, \quad b = b_1 b_2 \cdots b_n, \quad x = x_1 x_2 \cdots x_t,$$

où les $a_i, 1 \leq i \leq m, b_j, 1 \leq j \leq n, x_k, 1 \leq k \leq t$ sont irréductibles dans A . On en déduit l'égalité

$$a_1 \cdots a_m b_1 \cdots b_n = r x_1 \cdots x_t;$$

mais r étant irréductible, la condition (AF_2) implique :

$$(\exists i (1 \leq i \leq m) \text{ tel que } r \sim a_i) \quad \text{ou} \quad (\exists j (1 \leq j \leq n) \text{ tel que } r \sim b_j).$$

Dans le premier cas, on a $r|a$ et dans le second cas, $r|b$; on en conclut que r est premier dans A .

2°) (AF_1) et $(AF_2)' \implies (AF_1)$ et (AF_2) .

Considérons dans A l'égalité : $r_1 r_2 \cdots r_n = r'_1 r'_2 \cdots r'_p$, où les r_i et r'_j sont irréductibles, quels que soient $i (1 \leq i \leq n)$ et $j (1 \leq j \leq p)$. La condition $(AF_2)'$ implique que tous les r_i et r'_j sont premiers dans A ; d'après la proposition 5.26., on a alors : $n = p$ et il existe $\sigma \in S_n$ tel que pour tout $i (1 \leq i \leq n)$, $r_i \sim r'_{\sigma(i)}$, donc la condition (AF_2) est vérifiée. $\square$

Théorème 5.90. *Tout domaine principal est un anneau factoriel.*

Preuve : On sait que dans un domaine principal A tout élément irréductible est premier (Th. 5.23.), donc la condition $(AF_2)'$ est vérifiée, il reste à prouver que A satisfait à la condition (AF_1) . Pour cela, nous utiliserons l'axiome de Zorn (Cf. 2.69.).

On suppose que A ne vérifie pas (AF_1) ; l'ensemble E suivant est alors non vide :

$$E := \{a \in A^* \setminus U_A; a \text{ n'est pas produit d'éléments irréductibles}\}.$$

On remarque qu'un élément a de E est nécessairement non irréductible et que d'autre part, pour $a' \in A$:

$$(a \in E \text{ et } a' \sim a) \implies a' \in E.$$

Notons T l'ensemble des idéaux principaux (a) de A , engendrés par les éléments $a \in E$. L'ensemble T est non vide et partiellement ordonné par l'inclusion ; montrons que T est inductif (Déf. 2.68.). Soit

$$(a_0) \subseteq (a_1) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \cdots$$

une chaîne croissante d'idéaux principaux appartenant à T .

Posons $I = \bigcup_{n \in \mathbb{N}} (a_n)$; I est un idéal de A (Prop. 2.3.); I est non nul, car $(a) \in T$ implique $(a) \neq (0)$. A étant un D.P., il existe un $b \in A^*$ tel que $I = (b)$, alors

$$b \in I \implies \exists i \in \mathbb{N}, b \in (a_i).$$

Mais $I = (b) \subseteq (a_i)$ implique $I = (a_i)$, donc $I \in T$; or I est un majorant pour la famille totalement ordonnée des idéaux $(a_n), n \in \mathbb{N}$, considérée dans T , donc T est un ensemble inductif.

D'après l'axiome de Zorn, il existe au moins un élément maximal dans T ; notons (c) un tel élément maximal; nécessairement $c \in E$.

Supposons qu'il existe x, y dans A^* tels que $c = xy$; alors

$$c \in E \implies x \notin U_A, y \notin U_A \quad \text{et} \quad (x \in E \text{ ou } y \in E).$$

$$(x \in E \implies (x) \in T) \quad \text{et} \quad (c = xy \implies (c) \subsetneq (x)),$$

$$(y \in E \implies (y) \in T) \quad \text{et} \quad (c = xy \implies (c) \subsetneq (y));$$

ces résultats contredisent la maximalité de (c) dans T . Par suite E est vide, donc la condition (AF_1) est vérifiée et A est un anneau factoriel. $\square$

Exemple 5.91. Le théorème précédent permet d'affirmer que

- 1) Si K est un corps, alors l'anneau $K[X]$ est factoriel.
- 2) L'anneau des entiers de Gauss, $\mathbb{Z}[i]$, est factoriel.

Remarque 5.92. La réciproque du théorème 5.90. est fausse ; nous verrons plus loin des exemples d'anneaux factoriels qui ne sont pas principaux.

En vue de caractériser un anneau factoriel à l'aide de ses idéaux premiers (Th. 5.96), nous démontrons les deux lemmes suivants.

Lemme 5.93. Soit A un D.I. (qui n'est pas un corps). Soit S l'ensemble des éléments de A qui sont produits d'éléments premiers (en particulier, tout élément premier de A est dans S) ; alors

i) $0 \notin S, S \cap U_A = \emptyset; (u, a) \in U_A \times S \implies ua \in S.$

ii) $(a, b) \in S \times S \implies ab \in S.$

iii) $(ab \in S, a \notin U_A, b \notin U_A) \implies a \in S \text{ et } b \in S.$

Preuve : Les propriétés i) et ii) sont des conséquences directes de la définition de S ; ii) exprime que S est multiplicativement fermé.

iii) : Supposons $(a, b) \in A \times A, a \notin U_A, b \notin U_A$ et $ab \in S$. Il existe des éléments premiers dans $A, p_1, p_2, \dots, p_n, n \in \mathbb{N}^*$ tels que

$$ab = p_1 p_2 \dots p_n. \quad (5.17)$$

L'hypothèse $a \notin U_A, b \notin U_A$ implique $n \geq 2$. En effet, si $n = 1, p_1$ étant premier, p_1 est irréductible et

$$ab = p_1 \implies a \in U_A \text{ ou } b \in U_A.$$

Dans l'égalité (5.17), p_1 est premier et $p_1 | ab$ donc $p_1 | a$ ou $p_1 | b$.

Supposons $p_1 | a$; il existe $a_1 \in A^*$ tel que $a = p_1 a_1$ et A étant intègre :

$$p_1 a_1 b = p_1 p_2 \dots p_n \implies a_1 b = p_2 \dots p_n.$$

En réitérant le raisonnement précédent on aboutit nécessairement à l'existence d'un entier $j (1 \leq j \leq n-1)$ tel que

$$a = p_1 p_2 \dots p_j, b = p_{j+1} p_{j+2} \dots p_n, \text{ donc } a \in S \text{ et } b \in S;$$

on a $j \leq n-1$, car $j = n$ impliquerait $b = 1$, contraire à l'hypothèse $b \notin U_A$. $\square$

Remarque 5.94. La partie S de A définie dans le lemme précédent, n'est pas une partie multiplicative au sens donné au Ch.6 (Localisation), car ici $S \cap U_A = \emptyset$.

Lemme 5.95. A étant un D.I. (qui n'est pas un corps), on considère l'ensemble S défini dans le lemme 5.93. et on pose

$$\mathcal{I} := \{I \text{ idéal de } A; I \cap S = \emptyset\};$$

il existe alors, au moins un élément maximal dans $\mathcal{I}$ et un tel élément est un idéal premier de A .

Preuve : On vérifie que l'ensemble $\mathcal{I}$, partiellement ordonné par l'inclusion, est inductif (Déf. 2.68.), donc d'après l'axiome de Zorn, il existe au moins un élément maximal dans $\mathcal{I}$; soit P un tel élément. Montrons que P est un idéal premier de A .

Supposons $(a, b) \in A \times A$ tel que $ab \in P, a \notin P, b \notin P$; alors les idéaux $P + (a)$ et $P + (b)$ contiennent strictement l'idéal P et la maximalité de P dans $\mathcal{I}$ implique $(P + (a)) \notin \mathcal{I}$ et $(P + (b)) \notin \mathcal{I}$.

On en déduit qu'il existe x, x' dans P et y, y' dans A tels que

$$(x + ay) \in (P + (a)) \cap S \text{ et } (x' + by') \in (P + (b)) \cap S.$$

Posons $s = (x + ay)(x' + by')$; l'ensemble S étant multiplicativement fermé dans A , on a $s \in S$, or

$$s = (xx' + ayx' + by'x + abx'y') \in P, \text{ donc } s \in P \cap S$$

ce qui contredit l'hypothèse $P \in \mathcal{I}$. On en conclut que

$$ab \in P \implies a \in P \text{ ou } b \in P,$$

donc P est un idéal premier. $\square$

Théorème 5.96. *Un domaine d'intégrité A est un anneau factoriel si et seulement si tout idéal premier non nul de A contient un élément premier.*

Preuve :

Supposons A factoriel ; A possède au moins un idéal premier non nul P , car A n'est pas un corps. On a $P \neq A$, donc il existe $a \in P$ tel que $a \neq 0$ et $a \notin U_A$; alors a est un produit d'éléments premiers $p_1, \dots, p_n$ de A , $n \in \mathbb{N}^*$ et d'après la Prop. 2.55.,

$$a = p_1 p_2 \dots p_n \in P \implies \exists i (1 \leq i \leq n), \text{ tel que } p_i \in P.$$

Réciproquement, on suppose que A est un D.I. dans lequel tout idéal premier non nul contient un élément premier. Cette hypothèse entraîne que A n'est pas un corps. Considérons la partie S de A définie dans le lemme 5.93. et montrons que $S = A^* \setminus U_A$.

Supposons $S \neq A^* \setminus U_A$, donc il existe $c \in A$ tel que $c \neq 0$, $c \notin U_A$ et $c \notin S$. Soit (c) l'idéal principal de A engendré par c . Compte tenu des résultats et des notations des lemmes 5.93. et 5.95., on a

$$(c) \cap S = \emptyset \implies (c) \in \mathcal{I}$$

et il existe un élément maximal P dans $\mathcal{I}$ tel que

$$(c) \subseteq P \text{ et } P \text{ est un idéal premier de } A.$$

Par hypothèse, P contient un élément premier, donc $P \cap S \neq \emptyset$, ce qui est en contradiction avec $P \in \mathcal{I}$.

Il en résulte que tout élément de $A^* \setminus U_A$ est produit d'éléments premiers de A , donc A vérifie la condition (AF_1) de la définition 5.87.

De plus, si r est un élément irréductible de A , alors $r \in A^* \setminus U_A = S$, donc r est produit d'éléments premiers ; mais, dans A ,

$$(p \text{ premier, } r \text{ irréductible et } p \text{ divise } r) \implies p \text{ associé à } r,$$

donc tout élément irréductible de A est premier (Cond. $(AF_2)'$). On en conclut que l'anneau A est factoriel. $\square$

B. p.g.c.d. et p.p.c.m. dans un anneau factoriel

Proposition 5.97. *Dans tout anneau factoriel, les p.g.c.d. et p.p.c.m. existent.*

Preuve : Comme dans le cas de l'anneau $\mathbb{Z}$ (Cf. App. A), on montre que dans un anneau factoriel A , on peut écrire explicitement un p.g.c.d. et un p.p.c.m. de deux éléments non nuls a et b en fonction de leurs diviseurs irréductibles.

Soit $\{r_i\}_{i \in I}$ une famille de représentants des classes d'équivalence des éléments irréductibles de A , modulo l'association. Quel que soit l'élément irréductible $r \in A$, il existe un unique $i \in I$ tel que l'on ait $r \sim r_i$.

On en déduit que tout $a \in A^*$ s'écrit de façon unique :

$$a = u \prod_{i \in I} r_i^{n_i(a)},$$

où $u \in U_A$ et quel que soit $i \in I$, $n_i(a) \in \mathbb{N}$, les $n_i(a)$ étant nuls, sauf un nombre fini d'entre eux (ce que l'on exprime aussi en disant que les $n_i(a)$ sont presque tous nuls dans $\mathbb{N}$).

On vérifie facilement les propriétés suivantes :

- 1) $a \in U_A \iff \forall i \in I, n_i(a) = 0$.
- 2) $\forall (a, b) \in A^* \times A^*, \forall i \in I, n_i(ab) = n_i(a) + n_i(b)$.
- 3) $a|b$ dans $A^* \iff \forall i \in I, n_i(a) \leq n_i(b)$.
- 4) $a \sim b$ dans $A^* \iff \forall i \in I, n_i(a) = n_i(b)$.

Considérons a, b non nuls dans A et pour tout $i \in I$, posons

$$\alpha_i = \inf(n_i(a), n_i(b)) \quad \text{et} \quad \beta_i = \sup(n_i(a), n_i(b));$$

alors à l'aide des propriétés énoncées ci-dessus on prouve que

$$d = \prod_{i \in I} r_i^{\alpha_i} \quad \text{et} \quad m = \prod_{i \in I} r_i^{\beta_i}$$

sont, respectivement, *p.g.c.d.* et *p.p.c.m.* de a et b . □

Remarque 5.98. Nous avons noté plus haut (Rem. 5.92.) qu'un anneau factoriel n'est pas nécessairement principal, cependant, l'existence des *p.p.c.m.* dans un anneau factoriel implique que dans un tel anneau, *l'intersection de deux idéaux principaux est un idéal principal* (Cor. 5.59.).

C. Anneaux de polynômes sur un anneau factoriel

On rappelle (Ch. 4) que si A est un D.I., alors pour tout entier $n \geq 1$, l'anneau $A[X_1, \dots, X_n]$ est aussi un D.I., dont les seuls éléments inversibles sont les unités de A .

Le résultat important de ce paragraphe est le suivant :

Théorème 5.99. *Si A est un anneau factoriel, alors l'anneau de polynômes $A[X]$ est factoriel.*

La démonstration de ce théorème nécessite quelques notions et propriétés préliminaires. Dans tout ce qui suit on suppose que A est un anneau factoriel.

1. Notion de polynôme primitif dans $A[X]$

Définition 5.100. Soit $f \in A[X] \setminus A$. On appelle **contenu** de f un *p.g.c.d.* des coefficients du polynôme f ; on le notera $c(f)$.

Remarque 5.101. Pour un polynôme f non constant dans $A[X]$, le contenu $c(f)$ n'est défini qu'à une unité multiplicative près.

Définition 5.102. Un polynôme $f \in A[X]$ est dit **primitif** si $\deg f \geq 1$ et si ses coefficients sont premiers entre eux dans leur ensemble; on pourra écrire, dans ce cas, $c(f) = 1$.

Remarque 5.103. :

a) Tout polynôme f non constant dans $A[X]$ s'écrit $f = c(f) f_1$, où f_1 est un polynôme primitif dans $A[X]$.

b) Tout polynôme *unitaire* (Déf. 4.10) dans $A[X]$ est primitif.

Lemme 5.104. *Quels que soient les polynômes primitifs f_1, f_2 dans $A[X]$ et les constantes c_1, c_2 dans A^* , on a*

$$c_1 f_1 = c_2 f_2 \implies (c_1 \sim c_2 \text{ dans } A \text{ et } f_1 \sim f_2 \text{ dans } A[X]).$$

Preuve : Posons $f = c_1 f_1 = c_2 f_2$. Les polynômes f_1 et f_2 étant primitifs, c_1 et c_2 sont deux *p.g.c.d.* des coefficients de f , d'où $c_1 \sim c_2$.

Par suite, il existe $u \in U_A$ tel que $c_2 = u c_1$. L'anneau $A[X]$ étant intègre, on en déduit que

$$c_1 f_1 = u c_1 f_2 \implies f_1 = u f_2,$$

donc $f_1 \sim f_2$. □

Lemme 5.105. *Pour f et g dans $A[X]$, on a*

1) f et g primitifs $\iff fg$ primitif.

2) $c(fg) = c(f) c(g)$.

Preuve :

1) Supposons que l'on ait f et g primitifs et fg non primitif. Dans l'anneau factoriel A , il existe au moins un élément premier p divisant $c(fg)$, donc p divise tous les coefficients du polynôme fg .

Soit π la surjection canonique $A \rightarrow A/(p)$. L'idéal (p) est premier, donc $A/(p)$ est un D.I. Posons $B = A/(p)$; Le morphisme π se prolonge en

$$\begin{aligned}\hat{\pi} : A[X] &\longrightarrow B[X] \\ \sum_{0 \leq i \leq n} a_i X^i &\longmapsto \sum_{0 \leq i \leq n} \pi(a_i) X^i.\end{aligned}$$

Puisque $c(f) = c(g) = 1$, p ne divise pas tous les coefficients de f , ni tous les coefficients de g ; d'où $\hat{\pi}(f) \neq 0$ et $\hat{\pi}(g) \neq 0$ dans $B[X]$; or p divise $c(fg)$, donc divise tous les coefficients de fg , par suite $\hat{\pi}(fg) = 0$.

Mais $\hat{\pi}$ est un morphisme d'anneaux et $B[X]$ est intègre, donc

$$\hat{\pi}(f)\hat{\pi}(g) = 0 \implies \hat{\pi}(f) = 0 \text{ ou } \hat{\pi}(g) = 0,$$

d'où une contradiction; on en conclut que fg est primitif dans $A[X]$.

Réciproquement, supposons le polynôme fg primitif. On peut écrire :

$f = c(f)f_1$, $g = c(g)g_1$, où f_1 et g_1 sont primitifs dans $A[X]$; alors, d'après le lemme 5.104,

$$fg = c(f)c(g)f_1g_1 \implies c(f)c(g) \sim c(fg),$$

d'où $c(f)c(g) \in U_A$, puisque fg est primitif. On en déduit que $c(f) \in U_A$ et $c(g) \in U_A$, donc f et g sont primitifs.

2) En utilisant les notations ci-dessus et en posant $fg = c(fg)h_1$, où h_1 est primitif, on obtient : $c(f)c(g)f_1g_1 = c(fg)h_1$.

L'application du lemme 5.104 donne alors $c(fg) \sim c(f)c(g)$. □

2. Éléments irréductibles dans $A[X]$

L'anneau factoriel A est un D.I., on peut donc considérer le corps des fractions de A ; on pose $K = Fr A$.

Lemme 5.106. *Compte tenu des hypothèses et notations ci-dessus, tout $f \in K[X] \setminus K$ peut s'écrire :*

$$f = \gamma f_1, \text{ où } \gamma \in K^* \text{ et } f_1 \text{ est primitif dans } A[X].$$

Preuve : Soit f un polynôme non constant de $K[X]$ tel que

$$f(X) = \sum_{0 \leq i \leq n} \frac{a_i}{s_i} X^i,$$

où l'on peut toujours supposer que pour tout i ($0 \leq i \leq n$), $a_i \wedge s_i = 1$.

Dans l'anneau factoriel A , soit s un p.p.c.m. des s_i ; pour tout i , $0 \leq i \leq n$,

il existe $s'_i \in A^*$ tel que $s = s_i s'_i$ et en posant $a'_i = s'_i a_i$, on obtient

$$f(X) = \frac{1}{s} \sum_{0 \leq i \leq n} a'_i X^i.$$

Soit $d \in A^*$ un p.g.c.d. des a'_i , $0 \leq i \leq n$; alors $a'_i = db_i$, les b_i , $0 \leq i \leq n$, étant premiers entre eux dans leur ensemble (Prop. 5.43.). On en déduit que

$$f(X) = \frac{d}{s} \sum_{0 \leq i \leq n} b_i X^i,$$

où $\frac{d}{s} \in K^*$ et $f_1(X) = \sum_{0 \leq i \leq n} b_i X^i$ est primitif dans $A[X]$. □

Remarque 5.107. Avec les mêmes hypothèses et notations que précédemment, tout polynôme de $A[X]$ peut être considéré comme un polynôme de $K[X]$, car le plongement canonique α de A dans K se prolonge en le plongement canonique, $\hat{\alpha}$, de $A[X]$ dans $K[X]$.

La proposition suivante caractérise les éléments irréductibles de $A[X]$.

Proposition 5.108. *A étant un anneau factoriel, soit K son corps de fractions et r un élément non nul de $A[X]$.*

- 1) *r est irréductible dans $A[X]$ et $\deg r = 0$ si et seulement si r est irréductible dans A .*
- 2) *r est irréductible dans $A[X]$ et $\deg r > 0$ si et seulement si r est primitif dans $A[X]$ et irréductible dans $K[X]$.*

Preuve : L'anneau A étant intègre, on rappelle que $U_{A[X]} = U_A$.

1) Soit r un élément irréductible de A . On a $r \neq 0$ et $r \notin U_A$, donc r est un polynôme constant, non nul et non inversible dans $A[X]$.

Supposons $r = fg$ dans $A[X]$;

$$(\deg fg = 0 = \deg f + \deg g) \implies \deg f = \deg g = 0,$$

donc f et g sont non nuls dans A et r étant irréductible dans A , on a $f \in U_A = U_{A[X]}$ ou $g \in U_A = U_{A[X]}$, d'où r irréductible dans $A[X]$.

Réciproquement, soit r un élément irréductible de $A[X]$ et de degré 0; on a nécessairement, $r \in A^* \setminus U_A$. Supposons $r = ab$ dans A , donc aussi dans $A[X]$, alors,

$$r \text{ irréductible dans } A[X] \implies (a \in U_{A[X]} = U_A \text{ ou } b \in U_{A[X]} = U_A),$$

d'où r irréductible dans A .

2) Soit r un polynôme primitif dans $A[X]$ et irréductible dans $K[X]$, on a donc $\deg r > 0$. Supposons $r = fg$ dans $A[X]$. Les polynômes f et g sont non nuls dans $A[X]$, donc non nuls en tant que polynômes de $K[X]$. Mais r étant irréductible dans $K[X]$, on a f ou g dans $U_{K[X]} = K^*$; or les coefficients de f et g sont, par hypothèse, dans A , d'où $f \in A^*$ ou $g \in A^*$.

Considérons le cas où $f \in A^*$. Dans $A[X]$, on écrit : $g = c(g)g_1$, où $c(g)$ est le contenu de g et g_1 un polynôme primitif; alors

$$(r = fc(g)g_1, fc(g) \in A^* \text{ et } g_1 \text{ primitif}) \implies fc(g) \in U_A,$$

car r est primitif; par suite $f \in U_A = U_{A[X]}$.

Dans le cas où $g \in A^*$, on obtiendrait de même : $g \in U_A$. On en conclut que r est irréductible dans $A[X]$.

Réciproquement, supposons r irréductible dans $A[X]$ et $\deg r > 0$. On a $r = c(r)r_1$, avec $c(r) \in A^*$ et r_1 primitif dans $A[X]$. Mais r est irréductible dans $A[X]$; alors $\deg r_1 = \deg r > 0$ implique nécessairement $c(r) \in U_A$, donc r est primitif.

Supposons $r = fg$ dans $K[X]$, avec $\deg f > 0$ et $\deg g > 0$.

D'après le lemme 5.106., on a $f = \frac{d}{s}f_1$, $g = \frac{c}{t}g_1$, où $\frac{d}{s}$ et $\frac{c}{t}$ sont dans K^* ,

f_1 et g_1 étant des polynômes primitifs de $A[X]$, dont les degrés sont respectivement, ceux de f et g .

$$r(X) = f(X)g(X) \implies st r(X) = dc f_1(X)g_1(X).$$

De cette dernière égalité, on déduit, en appliquant le lemme 5.104., qu'il existe $u \in U_A$ tel que $r = uf_1g_1$; or par hypothèse, r est irréductible dans $A[X]$, d'où : $uf_1 \in U_{A[X]} = U_A$ ou $g_1 \in U_{A[X]} = U_A$, ce qui est contraire à l'hypothèse : $\deg f > 0$ et $\deg g > 0$; donc r est irréductible dans $K[X]$. $\square$

3. Démonstration du théorème 5.99.

Il s'agit de prouver que l'anneau $A[X]$ est factoriel, lorsque A est factoriel.

1°) Montrons que $A[X]$ vérifie la condition (AF_1) .

Soit $f \in A[X]$, $f \neq 0$, $f \notin U_A$.

Si $\deg f = 0$, dans A , on a $f = r_1 r_2 \cdots r_k$, où pour tout i , $1 \leq i \leq k$, r_i est irréductible dans A , donc dans $A[X]$, d'après la proposition 5.108. ; ainsi f vérifie la condition (AF_1) .

Si $\deg f > 0$, posons $n = \deg f$ et raisonnons par récurrence sur n .

On remarque que l'on peut se ramener au cas où f est primitif.

En effet, si f n'est pas primitif, on écrit : $f = c(f)f_1$, où $c(f) \in A^* \setminus U_A$, et f_1 est un polynôme primitif. Or, d'après ce qui précède, en tant que polynôme constant, $c(f)$ se décompose en un produit d'éléments irréductibles de $A[X]$, donc il reste à considérer le polynôme f_1 .

Pour la suite de la démonstration, on suppose f primitif.

Si $\deg f = 1$, on peut alors écrire : $f = u(X - a)$, où $u \in U_A$; $X - a$ étant irréductible dans $A[X]$, il en est de même de f ; la condition (AF_1) est donc vérifiée par f , dans le cas $n = 1$.

Si $\deg f = n > 1$ et si de plus f est irréductible dans $A[X]$, alors (AF_1) est vérifiée ; considérons le cas où f n'est pas irréductible. Compte tenu de ce qui précède, on suppose (AF_1) vérifiée par tout polynôme primitif de degré strictement inférieur à n . Dans $A[X]$, écrivons :

$$f = gh, \text{ avec } 0 < \deg g < \deg f, \quad 0 < \deg h < \deg f.$$

Le polynôme f étant primitif, g et h sont primitifs (Lem. 5.105.), alors l'hypothèse de récurrence implique que g et h sont produits d'éléments irréductibles de $A[X]$, donc il en est de même pour f .

2°) Montrons que $A[X]$ vérifie la condition (AF_2) .

Soit r un élément irréductible de $A[X]$, prouvons qu'il est premier dans $A[X]$.

Si $\deg r = 0$, alors r est premier dans A , car l'anneau A est factoriel ; il faut prouver, qu'en tant que polynôme constant, il est premier dans $A[X]$.

Supposons : $r \nmid fg$ dans $A[X]$; alors, nécessairement, r divise $c(f)c(g)$ dans A et comme r est premier dans A , on a $r \mid c(f)$ ou $r \mid c(g)$ dans A , par suite, $r \mid f$ ou $r \mid g$ dans $A[X]$, donc r est premier dans $A[X]$.

Si $\deg r > 0$, d'après la proposition 5.108., r est primitif dans $A[X]$ et irréductible dans $K[X]$, où $K = FrA$. Mais $K[X]$ est un anneau factoriel (Exemple 5.91.), donc r est premier dans $K[X]$.

Supposons $r \nmid fg$ dans $A[X]$; on a donc aussi $r \nmid fg$ dans $K[X]$, d'où $r \nmid f$ ou $r \nmid g$ dans $K[X]$. Considérons le cas où $r \nmid f$; il existe alors $q \in K[X]$ tel que $f = rq$. D'après le lemme

5.106., on a $q = \frac{d}{s}q_1$, où $\frac{d}{s} \in K^*$ et q_1 est un polynôme primitif dans $A[X]$. On en déduit que $sf = drq_1$ dans $A[X]$, où f et rq_1 sont des polynômes primitifs ; par suite, s et d sont associés dans A (Lem. 5.104). Il existe $u \in U_A$ tel que $d = us$, d'où $f = urq_1$ dans $A[X]$, donc $r \mid f$ dans $A[X]$. On en conclut que $r \nmid fg$ dans $A[X]$ implique $r \nmid f$ ou $r \nmid g$ dans $A[X]$, d'où r premier dans $A[X]$. $\square$

Exemple 5.109. L'anneau $\mathbb{Z}$ étant factoriel, $\mathbb{Z}[X]$ est un anneau factoriel.

Corollaire 5.110. :

1) Si A est un anneau factoriel, alors, pour tout entier $n \geq 1$, l'anneau $A[X_1, X_2, \dots, X_n]$ est factoriel.

2) Si K est un corps, alors, pour tout entier $n \geq 1$, l'anneau $K[X_1, X_2, \dots, X_n]$ est factoriel.

Preuve :

- 1) Le résultat s'obtient par récurrence sur n , à partir du théorème 5.99.
 2) $K[X_1]$ est un anneau factoriel (Exemple 5.91.) ; d'où la propriété énoncée, compte tenu du résultat 1) précédent. $\square$

Remarque 5.111. :

a) Exemples d'anneaux factoriels, non principaux

$\mathbb{Z}[X]$ et plus généralement, pour tout $n \geq 1$, $\mathbb{Z}[X_1, \dots, X_n]$ est un anneau factoriel, non principal (Cor. 5.110., Th. 5.85.).

Pour tout $n \geq 2$, l'anneau $K[X_1, X_2, \dots, X_n]$ est anneau factoriel, non principal (Cor. 5.110., Rem. 5.86.).

b) A étant un anneau factoriel, il n'est pas facile, en général, de reconnaître si un polynôme non constant de $A[X]$ est irréductible, d'où l'intérêt du critère d'irréductibilité ci-dessous.

Proposition 5.112. Critère d'Eisenstein

A étant un anneau factoriel, soit K son corps de fractions et $f \in A[X]$, tel que

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i, \quad n = \deg f > 0.$$

S'il existe un élément premier p , dans A , vérifiant les conditions

$$p \nmid a_n; \quad \forall i (0 \leq i \leq n-1), p | a_i; \quad p^2 \nmid a_0, \quad (5.18)$$

alors le polynôme f est irréductible dans $K[X]$.

Si de plus, f est primitif dans $A[X]$ (en particulier, si f est unitaire), alors f est irréductible dans $A[X]$.

Preuve : Montrons que l'on peut se ramener à l'étude du cas où f est primitif dans $A[X]$.

Si f est non primitif, on écrit $f = c(f)f_1$, où $c(f)$ est le contenu de f et f_1 est primitif dans $A[X]$. Vérifions que les coefficients du polynôme f_1 satisfont aux conditions (5.18). En effet, $c(f)$ étant un p.g.c.d. des coefficients de f , pour tout i ($0 \leq i \leq n$), on a $a_i = c(f)a'_i$, où les a'_i sont premiers entre eux dans leur ensemble et $f_1 = \sum_{0 \leq i \leq n} a'_i X^i$. On a alors,

$$p \nmid a_n \implies p \nmid a'_n; \quad p^2 \nmid a_0 \implies p^2 \nmid a'_0,$$

et pour $0 \leq i \leq n-1$, $p | a_i$ implique $p | a'_i$, car p est premier et $p \nmid c(f)$, puisque $p \nmid a_n$.

Ainsi les coefficients du polynôme primitif f_1 vérifient les mêmes hypothèses que ceux de f . On peut donc supposer, pour la démonstration du critère, que f est primitif.

Montrons que f est irréductible dans $A[X]$. Supposons :

$$f = gh \quad \text{dans } A[X], \quad 0 < \deg g < \deg f, \quad 0 < \deg h < \deg f.$$

f étant primitif, g et h sont primitifs (Lem. 5.105.). Posons

$$g(X) = \sum_{0 \leq j \leq q} b_j X^j, \quad h(X) = \sum_{0 \leq k \leq r} c_k X^k.$$

$$(a_n = b_q c_r \neq 0 \text{ et } p \nmid a_n) \implies p \nmid b_q \text{ et } p \nmid c_r.$$

$$(p | a_0, \quad p^2 \nmid a_0 \text{ et } a_0 = b_0 c_0) \implies p | b_0 c_0 \text{ et } p^2 \nmid b_0 c_0,$$

d'où $p \nmid b_0$ ou $p \nmid c_0$.

Considérons le cas où $p \nmid b_0$, alors $p | c_0$ car p est premier dans A . D'autre part, $p \nmid c_r$.

On en déduit qu'il existe un plus petit entier k tel que $1 \leq k \leq r$ et $p \nmid c_k$; considérons le coefficient

$$a_k = b_0 c_k + b_1 c_{k-1} + \dots + b_k c_0.$$

Le choix de k , implique $p \nmid b_0 c_k$ et pour tout i ($1 \leq i \leq k$), $p | b_i c_{k-i}$; donc $p \nmid a_k$, ce qui est contraire aux hypothèses. On en conclut que f est irréductible dans $A[X]$.

Revenons au polynôme $f = c(f)f_1$; d'après ce qui précède, les conditions (5.18) impliquent que le polynôme primitif f_1 est irréductible dans $A[X]$, donc est irréductible dans $K[X]$ (Prop. 5.108.); l'élément $c(f) \neq 0$ dans A est une unité dans K , par suite f est irréductible dans $K[X]$. $\square$

Exemple 5.113. Dans $\mathbb{Z}[X]$, le polynôme $X^5 + 4X^3 + 12X + 2$ est unitaire, donc primitif et on vérifie qu'il est irréductible, en appliquant le Critère d'Eisenstein, avec $p = 2$.

7. Exercices

Rappel de notations générales : A étant un anneau unitaire, commutatif, on pose $A^* = A \setminus \{0\}$ et U_A désigne le groupe des éléments inversibles (ou unités) de A ; pour tout $x \in A$, on note (x) l'idéal de A engendré par x .

1) On considère l'anneau $\mathbb{Z}/30\mathbb{Z}$.

1°) L'anneau $\mathbb{Z}/30\mathbb{Z}$ est-il un domaine principal ? (Déf. 2.7)

2°) Déterminer les idéaux de $\mathbb{Z}/30\mathbb{Z}$. Quels sont ceux qui sont maximaux ?

3°) Déterminer le groupe des unités de $\mathbb{Z}/30\mathbb{Z}$.

2) Soit $f(X) = X^2 + aX + b$ un polynôme de $\mathbb{Z}[X]$, sans racine réelle. Soit $\alpha \in \mathbb{C}$ une racine de $f(X)$. On pose :

$$\mathbb{Z}[\alpha] := \{x + y\alpha; (x, y) \in \mathbb{Z} \times \mathbb{Z}\}$$

$$\mathbb{Q}[\alpha] := \{u + v\alpha; (u, v) \in \mathbb{Q} \times \mathbb{Q}\}.$$

1°) Justifier la propriété : $\mathbb{Z}[\alpha]$ est un domaine d'intégrité.

Prouver que $\mathbb{Q}[\alpha]$ est un sous-corps de $\mathbb{C}$.

2°) Démontrer que $\mathbb{Q}[\alpha]$ est le corps des fractions de $\mathbb{Z}[\alpha]$ contenu dans $\mathbb{C}$.

3) Soit a, b, c, d dans $\mathbb{Z}^*$ tels que $ad - bc = \pm 1$.

Démontrer que pour tout couple (m, n) d'éléments non nuls de $\mathbb{Z}$, on a

$$m \wedge n = (am + cn) \wedge (bm + dn).$$

4) Vérifier que les p.g.c.d. existent dans un D.I. dans lequel tout idéal de type fini est principal (Voir plus loin, l'Ex. 26); en déduire que dans un tel D.I., on peut appliquer la relation de Bezout (Cf. Rem. 5.50.).

5) Démontrer la proposition 5.83. (Voir les preuves des propositions A.35. et A.36., App. A).

6) Autre démonstration du Théorème des restes chinois (Th. 2.47.).

Soit m et n des entiers premiers entre eux dans $\mathbb{Z}$. Etant donné a et b dans $\mathbb{Z}$, il s'agit de montrer qu'il existe $x \in \mathbb{Z}$ tel que

$$x \equiv a \pmod{m} \quad \text{et} \quad x \equiv b \pmod{n}.$$

a) Justifier l'existence de u et v dans $\mathbb{Z}$, tels que $um + vn = 1$.

b) A partir de l'égalité $a - b = (um + vn)(a - b)$, trouver h et k dans $\mathbb{Z}$, vérifiant $a + hm = b + kn$, et conclure.

7) Soit f un polynôme primitif dans $\mathbb{Z}[X]$ et $\frac{p}{q} \in \mathbb{Q}^*$ tel que $p \wedge q = 1$.

Démontrer que si $f = \sum_{1 \leq i \leq n} a_i X^i$, alors $f(\frac{p}{q}) = 0$ implique $p|a_0$ et $q|a_n$.

8) Soit K un corps et $f(X) \in K[X] \setminus K$ tel que

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

On pose $g(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n.$

Démontrer que si $f(X)$ est irréductible dans $K[X]$, alors il en est de même de $g(X)$.

- 9) A étant un anneau factoriel, prouver que le polynôme $f(X) = Y^3 + X^2Y^2 + X^3Y + X$ est irréductible dans $A[X, Y]$.
(Utiliser le critère d'Eisenstein)

- 10) Soit $I := \{f(X) = \sum_{1 \leq i \leq n} a_i X^i \in \mathbb{Z}[X], \text{ où } a_0 \in 2\mathbb{Z}\}$.

1°) Prouver que I est un idéal propre, non principal de $\mathbb{Z}[X]$.

2°) a) Montrer que (X) est un idéal premier, non maximal dans $\mathbb{Z}[X]$.

b) Prouver que (Y) est un idéal premier, non maximal dans $\mathbb{Q}[X, Y]$ (Considérer le quotient $\mathbb{Q}[X, Y]/(Y)$).

- 11) Soit q un nombre premier dans $\mathbb{Z}$ et $r \in \mathbb{N}^*$. On note π la surjection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/q^r\mathbb{Z}$.

1°) Montrer que $\mathbb{Z}/q^r\mathbb{Z}$ est un anneau local, dont l'unique idéal maximal est $\pi(q\mathbb{Z})$.

2°) On pose $\bar{M} = \pi(q\mathbb{Z})$, prouver que $\bigcap_{n \in \mathbb{N}} \bar{M}^n = (\bar{0})$, où $(\bar{0})$ est l'idéal nul de $\mathbb{Z}/q^r\mathbb{Z}$.

- 12) Pour tout $\frac{p}{q} \in \mathbb{Q}^*$, on supposera $p \wedge q = 1$. On pose

$$S := \left\{ \frac{p}{q} \in \mathbb{Q}^*; q \text{ impair} \right\} \cup \{0\}.$$

1°) Vérifier que S est un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$.

2°) Prouver que S est un anneau local, dont l'unique idéal maximal est

$$\mathcal{M} = \left\{ \frac{p}{q} \in \mathbb{Q}^*; p \text{ pair et } q \text{ impair} \right\} \cup \{0\}.$$

En déduire que $S/\mathcal{M} \simeq \mathbb{Z}/2\mathbb{Z}$.

3°) Démontrer que pour x, y, z dans le corps $\mathbb{Q}$,

$$x^2 + y^2 + z^2 = 1 \implies x, y, z \text{ dans } S.$$

- 13) Soit A un domaine d'intégrité.

1°) Etant donné, dans A , des éléments $c_0, c_1, \dots, c_n$ deux à deux distincts et des éléments quelconques $d_0, d_1, \dots, d_n$, où $n \in \mathbb{N}$, démontrer qu'il existe, *au plus*, un polynôme $f(X) \in A[X]$ tel que

$$\deg(f) = n+1 \quad \text{et} \quad \forall i (0 \leq i \leq n), f(c_i) = d_i. \quad (5.19)$$

2°) Montrer que dans le cas où A est un corps K , alors il existe un *unique* polynôme $f(X)$ satisfaisant aux conditions (5.19) et que

$$f(X) = \sum_{0 \leq i \leq n} \frac{(X - c_0)(X - c_1) \dots (X - c_{i-1})(X - c_{i+1}) \dots (X - c_n)}{(c_i - c_0)(c_i - c_1) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_i - c_n)} d_i.$$

L'égalité ci-dessus est connue sous le nom de "Formule d'interpolation de Lagrange".

- 14) Soit $\mathbb{Z}[i]$ l'anneau des entiers de Gauss.

1°) On note U le groupe des éléments inversibles de $\mathbb{Z}[i]$.

Déterminer les éléments de U ; en déduire que si q est un élément premier dans $\mathbb{Z}[i]$, alors $-q, iq$ et $-iq$ sont aussi des éléments premiers dans $\mathbb{Z}[i]$.

2°) Montrer, par quelques exemples, qu'il existe des nombres premiers $p \in \mathbb{Z}$ de la forme $p = a^2 + b^2$, $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ et qu'il existe aussi dans $\mathbb{Z}$, des nombres premiers qui ne sont pas de cette forme. On entend par *nombre premier*, un entier $p > 0$, premier dans $\mathbb{Z}$ (Cf. App. A).

3°) Soit p un nombre premier dans $\mathbb{Z}$.

a) Prouver que

$$p = a^2 + b^2 \text{ dans } \mathbb{Z} \implies p \text{ non premier dans } \mathbb{Z}[i].$$

b) Démontrer que p est premier dans $\mathbb{Z}[i]$ si et seulement si p n'est pas une somme de deux carrés dans $\mathbb{Z}$.

4°) Soit $q = a + bi$ dans $\mathbb{Z}[i]$, avec $a \neq 0$ et $b \neq 0$.

a) En désignant par $\bar{q}$ l'imaginaire conjugué de q dans $\mathbb{C}$, vérifier que

$$q \text{ premier dans } \mathbb{Z}[i] \iff \bar{q} \text{ premier dans } \mathbb{Z}[i].$$

b) Démontrer que, pour a et b non nuls dans $\mathbb{Z}$,

$$a^2 + b^2 \text{ premier dans } \mathbb{Z} \implies q = a + bi \text{ premier dans } \mathbb{Z}[i].$$

c) Pour quelles valeurs de a et b , non nuls dans $\mathbb{Z}$, $a + bi$ et $a - bi$ sont-ils des éléments premiers associés dans $\mathbb{Z}[i]$?

d) Prouver que $q = a + bi$, où a et b sont non nuls dans $\mathbb{Z}$, est premier dans $\mathbb{Z}[i]$ si et seulement si $a^2 + b^2$ est premier dans $\mathbb{Z}$.

5°) Utiliser l'algorithme d'Euclide pour trouver un p.g.c.d. de $17 - 7i$ et $3 + 11i$ dans $\mathbb{Z}[i]$. En déduire une factorisation de $17 - 7i$ et de $3 + 11i$ en un produit d'éléments premiers de $\mathbb{Z}[i]$.

15) Soit $j = \exp \frac{2i\pi}{3}$ dans le corps des nombres complexes $\mathbb{C}$. On pose :

$$\mathbb{Z}[j] := \{a + bj : (a, b) \in \mathbb{Z} \times \mathbb{Z}\}.$$

1°) Justifier la propriété : $\mathbb{Z}[j]$ est un domaine d'intégrité.

2°) Pour $z = a + bj$ dans $\mathbb{Z}[j]$, calculer $z\bar{z}$, où $\bar{z}$ est l'imaginaire conjugué de z dans $\mathbb{C}$. Vérifier que $z\bar{z} \in \mathbb{N}$ et $(z\bar{z} = 0 \iff z = 0)$.

3°) On considère l'application



$$\delta : \mathbb{Z}[j] \longrightarrow \mathbb{N}$$

$$z \longmapsto z\bar{z}.$$

Démontrer que $\mathbb{Z}[j]$ est un anneau euclidien dont le stathme est défini par δ . [Pour définir la division euclidienne dans $\mathbb{Z}[j]$, utiliser la même méthode que dans le cas de l'anneau de Gauss, $\mathbb{Z}[i]$ (Cf. Exemple 5.75.)].

16) On considère l'anneau euclidien $\mathbb{Z}[j]$ défini dans l'exercice 15) précédent.

1°) On note U le groupe des éléments inversibles de $\mathbb{Z}[j]$. Caractériser et déterminer les éléments de U .

2°) Soit $z \in \mathbb{Z}[j]$; justifier les propriétés suivantes :

a) z premier dans $\mathbb{Z}[j] \iff \bar{z}$ premier dans $\mathbb{Z}[j]$.

b) $\delta(z)$ premier dans $\mathbb{Z} \implies z$ premier dans $\mathbb{Z}[j]$.

c) $1 - j$ est premier dans $\mathbb{Z}[j]$.

En déduire que 3 n'est pas premier dans $\mathbb{Z}[j]$.

3°) On désigne par q un élément premier de $\mathbb{Z}[j]$.

a) Prouver qu'il existe un nombre premier $p \in \mathbb{Z}$ tel que q divise p dans $\mathbb{Z}[j]$ et qu'alors

$$\delta(q) = p \text{ ou } \delta(q) = p^2.$$

b) Démontrer que pour un nombre premier $p \in \mathbb{Z}$, les trois conditions suivantes sont équivalentes :

i) il existe q premier dans $\mathbb{Z}[j]$ tel que $\delta(q) = p$;

ii) il existe $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ tel que $p = a^2 + b^2 - ab$;

iii) p n'est pas premier dans $\mathbb{Z}[j]$.

• Trouver quelques exemples de nombres premiers p vérifiant la condition ii) et dans chaque cas, donner (à une unité multiplicative près) un élément $q \in \mathbb{Z}[j]$ tel que $\delta(q) = p$.

- Prouver que pour un nombre premier $p \in \mathbb{Z}$, on a :

$$p \text{ non premier dans } \mathbb{Z}[j] \text{ et } p \neq 3 \implies p \equiv 1 \pmod{3} \text{ dans } \mathbb{Z}.$$

Indication : Calculer $4p$ à partir de la condition ii).

- En déduire que pour un nombre premier $p \in \mathbb{Z}$, on a :

$$p \equiv 2 \pmod{3} \text{ dans } \mathbb{Z} \implies p \text{ premier dans } \mathbb{Z}[j].$$

Donner quelques exemples de tels nombres premiers.

c) Montrer que si p est un nombre premier dans $\mathbb{Z}$ et s'il existe un élément q premier dans $\mathbb{Z}[j]$ tel que $\delta(q) = p^2$, alors :

$$p \text{ est premier dans } \mathbb{Z}[j] \text{ et } (q = \pm p \text{ ou } \pm jp \text{ ou } \pm j^2 p).$$

4°) En conclusion, prouver que z est un élément premier dans $\mathbb{Z}[j]$ si et seulement si :

- soit : $\delta(z) = p$, p étant premier dans $\mathbb{Z}$ et non premier dans $\mathbb{Z}[j]$,

- soit : $\delta(z) = p^2$, p étant, à la fois, premier dans $\mathbb{Z}$ et premier dans $\mathbb{Z}[j]$.

17) On suppose connues les propriétés de l'anneau $\mathbb{Z}[j]$ vues dans les exercices 15) et 16) précédents.

On note J l'idéal de $\mathbb{Z}[j]$ engendré par l'élément $1 - j$.

1°) Prouver que

a) $\mathbb{Z}[j]/J$ est un corps ;

b) 3 est associé à $(1 - j)^2$ dans $\mathbb{Z}[j]$.

2°) En considérant le diagramme :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\mu} & \mathbb{Z}[j] \\ \pi \downarrow & & \downarrow \sigma \\ \mathbb{Z}/3\mathbb{Z} & \xrightarrow{\quad} & \mathbb{Z}[j]/J \end{array}$$

où π et σ sont les surjections canoniques, démontrer que le corps $\mathbb{Z}[j]/J$ est isomorphe au corps $\mathbb{Z}/3\mathbb{Z}$.

18) En application de l'étude de l'anneau $\mathbb{Z}[j]$ faite dans les exercices 15) à 17) ci-dessus, on peut prouver qu'il est impossible de trouver x, y, z dans $\mathbb{Z}$ tels que $xyz \neq 0$ et

$$x^3 + y^3 + z^3 = 0. \quad (5.20)$$

La méthode proposée consiste à montrer que l'équation (5.20) n'a pas de solution non nulle en x, y, z , dans $\mathbb{Z}[j]$.

En vue de faire un raisonnement par l'absurde, on suppose qu'il existe x, y, z non nuls dans $\mathbb{Z}[j]$ vérifiant l'équation (5.20).

1°) Vérifier que l'on peut supposer x, y, z deux à deux premiers entre eux dans $\mathbb{Z}[j]$; c'est cette hypothèse que l'on fera pour la suite.

2°) On pose $\rho = x + y$, $\sigma = y + z$, $\tau = z + x$.

a) Vérifier que $(\rho + \sigma + \tau)^3 = 24\rho\sigma\tau$.

b) Moyennant les résultats des exercices 15) à 17) précédents, montrer que dans $\mathbb{Z}[j]$, $1 - j$ divise ρ ou σ ou τ et par suite, divise x ou y ou z .

Pour la suite, on suppose que $1 - j$ divise z .

3°) On pose $\alpha = x + jy$, $\beta = jx + y$, $\gamma = j^2(x + y)$.

a) Vérifier que $\alpha\beta\gamma = -z^3$.

En déduire que $1 - j$ divise chacun des éléments α, β, γ dans $\mathbb{Z}[j]$.

b) On pose $\alpha = (1 - j)\alpha'$, $\beta = (1 - j)\beta'$, $\gamma = (1 - j)\gamma'$.

Prouver que α', β', γ' sont des représentants des trois éléments de $\mathbb{Z}[j]/(1 - j)$ (Cf. Ex. 17)).

En déduire qu'un seul de ces trois éléments est divisible par $1 - j$ dans $\mathbb{Z}$.

c) Prouver que α', β', γ' sont deux à deux premiers entre eux dans $\mathbb{Z}[j]$.

4°) a) Vérifier que $\alpha' + \beta' + \gamma' = 0$.

b) Démontrer qu'il existe un entier $k \geq 2$ et $z_0 \in \mathbb{Z}[j]$ tels que

$$-z = (1-j)^k z_0 \quad \text{et} \quad (1-j) \wedge z_0 = 1.$$

Vérifier que chacun des éléments α', β', γ' est un cube dans $\mathbb{Z}[j]$.

En déduire une solution non nulle (x', y', z') de l'équation (5.20) dans $\mathbb{Z}[j]$, où les éléments x', y', z' sont deux à deux premiers entre eux et $(1-j)^{k-1}$ divise z' dans $\mathbb{Z}[j]$.

5°) Montrer, qu'en réitérant le processus à partir de (x', y', z') comme on l'a fait à partir de la solution (x, y, z) , on aboutit, après un nombre fini d'opérations, à une contradiction avec le résultat du 2°), b) et conclure.

19) 1°) Soit A un D.I. et $f(X) \in A[X]$ tel que $\deg f = n > 0$; on pose

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i.$$

Etant donné $b \in A$, on considère : $f(X-b) := \sum_{0 \leq i \leq n} a_i (X-b)^i$.

Prouver que dans l'anneau $A[X]$:

$$f(X) \text{ irréductible} \iff f(X-b) \text{ irréductible}.$$

2°) Soit $f(X) = \sum_{0 \leq i \leq 4} X^i$ dans $\mathbb{Z}[X]$. En considérant $f(X+1)$, montrer que $f(X)$ est irréductible dans $\mathbb{Z}[X]$.

3°) Pour tout entier $n > 0$, on pose $q_n(X) = \sum_{0 \leq i \leq n} X^i$. Calculer $q_n(X+1)$; en déduire que, pour $n > 0$ et $n+1$ premier, $q_n(X)$ est irréductible dans $\mathbb{Z}[X]$.

20) *Caractérisation des idéaux premiers de $\mathbb{Z}[X]$.*

1°) Justifier l'assertion : (0) est un idéal premier dans $\mathbb{Z}[X]$.

Dans toute la suite, on suppose que P est un idéal premier, non nul de $\mathbb{Z}[X]$.

2°) Prouver que

- soit, $\mathbb{Z} \cap P = (0)$,

- soit, il existe un nombre premier $p \in \mathbb{Z}$ tel que $\mathbb{Z} \cap P = p\mathbb{Z}$.

3°) On suppose que $\mathbb{Z} \cap P = (0)$.

a) Montrer qu'il existe, dans P , au moins un polynôme $f_1(X)$, de degré minimum, primitif dans $\mathbb{Z}[X]$.

b) Démontrer que le polynôme $f_1(X)$ est irréductible dans $\mathbb{Z}[X]$.

c) Soit $g(X) \in \mathbb{Z}[X]$. Démontrer qu'il existe $q(X), r(X)$ dans $\mathbb{Z}[X]$ et $a \in \mathbb{Z}$ tels que

$$ag(X) = f_1(X)q(X) + r(X) \quad \text{et} \quad (r(X) = 0 \quad \text{ou} \quad \deg r < \deg f_1).$$

d) En déduire que $P \neq (0)$ est un idéal premier de $\mathbb{Z}[X]$, tel que $\mathbb{Z} \cap P = (0)$ si et seulement si P est engendré par un polynôme primitif et irréductible dans $\mathbb{Z}[X]$.

4°) On suppose $\mathbb{Z} \cap P = p\mathbb{Z}$, où $p > 0$ est premier dans $\mathbb{Z}$.

Soit π la surjection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ qui se prolonge naturellement en

$$\hat{\pi} : \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X].$$

Pour tout $f(X) \in \mathbb{Z}[X]$, on pose $\bar{f}(X) = \hat{\pi}(f(X))$; alors,

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i \implies \bar{f}(X) = \sum_{0 \leq i \leq n} \bar{a}_i X^i, \quad \text{où } \bar{a}_i = \pi(a_i).$$

a) Vérifier que $\text{Ker } \hat{\pi} \subseteq P$ et que $(\mathbb{Z}/p\mathbb{Z})[X]$ est un domaine principal.

b) Soit I un idéal de $\mathbb{Z}[X]$ contenant $\text{Ker } \hat{\pi}$. Vérifier que pour un polynôme $g(X)$ dans $\mathbb{Z}[X]$, on a

$$\bar{g}(X) \in \hat{\pi}(I) \implies g(X) \in I.$$

c) Démontrer que la correspondance $P \rightarrow \hat{\pi}(P)$ définit une bijection de l'ensemble des idéaux premiers de $\mathbb{Z}[X]$ tels que $\mathbb{Z} \cap P = p\mathbb{Z}$ sur l'ensemble des idéaux premiers de $(\mathbb{Z}/p\mathbb{Z})[X]$.

- d) Prouver que P est un idéal premier de $\mathbb{Z}[X]$ tel que $\mathbb{Z} \cap P = p\mathbb{Z}$ si et seulement si :
 -soit, $P = p\mathbb{Z}$,
 -soit, il existe $k(X) \in \mathbb{Z}[X]$ tel que $\bar{k}(X)$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ et P est l'idéal de $\mathbb{Z}[X]$ engendré par p et $k(X)$.

21) Soit A un D.I. qui n'est pas un corps.

1°) a) Démontrer que les conditions suivantes sont équivalentes :

i) r est un élément premier de A .

ii) r est élément irréductible de A et pour tout $a \in A$, $(a) \cap (r)$ est un idéal principal de A ; de plus si r ne divise pas a , alors $(a) \cap (r) = (ar)$.

b) Prouver que si A est un D.I. dans lequel l'intersection de deux idéaux principaux est un idéal principal, alors tout élément irréductible de A est premier (Retrouver ainsi le Th. 5.23.).

2°) Compte tenu de ce qui précède, vérifier qu'un domaine d'intégrité A est un anneau factoriel si et seulement si A vérifie les deux conditions suivantes :

(AF_1) : Tout $a \in A^* \setminus U_A$ est produit d'éléments irréductibles de A .

$(AF_2)''$: L'intersection de deux idéaux principaux est un idéal principal.

3°) Démontrer qu'un domaine d'intégrité A est un anneau factoriel si et seulement s'il satisfait aux deux conditions suivantes :

$(AF_1)'$: L'ensemble des idéaux principaux de A (ordonné par l'inclusion) vérifie la C.C.A. (Cf. Déf. 2.78.)

$(AF_2)''$: voir le 2°) ci-dessus.

22) On dit qu'un anneau unitaire, commutatif A est un *anneau de Jacobson* (en abrégé, un J-anneau) si tout idéal premier de A est l'intersection de tous les idéaux maximaux qui le contiennent.

1°) Vérifier les propriétés suivantes :

a) Tout corps est un J-anneau.

b) Un anneau local, intègre, qui n'est pas un corps, n'est pas un J-anneau.

c) L'anneau $\mathbb{Z}$ est un J-anneau.

2°) a) Soit $p_1, p_2, \dots, p_k$ des nombres premiers dans $\mathbb{Z}$, $k \geq 1$. On pose

$$A := \left\{ \frac{m}{n} \in \mathbb{Q} ; \forall i (1 \leq i \leq k), p_i \nmid n \right\};$$

Si $m \neq 0$, on suppose $m \wedge n = 1$.

Démontrer que A est un domaine principal contenant $\mathbb{Z}$, mais n'est pas un J-anneau.

b) Démontrer que tout D.P. ayant une infinité d'idéaux premiers est un J-anneau. Prouver alors, que pour tout corps K , l'anneau $K[X]$ est un J-anneau.

3°) a) Démontrer qu'un anneau unitaire, commutatif A est un J-anneau si et seulement si, quel que soit l'idéal I de A , A/I est un J-anneau.

b) Montrer (par un contre-exemple, voir le 1°) que si A est un anneau unitaire, commutatif et s'il existe un idéal I de A tel que A/I est un J-anneau alors A n'est pas nécessairement un J-anneau.

4°) Démontrer qu'un anneau unitaire, commutatif A est un J-anneau si et seulement si, pour tout idéal premier P de A , quel que soit $x \in A \setminus P$, il existe un idéal maximal M de A tel que $P \subseteq M$ et $x \notin M$.

23) Soit A un anneau unitaire, commutatif ; on suppose que A n'est pas un corps. On désigne par $\mathcal{P}$ un idéal premier, non nul de $A[X]$ et on pose $P = \mathcal{P} \cap A$.

1°) Vérifier que P est un idéal premier de A .

On suppose dans la suite $P \neq \{0\}$ et on note $P[X]$ l'ensemble des polynômes de $A[X]$ dont tous les coefficients sont dans P .

2°) Démontrer que $P[X]$ est un idéal premier de $A[X]$ tel que

$$P \subsetneq P[X] \subsetneq \mathcal{P}.$$

Dans les questions 3°) et 4°) qui suivent, on suppose $P[X] \subsetneq \mathcal{P}$.

3°) Soit π la surjection canonique $A \rightarrow A/P$. Pour tout $a \in A$, on pose $\bar{a} = \pi(a)$ et $\bar{\pi}$ désigne le morphisme de $A[X]$ dans $A/P[X]$ prolongeant π (Cor. 4.8.).

Pour tout $f(X) \in A[X]$, on pose $\bar{f}(X) = \bar{\pi}(f(X))$.

a) Déterminer $\text{Ker } \bar{\pi}$.

On pose $\bar{\mathcal{P}} = \bar{\pi}(\mathcal{P})$; démontrer que $\bar{\mathcal{P}}$ est un idéal premier de $A/P[X]$.

b) Soit F le corps des fractions de $A/P[X]$; justifier l'existence de F .

Soit γ l'injection canonique $A/P \rightarrow F$ et $\Gamma: A/P[X] \rightarrow F[X]$ le morphisme prolongeant γ et permettant d'identifier $A/P[X]$ à un sous-anneau de $F[X]$.

$\bar{\mathcal{P}}$ étant ainsi identifié à $\Gamma(\bar{\mathcal{P}})$, on note $(\bar{\mathcal{P}})$ l'idéal de $F[X]$ engendré par $\bar{\mathcal{P}}$.

Démontrer que $(\bar{\mathcal{P}})$ est un idéal premier de $F[X]$; en déduire qu'il existe un polynôme noté $\bar{r}(X)$, irréductible dans $F[X]$ tel que $(\bar{\mathcal{P}}) = \bar{r}(X)F[X]$ et

$$\bar{r}(X) = \sum_{0 \leq i \leq d} \bar{c}_i X^i, \text{ où } d \in \mathbb{N}^*, \forall i (1 \leq i \leq d), \bar{c}_i \in A/P \text{ et } \bar{c}_d \neq 0. \quad (5.21)$$

4°) Soit $h(X) \in A[X]$ et $r(X) \in \bar{\pi}^{-1}(\bar{r}(X))$, prouver que les deux conditions suivantes sont équivalentes :

i) $h(X) \notin \mathcal{P}$.

ii) Il existe $a \in A$, $u(X)$ et $v(X)$ dans $A[X]$ tels que

$$a \notin P, u(X)h(X) + v(X)r(X) \equiv a \pmod{P[X]}. \quad (5.22)$$

5°) On suppose, dans cette question, que A (qui n'est pas un corps) est un J-anneau (Cf. Ex. 22, ci-dessus) et on se propose de montrer que $A[X]$ est aussi un J-anneau. Les notations sont celles des questions précédentes.

$\mathcal{P}$ étant un idéal premier de $A[X]$, soit $h(X) \in A[X] \setminus \mathcal{P}$ et $\bar{h}(X) = \bar{\pi}(h(X))$.

a) 1^{er} cas : $\mathcal{P} = P[X]$; démontrer qu'il existe un idéal maximal $\bar{M}$ de $A[X]/P[X]$ tel que $\bar{h}(X) \notin \bar{M}$.

b) 2^{ème} cas : $P[X] \subsetneq \mathcal{P}$; prouver qu'il existe un idéal $\mathcal{M}$ de A tel que

$$\mathcal{P} \cap A = P \subsetneq \mathcal{M} \quad \text{et} \quad ac_d \notin \mathcal{M},$$

(c_d et a étant définis par les relations (5.21) et (5.22).

Soit Q l'idéal de $A[X]$ engendré par $\mathcal{M}$ et $r(X)$; démontrer que $Q \cap A = \mathcal{M}$.

c) Soit M un idéal maximal de $A[X]$ contenant Q , vérifier que $ac_d \notin M$.

d) Prouver que $A[X]$ est un J-anneau (Cf. Ex. 22, 4°), ci-dessus).

24) Soit A un anneau euclidien relativement à un stathme δ .

1°) Justifier l'existence d'un élément $x \in A^* \setminus U_A$ tel que $\delta(x)$ soit *minimal*.

Pour un tel élément x , on considère l'anneau quotient $A/(x)$ et on note π la surjection canonique $A \rightarrow A/(x)$; pour tout $a \in A$, on pose $\pi(a) := \bar{a}$.

2°) Prouver que pour tout $a \in A$, on a

$$\bar{a} = \bar{0} \quad \text{ou} \quad \bar{a} = \bar{r}, \text{ avec } r \in U_A. \quad (5.23)$$

En déduire que la restriction de π à $U_A \cup \{0\}$ est surjective.

Montrer que $A/(x)$ est un corps. Que peut-on en conclure pour l'idéal (x) ?

25) $\mathbb{R}$ désigne le corps des nombres réels. Dans $\mathbb{R}[X, Y]$, on considère le polynôme $X^2 + Y^2 + 1$. On note I l'idéal de $\mathbb{R}[X, Y]$ engendré par $X^2 + Y^2 + 1$.

1°) Prouver que l'anneau quotient $A := \mathbb{R}[X, Y]/I$ est un D.I.

2°) Soit π la surjection canonique : $\mathbb{R}[X, Y] \longrightarrow A$.

a) Montrer que pour tout $n \in \mathbb{N}$, il existe un représentant de Y^{2n} modulo I dans $\mathbb{R}[X]$ et un représentant de Y^{2n+1} modulo I dans $Y\mathbb{R}[X]$.

b) On pose $\bar{X} := \pi(X)$ et $\bar{Y} := \pi(Y)$.

Démontrer que pour tout polynôme $p(X, Y) \in \mathbb{R}[X, Y]$, il existe un unique couple (f, g) de polynômes à une indéterminée sur $\mathbb{R}$ tel que

$$\pi(p(X, Y)) = f(\bar{X}) + \bar{Y}g(\bar{X}).$$

3°) $\mathbb{C}$ désigne le corps des nombres complexes.

a) Montrer que la donnée d'un morphisme de $\mathbb{R}$ -algèbres de $A = \mathbb{R}[X, Y]/I$ dans $\mathbb{C}$ équivaut à la donnée d'un couple $(x, y) \in \mathbb{C} \times \mathbb{C}$ tel que $x^2 + y^2 + 1 = 0$.

En déduire qu'il existe une infinité de tels morphismes.

b) Démontrer que $U_A = \mathbb{R}^*$.

c) En utilisant la conclusion de l'exercice 21) ci-dessus, prouver que le D.I. $A = \mathbb{R}[X, Y]/I$ n'est pas euclidien.

26) Soit $\mathbb{Q}$ le corps des nombres rationnels. On désigne par $\mathbb{Q}_{\mathbb{Z}}[X]$ l'ensemble des polynômes de $\mathbb{Q}[X]$ dont le terme constant appartient à $\mathbb{Z}$.

Vérifier que $\mathbb{Q}_{\mathbb{Z}}[X]$ est un sous-anneau unitaire de $\mathbb{Q}[X]$ et donc un D.I.

Le but de ce problème est de prouver que les *p.g.c.d.* et *p.p.c.m.* existent dans $\mathbb{Q}_{\mathbb{Z}}[X]$ (Cf. Rem. 5.33.), alors que $\mathbb{Q}_{\mathbb{Z}}[X]$ n'est pas un anneau factoriel.

1°) Soit $f_0(X)$ et $g_0(X)$ deux polynômes non nuls dans $\mathbb{Q}_{\mathbb{Z}}[X]$ et premiers entre eux dans $\mathbb{Q}[X]$.

a) Soit a et b les termes constants, respectivement, de f_0 et g_0 . On pose :

$$f_0(X) = f_1(X) + a, \quad g_0(X) = g_1(X) + b.$$

Vérifier que $f_1(X)$ et $g_1(X)$ sont dans $\mathbb{Q}_{\mathbb{Z}}[X]$ et que l'un, au moins, des entiers a et b est non nul.

b) Justifier l'existence de deux polynômes $m(X)$ et $n(X)$ dans $\mathbb{Q}_{\mathbb{Z}}[X]$ et d'un entier $k \in \mathbb{Z}^*$ tels que

$$m(X)f_0(X) + n(X)g_0(X) = k.$$

c) Si $ab \neq 0$, on pose : $c = a \wedge b$ dans $\mathbb{Z}$.

Si $ab = 0$, on désigne par c celui des entiers a et b qui n'est pas nul.

Démontrer que c divise k dans $\mathbb{Z}$.

d) On note $\langle f_0, g_0 \rangle$ l'idéal de $\mathbb{Q}_{\mathbb{Z}}[X]$ engendré par $f_0(X)$ et $g_0(X)$. Montrer que a et b appartiennent à l'idéal $\langle f_0, g_0 \rangle$.

En déduire que $\langle f_0, g_0 \rangle = \langle c \rangle$, où $\langle c \rangle$ est l'idéal de $\mathbb{Q}_{\mathbb{Z}}[X]$ engendré par c .

2°) Soit $f(X)$ et $g(X)$ deux polynômes non nuls de $\mathbb{Q}_{\mathbb{Z}}[X]$ et $d(X)$ un diviseur commun à $f(X)$ et $g(X)$ dans $\mathbb{Q}_{\mathbb{Z}}[X]$, de degré maximal.

Dans $\mathbb{Q}_{\mathbb{Z}}[X]$, on pose $f(X) = f_0(X)d(X)$, $g(X) = g_0(X)d(X)$.

a) Démontrer que $f_0(X)$ et $g_0(X)$ sont premiers entre eux dans $\mathbb{Q}[X]$.

b) Compte tenu des résultats de la question 1°), montrer que l'idéal $\langle f, g \rangle$ de $\mathbb{Q}_{\mathbb{Z}}[X]$, engendré par $f(X)$ et $g(X)$, est principal. En conclure que dans le domaine d'intégrité $\mathbb{Q}_{\mathbb{Z}}[X]$, deux éléments non nuls quelconques ont un *p.g.c.d.* et par suite, un *p.p.c.m.*

3°) En considérant les égalités :

$$X = \left(\frac{1}{2}X\right)2 = \left(\frac{1}{2^2}X\right)2^2 = \dots$$

prouver que $\mathbb{Q}_Z[X]$ n'est pas un anneau factoriel.

- 27) Soit A un D.I. dans lequel deux éléments non nuls *quelconques* n'ont pas nécessairement un *p.g.c.d.* ni un *p.p.c.m.*.

1°) Soit a et b deux éléments non nuls de A ayant un *p.p.c.m.* noté m .

a) Justifier l'existence de α, β, γ dans A^* tels que $m = a\alpha = b\beta$, $ab = m\gamma$. Démontrer que α et β sont premiers entre eux dans A .

b) Prouver que γ est un *p.g.c.d.* de a et b .

On montre ainsi que dans un D.I. *quelconque*, si deux éléments ont un *p.p.c.m.*, alors ils ont un *p.g.c.d.*; mais la réciproque est fausse, comme le montre l'exemple développé dans la question suivante.

2°) Soit $A := \{k + X^2 f(X); k \in \mathbb{Z}, f(X) \in \mathbb{Z}[X]\}$.

a) Vérifier que A est un sous-anneau unitaire de $\mathbb{Z}[X]$, donc un D.I.

b) Prouver que X^2 et X^3 sont premiers entre eux dans A , donc $X^2 \wedge X^3 = 1$.

Démontrer que, par contre, X^2 et X^3 n'ont pas de *p.p.c.m.* dans A .

Indication : On remarquera que seuls X^5 et $-X^5$ pourraient, a priori, être *p.p.c.m.* de X^2 et X^3 et on prouvera que X^5 n'est pas un *p.p.c.m.* de X^2 et X^3 dans A .

- 28) D'après les résultats du problème 26) ci-dessus, il existe des D.I. qui ne sont pas factoriels et dans lesquels cependant, deux éléments *quelconques* ont un *p.g.c.d.* et un *p.p.c.m.*. Un tel D.I. est appelé un *domaine pseudo-bezoutien*.

1°) Soit A un domaine pseudo-bezoutien ; on suppose que A contient au moins un élément irréductible p .

a) Vérifier que pour $x \in A$, on a $x \notin (p) \iff x \text{ et } p \text{ premiers entre eux}$.

b) Démontrer que p est premier dans A .

2°) A étant un domaine pseudo-bezoutien ; on suppose de plus, que A est *noethérien*.

a) Prouver (en utilisant l'axiome de Zorn) que l'ensemble des idéaux principaux, propres de A contient au moins un élément maximal.

En déduire que l'ensemble des éléments irréductibles de A n'est pas vide.

b) Démontrer que A est un anneau factoriel.

En conclure que l'anneau $\mathbb{Q}_Z[X]$ du problème 26) ci-dessus, n'est pas noethérien.

- 29) Soit $A := K[X, Y, Z]$, où K est un corps.

1°) Démontrer que $X^2 - YZ$ est un polynôme irréductible dans A .

En déduire que l'idéal principal $I := (X^2 - YZ)$ est un idéal premier de A .

2°) On considère l'anneau quotient $B := A/I$; soit π la surjection canonique $A \rightarrow B$.

Prouver que tout élément de B a un *unique* représentant modulo I de la forme :

$$g_0(Y, Z) + X g_1(Y, Z), \text{ où } g_0(Y, Z) \text{ et } g_1(Y, Z) \text{ sont dans } K[Y, Z].$$

3°) Montrer que B est un D.I. dans lequel :

i) $\pi(X)$ n'est pas un élément premier ;

ii) $\pi(X)$ est irréductible ;

iii) $\pi(X)$ et $\pi(Y)$ n'ont pas de *p.p.c.m.*.

En déduire que B n'est pas un anneau factoriel.

Chapitre 6 Localisation

Le processus dit de **localisation** dans les anneaux unitaires, commutatifs, est une généralisation de la construction du corps des fractions d'un domaine d'intégrité (Ch. 5).

Dans ce chapitre, A désigne un anneau unitaire, commutatif.

1. Localisation par une partie multiplicative de A

A. Notion de partie multiplicative

Définition 6.1. Soit S une partie non vide de l'anneau A , on dit que S est une **partie multiplicative** de A si

$$0 \notin S, 1 \in S \quad \text{et} \quad (s, t) \in S \times S \implies st \in S.$$

Cette notion a déjà été utilisée au Chapitre 2 (Ex. 10 et 11).

Exemple 6.2. :

- 1) Si A est un domaine d'intégrité, alors $A^* = A \setminus \{0\}$ est une partie multiplicative de A .
- 2) Dans A , l'ensemble des non diviseurs de zéro est une partie multiplicative. Les non diviseurs de zéro sont aussi appelés les **éléments réguliers** de A . Lorsque A est intègre, les éléments réguliers sont les éléments non nuls.
- 3) Si P est un idéal premier de A , alors $S = A \setminus P$ est une partie multiplicative de A (Ch. 2, Ex. 10).
- 4) Pour tout $x \in A^*$, $S = \{x^n; n \in \mathbb{N}\}$ est une partie multiplicative de A .
- 5) Pour tout idéal non nul I de A , $S = 1 + I = \{1 + x; x \in I\}$ est une partie multiplicative de A .

B. Localisé de A par une partie multiplicative

S désigne une partie multiplicative de A .

1. Relation d'équivalence associée à S

On définit, sur $A \times S$, une relation binaire $\mathcal{R}_S$ par :

$$(a, s) \mathcal{R}_S (a', s') \iff \exists t \in S, t(as' - a's) = 0. \quad (6.1)$$

On remarquera que si A est intègre, on a

$$(a, s) \mathcal{R}_S (a', s') \iff as' - a's = 0. \quad (6.2)$$

Vérifions que $\mathcal{R}_S$ est une relation d'équivalence dans $A \times S$.

Il est immédiat que $\mathcal{R}_S$ est réflexive et symétrique, montrons que $\mathcal{R}_S$ est transitive.

Supposons : $(a, s) \mathcal{R}_S (a', s')$ et $(a', s') \mathcal{R}_S (a'', s'')$.

Il existe alors t et u dans S tels que

$$t(as' - a's) = 0 \quad \text{et} \quad u(a's'' - a''s') = 0.$$

En multipliant les relations ci-dessus, respectivement, par us'' et ts on obtient

$$ut(s''sa' - s''s'a + ss'a'' - ss's'a') = 0,$$

d'où $uts'(sa'' - s'a) = 0$ et par suite $(a, s) \mathcal{R}_S (a'', s'')$.

La classe d'équivalence d'un couple $(a, s) \in A \times S$, modulo $\mathcal{R}_S$, sera notée $\frac{a}{s}$ et appelée **fraction**. L'ensemble quotient

$$(A \times S) / \mathcal{R}_S = \left\{ \frac{a}{s}; (a, s) \in A \times S \right\}$$

sera noté $S^{-1}A$ (dans certains ouvrages, cet ensemble est noté A_S).

2. Structure d'anneau de $S^{-1}A$

On définit les correspondances σ et μ de $S^{-1}A \times S^{-1}A$ dans $S^{-1}A$ par

$$\sigma : \left(\frac{a}{s}, \frac{a'}{s'} \right) \mapsto \frac{as' + a's}{ss'} \quad (6.3)$$

$$\mu : \left(\frac{a}{s}, \frac{a'}{s'} \right) \mapsto \frac{aa'}{ss'}. \quad (6.4)$$

On vérifie que σ et μ sont des applications ; en effet, supposons

$$\frac{b}{t} = \frac{a}{s} \quad \text{et} \quad \frac{b'}{t'} = \frac{a'}{s'} \quad \text{dans } S^{-1}A,$$

donc il existe u et v dans S tels que

$$u(bs - at) = 0 \quad \text{et} \quad v(b's' - a't') = 0;$$

alors, $uv((b't' + b't)ss' - (as' + a's)tt') = uv((bs - at)t's' + (b's' + a't')ts) = 0$,

$$\text{d'où,} \quad \frac{b't' + b't}{tt'} = \frac{as' + a's}{ss'}.$$

D'autre part : $uv(bb'ss' - aa'tt') = uv((bs - at)b's' + (b's' - a't')at) = 0$,

$$\text{d'où,} \quad \frac{bb'}{tt'} = \frac{aa'}{ss'}.$$

Ainsi les applications σ et μ définissent deux lois de composition internes dans $S^{-1}A$ notées, respectivement, additivement et multiplicativement ; on pose :

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'} \quad \text{et} \quad \frac{a}{s} \frac{a'}{s'} := \frac{aa'}{ss'}.$$

Les éléments $\frac{0}{1}$ et $\frac{1}{1}$ sont, respectivement, éléments neutres pour l'addition et la multiplication dans $S^{-1}A$.

L'ensemble $S^{-1}A$ est alors muni d'une structure d'anneau unitaire et commutatif induite par celle de A (à vérifier par le lecteur).

Définition 6.3. S étant une partie multiplicative d'un anneau unitaire, commutatif A , l'anneau $S^{-1}A$ est appelé le **localisé de A par S** .

L'application $\alpha_S : A \longrightarrow S^{-1}A$ telle que $\alpha_S(a) = \frac{a}{1}$ est un morphisme d'anneaux unitaires appelé **morphisme canonique de A dans $S^{-1}A$** .

Proposition 6.4. *Le morphisme canonique $\alpha_S : A \longrightarrow S^{-1}A$ est injectif si et seulement si S est contenu dans l'ensemble des non diviseurs de zéro (ou éléments réguliers) de A .*

Preuve : $a \in \text{Ker}(\alpha_S) \iff \frac{a}{1} = \frac{0}{1} \iff \exists t \in S, ta = 0.$

On en déduit que $\text{Ker}(\alpha_S) = (0)$ si et seulement si

$$\forall t \in S, (a \in A \text{ et } ta = 0) \implies a = 0,$$

c'est-à-dire que tout $t \in S$ est régulier dans A. $\square$

Corollaire 6.5. Si A est intègre, alors pour toute partie multiplicative S de A, le morphisme α_S est injectif.

Remarque 6.6. :

a) Lorsque le morphisme canonique $\alpha_S : A \longrightarrow S^{-1}A$ est injectif, l'anneau A peut être identifié à $\text{Im}(\alpha_S)$; on écrit a à la place de $\frac{a}{1}$ et dans ce cas, A est considéré comme un sous-anneau du localisé $S^{-1}A$.

b) Quels que soient $\frac{a}{s} \in S^{-1}A$ et $t \in S$, on a $\frac{a}{s} = \frac{at}{st}$, car $1 \in S$.

En particulier, pour tout $s \in S$, $\frac{0}{1} = \frac{0}{s} = 0$ et $\frac{1}{1} = \frac{s}{s} = 1$.

Exemple 6.7. :

1) Si A est un D.I. et $S = A^*$, alors $S^{-1}A$ est le corps des fractions de A, noté $\text{Fr}A$, et A est un sous-anneau du corps $\text{Fr}A$ (Déf. 5.2.).

2) Si S_0 désigne l'ensemble des éléments réguliers de l'anneau unitaire, commutatif A, alors $S_0^{-1}A$ est appelé l'anneau total des fractions de A et noté $\text{Fr}A$ (car lorsque A est intègre, $S_0 = A^*$ et $\text{Fr}A$ est le corps des fractions de A). La proposition 6.4. et la remarque 6.6. impliquent que A est un sous-anneau de son anneau total de fractions.

3) Si $S = A \setminus P$, où P est un idéal premier de A, (Exemple 6.2., 3)) alors le localisé $S^{-1}A$ est généralement noté A_P et appelé le localisé de A en P.

En particulier, lorsque A est un D.I., $\text{Fr}A$ est le localisé de A en l'idéal premier (0).

4) $S = \{10^n; n \in \mathbb{N}\}$ est une partie multiplicative de $\mathbb{Z}$ et

$$\mathbb{D} := S^{-1}\mathbb{Z} = \left\{ \frac{a}{10^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

est l'anneau des nombres décimaux.

Proposition 6.8. Lorsque A est un D.I., pour toute partie multiplicative S de A, l'anneau $S^{-1}A$ est un D.I. tel que

$$A \subseteq S^{-1}A \subseteq \text{Fr}A.$$

Preuve : A étant un D.I., toute partie multiplicative S de A est contenue dans A^* , la relation d'équivalence $\mathcal{R}_S$ est alors la restriction à $A \times S$ de la relation $\mathcal{R}$ définie dans $A \times A^*$ pour la construction du corps des fractions de A. On en déduit que tout localisé $S^{-1}A$ est un sous-anneau du corps $\text{Fr}A$, c'est donc un D.I. et $A \subseteq S^{-1}A \subseteq \text{Fr}A$. $\square$

En particulier, l'anneau $\mathbb{D}$ des nombres décimaux (Exemple 6.7.) est un sous-anneau du corps $\mathbb{Q}$ des nombres rationnels.

Théorème 6.9. Propriété universelle du couple $(S^{-1}A, \alpha_S)$

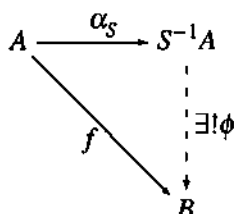
Soit S une partie multiplicative d'un anneau unitaire, commutatif A; alors quels que soient l'anneau unitaire, commutatif B et le morphisme d'anneaux unitaires $f : A \longrightarrow B$ vérifiant la condition : $f(S) \subseteq U_B$, il existe un unique morphisme $\phi \in \text{Hom}(S^{-1}A, B)$ tel que

$$\phi \circ \alpha_S = f, \text{ où } \alpha_S \text{ est le morphisme canonique de A dans } S^{-1}A.$$

U_B désigne l'ensemble des éléments inversibles de l'anneau B.

Le théorème 6.9 exprime que la condition $f(S) \subseteq U_B$ implique l'existence et l'unicité du

diagramme commutatif suivant :



Preuve :

a) *Unicité de ϕ* : on suppose l'existence du morphisme ϕ ;

$$\begin{aligned}
 \forall \frac{a}{s} \in S^{-1}A, \quad \phi\left(\frac{a}{s}\right) &= \phi\left(\frac{a}{1} \frac{1}{s}\right) = \phi\left(\frac{a}{1}\right) \phi\left(\frac{1}{s}\right). \\
 \phi \circ \alpha_S = f &\implies \phi\left(\frac{a}{1}\right) = f(a), \\
 \phi\left(\frac{1}{s}\right) &= 1 = \phi\left(\frac{1}{s}\right) \phi\left(\frac{s}{1}\right) = \phi\left(\frac{1}{s}\right) f(s);
 \end{aligned}$$

Par hypothèse, $f(S) \subseteq U_B$, d'où $\phi\left(\frac{1}{s}\right) = (f(s))^{-1}$ et par suite,

$$\phi\left(\frac{a}{s}\right) = f(a)(f(s))^{-1}. \quad (6.5)$$

On en déduit que si $\psi \in \text{Hom}(S^{-1}A, B)$ est tel que $\psi \circ \alpha_S = f$, alors,

$$\forall \frac{a}{s} \in S^{-1}A, \quad \psi\left(\frac{a}{s}\right) = f(a)(f(s))^{-1} = \phi\left(\frac{a}{s}\right), \quad \text{d'où } \psi = \phi.$$

b) *Existence de ϕ* : ce qui précède conduit à considérer la correspondance $\phi : S^{-1}A \longrightarrow B$ telle que $\phi\left(\frac{a}{s}\right) = f(a)(f(s))^{-1}$.

On vérifie alors que ϕ est une application : on suppose $\frac{a'}{s'} = \frac{a}{s}$ dans $S^{-1}A$, donc il existe $t \in S$ tel que $t(a's - as') = 0$, par suite

$$f(t)f(a')f(s) = f(t)f(a)f(s').$$

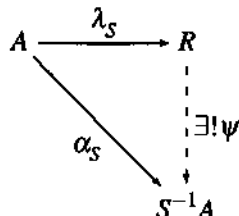
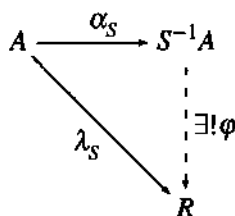
t, s, s' étant dans S , on a $f(t), f(s), f(s')$ dans U_B , d'où

$$f(a')(f(s'))^{-1} = f(a)(f(s))^{-1}.$$

Pour montrer que ϕ est un morphisme d'anneaux unitaires, il suffit de reprendre la preuve faite dans le cas du corps des fractions d'un D.I. (Th. 5.5.). $\square$

Corollaire 6.10. *Etant donné le couple $(S^{-1}A, \alpha_S)$, s'il existe un anneau unitaire, commutatif R , un morphisme $\lambda_S \in \text{Hom}(A, R)$ vérifiant la condition $\lambda_S(S) \subseteq U_R$ et si le couple (R, λ_S) , satisfait à la propriété universelle du couple $(S^{-1}A, \alpha_S)$ (Th. 6.9.), alors il existe un unique isomorphisme ϕ de $S^{-1}A$ sur R tel que $\phi \circ \alpha_S = \lambda_S$.*

Preuve : En appliquant la propriété universelle (Th. 6.9.), respectivement, aux couples $(S^{-1}A, \alpha_S)$ et (R, λ_S) , on obtient les deux diagrammes commutatifs suivants



donc $\varphi \circ \alpha_S = \lambda_S$ et $\psi \circ \lambda_S = \alpha_S$.

On en déduit que $\psi \circ \varphi \circ \alpha_S = \alpha_S$ et $\varphi \circ \psi \circ \lambda_S = \lambda_S$.

La propriété universelle vérifiée par les couples $(S^{-1}A, \alpha_S)$ et (R, λ_S) implique alors : $\psi \circ \varphi = id_{S^{-1}A}$ et $\varphi \circ \psi = id_R$.

Par suite φ est un isomorphisme et $\varphi^{-1} = \psi$. $\square$

Remarque 6.11. Le corollaire 6.10. exprime que pour toute partie multiplicative S de A , le localisé de A par S est unique à un isomorphisme près.

2. Idéaux de $S^{-1}A$

Les notations générales seront celles du paragraphe précédent.

S étant une partie multiplicative de A , pour tout idéal I de A , on pose

$$I_S := \left\{ \frac{a}{s} ; a \in I, s \in S \right\}.$$

Remarque 6.12. :

a) Pour tout idéal propre I de A , on a $S \not\subset I$, car $1 \in S$, donc S n'est pas une partie multiplicative de I , considéré comme sous anneau de A .

b) $\frac{b}{t} \in I_S \iff \exists (a, s) \in I \times S, \frac{a}{s} = \frac{b}{t}$.



Proposition 6.13. Pour tout idéal I de A , I_S est l'idéal de $S^{-1}A$ engendré par $\alpha_S(I)$ et

$$I_S \neq S^{-1}A \iff I \cap S = \emptyset.$$

Inversement, si Q est un idéal de $S^{-1}A$, alors

$$Q = I_S, \text{ où } I := \alpha_S^{-1}(Q) = \left\{ a \in A ; \frac{a}{1} \in Q \right\}.$$

Preuve : Soit $\frac{a}{s}$ et $\frac{a'}{s'}$ dans I_S ; on peut supposer a et a' dans I (Rem. 6.12.). On a $\frac{0}{1} \in I_S$ et $\frac{a}{s} - \frac{a'}{s'} = \frac{as' - a's}{ss'} \in I_S$; de plus, quel que soit $\frac{b}{t} \in S^{-1}A$, $\frac{a}{s} \frac{b}{t} = \frac{ab}{st} \in I_S$, donc I_S est un idéal de $S^{-1}A$.

Désignons par Σ l'idéal de $S^{-1}A$ engendré par $\alpha_S(I)$. Soit $\frac{a}{s} \in I_S$; on suppose $a \in I$, alors,

$$\frac{a}{s} = \frac{a}{1} \frac{1}{s}; \quad \frac{a}{1} = \alpha_S(a) \quad \text{et} \quad \frac{1}{s} \in S^{-1}A, \quad \text{d'où } I_S \subseteq \Sigma.$$

D'autre part, tout $x \in \Sigma$ s'écrit sous la forme

$$x = \sum_{1 \leq i \leq k} \frac{a_i b_i}{1 s_i}, \quad k \in \mathbb{N}^*, \quad \forall i (1 \leq i \leq k), \quad \frac{a_i}{1} \in \alpha_S(I) \text{ et } \frac{b_i}{s_i} \in S^{-1}A.$$

On suppose que pour tout $i (1 \leq i \leq k)$, $a_i \in I$, on a alors $\frac{a_i b_i}{s_i} \in I_S$, d'où $x \in I_S$.

On en conclut que $I_S = \Sigma$. D'autre part,

$$I_S = S^{-1}A \iff \frac{1}{1} \in I_S \iff \exists (a, s) \in I \times S, \frac{a}{s} = \frac{1}{1}.$$

$$\frac{a}{s} = \frac{1}{1} \iff \exists t \in S, t(a - s) = 0$$

$$ta = ts \implies ts \in I \cap S \implies I \cap S \neq \emptyset,$$

$$\text{ainsi, } I_S = S^{-1}A \implies I \cap S \neq \emptyset.$$

$$\text{Mais, } I \cap S \neq \emptyset \implies 1 \in I_S \implies I_S = S^{-1}A, \text{ d'où}$$

$$I_S = S^{-1}A \iff I \cap S \neq \emptyset.$$

$$\text{Ce qui équivaut à } I_S \neq S^{-1}A \iff I \cap S = \emptyset.$$

Soit Q un idéal de $S^{-1}A$; α_S est un morphisme d'anneaux unitaires de A dans $S^{-1}A$, donc $\alpha_S^{-1}(Q)$ est un idéal de A . (Prop. 1.53.)

$$I := \alpha_S^{-1}(Q) = \{a \in A; \frac{a}{1} \in Q\} \implies I_S = \{\frac{a}{s}; \frac{a}{1} \in Q\} \subseteq Q.$$

D'autre part, si $\frac{a}{s} \in Q$, alors $\frac{as}{s1} = \frac{a}{1} \in Q$, car Q est un idéal de $S^{-1}A$.

On en conclut que $I_S = Q$. □

Définition 6.14. Pour un idéal I de A , l'idéal I_S de $S^{-1}A$, considéré ci-dessus, est appelé l'idéal de $S^{-1}A$ engendré par I .

Remarque 6.15. Dans le contexte précédent, pour I et I' , idéaux de A et Q et Q' , idéaux de $S^{-1}A$, on a

$$I \subseteq I' \implies I_S \subseteq I'_S; \quad Q \subseteq Q' \implies \alpha_S^{-1}(Q) \subseteq \alpha_S^{-1}(Q').$$

Théorème 6.16. A étant un anneau unitaire, commutatif, pour toute partie multiplicative S , on a

$$A \text{ noethérien} \implies S^{-1}A \text{ noethérien.}$$

Preuve : Dans l'anneau $S^{-1}A$, les idéaux (0) et $S^{-1}A$ sont principaux, montrons que tout idéal propre, non nul, Q de $S^{-1}A$ est de type fini.

Soit $I := \alpha_S^{-1}(Q)$, I est un idéal de A , donc I est de type fini ; or, d'après la Prop. 6.13., dans $S^{-1}A$, l'idéal Q est engendré par $\alpha_S(I)$, on en déduit que l'idéal Q est de type fini. □

Proposition 6.17. Soit I et J deux idéaux de A ; alors dans $S^{-1}A$, on a :

$$(I + J)_S = I_S + J_S \tag{6.6}$$

$$(IJ)_S = I_S J_S \tag{6.7}$$

$$(I \cap J)_S = I_S \cap J_S. \tag{6.8}$$

Preuve : Soit $a \in I$ et $b \in J$, alors pour tout $s \in S$,

$$\frac{a+b}{s} = (\frac{a}{1} + \frac{b}{1})\frac{1}{s} = \frac{a}{s} + \frac{b}{s},$$

d'où $(I + J)_S \subseteq I_S + J_S$. Réciproquement, soit $\frac{a}{s} \in I_S$ et $\frac{b}{t} \in J_S$; on suppose $a \in I$ et $b \in J$, alors

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in (I + J)_S, \text{ d'où } I_S + J_S \subseteq (I + J)_S.$$

Les deux inclusions obtenues impliquent l'égalité (6.6).

Soit $\frac{a}{s} \in (IJ)_S$; on suppose $a \in IJ$ donc

$$a = \sum_{1 \leq i \leq k} x_i y_i, \quad k \in \mathbb{N}^* \text{ et } \forall i (1 \leq i \leq k), x_i \in I, y_i \in J.$$

$$\frac{a}{s} = \sum_{1 \leq i \leq k} \frac{x_i y_i}{1 \cdot s} \in I_S J_S \implies (IJ)_S \subseteq I_S J_S.$$

D'autre part, soit $x \in I_S J_S$ tel que

$$x = \sum_{1 \leq i \leq k} \frac{a_i b_i}{s_i t_i}, \quad \text{où } k \in \mathbb{N}^*, \forall i (1 \leq i \leq k), \frac{a_i}{s_i} \in I_S \text{ et } \frac{b_i}{t_i} \in J_S.$$

On a alors

$$x = \frac{\sum_{1 \leq i \leq k} (a_i b_i \prod_{j \neq i} s_j t_j)}{\prod_{1 \leq i \leq k} s_i t_i} \in (IJ)_S,$$

donc $I_S J_S \subseteq (IJ)_S$, d'où l'égalité (6.7).

Soit $\frac{a}{s} \in (I \cap J)_S$; on peut supposer $a \in I \cap J$, donc $\frac{a}{s} \in I_S \cap J_S$.

Réciproquement, soit $x \in I_S \cap J_S$; supposons $x = \frac{a}{s} = \frac{b}{t}$, où $a \in I, b \in J, (s, t) \in S \times S$.

Il existe alors $u \in S$ tel que $u(at - bs) = 0$.

$$(aut = bus \in I \cap J) \implies \frac{a}{s} = \frac{aut}{sut} = \frac{bus}{sut} \in (I \cap J)_S,$$

donc $I_S \cap J_S \subseteq (I \cap J)_S$ et on en déduit l'égalité (6.8). □

Proposition 6.18. *Etant donné un idéal I et une partie multiplicative S de A , si π désigne la surjection canonique $A \rightarrow A/I$ et $\bar{S} := \pi(S)$, alors $\bar{S}$ est une partie multiplicative de A/I et*

$$S^{-1}A/I_S \simeq \bar{S}^{-1}(A/I).$$

Preuve : Pour tout $x \in A$, posons $\pi(x) = \bar{x}$; π étant un morphisme d'anneaux unitaires, il est immédiat que $\bar{S}$ est une partie multiplicative de A/I . Considérons la correspondance $f: S^{-1}A \rightarrow \bar{S}^{-1}(A/I)$ telle que $f(\frac{a}{s}) = \frac{\bar{a}}{\bar{s}}$ et montrons que f est une application.

Soit $\frac{a}{s} = \frac{b}{t}$ dans $S^{-1}A$; il existe $z \in S$ tel que $z(at - bs) = 0$ et

$$z(at - bs) = 0 \implies \bar{z}(\bar{a}\bar{t} - \bar{b}\bar{s}) = \bar{0} \implies \frac{\bar{a}}{\bar{s}} = \frac{\bar{b}}{\bar{t}}.$$

On vérifie que f est un morphisme d'anneaux unitaires tel que $I_S \subseteq \text{Ker } f$, et

$$\begin{aligned} \frac{a}{s} \in \text{Ker } f &\iff \frac{\bar{a}}{\bar{s}} = \frac{\bar{0}}{\bar{1}} \iff \exists \bar{z} \in \bar{S} \text{ tel que } \bar{z}\bar{a} = \bar{0} \\ \bar{z}\bar{a} = \bar{0} &\iff \exists z \in S \text{ tel que } za \in I; \\ za \in I &\implies \frac{za}{zs} = \frac{a}{s} \in I_S, \quad \text{d'où } \text{Ker } f = I_S. \end{aligned}$$

Soit π_S la surjection canonique de $S^{-1}A$ sur $S^{-1}A/I_S$; la propriété universelle de l'anneau quotient $S^{-1}A/I_S$ implique l'existence d'un unique morphisme ϕ de $S^{-1}A/I_S$ dans $\bar{S}^{-1}(A/I)$ tel que $\phi \circ \pi_S = f$.

La définition de f implique sa surjectivité, par suite ϕ est surjectif; l'égalité $\text{Ker } f = I_S$ entraîne l'injectivité de ϕ (Cor. 2.32.), donc ϕ est un isomorphisme. □

On rappelle (Déf. 2.59.) que l'ensemble des idéaux premiers d'un anneau unitaire, commutatif A est appelé le *Spectre* de A et noté $\text{Spec}(A)$. On désignera alors par $\text{Spec}_S(A)$, l'ensemble des idéaux $P \in \text{Spec}(A)$ tels que $P \cap S = \emptyset$.

Proposition 6.19. *Compte tenu des notations ci-dessus, on a*

$$P \in \text{Spec}_S(A) \implies P_S \in \text{Spec}(S^{-1}A) \quad (6.9)$$

$$Q \in \text{Spec}(S^{-1}A) \implies \alpha_S^{-1}(Q) \in \text{Spec}_S(A) \quad (6.10)$$

et les applications

$$\begin{aligned} f: \text{Spec}_S(A) &\longrightarrow \text{Spec}(S^{-1}A) & \text{et} & & g: \text{Spec}(S^{-1}A) &\longrightarrow \text{Spec}_S(A) \\ P &\longmapsto P_S & & & Q &\longmapsto \alpha_S^{-1}(Q) \end{aligned}$$

sont des bijections inverses l'une de l'autre.

Preuve : Soit $P \in \text{Spec}_S(A)$, montrons que P_S est un idéal premier dans $S^{-1}A$.

$$\begin{aligned} \frac{ab}{st} = \frac{ab}{st} \in P_S &\iff \exists (x, y) \in P \times S, \text{ tel que } \frac{ab}{st} = \frac{x}{y}. \\ \frac{ab}{st} = \frac{x}{y} &\iff \exists z \in S, \text{ tel que } z(aby - stx) = 0, \end{aligned}$$

d'où $abyz = stxz \in P$, car $x \in P$; alors, P étant un idéal premier de A ,

$$abyz \in P \implies ab \in P \text{ ou } yz \in P;$$

mais $yz \in S$ et $P \cap S = \emptyset$, donc nécessairement $ab \in P$.

$$ab \in P \implies (a \in P \text{ ou } b \in P) \implies \frac{a}{s} \in P_S \text{ ou } \frac{b}{t} \in P_S,$$

l'idéal P_S est donc premier dans $S^{-1}A$, d'où la relation (6.9).

Soit $Q \in \text{Spec}(S^{-1}A)$; posons $I = \alpha_S^{-1}(Q)$. On sait que I est un idéal de A et que $Q = I_S$ (Prop. 6.13.); démontrons que $I \in \text{Spec}_S(A)$. Q est un idéal premier, donc un idéal propre de $S^{-1}A$, par suite on a $I \cap S = \emptyset$ (Prop. 6.13.).

D'autre part, pour a et b dans A ,

$$ab \in I \implies \frac{ab}{1 \cdot 1} \in Q \implies \frac{a}{1} \in Q \text{ ou } \frac{b}{1} \in Q,$$

d'où $a \in I$ ou $b \in I$, ce qui prouve que I est un idéal premier de A .

Comme $I \cap S = \emptyset$, on a $I = \alpha_S^{-1}(Q) \in \text{Spec}_S(A)$, d'où la relation (6.10).

Les résultats précédents impliquent que pour tout $P \in \text{Spec}_S(A)$, on a

$$g(f(P)) = g(P_S) = \alpha_S^{-1}(P_S) \in \text{Spec}_S(A).$$

Démontrons que $\alpha_S^{-1}(P_S) = P$.

$$a \in P \implies \frac{a}{1} \in P_S \implies a \in \alpha_S^{-1}(P_S),$$

d'où $P \subseteq \alpha_S^{-1}(P_S)$. D'autre part,

$$\begin{aligned} a \in \alpha_S^{-1}(P_S) &\iff \frac{a}{1} \in P_S \iff \exists (x, y) \in P \times S, \text{ tel que } \frac{a}{1} = \frac{x}{y}; \\ \frac{a}{1} = \frac{x}{y} &\iff \exists z \in S, \text{ tel que } z(ay - x) = 0. \end{aligned}$$

$$(ayz = xz \text{ et } x \in P) \implies ayz \in P;$$

$$(ayz \in P, P \text{ premier et } P \cap S = \emptyset) \implies a \in P, \text{ d'où } \alpha_S^{-1}(P_S) \subseteq P.$$

On en déduit que $\alpha_S^{-1}(P_S) = P$, donc $g \circ f = \text{id}_{\text{Spec}_S(A)}$.

Soit $Q \in \text{Spec}(S^{-1}A)$, alors $f \circ g(Q) = f(\alpha_S^{-1}(Q)) \in \text{Spec}(S^{-1}A)$.

Démontrons que $f(\alpha_S^{-1}(Q)) = Q$. Soit $\frac{a}{s} \in Q$.

$$\frac{a}{s} \in Q \text{ et } Q \text{ idéal premier} \implies \frac{a}{1} \in Q \text{ ou } \frac{1}{s} \in Q;$$

mais $\frac{1}{s} \in Q$ implique $\frac{s}{1} \frac{1}{s} = \frac{1}{1} \in Q$, ce qui est impossible, car Q est un idéal premier, donc $\frac{a}{1} \in Q$; alors

$$a \in \alpha_S^{-1}(Q) \implies \frac{a}{s} \in f(\alpha_S^{-1}(Q)), \text{ d'où } Q \subseteq f \circ g(Q).$$

Inversement, considérons $\frac{a}{s} \in f \circ g(Q)$,

$$\frac{a}{s} \in f(\alpha_S^{-1}(Q)) \iff \exists (x, y) \in \alpha_S^{-1}(Q) \times S, \text{ tel que } \frac{a}{s} = \frac{x}{y},$$

$$\frac{a}{s} = \frac{x}{y} \implies \exists t \in S, t(ay - xs) = 0.$$

$$(aty = xts \text{ et } x \in \alpha_S^{-1}(Q)) \implies aty \in \alpha_S^{-1}(Q);$$

$$(\alpha_S^{-1}(Q) \in \text{Spec}_S(A) \text{ et } ty \in S) \implies a \in \alpha_S^{-1}(Q),$$

donc $\frac{a}{s} \in Q$, d'où $f \circ g(Q) \subseteq Q$. On en conclut que $f \circ g = \text{id}_{\text{Spec}(S^{-1}A)}$.

Ainsi f et g sont des bijections inverses l'une de l'autre. $\square$

Théorème 6.20. Soit P un idéal premier d'un anneau unitaire, commutatif A , alors le localisé de A en P , noté A_P , est un anneau local, dont l'unique idéal maximal est P_S , où $S = A \setminus P$.

Preuve : A_P est le localisé de A par la partie multiplicative $S = A \setminus P$ (Exemple 6.7., 3)). P est un idéal premier de A et $P \cap S = P \cap (A \setminus P) = \emptyset$, donc $P_S \in \text{Spec}(A_P)$ (Prop. 6.19.).

D'autre part, A_P est un anneau commutatif, unitaire, donc il contient au moins un idéal maximal $\mathcal{M}$ (Th. 2.67.). L'idéal $\mathcal{M}$ est premier (Cor. 2.63.), par suite (Prop. 6.19.), il existe $Q \in \text{Spec}_S(A)$ tel que $\mathcal{M} = Q_S$; alors $Q \cap S = \emptyset$ et $S = A \setminus P$ impliquent $Q \subseteq P$, d'où $\mathcal{M} = Q_S \subseteq P_S$.

On en conclut que $\mathcal{M} = P_S$, puisque $\mathcal{M}$ est un idéal maximal; ainsi P_S est l'unique idéal maximal de A_P , qui est donc un anneau local. $\square$

Théorème 6.21. Si P est un idéal premier d'un anneau unitaire, commutatif A , alors le corps résiduel de l'anneau local A_P est isomorphe au corps des fractions du domaine d'intégrité A/P .

Preuve : En appliquant la proposition 6.18., avec $I = P$ et $S = A \setminus P$, on obtient

$$S^{-1}A/P_S \simeq \bar{S}^{-1}(A/P).$$

Or, d'après le théorème précédent, $S^{-1}A/P_S = A_P/P_S$ est le corps résiduel de l'anneau local A_P . D'autre part, $\bar{S}$ est ici l'ensemble des éléments non nuls de A/P , donc $\bar{S}^{-1}(A/P)$ est le corps des fractions du domaine d'intégrité A/P , d'où le résultat énoncé. $\square$

3. Localisés d'un domaine d'intégrité

Dans tout ce paragraphe, A désigne un D.I. et S est une partie multiplicative de A . On rappelle que dans ce cas (Cor. 6.5. et Prop. 6.8.) le morphisme canonique α_S est injectif,

$S^{-1}A$ est un D.I. et

$$A \subseteq S^{-1}A \subseteq \text{Fr}A.$$

Remarque 6.22. Pour tout idéal J de $S^{-1}A$, $\alpha_S^{-1}(J) = J \cap A$. En effet,

$$a \in \alpha_S^{-1}(J) \iff \frac{a}{1} \in J \iff a \in J \cap A.$$

Par suite, $J = (J \cap A)_S$.

Théorème 6.23. A domaine principal $\implies S^{-1}A$ domaine principal.

Preuve : Les idéaux (0) et $S^{-1}A$ sont principaux ; d'autre part, soit J un idéal propre, non nul de $S^{-1}A$, alors $J \cap A$ est un idéal principal de A . Par suite l'idéal J , engendré par $\alpha_S(J \cap A)$ dans $S^{-1}A$, est aussi un idéal principal. $\square$

Lemme 6.24. U_A et $U_{S^{-1}A}$ désignant, respectivement, le groupe des unités des domaines d'intégrité A et $S^{-1}A$, on a

$$1) U_A \subseteq U_{S^{-1}A}.$$

$$2) a \in A \cap U_{S^{-1}A} \iff \exists s \in S, \text{ tel que } a|s \text{ dans } A.$$

$$3) (p \text{ premier dans } A \text{ et } p \notin U_{S^{-1}A}) \implies p \text{ irréductible dans } S^{-1}A.$$

Preuve :

1) Soit $u \in U_A$; il existe alors $u^{-1} \in A$ tel que $uu^{-1} = 1$ dans A , d'où $uu^{-1} = 1$ dans $S^{-1}A$, donc $u \in U_{S^{-1}A}$.

$$2) a \in A \cap U_{S^{-1}A} \iff \exists \frac{b}{s} \in S^{-1}A \text{ tel que } \frac{ab}{s} = 1 ;$$

$$\frac{ab}{s} = 1 \iff ab = s \iff a|s \text{ dans } A.$$

$$3) p \notin U_{S^{-1}A} \iff (\forall s \in S, p \nmid s \text{ dans } A), \text{ d'après 2).}$$

Supposons $p = \frac{ab}{st}$ dans $S^{-1}A$, donc $pst = ab$ dans A ; par suite

$$(p \text{ premier dans } A \text{ et } pst = ab) \implies p|a \text{ ou } p|b \text{ dans } A.$$

Si $p|a$, il existe $q \in A^*$ tel que $a = pq$; alors l'intégrité de A implique $st = qb$;

$$st = qb \implies \frac{qb}{st} = 1, \text{ dans } S^{-1}A,$$

donc $\frac{b}{t} \in U_{S^{-1}A}$. Dans le cas où $p|b$, on obtient de même $\frac{a}{s} \in U_{S^{-1}A}$. On en conclut que p est irréductible dans $S^{-1}A$. $\square$

Théorème 6.25. A anneau factoriel $\implies S^{-1}A$ anneau factoriel.

Preuve : Posons $Q := \{q \in A^* ; q \text{ irréductible dans } A \text{ et } q \notin U_{S^{-1}A}\}$.

L'anneau A étant factoriel, tout élément irréductible de A est premier ; alors d'après le lemme 6.24.,

$$q \in Q \implies q \text{ irréductible dans } S^{-1}A.$$

a) Vérifions que dans le domaine d'intégrité $S^{-1}A$, tout élément $\frac{a}{s}$, non nul et non inversible, est produit d'éléments irréductibles.

$$\left(\frac{a}{s} \neq 0 \text{ et } \frac{a}{s} \notin U_{S^{-1}A}\right) \implies (a \neq 0 \text{ et } a \notin U_{S^{-1}A}).$$

Dans l'anneau factoriel A , écrivons $a = p_1 p_2 \dots p_n$, où $n \in \mathbb{N}^*$ et pour tout i ($1 \leq i \leq n$), p_i est premier dans A .

$a \notin U_{S^{-1}A}$ implique que les p_i , $1 \leq i \leq n$, ne sont pas tous des unités de $S^{-1}A$; donc, pour un ordre convenable des p_i , il existe k , $1 \leq k \leq n$, tel que

$$\forall i (1 \leq i \leq k), \quad p_i \notin U_{S^{-1}A}, \text{ donc } p_i \in Q;$$

$$\forall i (k+1 \leq i \leq n), \quad p_i \in U_{S^{-1}A}.$$

Si $1 \leq k < n$, posons $e = p_{k+1} \dots p_n$; alors $e \in U_{S^{-1}A}$ et $a = ep_1 p_2 \dots p_k$.

Pour $1 \leq i \leq k$, $p_i \in Q$, donc p_i est irréductible dans $S^{-1}A$ et

$$\frac{a}{s} = \frac{e}{s} p_1 p_2 \dots p_k, \text{ où } \frac{e}{s} \in U_{S^{-1}A}. \quad (6.11)$$

Si $k = n$, on a $e = 1$.

b) Montrons que tout élément irréductible de $S^{-1}A$ est premier.

La factorisation (6.11), obtenue pour un élément $\frac{a}{s}$ non nul et non inversible de $S^{-1}A$,

montre que si $\frac{a}{s}$ est irréductible, alors

$$k = 1 \text{ et } \frac{a}{s} = \frac{e}{s} p_1 \implies \frac{a}{s} \sim p_1 \text{ dans } S^{-1}A.$$

On en déduit que

$$\frac{a}{s} \text{ irréductible dans } S^{-1}A \iff \exists q \in Q, \text{ tel que } \frac{a}{s} \sim q \text{ dans } S^{-1}A.$$

On est ramené à prouver que tout élément $q \in Q$ est premier dans $S^{-1}A$.

Soit $q \in Q$ tel que q divise $\frac{bc}{tu}$ dans $S^{-1}A$. Il existe alors $\frac{d}{v} \in S^{-1}A$ tel que

$$\frac{bc}{tu} = \frac{d}{v} q,$$

d'où $bcv = tudq$ dans A .

$q \in Q$, donc q est premier dans A et q ne divise aucun élément de S ; en particulier, $q \nmid v$, donc $q|bc$, par suite, $q|b$ ou $q|c$ dans A .

Supposons $q|b$, il existe alors $b' \in A^*$ tel que $b = qb'$; d'où

$$\frac{b}{t} = \frac{b'}{t} q \implies q | \frac{b}{t} \text{ dans } S^{-1}A.$$

Dans le cas où $q|c$, on obtient $q | \frac{c}{u}$ dans $S^{-1}A$; q est donc premier dans $S^{-1}A$.

Ainsi le domaine d'intégrité $S^{-1}A$ satisfait aux conditions (AF_1) et $(AF_2)'$ qui caractérisent un anneau factoriel (Th. 5.89.). $\square$

Théorème 6.26. A anneau euclidien $\implies S^{-1}A$ anneau euclidien.

Preuve : On suppose que l'anneau A est euclidien relativement à un stathme δ (Déf 5.70.).

On sait (Cf. Ch. 5 et Th. 6.25.) que

$$A \text{ euclidien} \implies A \text{ factoriel} \implies S^{-1}A \text{ factoriel}.$$

Soit $x \in S^{-1}A \setminus \{0\}$. En reprenant les notations de la preuve du théorème précédent, pour x non inversible, on peut écrire

$$x = up_1 p_2 \dots p_k \text{ où } u \in U_{S^{-1}A} \text{ et } \forall i (1 \leq i \leq k), p_i \in Q.$$

D'après la définition de l'ensemble Q , les p_i , $1 \leq i \leq k$, sont irréductibles dans A . Posons $a = p_1 p_2 \dots p_k$; alors

$$x = ua \text{ avec } u \in U_{S^{-1}A} \text{ et } a \in A^* \setminus U_A.$$

Considérons la correspondance $\varphi : S^{-1}A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que

$$\forall u \in U_{S^{-1}A}, \varphi(u) = \delta(1) \text{ et } \forall x = ua \in A^* \setminus U_{S^{-1}A}, \varphi(x) = \delta(a).$$

Vérifions que la correspondance φ est une application. Supposons $x = ua = u'a'$, où u et u' sont dans $U_{S^{-1}A}$, a et a' dans $A^* \setminus U_A$; alors

$$a' = u'^{-1}ua \implies \varphi(a') = \delta(a) \implies \varphi(ua) = \varphi(u'a').$$

Soit x et y non nuls dans $S^{-1}A$, démontrons que

$$x|y \text{ dans } S^{-1}A \implies \varphi(x) \leq \varphi(y).$$

L'hypothèse $x|y$ dans $S^{-1}A$ entraîne qu'il existe $z \in S^{-1}A$ tel que $y = xz$.

Posons $x = ua$, $y = vb$, $z = wt$, où u, v, w sont dans $U_{S^{-1}A}$ et a, b, t sont dans $A^* \setminus U_A$; on a

$$\varphi(x) = \delta(a), \varphi(y) = \delta(b).$$

$$y = xz \implies y = uat \implies \varphi(y) = \delta(at);$$

alors, $a|at$ dans A entraîne $\delta(a) \leq \delta(at) = \delta(b)$, d'où $\varphi(x) \leq \varphi(y)$.

Montrons que la division euclidienne de A induit une division euclidienne dans $S^{-1}A$. Considérons, comme plus haut, $x = ua$ et $y = vb$ non nuls dans $S^{-1}A$. La division euclidienne de a par b dans A donne

$$a = bq + r, \text{ avec } r = 0 \text{ ou } \delta(r) < \delta(b),$$

alors, $u^{-1}x = v^{-1}yq + r$ implique $x = yuv^{-1}q + ur$, avec

$$ur = 0 \quad \text{ou} \quad \varphi(ur) = \delta(r) < \delta(b) = \varphi(y).$$

On en conclut que l'anneau $S^{-1}A$ est euclidien. $\square$

4. Localisé d'un A-module

Comme dans le paragraphe précédent, S désigne une *partie multiplicative* de l'anneau unitaire, commutatif A .

A. Localisé d'un A-module par S

Etant donné un A -module M , on définit sur $M \times S$ la relation binaire $\mathcal{R}_S$ telle que

$$(x, s) \mathcal{R}_S (x', s') \iff \exists t \in S, t(sx' - s'x) = 0.$$

Comme pour la localisation de A par S , on montre que $\mathcal{R}_S$ est une relation d'équivalence ; on note $\frac{x}{s}$ la classe d'équivalence modulo $\mathcal{R}_S$ du couple $(x, s) \in M \times S$. On pose

$$S^{-1}M := \left\{ \frac{x}{s}; (x, s) \in M \times S \right\}.$$

Définition 6.27. $S^{-1}M$ est appelé le **localisé** du A -module à gauche M par la partie multiplicative S de A .

Proposition 6.28. $S^{-1}M$ est un $S^{-1}A$ -module à gauche.

Preuve : Le lecteur vérifiera que les correspondances

$$\begin{aligned} S^{-1}M \times S^{-1}M &\longrightarrow S^{-1}M & \text{et} & & S^{-1}A \times S^{-1}M &\longrightarrow S^{-1}M \\ \left(\frac{x}{s}, \frac{x'}{s'} \right) &\longmapsto \frac{s'x + sx'}{ss'} & & & \left(\frac{a}{t}, \frac{x}{s} \right) &\longmapsto \frac{ax}{st} \end{aligned}$$

sont des applications qui définissent respectivement, dans $S^{-1}M$, une addition et une multiplication externes à opérateurs dans l'anneau $S^{-1}A$ telles que $S^{-1}M$ est un $S^{-1}A$ -module à gauche. $\square$

Remarque 6.29. Dans le cas où $S = A \setminus P$, P étant un idéal premier de A , le A_P -module $S^{-1}M$ sera noté M_P et appelé le **localisé de M en P** .

B. Localisé d'un morphisme de A-modules

M et N étant deux A -modules à gauche, à tout $f \in \text{Hom}_A(M, N)$, on associe la correspondance de $S^{-1}M$ dans $S^{-1}N$, notée $S^{-1}f$, telle que

$$\forall \frac{x}{s} \in S^{-1}M, \quad S^{-1}f\left(\frac{x}{s}\right) = \frac{f(x)}{s}.$$

On vérifie alors, que $S^{-1}f$ est une application et que $S^{-1}f$ est un morphisme de $S^{-1}A$ -modules. Si P est un A -module et $g \in \text{Hom}_A(N, P)$, on montre que

$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f.$$

Proposition 6.30. *Etant donné une suite de A -modules à gauche :*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \quad \text{exacte en } M,$$

la suite de $S^{-1}A$ -modules

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \quad \text{est exacte en } S^{-1}M.$$

Preuve : La notion de suite exacte a été définie au chapitre 3 (Déf. 3.70.).

Par hypothèse on a $g \circ f = 0$, par suite $S^{-1}g \circ S^{-1}f = 0$, d'où

$$\text{Im}(S^{-1}f) \subseteq \text{Ker}(S^{-1}g).$$

Démontrons l'inclusion inverse.

Soit $\frac{x}{s} \in \text{Ker}(S^{-1}g)$, donc $\frac{g(x)}{s} = 0$ dans $S^{-1}M''$; nécessairement il existe $u \in S$ tel que $ug(x) = 0$ dans M'' , d'où $g(ux) = 0$; ainsi

$$ux \in \text{Ker } g = \text{Im } f, \implies \exists x' \in M' \text{ tel que } ux = f(x'); \text{ alors,}$$

$$\frac{x}{s} = \frac{ux}{us} = \frac{f(x')}{us} = S^{-1}f\left(\frac{x'}{us}\right) \implies \text{Ker}(S^{-1}g) \subseteq \text{Im}(S^{-1}f). \quad \square$$

Remarque 6.31. :

a) Si N est un sous- A -module de M , alors l'injection canonique i de N dans M induit une injection de $S^{-1}A$ -modules, $S^{-1}i : S^{-1}N \longrightarrow S^{-1}M$, donc $S^{-1}N$ peut être considéré comme un sous- $S^{-1}A$ -module de $S^{-1}M$.

b) Toute suite exacte courte de A -modules à gauche est transformée, par localisation par S , en une suite exacte courte de $S^{-1}A$ -modules à gauche.

Corollaire 6.32. *N et P étant des sous-modules d'un A -module M , on a*

$$1) S^{-1}(N + P) = S^{-1}N + S^{-1}P;$$

$$2) S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P;$$

$$3) \text{ les } S^{-1}A\text{-modules } S^{-1}(M/N) \text{ et } S^{-1}M/S^{-1}N \text{ sont isomorphes.}$$

Démonstration en exercice (n° 1, Ch. 6).

Remarque 6.33. Etant donné un A -module à gauche M , le morphisme canonique α_S de A dans $S^{-1}A$ permet de considérer (par restriction des scalaires, Cf. App. B) le $S^{-1}A$ -module à gauche $S^{-1}M$, comme un A -module à gauche, grâce l'application :

$$\begin{aligned} A \times S^{-1}M &\longrightarrow S^{-1}M \\ (a, \frac{x}{s}) &\longmapsto \frac{ax}{1s} = \frac{ax}{s}. \end{aligned}$$

En particulier, $S^{-1}A$ est un A -module à gauche. On en déduit (par extension des scalaires, Cf. App. B) que le A -module à gauche $S^{-1}A \otimes_A M$ peut être muni d'une structure de $S^{-1}A$ -module à gauche, par à l'application

$$\begin{aligned} S^{-1}A \times (S^{-1}A \otimes_A M) &\longrightarrow S^{-1}A \otimes_A M \\ (\frac{a}{t}, \frac{b}{s} \otimes x) &\longmapsto \frac{ab}{ts} \otimes x. \end{aligned}$$

C. Propriétés des modules localisés

Proposition 6.34. Pour tout A -module M on a

$$S^{-1}M \simeq S^{-1}A \otimes_A M \quad (\text{isomorphisme de } S^{-1}A\text{-modules}).$$

Preuve : Vérifions que la correspondance

$$\begin{aligned} \varphi : S^{-1}M &\longrightarrow S^{-1}A \otimes_A M \\ \frac{x}{s} &\longmapsto \frac{1}{s} \otimes x \end{aligned}$$

est une application. Soit $\frac{x'}{s'} = \frac{x}{s}$ dans $S^{-1}M$; il existe $t \in S$ tel que $t(s'x - sx') = 0$, d'où

$$\begin{aligned} \frac{1}{s} \otimes x - \frac{1}{s'} \otimes x' &= \frac{1}{ss't} \otimes ts'x - \frac{1}{ss't} \otimes tsx' \\ &= \frac{1}{ss't} \otimes (t(s'x - sx')) = 0. \end{aligned}$$

L'application φ est $S^{-1}A$ -linéaire ; en effet, pour $\frac{a}{r} \in S^{-1}A$ et $(\frac{x}{s}, \frac{y}{t}) \in S^{-1}M \times S^{-1}M$,

$$\begin{aligned} \varphi\left(\frac{x}{s} + \frac{y}{t}\right) &= \varphi\left(\frac{tx + sy}{st}\right) = \frac{1}{st} \otimes (tx + sy) = \frac{1}{s} \otimes x + \frac{1}{t} \otimes y = \varphi\left(\frac{x}{s}\right) + \varphi\left(\frac{y}{t}\right); \\ \varphi\left(\frac{a}{r} \frac{x}{s}\right) &= \varphi\left(\frac{ax}{rs}\right) = \frac{1}{rs} \otimes ax = \frac{a}{rs} \otimes x = \frac{a}{r} \left(\frac{1}{s} \otimes x\right) = \frac{a}{r} \varphi\left(\frac{x}{s}\right). \end{aligned}$$

De plus, le morphisme φ est surjectif, car les générateurs du A -module $S^{-1}A \otimes_A M$ sont les $\frac{a}{s} \otimes x$ pour $(\frac{a}{s}, x) \in S^{-1}A \times M$ et

$$\frac{a}{s} \otimes x = \frac{1}{s} \otimes ax = \varphi\left(\frac{ax}{s}\right).$$

La surjectivité de φ implique que tout élément de $S^{-1}A \otimes_A M$ peut s'écrire sous la forme $\frac{1}{s} \otimes x$. Considérons d'autre part, la correspondance

$$\begin{aligned} \mu : S^{-1}A \times M &\longrightarrow S^{-1}M \\ \left(\frac{a}{s}, x\right) &\longmapsto \frac{ax}{s}. \end{aligned}$$

Supposons $\frac{a'}{s'} = \frac{a}{s}$ dans $S^{-1}A$; il existe $t \in S$ tel que $t(s'a - sa') = 0$ et

$$t(s'ax - sa'x) = 0 \implies \frac{ax}{s} = \frac{a'x}{s'}.$$

On en déduit que μ est une application et on vérifie que μ est A -bilinéaire. La propriété universelle du produit tensoriel (Cf. App. B) implique alors qu'il existe un unique morphisme de A -modules, ψ , tel que

$$\begin{aligned} \psi : S^{-1}A \otimes_A M &\longrightarrow S^{-1}M \\ \frac{a}{s} \otimes x &\longmapsto \mu\left(\frac{a}{s}, x\right) = \frac{ax}{s}. \end{aligned}$$

Vérifions que ψ est un morphisme de $S^{-1}A$ -modules. On a remarqué plus haut que tout élément y de $S^{-1}A \otimes_A M$ pouvait s'écrire sous la forme

$$y = \frac{1}{s} \otimes x, \text{ où } (\frac{1}{s}, x) \in S^{-1}A \times M;$$

par suite, quel que soit $\frac{a}{t} \in S^{-1}A$,

$$\psi(\frac{a}{t}y) = \psi(\frac{a}{ts} \otimes x) = \frac{ax}{ts} = \frac{a}{t} \psi(y).$$

D'autre part, quels que soient $\frac{x}{s} \in S^{-1}M$ et $\frac{a}{s} \otimes x \in S^{-1}A \otimes_A M$, on a

$$\begin{aligned} \psi \circ \phi(\frac{x}{s}) &= \psi(\frac{1}{s} \otimes x) = \frac{x}{s} \\ \phi \circ \psi(\frac{a}{s} \otimes x) &= \phi(\frac{ax}{s}) = \frac{1}{s} \otimes ax = \frac{a}{s} \otimes x. \end{aligned}$$

On en conclut que ϕ et ψ sont des $S^{-1}A$ -isomorphismes et $\psi = \phi^{-1}$. □

Corollaire 6.35. Pour toute partie multiplicative S de A , $S^{-1}A$ est un A -module plat (Cf. App. B, Déf. B.21).

Cette propriété est une conséquence des propositions 6.30. et 6.34.

Proposition 6.36. M et N étant deux A -modules à gauche, on a $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq S^{-1}(M \otimes_A N)$ (isomorphisme de $S^{-1}A$ -modules).

Preuve : D'après la proposition 6.34, les $S^{-1}A$ -modules $S^{-1}(M \otimes_A N)$ et $S^{-1}A \otimes_A (M \otimes_A N)$ sont isomorphes. On considère

$$\begin{aligned} \lambda : S^{-1}M \times S^{-1}N &\longrightarrow S^{-1}A \otimes_A (M \otimes_A N) \\ (\frac{x}{s}, \frac{y}{t}) &\longmapsto \frac{1}{st} \otimes (x \otimes y). \end{aligned}$$

On vérifie que λ est une application $S^{-1}A$ -bilinéaire. La propriété universelle du produit tensoriel, implique qu'il existe un unique morphisme Λ , de $S^{-1}A$ -modules, tel que

$$\begin{aligned} \Lambda : S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\longrightarrow S^{-1}A \otimes_A (M \otimes_A N) \\ (\frac{x}{s} \otimes \frac{y}{t}) &\longmapsto \frac{1}{st} \otimes (x \otimes y). \end{aligned}$$

$$\begin{aligned} \text{De même, soit } \lambda' : S^{-1}A \times (M \otimes_A N) &\longrightarrow S^{-1}M \otimes_{S^{-1}A} S^{-1}N \\ (\frac{a}{s}, x \otimes y) &\longmapsto \frac{a}{s} (\frac{x}{1} \otimes \frac{y}{1}). \end{aligned}$$

On montre que λ' est A -bilinéaire et on en déduit, comme précédemment, qu'il existe un unique morphisme de A -modules, Λ' , tel que

$$\begin{aligned} \Lambda' : S^{-1}A \otimes_A (M \otimes_A N) &\longrightarrow S^{-1}M \otimes_{S^{-1}A} S^{-1}N \\ \frac{a}{s} \otimes (x \otimes y) &\longmapsto \frac{a}{s} (\frac{x}{1} \otimes \frac{y}{1}). \end{aligned}$$

On vérifie que Λ' est $S^{-1}A$ -linéaire et de plus

$$\begin{aligned}\Lambda \circ \Lambda' \left(\frac{a}{s} \otimes (x \otimes y) \right) &= \Lambda \left(\frac{a}{s} \left(\frac{x}{1} \otimes \frac{y}{1} \right) \right) = \Lambda \left(\frac{ax}{s} \otimes \frac{y}{1} \right) \\ &= \frac{1}{s} \otimes (ax \otimes y) = \frac{a}{s} \otimes (x \otimes y). \\ \Lambda' \circ \Lambda \left(\frac{x}{s} \otimes \frac{y}{t} \right) &= \Lambda' \left(\frac{1}{st} \otimes (x \otimes y) \right) = \frac{x}{s} \otimes \frac{y}{t}.\end{aligned}$$

Ainsi, Λ et Λ' sont des $S^{-1}A$ -isomorphismes inverses l'un de l'autre. $\square$

Corollaire 6.37. *P étant un idéal premier de A, quels que soient les A-modules à gauche M et N, on a*

$$M_P \otimes_{A_P} N_P \simeq (M \otimes_A N)_P \quad (\text{isomorphisme de } A_P\text{-modules}).$$

Ce résultat s'obtient en appliquant la Prop. 6.36 au cas où $S = A \setminus P$.

5. Exercices

Les notations générales sont celles habituellement utilisées dans le Chapitre 6 et dans les chapitres précédents. Les morphismes d'anneaux sont des morphismes d'anneaux unitaires.

1) Démontrer le corollaire 6.32.

2) Vérifier que toute partie multiplicative S , d'un anneau unitaire, commutatif A , est une partie multiplicative de l'anneau de polynômes $A[X]$ et prouver que $(S^{-1}A)[X] = S^{-1}(A[X])$.

3) Posons $S := \mathbb{Z} \setminus 2\mathbb{Z}$ et soit π la surjection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$.

1°) Vérifier que $\pi(S)$ est une partie multiplicative de l'anneau $\mathbb{Z}/6\mathbb{Z}$. On pose $\Sigma := \pi(S)$; expliciter les éléments de Σ .

2°) Soit $A := \Sigma^{-1}(\mathbb{Z}/6\mathbb{Z})$ le localisé de $\mathbb{Z}/6\mathbb{Z}$ par Σ .

Démontrer que A est un corps isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

4) Généralisation de l'exercice 3) ci-dessus

Soit $n > 1$ dans $\mathbb{Z}$ et p un nombre premier. On note π la surjection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ et on pose $\bar{P} := \pi(p\mathbb{Z})$.

1°) Prouver que $\bar{P}$ est un idéal propre de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $p|n$.

2°) On suppose que $p|n$, démontrer que $\bar{P}$ est un idéal premier de $\mathbb{Z}/n\mathbb{Z}$.

3°) On suppose $p|n$ et $p \neq n$. Soit $(\mathbb{Z}/n\mathbb{Z})_{\bar{P}}$ le localisé de $\mathbb{Z}/n\mathbb{Z}$ en $\bar{P}$, c'est-à-dire le localisé de $\mathbb{Z}/n\mathbb{Z}$ par $\Sigma := \mathbb{Z}/n\mathbb{Z} \setminus \bar{P}$ (Cf. Exemples 6.7).

Démontrer que l'idéal $\bar{P}_{\Sigma}$, engendré par $\bar{P}$ dans $(\mathbb{Z}/n\mathbb{Z})_{\bar{P}}$ (Déf. 6.14), est nul.

En déduire que $(\mathbb{Z}/n\mathbb{Z})_{\bar{P}} \simeq \mathbb{Z}/p\mathbb{Z}$ (Cf. Th. 6.20 et 6.21).

5) Soit S une partie multiplicative d'un anneau unitaire, commutatif A .

1°) Soit, respectivement, $\mathcal{N}(A)$ et $\mathcal{N}(S^{-1}A)$ le nilradical de A et de $S^{-1}A$. Démontrer que $(\mathcal{N}(A))_S = \mathcal{N}(S^{-1}A)$.

2°) I étant un idéal propre, non nul de A , prouver que, dans $S^{-1}A$, on a $(\sqrt{I})_S = \sqrt{I}_S$ (Cf. Ch. 2, Ex. 14).

- 6) Soit A un D.I. ; pour tout $P \in \text{Spec}(A)$, A_P désigne le localisé de A en P .

Le but de cet exercice est de prouver que $\bigcap_{P \in \text{Spec}(A)} A_P = A$.

1°) Justifier l'inclusion $A \subseteq \bigcap_{P \in \text{Spec}(A)} A_P$.

2°) On suppose qu'il existe $\frac{a}{b} \in (\bigcap_{P \in \text{Spec}(A)} A_P) \setminus A$.

a) Vérifier que pour tout $P \in \text{Spec}(A)$, il existe $s \in A \setminus P$ tel que $as \in bA$. On pose

$$B_P = \{s \in A \setminus P ; as \in bA\}.$$

Soit B l'idéal de A engendré par $\bigcup_{P \in \text{Spec}(A)} B_P$. Prouver que, pour tout $x \in B$, on a $ax \in bA$.

b) On suppose $B \neq A$. Montrer que l'existence d'un idéal maximal de A contenant B conduit à une contradiction. En déduire que $\bigcap_{P \in \text{Spec}(A)} A_P = A$.

- 7) Soit S et S' deux parties multiplicatives d'un anneau unitaire, commutatif A telles que $S \subset S'$. On note, α_S et $\alpha_{S'}$ les morphismes canoniques de A dans, respectivement, $S^{-1}A$ et $S'^{-1}A$.

1°) Montrer qu'il existe un unique morphisme d'anneaux unitaires de $S^{-1}A$ dans $S'^{-1}A$, que l'on notera $\phi_{S,S'}$, tel que $\phi_{S,S'} \circ \alpha_S = \alpha_{S'}$ (Th. 6.9).

2°) Si l'on suppose, de plus, $\alpha_{S'}(S') \subseteq U_{S^{-1}A}$, prouver que $\phi_{S,S'}$ est un isomorphisme dont on précisera l'inverse (voir Cor. 6.10).

- 8) Comme dans l'exercice précédent, on considère deux parties multiplicatives S et S' d'un anneau unitaire commutatif A telles que $S \subset S'$.

1°) On désigne par $S'/1$, l'ensemble $\alpha_{S'}(S') = \{\frac{s'}{1} ; s' \in S'\}$.

a) Vérifier que $S'/1$ est une partie multiplicative de $S^{-1}A$. On notera $(S'/1)^{-1}(S^{-1}A)$ le localisé de $S^{-1}A$ par $S'/1$.

b) Soit B un anneau unitaire commutatif et f un morphisme de A dans B tel que $f(S') \subseteq U_B$; vérifier (Th. 6.9) qu'il existe un unique morphisme $\phi_{S,S'} \in \text{Hom}((S'/1)^{-1}(S^{-1}A), B)$ tel que

$$\phi_{S,S'} \circ \alpha_{(S'/1)} \circ \alpha_S = f.$$

En déduire que les anneaux $S'^{-1}A$ et $(S'/1)^{-1}(S^{-1}A)$ sont isomorphes (voir Cor. 6.10).

2°) On pose $S'/S := \{\frac{s'}{s} \in S^{-1}A ; s \in S, s' \in S'\}$.

a) Vérifier que S'/S est une partie multiplicative de $S^{-1}A$ contenant $S'/1$.

En déduire qu'il existe un unique morphisme d'anneaux unitaires $\phi_{S,S'}$ de $(S'/1)^{-1}(S^{-1}A)$ dans $(S'/S)^{-1}(S^{-1}A)$ tel que $\phi_{S,S'} \circ \alpha_{(S'/1)} = \alpha_{(S'/S)}$ (Cf. Ex. 7, 1°)).

b) Prouver que le morphisme $\phi_{S,S'}$ est un isomorphisme (Cf. Ex. 7, 2°)).

3°) Soit S et T deux parties multiplicatives de A . On pose $ST := \{st \in A ; s \in S, t \in T\}$.

Vérifier que ST est une partie multiplicative de A contenant S et T .

En appliquant les résultats du 1°), démontrer que les anneaux $(ST)^{-1}A, (\alpha_S(T))^{-1}(S^{-1}A)$ et $(\alpha_T(S))^{-1}(T^{-1}A)$ sont isomorphes.

4°) Soit S une partie multiplicative de A et Σ une partie multiplicative de $S^{-1}A$, on pose

$$S' := \{a \in A ; \exists s \in S, \frac{a}{s} \in \Sigma\}.$$

Vérifier que S' est une partie multiplicative de A contenant S .

Soit $\Sigma^{-1}(S^{-1}A)$ le localisé de $S^{-1}A$ par Σ ; en utilisant les résultats du 1°) et du 2°), montrer que les anneaux $S'^{-1}A$ et $\Sigma^{-1}(S^{-1}A)$ sont isomorphes.

- 9) On rappelle (Ch. 5, Ex. 22) qu'un anneau A unitaire, commutatif est un J -anneau si tout idéal premier de A est l'intersection des idéaux maximaux qui le contiennent.

K étant un corps, l'anneau $K[X]$ est un J-anneau (Ch. 5, Ex. 22, 2°)).

Soit (X) l'idéal de $K[X]$ engendré par X . Justifier les propriétés suivantes :

i) (X) est un idéal premier de $K[X]$.

ii) Le localisé de $K[X]$ en (X) n'est pas un J-anneau (Ch. 5, Ex. 22, 1°)).

10) Etant donné un domaine d'intégrité B et un élément $b \neq 0$ dans B , on considère la partie multiplicative $S_b := \{b^n ; n \in \mathbb{N}\}$.

1°) Soit $S_b^{-1}B$ le localisé de B par S_b . Si I est un idéal de B , on notera I_b l'idéal de $S_b^{-1}B$ engendré par I (Déf. 6.14).

a) Comment s'écrivent les éléments de I_b ?

b) Vérifier qu'un idéal Q de $S_b^{-1}B$ est premier si et seulement si $Q = P_b$, où P est un idéal premier de B tel que $b \notin P$.

2°) L'objet de cette question est de prouver que pour un anneau unitaire, commutatif A , les deux propriétés suivantes sont équivalentes.

($\mathcal{P}_1$) : A est un J-anneau (Cf. Ex. précédent et Ex. 22, Ch. 5).

($\mathcal{P}_2$) : Si P est un idéal premier de A et si $B := A/P$ contient un élément $b \neq 0$ tel que $S_b^{-1}B$ est un corps, alors B est un corps (c'est-à-dire que l'idéal P est maximal).

a) On suppose que A est un J-anneau et que P est un idéal premier de A , pour lequel il existe $b \neq 0$ dans $B := A/P$ tel que $S_b^{-1}B$ est un corps.

- Vérifier que B est un J-anneau (Ch. 5, Ex. 22, 3°, a)).

- Prouver alors que b appartient à tout idéal maximal non nul de B .

- En déduire que B est un corps. En conclure que ($\mathcal{P}_1$) $\implies$ ($\mathcal{P}_2$).

b) On suppose que A vérifie la propriété ($\mathcal{P}_2$).

Soit Q un idéal premier de A et I l'intersection des idéaux maximaux de A contenant Q . On suppose $I \neq Q$, donc il existe $t \in I \setminus Q$.

1. Soit E l'ensemble des idéaux premiers P de A tels que $Q \subseteq P$ et $t \notin P$.

- Démontrer qu'il existe au moins un élément maximal dans l'ensemble E ordonné par l'inclusion ; soit T un tel élément.

- Montrer que T n'est pas un idéal maximal de A , mais que T_t est un idéal maximal de $S_t^{-1}A$.

2. On considère les morphismes canoniques :

$$\pi : A \longrightarrow A/T, \quad \alpha : A \longrightarrow S_t^{-1}A, \quad \beta : A/T \longrightarrow S_t^{-1}A/T, \quad \text{où } \bar{t} = \pi(t).$$

- Prouver qu'il existe un unique $\varphi \in \text{Hom}(S_t^{-1}A, S_t^{-1}A/T)$ tel que $\varphi \circ \alpha = \beta \circ \pi$.

- Vérifier que φ est surjectif.

- Soit σ la surjection canonique : $S_t^{-1}A \longrightarrow S_t^{-1}A/T_t$. Justifier l'existence d'un unique morphisme $\psi \in \text{Hom}(S_t^{-1}A/T_t, S_t^{-1}A/T)$ tel que $\psi \circ \sigma = \varphi$.

- Prouver que ψ est un isomorphisme. En déduire une contradiction avec l'hypothèse ($\mathcal{P}_2$) et conclure.

Chapitre 7

Séries Formelles

Dans tout ce chapitre, A désigne un anneau unitaire et commutatif.

1. Séries formelles à une indéterminée sur A

A. Algèbre des séries formelles à une indéterminée sur A

1. $\mathbb{N}$ étant l'ensemble des entiers naturels, on considère le A -module à gauche $A^{\mathbb{N}}$ (Ch. 3).

$$A^{\mathbb{N}} = \{(a_n)_{n \in \mathbb{N}} ; \forall n \in \mathbb{N}, a_n \in A\}.$$

On définit une multiplication dans $A^{\mathbb{N}}$, par l'application

$$\begin{aligned} A^{\mathbb{N}} \times A^{\mathbb{N}} &\longrightarrow A^{\mathbb{N}} \\ ((a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}}) &\longmapsto (c_n)_{n \in \mathbb{N}}, \end{aligned}$$

$$\text{où, } c_n = \sum_{p+q=n} a_p b_q = \sum_{0 \leq p \leq n} a_p b_{n-p}.$$

On peut vérifier que le A -module à gauche $A^{\mathbb{N}}$ est alors muni d'une structure de **A -algèbre commutative** dont l'élément unité est $1 = (\delta_n)_{n \in \mathbb{N}}$, où $\delta_0 = 1$ et pour tout $n \geq 1$, $\delta_n = 0$.

2. L'application

$$\begin{aligned} \lambda : A &\longrightarrow A^{\mathbb{N}} \\ a &\longmapsto (a_n)_{n \in \mathbb{N}}, \text{ où } a_0 = a \text{ et } \forall n \geq 1, a_n = 0 \end{aligned}$$

est un morphisme *injectif* de A -algèbres qui permet d'identifier A à la sous-algèbre $\text{Im } \lambda$ de $A^{\mathbb{N}}$; pour tout $a \in A$, on écrira a à la place de $\lambda(a)$.

3. Changement de notation

On considère, dans $A^{\mathbb{N}}$, les éléments $e_0 = (1, 0, \dots)$, $e_1 = (0, 1, 0, \dots)$ et plus généralement,

$$e_i = (\alpha_n)_{n \in \mathbb{N}}, \text{ où } \alpha_i = 1 \text{ et } \forall n \neq i, \alpha_n = 0.$$

On en déduit qu'un élément $f = (a_n)_{n \in \mathbb{N}}$ s'écrit :

$$\begin{aligned} f &= a_0 e_0 + a_1 e_1 + \dots + a_n e_n + \dots \\ &= a_0 e_1^0 + a_1 e_1 + \dots + a_n e_1^n + \dots \end{aligned}$$

et on écrira, "formellement", $f = \sum_{n \in \mathbb{N}} a_n e_1^n$.

Il s'agit d'une écriture "formelle", car le signe $\sum$ ne désigne pas ici une somme finie d'éléments.

En posant $X = e_1$, un élément $f = (a_n)_{n \in \mathbb{N}}$ de $A^{\mathbb{N}}$ s'écrit

$$f = \sum_{n \in \mathbb{N}} a_n X^n, \text{ où } \forall n \in \mathbb{N}, a_n \in A. \quad (7.1)$$

On utilisera aussi la notation : $f = \sum_{n \geq 0} a_n X^n$.

Définition 7.1. :

a) L'élément e_1 de $A^{\mathbb{N}}$, que nous avons noté X , est appelé **indéterminée**.

b) Un élément quelconque $f = \sum_{n \in \mathbb{N}} a_n X^n$ dans $A^{\mathbb{N}}$ est appelé **série formelle à une indéterminée sur A** .

Les éléments $a_n, n \in \mathbb{N}$, sont les **coefficients** de la série formelle f et a_0 est son **terme constant**.

c) L'indéterminée ayant été notée X , l'algèbre $A^{\mathbb{N}}$ sera notée $A[[X]]$ et appelée **algèbre des séries formelles à une indéterminée sur A** .

Remarque 7.2. :

a) On sait que l'algèbre des polynômes à une indéterminée sur A est

$$A[X] = \{ \sum_{n \in \mathbb{N}} a_n X^n ; (a_n)_{n \in \mathbb{N}} \in A^{(\mathbb{N})} \}.$$

$A[X]$ est donc une sous-algèbre de $A[[X]]$ et on a les inclusions strictes

$$A \subset A[X] \subset A[[X]].$$

A est appelé sous-algèbre des séries formelles **constantes** de $A[[X]]$.

b) Comme dans le cas de l'algèbre $A[X]$, la construction de $A[[X]]$ montre que cette Algèbre est (à un isomorphisme près) indépendante du symbole X choisi pour désigner l'indéterminée. On pourra vérifier, par exemple, que les A -algèbres $A[[X]]$ et $A[[Y]]$ sont isomorphes par l'application

$$\begin{aligned} A[[X]] &\longrightarrow A[[Y]] \\ \sum_{n \geq 0} X^n &\longmapsto \sum_{n \geq 0} Y^n. \end{aligned}$$

Premiers exemples : Les développements en séries entières des fonctions réelles ou complexes classiques sont des séries formelles dans $\mathbb{R}[[X]]$ ou $\mathbb{C}[[X]]$; en particulier,

$$\frac{1}{1-X} = \sum_{n \geq 0} X^n, \quad \text{Exp}(X) = \sum_{n \geq 0} \frac{1}{n!} X^n, \quad \text{Log}(1+X) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} X^n.$$

Remarque 7.3. Comme le montre le premier exemple ci-dessus, dans tout anneau de séries formelles $A[[X]]$, on a

$$(1-X) \left(\sum_{n \geq 0} X^n \right) = 1;$$

ce qui prouve que $1-X$ et $\sum_{n \geq 0} X^n$ sont inversibles dans $A[[X]]$.

Nous caractériserons plus loin les éléments inversibles d'un anneau de séries formelles.

B. Notion d'ordre d'une série formelle

Définition 7.4. Soit $f = \sum_{n \geq 0} a_n X^n$ dans $A[[X]]$; si $f \neq 0$, on appelle **ordre** de f , l'entier noté $\omega(f)$ défini par

$$\omega(f) = \inf \{ n \in \mathbb{N} ; a_n \neq 0 \}.$$

$\omega(0)$ est considéré comme plus grand que l'ordre de toute série formelle non nulle et est symboliquement noté $+\infty$ avec les conventions :

$$(+\infty) + (+\infty) = +\infty \quad \text{et} \quad \forall p \in \mathbb{N}, (+\infty) + p = +\infty.$$

Remarque 7.5. D'après la définition 7.4., on peut considérer ω comme une application de $A[[X]]$ dans $\mathbb{N}$ et pour tout $f \neq 0$ dans $A[[X]]$, on a

$$\omega(f) = p \iff a_0 = a_1 = \dots = a_{p-1} = 0, a_p \neq 0$$

$$\iff f = X^p (\sum_{n \geq p} a_n X^{n-p}), a_p \neq 0.$$

D'autre part, pour tout $n \in \mathbb{N}$, on peut écrire $f = f_n + r_n$, où

$$f_n = \sum_{0 \leq i \leq n} a_i X^i \quad \text{et} \quad r_n = \sum_{i > n} a_i X^i,$$

donc $f_n \in A[X]$ et $r_n \in A[[X]]$, $\omega(r_n) > n$.

Théorème 7.6. *Quels que soient f et g dans $A[[X]]$,*

- 1) $\omega(f+g) \geq \inf\{\omega(f), \omega(g)\}$;
 $\omega(f) \neq \omega(g) \implies \omega(f+g) = \inf\{\omega(f), \omega(g)\}$
- 2) $\omega(fg) \geq \omega(f) + \omega(g)$;
 $\omega(fg) = \omega(f) + \omega(g)$, si A est intègre.

Preuve : Soit f et g dans $A[[X]]$.

1) De la définition 7.4., on déduit que, pour f et g non nuls,

$$\begin{aligned}\omega(f) = \omega(g) = p \in \mathbb{N} &\implies \omega(f+g) \geq p, \\ (\omega(f) = p, \omega(g) = q, p < q) &\implies \omega(f+g) = p.\end{aligned}$$

D'autre part,

$$\begin{aligned}f = g = 0 &\implies +\infty = \omega(f) = \omega(g) = \omega(f+g) \\ (f = 0, \omega(g) = p \in \mathbb{N}) &\implies \omega(f+g) = \omega(g) = p;\end{aligned}$$

d'où les résultats 1) du théorème.

2) Si $fg \neq 0$ et $f = \sum_{n \geq 0} a_n X^n$, $g = \sum_{n \geq 0} b_n X^n$, on a

$$fg = \sum_{n \geq 0} c_n X^n, \text{ où } \forall n \in \mathbb{N}, c_n = \sum_{i+j=n} a_i b_j;$$

alors $(\omega(f) = p, \omega(g) = q, n < p+q) \implies c_n = 0$ et $c_{p+q} = a_p b_q$, d'où

$$\omega(fg) \geq p+q; \quad \omega(fg) = p+q, \text{ si } A \text{ est intègre.}$$

Si $fg = 0$, $\omega(fg) = +\infty \geq \omega(f) + \omega(g)$. □

Corollaire 7.7. *L'anneau A étant unitaire, commutatif, $A[[X]]$ est intègre $\iff A$ est intègre.*

En particulier, si K est un corps, $K[[X]]$ est intègre.

Preuve : Si A est intègre, alors d'après le 2) du théorème 7.6., quels que soient f et g non nuls dans $A[[X]]$, on a

$$\omega(fg) = \omega(f) + \omega(g),$$

donc $fg \neq 0$; par suite $A[[X]]$ est intègre.

Réciproquement, si $A[[X]]$ est intègre, alors A est intègre, en tant que sous-anneau de $A[[X]]$. □

Remarque 7.8. Dans le cas où A est intègre, l'ordre ω est une *valuation* ([39], [63]), car pour f et g non nuls on a $\omega(fg) = \omega(f) + \omega(g)$.

Proposition 7.9. *Pour tout anneau unitaire, commutatif A , et tout $m \in \mathbb{N}$, l'ensemble J_m des séries formelles $f \in A[[X]]$ telles que $\omega(f) \geq m$ est l'idéal de $A[[X]]$ engendré par X^m .*

Preuve : On remarque que pour tout $m \in \mathbb{N}$, $0 \in J_m$ et le Th. 7.6. permet de vérifier que

$$\begin{aligned}(f, g) \in J_m \times J_m &\implies (f+g) \in J_m; \quad f \in J_m \implies -f \in J_m; \\ (f, h) \in J_m \times A[[X]] &\implies fh = hf \in J_m.\end{aligned}$$

On en conclut que J_m est un idéal de $A[[X]]$. De plus

$$\begin{aligned}(f \in J_0 &\iff \omega(f) \geq 0), \text{ donc } J_0 = A[[X]]; \\ (\forall m \geq 1) (f \in J_m &\iff f = X^m g, \omega(g) \geq 0),\end{aligned}$$

donc $J_m = X^m A[[X]]$. □

C. Notion de famille sommable dans $A[[X]]$

Définition 7.10. Soit $\{f_\lambda\}_{\lambda \in \Lambda}$ une famille non vide de séries formelles dans $A[[X]]$. Cette famille est dite **sommable** si pour tout $n \in \mathbb{N}$, il n'existe qu'un nombre fini d'éléments $\lambda \in \Lambda$ pour lesquels $\omega(f_\lambda) \leq n$.

Remarque 7.11. $\{f_\lambda\}_{\lambda \in \Lambda}$ étant une famille sommable dans $A[[X]]$, pour tout $\lambda \in \Lambda$, posons $f_\lambda = \sum_{n \geq 0} a_{\lambda,n} X^n$; alors, quel que soit n fixé dans $\mathbb{N}$, l'ensemble

$$\{\lambda \in \Lambda; a_{\lambda,n} \neq 0\}$$

est une partie finie de Λ , autrement dit, la suite $(a_{\lambda,n})_{\lambda \in \Lambda}$ est à support fini.

On en déduit que $\sum_{\lambda \in \Lambda} a_{\lambda,n}$ est la somme d'un nombre fini d'éléments de A .

Pour tout $n \in \mathbb{N}$, on pose

$$c_n := \sum_{\lambda \in \Lambda} a_{\lambda,n};$$

on considère alors, la série formelle

$$f := \sum_{n \geq 0} c_n X^n. \quad (7.2)$$

Définition 7.12. Dans le contexte ci-dessus, la série formelle f définie par la relation (7.2) est appelée **somme** de la famille sommable $\{f_\lambda\}_{\lambda \in \Lambda}$ et on écrit symboliquement

$$f = \sum_{\lambda \in \Lambda} f_\lambda.$$

Remarque 7.13. Toute sous-famille d'une famille sommable est sommable.

Exemple 7.14. :

1) Toute famille finie de séries formelles de $A[[X]]$ est sommable.

2) Toute série formelle $f = \sum_{n \geq 0} a_n X^n$ dans $A[[X]]$ peut être considérée comme la somme de la famille sommable $\{f_n = a_n X^n\}_{n \in \mathbb{N}}$.

Proposition 7.15. Dans $A[[X]]$, une famille de séries formelles $\{f_k\}_{k \in \mathbb{N}}$ telle que pour tout $k \in \mathbb{N}$, $\omega(f_k) \geq k$, est sommable.

Preuve : Pour tout $k \in \mathbb{N}$, posons $f_k = \sum_{n \geq 0} a_{k,n} X^n$.

Par hypothèse, pour tout $k \in \mathbb{N}$, on a $\omega(f_k) \geq k$; alors pour k fixé dans $\mathbb{N}$,

$$(n \in \mathbb{N} \text{ et } 0 \leq n < k) \implies a_{k,n} = 0.$$

Par suite, pour tout n dans $\mathbb{N}$,

$$a_{k,n} \neq 0 \implies 0 \leq k \leq n,$$

donc la famille $\{f_k\}_{k \in \mathbb{N}}$ considérée est sommable. $\square$

Corollaire 7.16. Si A est intègre et si $f \in A[[X]]$ est tel que $\omega(f) \geq 1$, alors quel que soit $g = \sum_{n \geq 0} b_n X^n$ dans $A[[X]]$, la famille $\{b_n f^n\}_{n \in \mathbb{N}}$ est sommable.

Preuve : Si A est intègre, alors (Th. 7.6.) quel que soit $n \in \mathbb{N}$, on a

$$(\omega(f^n) = n\omega(f) \geq n) \implies \omega(b_n f^n) \geq n,$$

donc, d'après la proposition 7.15., la famille $\{b_n f^n\}_{n \in \mathbb{N}}$ est sommable. $\square$

Théorème 7.17. Soit $\{f_\lambda\}_{\lambda \in \Lambda}$ une famille sommable dans $A[[X]]$.

1) Pour tout $g \in A[[X]]$, la famille $\{f_\lambda g\}_{\lambda \in \Lambda}$ est sommable et

$$\sum_{\lambda \in \Lambda} f_\lambda g = (\sum_{\lambda \in \Lambda} f_\lambda) g.$$

2) Si $\{P_i\}_{i \in I}$ est une partition de l'ensemble Λ et si pour tout $i \in I$, on pose $g_i := \sum_{\lambda \in P_i} f_\lambda$, alors

$$\sum_{\lambda \in \Lambda} f_\lambda = \sum_{i \in I} g_i.$$

Preuve : Pour tout $\lambda \in \Lambda$, posons $f_\lambda = \sum_{n \geq 0} a_{\lambda,n} X^n$ et considérons un élément quelconque $g = \sum_{n \geq 0} b_n X^n$ dans $A[[X]]$.

1) Par hypothèse, pour n fixé dans $\mathbb{N}$, il n'existe qu'un nombre fini d'éléments $\lambda \in \Lambda$ tels que $a_{\lambda,n} \neq 0$. D'autre part,

$$f_\lambda g = \sum_{n \geq 0} c_{\lambda,n} X^n, \text{ où } c_{\lambda,n} = \sum_{0 \leq p \leq n} a_{\lambda,p} b_{n-p}. \quad (7.3)$$

Si n est fixé dans $\mathbb{N}$, alors pour tout entier p , $0 \leq p \leq n$, il n'existe qu'un nombre fini de $\lambda \in \Lambda$ tels que $a_{\lambda,p} \neq 0$. On en déduit qu'il n'existe qu'un nombre fini de $f_\lambda g$ tels que pour tout $n \in \mathbb{N}$, $\omega(f_\lambda g) \leq n$, donc la famille $\{f_\lambda g\}_{\lambda \in \Lambda}$ est sommable ; calculons sa somme.

Pour la famille sommable $\{f_\lambda\}_{\lambda \in \Lambda}$, on peut écrire

$$\sum_{\lambda \in \Lambda} f_\lambda := \sum_{n \geq 0} c_n X^n, \text{ où } c_n = \sum_{\lambda \in \Lambda} a_{\lambda,n}.$$

$$\begin{aligned} \text{On en déduit : } (\sum_{\lambda \in \Lambda} f_\lambda)g &= \sum_{n \geq 0} (\sum_{0 \leq p \leq n} c_p b_{n-p}) X^n, \\ c_p b_{n-p} &= (\sum_{\lambda \in \Lambda} a_{\lambda,p}) b_{n-p} = \sum_{\lambda \in \Lambda} a_{\lambda,p} b_{n-p}, \end{aligned}$$

$$\text{d'où } \sum_{0 \leq p \leq n} c_p b_{n-p} = \sum_{\lambda \in \Lambda} (\sum_{0 \leq p \leq n} a_{\lambda,p} b_{n-p}) = \sum_{\lambda \in \Lambda} c_{\lambda,n}.$$

En tenant compte de la relation (7.3), on obtient

$$(\sum_{\lambda \in \Lambda} f_\lambda)g = \sum_{n \geq 0} (\sum_{\lambda \in \Lambda} c_{\lambda,n}) X^n = \sum_{\lambda \in \Lambda} (f_\lambda g).$$

2) Par hypothèse, $\{f_\lambda\}_{\lambda \in \Lambda}$ est une famille sommable, donc pour tout $i \in I$, la sous-famille $\{f_\lambda\}_{\lambda \in P_i}$ est sommable et si g_i est sa somme, on a

$$g_i = \sum_{\lambda \in P_i} f_\lambda = \sum_{n \geq 0} b_{i,n} X^n, \text{ où } \forall (i, n) \in I \times \mathbb{N}, b_{i,n} = \sum_{\lambda \in P_i} a_{\lambda,n}.$$

Quels que soient $n \in \mathbb{N}$ et $i \in P_i$, il n'existe qu'un nombre fini de $\lambda \in P_i$ tels que $\omega(f_\lambda) \leq n$; on en déduit que pour la famille de séries formelles $\{g_i\}_{i \in I}$ il n'existe qu'un nombre fini d'éléments $i \in I$ tels que $\omega(g_i) \leq n$; donc la famille $\{g_i\}_{i \in I}$ est sommable et

$$\sum_{\lambda \in \Lambda} f_\lambda = \sum_{i \in I} (\sum_{\lambda \in P_i} f_\lambda) = \sum_{i \in I} g_i. \quad \square$$

D. Substitution d'une série formelle dans une autre

Définition 7.18. Soit $f \in A[[X]]$ tel que $\omega(f) \geq 1$.

Quel que soit $g = \sum_{n \geq 0} b_n X^n$, non nul, dans $A[[X]]$, on appelle composée de g par f la série formelle notée $g \circ f$ ou $g(f)$ telle que

$$g \circ f := \sum_{n \geq 0} b_n f^n.$$

On dit que la série formelle $g \circ f$ est obtenue par **substitution** de f à X dans g . Dans le cas où $g = 0$, on a $g \circ f = 0$.

Exemple 7.19. Avec les hypothèses et notations de la définition 7.18.,

$$1) g = X \implies g \circ f = f.$$

$$2) f = X \implies g \circ f = g.$$

Proposition 7.20. Pour f et g dans $A[[X]]$ tels que $\omega(f) \geq 1$, on a

$$\omega(g \circ f) \geq \omega(g) \omega(f).$$

Preuve : On suppose $g \neq 0$ et $g = \sum_{n \geq 0} b_n X^n$. Si $\omega(g) = p$, alors

$$g \circ f = f^p \sum_{n \geq p} b_n f^{n-p}, \quad b_p \neq 0.$$

D'après le résultat 2) du théorème 7.6., on a $\omega(f^p) \geq p \omega(f)$, d'où $\omega(g \circ f) \geq \omega(g) \omega(f)$. □

Théorème 7.21. *Si A est un D.I., alors*

1) *Pour tout $f \in A[[X]]$ tel que $\omega(f) \geq 1$, l'application*

$$\begin{aligned} \phi : A[[X]] &\longrightarrow A[[X]] \quad \text{est un morphisme de } A\text{-algèbres.} \\ s &\longmapsto s \circ f \end{aligned}$$

2) *Quels que soient f, g, h dans $A[[X]]$ tels que $\omega(f) \geq 1, \omega(g) \geq 1$,*

$$h \circ (g \circ f) = (h \circ g) \circ f. \quad (7.4)$$

Preuve :

1) On vérifie facilement que ϕ est A -linéaire.

Soit s_1, s_2 dans $A[[X]]$, montrons que $\phi(s_1 s_2) = \phi(s_1) \phi(s_2)$.

Pour $i = 1, 2$, posons $s_i = \sum_{n \geq 0} a_{i,n} X^n$;

$$\begin{aligned} s_1 s_2 &= \sum_{n \geq 0} b_n X^n, \quad \text{où } b_n = \sum_{p+q=n} a_{1,p} a_{2,q}; \\ s_1 s_2 \circ f &= \sum_{n \geq 0} b_n f^n = \sum_{n \geq 0} \left(\sum_{p+q=n} a_{1,p} a_{2,q} \right) f^p f^q. \end{aligned}$$

Par hypothèse, A est intègre et $\omega(f) \geq 1$; par suite, la famille $(f^n)_{n \in \mathbb{N}} = (f^{p+q})_{(p+q) \in \mathbb{N}}$ est sommable (Cor. 7.16.), d'où (Th. 7.17.)

$$\begin{aligned} \sum_{(p,q) \in \mathbb{N}} a_{1,p} a_{2,q} f^p f^q &= \sum_{q \in \mathbb{N}} a_{2,q} \left(\sum_{p \in \mathbb{N}} a_{1,p} f^p \right) f^q \\ &= (s_1 \circ f)(s_2 \circ f); \\ \sum_{(p,q) \in \mathbb{N}} a_{1,p} a_{2,q} f^{p+q} &= \sum_{n \in \mathbb{N}} \left(\sum_{p+q=n} a_{1,p} a_{2,q} \right) f^{p+q}; \end{aligned}$$

on en conclut que $s_1 s_2 \circ f = (s_1 \circ f)(s_2 \circ f)$.

2) En tenant compte des hypothèses : $\omega(f) \geq 1, \omega(g) \geq 1$, on démontre la relation (7.4).

Soit $h \in A[[X]]$, pour tout $n \in \mathbb{N}$, on écrit (Rem. 7.5., b)) :

$$\begin{aligned} h &= h_n + r_n, \quad \text{où } h_n \in A[X], r_n \in A[[X]], \omega(r_n) > n; \\ \text{alors, } h \circ (g \circ f) - (h \circ g) \circ f &= h_n \circ (g \circ f) - (h_n \circ g) \circ f + v_n, \\ \text{et } (v_n = r_n \circ (g \circ f) - (r_n \circ f) \circ g) &\implies \omega(v_n) \geq \omega(r_n) > n. \end{aligned}$$

Alors, $(\omega(h \circ (g \circ f) - (h \circ g) \circ f) > n, \forall n \in \mathbb{N}) \implies h \circ (g \circ f) - (h \circ g) \circ f = 0$. □

E. Notion de série formelle dérivée dans $A[[X]]$

Définition 7.22. Soit $f = \sum_{n \geq 0} a_n X^n$ dans $A[[X]]$; on appelle **série formelle dérivée** de f la série formelle notée f' telle que

$$f' := \sum_{n \geq 0} (n+1) a_{n+1} X^n.$$

Propriétés élémentaires (à vérifier par le lecteur)

$$\begin{array}{lll} \text{L'application} & \delta : A[[X]] \longrightarrow A[[X]] & \text{est } A\text{-linéaire} \\ & f \longmapsto f' & \end{array}$$

et quels que soient f et g dans $A[[X]]$,

$$1) (fg)' = f'g + fg'.$$

$$2) \text{ En supposant } \omega(f) \geq 1, (g \circ f)' = (g' \circ f)f'.$$

$$3) \text{ Si } f \text{ est inversible, alors } (f^{-1})' = -f^{-2}f'.$$

$$4) \text{ Lorsque } \text{car} A = 0, \text{ on a } \text{Ker } \delta = A.$$

$$5) \text{ Si } A \text{ est un corps noté } K \text{ et } \text{car} K = 0, \text{ alors } \delta \text{ est surjectif et pour}$$

$$f = \sum_{n \geq 0} a_n X^n \text{ dans } K[[X]], \text{ on a}$$

$$f = \delta(f_1), \text{ où } f_1 = c + \sum_{n \geq 0} \frac{a_n}{n+1} X^{n+1}, c \text{ étant quelconque dans } K.$$

2. Éléments inversibles dans l'anneau $A[[X]]$

L'exemple de la série formelle $\sum_{n \geq 0} X^n = (1 - X)^{-1}$ montre que, quel que soit l'anneau unitaire commutatif A , il existe, dans $A[[X]]$, des éléments inversibles autres que les unités de A (Rem. 7.3.) ; ces éléments sont caractérisés par la propriété suivante.

Théorème 7.23. Dans l'anneau unitaire commutatif $A[[X]]$, un élément

$f = \sum_{n \geq 0} a_n X^n$ est inversible si et seulement si le coefficient a_0 est inversible dans A .

En particulier, si K est un corps, alors

$$f \in K[[X]] \text{ est inversible} \iff \omega(f) = 0.$$

Preuve : Soit $f = \sum_{n \geq 0} a_n X^n$ dans $A[[X]]$. Supposons a_0 inversible dans A et posons

$$f_1 = a_0^{-1} f = 1 + \sum_{n \geq 1} b_n X^n, \text{ où } \forall n \geq 1, b_n = a_0^{-1} a_n.$$

Cherchons $g_1 := \sum_{n \geq 0} c_n X^n$ dans $A[[X]]$ tel que $f_1 g_1 = 1$.

$$f_1 g_1 = 1 \iff c_0 = 1 \text{ et } \forall n \geq 1, \sum_{i+j=n} b_i c_j = 0.$$

$$c_0 = 1 \text{ et } b_1 c_0 + c_1 = 0 \implies c_1 = -b_1$$

$$b_2 c_0 + b_1 c_1 + c_2 = 0 \implies c_2 = b_1^2 - b_2.$$

Ainsi, par récurrence sur $n \geq 1$, le coefficient c_n peut être calculé en fonction des $b_i, i \geq 0$, où $b_0 = 1$, d'où l'existence de $g_1 = f_1^{-1}$ et

$$f_1 g_1 = 1 \implies a_0^{-1} f g_1 = 1 \implies a_0^{-1} g_1 = a_0^{-1} f_1^{-1} = f^{-1}$$

Réciproquement, si f est inversible dans $A[[X]]$ et g est son inverse, alors

$$(f = \sum_{n \geq 0} a_n X^n, g = \sum_{n \geq 0} c_n X^n, fg = 1) \implies a_0 c_0 = 1,$$

donc a_0 est inversible dans A . □

Remarque 7.24. D'après le théorème précédent, si $f = \sum_{n \geq 0} a_n X^n$ est tel que $a_0 = 0$, alors $1 - f$ est inversible dans $A[[X]]$ et on obtient $(1 - f)^{-1}$ en substituant f à X dans la relation $(1 - X)(\sum_{n \geq 0} X^n) = 1$, d'où

$$(1 - f)^{-1} = \sum_{n \geq 0} f^n.$$

Appliquons cette remarque dans la première partie de la preuve du théorème 7.23. ; avec les notations de cette preuve, on a

$$1 - f_1 = \sum_{n \geq 0} -b_n X^n, \text{ où } b_0 = 0.$$

Par suite, $1 - (1 - f_1) = f_1$ est inversible et $f_1^{-1} = \sum_{n \geq 0} (\sum_{i \geq 1} -b_i X^i)^n$, d'où l'on déduit, $f^{-1} = a_0^{-1} f_1^{-1}$.

Corollaire 7.25. Si A est un D.I. et $f = \sum_{n \geq 0} a_n X^n \in A[[X]]$, alors a_0 irréductible dans $A \implies f$ irréductible dans $A[[X]]$.

(La réciproque est fausse).

Preuve : Le terme constant a_0 de f étant irréductible dans A , supposons g et h dans $A[[X]]$ tels que $f = gh$.

Si les termes constants de g et h sont, respectivement, b_0 et c_0 , alors

$$(a_0 = b_0 c_0 \text{ et } a_0 \text{ irréductible}) \implies b_0 \in U_A \text{ ou } c_0 \in U_A.$$

Par suite (Th. 7.23.), g est inversible ou h est inversible, donc f est irréductible dans le domaine d'intégrité $A[[X]]$.

La réciproque est fausse, car, par exemple, X est irréductible dans $A[[X]]$ et son terme constant est nul. $\square$

Notations : K étant un corps, pour tout $f = \sum_{n \geq 0} a_n X^n$ dans $K[[X]]$ et tout entier $k \geq 0$, on pose (Rem. 7.5., b))

$$f_k = \sum_{0 \leq i \leq k} a_i X^i, \text{ donc } \omega(f - f_k) \geq k + 1.$$

Proposition 7.26. Compte tenu des notations ci-dessus, soit f et g dans $K[[X]]$; si g est inversible dans $K[[X]]$ et si l'on considère la série formelle fg^{-1} , alors pour tout $k \in \mathbb{N}$, le polynôme $(fg^{-1})_k$ est le quotient de la division suivant les puissances croissantes, à l'ordre k , de f_k par g_k (Cf. Th. 4.51.).

Preuve : L'entier k étant fixé dans $\mathbb{N}$, posons

$$r_k = f - f_k, s_k = g - g_k, \text{ d'où } \omega(r_k) \geq k + 1, \omega(s_k) \geq k + 1.$$

g est inversible dans $K[[X]]$, donc $\omega(g) = \omega(g_k) = 0$, par suite g_k est inversible dans $K[[X]]$ et

$$\begin{aligned} f g_k - f_k g &= (f g^{-1} - f_k g_k^{-1}) g g_k, \\ f g_k - f_k g &= (r_k + f_k) g_k - f_k (s_k + g_k) \\ &= r_k g_k - f_k s_k, \quad \text{d'où} \end{aligned}$$

$$f g^{-1} - f_k g_k^{-1} = (g g_k)^{-1} (r_k g_k - f_k s_k) \implies \omega(f g^{-1} - f_k g_k^{-1}) \geq k + 1.$$

Or la division suivant les puissances croissantes de f_k par g_k à l'ordre k donne

$$f_k = g_k q_k + \sigma_k X^{k+1}, \text{ où } q_k, \sigma_k \text{ sont uniques dans } K[X] \text{ et } \deg q_k \leq k.$$

On a donc $\omega(f_k g_k^{-1} - q_k) \geq k + 1$ et par suite

$$\omega(f g^{-1} - q_k) \geq \inf \{ \omega(f g^{-1} - f_k g_k^{-1}), \omega(f_k g_k^{-1} - q_k) \} \geq k + 1.$$

On en conclut que $(f g^{-1})_k = q_k$. $\square$

3. Propriétés de l'anneau $A[[X]]$

Proposition 7.27. Si K est un corps, alors $K[[X]]$ est un anneau local.

Preuve : Pour montrer que $K[[X]]$ est un anneau local, il suffit de prouver que dans cet anneau, l'ensemble, noté M , des éléments non inversibles forme un idéal (Th. 2.77.). Le théorème 7.23. implique que pour $f \in K[[X]]$, on a

$$f \in M \iff \omega(f) \geq 1;$$

par suite, M est l'idéal de $K[[X]]$ engendré par X (Prop. 7.9.), c'est alors l'unique idéal maximal de $K[[X]]$ (Voir la preuve du Th. 2.77.). $\square$

Remarque 7.28. Compte tenu de la proposition 7.9., pour tout entier $k \geq 1$, l'ensemble des éléments f de $K[[X]]$ tels que $\omega(f) \geq k$ forme l'idéal M^k engendré par X^k ; on en déduit que

$$\bigcap_{k \geq 1} M^k = (0).$$

Théorème 7.29. K étant un corps, l'anneau $K[[X]]$ est un domaine principal et les idéaux de $K[[X]]$ sont les (X^p) , pour $p \in \mathbb{N}$.

Preuve : On sait que $K[[X]]$ est un D.I., il reste à montrer que tout idéal propre, non nul I de $K[[X]]$ est principal.

Soit f un élément d'ordre minimal dans I . Supposons $\omega(f) = p$; on a $p \geq 1$, car I est un idéal propre de $K[[X]]$.

On peut écrire $f = X^p g$, où $\omega(g) = 0$, donc g est inversible dans $K[[X]]$; alors,

$$f g^{-1} = X^p \in I \implies (X^p) = X^p K[[X]] \subseteq I.$$

D'autre part, la minimalité de l'ordre de f implique $\omega(h) \geq p$, pour tout $h \in I$, d'où $I \subseteq (X^p)$ (Prop. 7.9); donc I est l'idéal principal de $K[[X]]$ engendré par X^p . $\square$

Théorème 7.30. Si A est un anneau local, alors $A[[X]]$ est local.

Preuve : Notons $\mathcal{M}$ l'unique idéal maximal de A . On sait que $\mathcal{M}$ est l'ensemble des éléments non inversibles de A . Soit M l'ensemble des éléments non inversibles de $A[[X]]$. On a nécessairement (Th. 7.23),

$$f = \sum_{n \geq 0} a_n X^n \in M \iff a_0 \in \mathcal{M}.$$

Vérifions que M est un idéal de $A[[X]]$. On a $0 \in M$; et si f et g , dans M , ont pour termes constants respectifs a_0 et b_0 , alors,

$$(a_0, b_0) \in \mathcal{M} \times \mathcal{M} \implies (a_0 - b_0) \in \mathcal{M}$$

$$\text{d'où } (f, g) \in M \times M \implies (f - g) \in M.$$

D'autre part, quels que soient $f \in M$ et $s \in A[[X]]$, de termes constants respectifs a_0 et s_0 ,

$$(a_0 \in \mathcal{M}, s_0 \in A) \implies a_0 s_0 \in \mathcal{M} \implies fs \in M.$$

Ainsi, dans $A[[X]]$, l'ensemble M des éléments non inversibles est un idéal, donc $A[[X]]$ est un anneau local (Th. 2.77). $\square$

Remarque 7.31. La proposition 7.27. peut apparaître comme un corollaire du théorème 7.30., puisqu'un corps est un anneau local.

Théorème 7.32. A étant un anneau unitaire, commutatif, alors

$$A \text{ noethérien} \implies A[[X]] \text{ noethérien}.$$

Preuve : Soit B un idéal propre et non nul de $A[[X]]$. Il s'agit de prouver que B est de type fini. Pour tout $j \in \mathbb{N}$, posons

$$I_j = \{b_j \in A; \exists g_j \in A[[X]], \text{ tel que } \omega(g_j) > j \text{ et } (b_j X^j + g_j) \in B\}.$$

On a $0 \in I_j$, donc $I_j \neq \emptyset$; vérifions que pour tout $j \in \mathbb{N}$, I_j est un idéal de A et $I_j \subseteq I_{j+1}$.

Soit b_j et c_j dans I_j ; il existe g_j et h_j dans $A[[X]]$ tels que

$$(b_j X^j + g_j) \in B, \omega(g_j) > j \quad \text{et} \quad (c_j X^j + h_j) \in B, \omega(h_j) > j.$$

B est un idéal de $A[[X]]$, donc

$$(b_j - c_j) X^j + (g_j - h_j) \in B$$

$$\text{et } \omega(g_j - h_j) \geq \inf \{\omega(g_j), \omega(h_j)\} > j \implies (b_j - c_j) \in I_j.$$

D'autre part, soit $a \in A$ et $b_j \in I_j$; B étant un idéal,

$(b_j X^j + g_j) \in B$, $\omega(g_j) > j \implies (ab_j X^j + ag_j) \in B$, $\omega(ag_j) > j$,
d'où $ab_j \in I_j$. On en déduit que I_j est un idéal de A ; de plus,

$(b_j X^j + g_j) \in B$, $\omega(g_j) > j \implies (b_j X^{j+1} + g_j X) \in B$, $\omega(g_j X) > j+1$;
par suite $b_j \in I_j$ implique $b_j \in I_{j+1}$, on a ainsi $I_j \subseteq I_{j+1}$.

Par hypothèse A est noethérien, donc la chaîne croissante d'idéaux

$$I_0 \subseteq I_1 \subseteq \dots \subseteq I_j \subseteq I_{j+1} \dots$$

est finie; il existe $m \in \mathbb{N}$ tel que pour tout $j \geq m$, $I_j = I_m$, par suite

$$\bigcup_{j \in \mathbb{N}} I_j = \bigcup_{0 \leq j \leq m} I_j = I_m. \quad (7.5)$$

Pour tout $j \in \mathbb{N}$, l'idéal I_j de A est de type fini; soit $\{b_{j,1}, \dots, b_{j,k_j}\}$, où $k_j \in \mathbb{N}^*$, une famille génératrice finie de I_j . Pour tout i ($1 \leq i \leq k_j$), il existe $g_{j,i} \in A[[X]]$ tel que

$$\omega(g_{j,i}) > j \quad \text{et} \quad f_{j,i} := (b_{j,i} X^j + g_{j,i}) \in B. \quad (7.6)$$

Démontrons que l'idéal B est engendré par la famille finie

$$\mathcal{F} := \{f_{0,1}, \dots, f_{0,k_0}, f_{1,1}, \dots, f_{1,k_1}, \dots, f_{m,1}, \dots, f_{m,k_m}\}. \quad (7.7)$$

Soit J_m l'idéal de $A[[X]]$ formé par l'ensemble des séries formelles s telles que $\omega(s) \geq m$ (Prop. 7.9.). Posons $B_m = B \cap J_m$; B_m est un idéal de $A[[X]]$.

1) Soit $f \in B_m$; on a donc $f \in B$ et $n := \omega(f) \geq m$. On peut écrire

$$f = bX^n + g, \quad \text{où } b \in A^*, g \in A[[X]], \omega(g) > n \geq m.$$

D'après la définition des idéaux I_j de A et la relation (7.6), $f \in B$ entraîne $b \in I_n = I_m$.

L'idéal I_m est engendré par $\{b_{m,1}, \dots, b_{m,k_m}\}$, d'où

$$b = \sum_{1 \leq i \leq k_m} a_{1,i} b_{m,i}, \quad \text{où } \forall i (1 \leq i \leq k_m), a_{1,i} \in A,$$

$$\text{et} \quad f = (\sum_{1 \leq i \leq k_m} a_{1,i} b_{m,i}) X^n + g.$$

Posons $h_1 := \sum_{1 \leq i \leq k_m} a_{1,i} X^{n-m} f_{m,i}$; on a $h_1 \in B$, donc

$$(f - h_1) \in B \quad \text{et} \quad n_1 := \omega(f - h_1) \implies n_1 > n \geq m.$$

En réitérant le procédé à partir de $f - h_1$, on obtient $h_2 \in B$ de la forme

$$h_2 = \sum_{1 \leq i \leq k_m} a_{2,i} X^{n_1-m} f_{m,i}, \quad \text{où } \forall i (1 \leq i \leq k_m), a_{2,i} \in A,$$

$$\text{et} \quad (f - h_1 - h_2) \in B, \quad n_2 := \omega(f - h_1 - h_2) \implies n_2 > n_1 > n \geq m.$$

Ainsi, par récurrence, on détermine, pour tout $r \in \mathbb{N}^*$, la série formelle h_r telle que

$$h_r = \sum_{1 \leq i \leq k_m} a_{r,i} X^{n_{r-1}-m} f_{m,i}, \quad \text{où } \forall i (1 \leq i \leq k_m), a_{r,i} \in A \text{ et}$$

$$(f - \sum_{1 \leq p \leq r} h_p) \in B, \quad \omega(f - \sum_{1 \leq p \leq r} h_p) = n_r > n_{r-1} > \dots > n_1 > n \geq m.$$

Pour tout i ($1 \leq i \leq k_m$), posons $s_i = \sum_{r \geq 1} a_{r,i} X^{n_{r-1}-m}$ dans $A[[X]]$; alors

$$f - \sum_{1 \leq i \leq k_m} s_i f_{m,i} = f - \sum_{r \geq 1} h_r.$$

Or la suite des entiers $n_r = \omega(f - \sum_{1 \leq p \leq r} h_p)$ est strictement croissante dans $\mathbb{N}$, ce qui entraîne

$$f - \sum_{r \geq 1} h_r = 0, \quad \text{d'où} \quad f = \sum_{1 \leq i \leq k_m} s_i f_{m,i}.$$

On en déduit que l'idéal $B_m = B \cap J_m$ est engendré par $\{f_{m,1}, \dots, f_{m,k_m}\}$.

2) Supposons $f \in B$ et $\omega(f) = j$, $0 \leq j < m$. Notons B' l'idéal de $A[[X]]$ engendré par $\mathcal{F} \setminus \{f_{m,1}, \dots, f_{m,k_m}\}$ et montrons qu'il existe $\varphi \in B'$ tel que $(f - \varphi) \in B_m$.

$$\begin{aligned} \omega(f) = j &\implies f = bX^j + g, \quad b \in A^*, \quad g \in A[[X]], \quad \omega(g) \geq j+1; \\ f \in B &\implies b \in I_j \implies b = \sum_{1 \leq i \leq k_j} a_{1,i} b_{j,i}, \quad \text{où } \forall i (1 \leq i \leq k_j), a_{1,i} \in A. \end{aligned}$$

Posons $\varphi_1 := \sum_{1 \leq i \leq k_j} a_{1,i} f_{j,i}$; on a alors $\varphi_1 \in B' \subset B$ et

$$j_1 := \omega(f - \varphi_1) \implies j_1 \geq j+1 > j.$$

Si $j_1 < m$, on réitère le procédé à partir de $(f - \varphi_1) \in B$; on obtient

$$\begin{aligned} \varphi_2 &= \sum_{1 \leq i \leq k_{j_1}} a_{2,i} f_{j_1,i}, \quad \varphi_2 \in B', \quad (f - \varphi_1 - \varphi_2) \in B \\ j_2 &:= \omega(f - \varphi_1 - \varphi_2) \implies j_2 \geq j_1 + 1 \geq j+1 > j. \end{aligned}$$

Si $j_2 < m$, on poursuit le raisonnement par récurrence et il existe, nécessairement, un plus petit entier $r \geq 1$ tel que $\omega(f - \varphi_1 - \varphi_2 - \dots - \varphi_r) \geq m$.

Les φ_p , pour $1 \leq p \leq r$, sont dans B' . Posons $\varphi := \sum_{1 \leq p \leq r} \varphi_p$; alors

$$\varphi \in B', \quad (f - \varphi) \in B, \quad \omega(f - \varphi) \geq m, \quad \text{donc } (f - \varphi) \in B_m.$$

On en conclut, compte tenu de la première partie de la démonstration, que l'idéal B est engendré par la famille finie $\mathcal{F}$ (Cf. Rel. (7.7)). $\square$

Remarque 7.33. Si A est un anneau factoriel, alors $A[[X]]$ n'est pas nécessairement factoriel. Pierre SAMUEL a prouvé l'existence d'un anneau factoriel et noethérien A tel que l'anneau $A[[X]]$ n'est pas factoriel [54].

On a cependant le résultat suivant.

Théorème 7.34. Si A est un domaine principal, alors $A[[X]]$ est un anneau factoriel et noethérien.

Preuve : Si A est un domaine principal, alors A est noethérien, donc $A[[X]]$ est noethérien (Th. 7.32.).

Pour démontrer que $A[[X]]$ est factoriel il suffit de prouver que tout idéal premier, non nul, P de $A[[X]]$ contient un élément premier (Cf. Th. 5.96.).

X est un élément premier dans le domaine d'intégrité $A[[X]]$, donc tout idéal premier P contenant X contient un élément premier.

Considérons un idéal premier, non nul P de $A[[X]]$ tel que $X \notin P$. Soit

$$\begin{aligned} \sigma : A[[X]] &\longrightarrow A \\ \sum_{n \geq 0} a_n X^n &\longmapsto a_0 \end{aligned}$$

Posons $P_0 = \sigma(P)$; σ est un morphisme surjectif de A -algèbres, par suite P_0 est un idéal non nul du domaine principal A , donc il existe $b \neq 0$ dans A , tel que $P_0 = (b)$. On en déduit qu'il existe $f \in P$ tel que $\sigma(f) = b$ donc f s'écrit

$$f = b + X f_1, \text{ où } f_1 \in A[[X]].$$

Montrons que f engendre l'idéal P , dans $A[[X]]$. Soit $g \in P$;

$$\sigma(g) = a \implies g = a + X g_0, \text{ où } g_0 \in A[[X]],$$

$$a \in P_0 \implies \exists a_0 \in A \text{ tel que } a = a_0 b.$$

En posant $h_0 = g_0 - a_0 f_1$, on obtient

$$g - a_0 f = X h_0 \implies \omega(g - a_0 f) \geq 1.$$

$$(f \text{ et } g \text{ dans } P) \implies X h_0 \in P,$$

mais P est un idéal premier, $X \notin P$, donc $h_0 \in P$.

$$\sigma(h_0) \in (b) \implies \sigma(h_0) = a_1 b, a_1 \in A, \text{ alors } h_0 = a_1 b + X g_1, \text{ où } g_1 \in A[[X]]$$

$$\text{et } f = b + X f_1 \implies h_0 - a_1 f = X(f_1 - a_1 g_1).$$

En posant $h_1 = f_1 - a_1 g_1$, on peut écrire

$$h_0 - a_1 f = X h_1 \text{ et } h_1 \in P, \text{ car } X \notin P;$$

$$\text{d'où } g - (a_0 + a_1 X) f = X^2 h_1 \implies \omega(g - (a_0 + a_1 X) f) \geq 2.$$

Par récurrence, on obtient, pour tout entier $r \geq 1$,

$$g - (a_0 + a_1 X + a_2 X^2 + \dots + a_r X^r) f = X^{r+1} h_r, \text{ où } h_r \in P,$$

$$\text{donc, } \omega(g - (\sum_{0 \leq i \leq r} a_i X^i) f) \geq r+1.$$

On détermine ainsi la série formelle $s = \sum_{i \geq 0} a_i X^i$; la croissance des ordres

$\omega(g - (\sum_{0 \leq i \leq r} a_i X^i) f)$ en fonction de $r \in \mathbb{N}$ entraîne $g = s f$, d'où $P = (f)$.

P étant un idéal premier non nul, l'élément f est premier dans $A[[X]]$ (Prop. 5.22.).

On en conclut (Th. 5.96.) que $A[[X]]$ est un anneau factoriel. $\square$

Remarque 7.35. :

a) Si A est un D.P., il n'en n'est pas de même de $A[[X]]$.

On pourra vérifier, en particulier, que l'anneau $\mathbb{Z}[[X]]$ n'est pas principal, en montrant que l'idéal engendré par 2 et X n'est pas principal.

b) On peut s'inspirer de la méthode utilisée dans la preuve du théorème 7.34., pour donner une autre démonstration du théorème 7.32. Celle-ci consiste à montrer que, si A est noethérien, alors tout idéal premier de $A[[X]]$ est de type fini, ce qui entraîne $A[[X]]$ noethérien (Th. 2.85.).

(Voir Ex. 3, à la fin du chapitre.)

4. Séries formelles et fractions rationnelles

Dans tout ce paragraphe, on considère des séries formelles et des fractions rationnelles à coefficients dans un corps K .

A priori, on supposera qu'une fraction rationnelle non nulle $\frac{p}{q}$ est écrite sous sa forme irréductible, c'est-à-dire $p \wedge q = 1$ dans l'anneau $K[X]$.

On sait que tout polynôme de $K[X]$, dont le terme constant est non nul, est inversible dans l'anneau $K[[X]]$ (Th. 7.23.). On en déduit qu'à toute fraction rationnelle non nulle

$f = \frac{p}{q} \in K(X)$ telle que $q(0) \neq 0$, on peut associer l'élément $p q^{-1}$ de $K[[X]]$.

Notons $K(X)_0$ l'ensemble des éléments $\frac{p}{q}$ du corps $K(X)$ n'ayant pas le pôle 0, c'est-à-dire tels que $q(0) \neq 0$. On vérifie facilement que $K(X)_0$ est une sous-K-algèbre du corps $K(X)$ et il est immédiat que $K[X] \subset K(X)_0$.

Proposition 7.36. *Il existe un unique morphisme injectif de K-algèbres, de $K(X)_0$ dans $K[[X]]$, que l'on notera ψ , tel que $\psi|_{K[X]} = id_{K[X]}$.*

Preuve :

a) *Existence du morphisme ψ :* Considérons la correspondance

$$\begin{aligned}\psi : K(X)_0 &\longrightarrow K[[X]] \\ \frac{p}{q} &\longmapsto pq^{-1}.\end{aligned}$$

Vérifions que ψ est une application. Supposons $\frac{p_1}{q_1} = \frac{p}{q}$ dans $K(X)_0$; q et q_1 sont alors des éléments inversibles dans $K[[X]]$, par suite

$$\begin{aligned}\frac{p_1}{q_1} = \frac{p}{q} \text{ dans } K(X)_0 &\iff p_1 q = q_1 p \text{ dans } K[X], \\ p_1 q = q_1 p \text{ dans } K[X] &\implies p_1 q_1^{-1} = p q^{-1} \text{ dans } K[[X]], \\ \text{d'où } \frac{p_1}{q_1} = \frac{p}{q} \text{ dans } K(X)_0 &\implies \psi\left(\frac{p_1}{q_1}\right) = \psi\left(\frac{p}{q}\right).\end{aligned}$$

La correspondance ψ est donc une application et

$$(\psi(p) = p, \forall p \in K[X]) \implies \psi|_{K[X]} = id_{K[X]}.$$

ψ est une application injective, car quels que soient $\frac{p}{q}$ et $\frac{r}{s}$ dans $K(X)_0$,

$$\psi\left(\frac{p}{q}\right) = \psi\left(\frac{r}{s}\right) \iff (pq^{-1} = rs^{-1}) \implies (ps = rq) \implies \left(\frac{p}{q} = \frac{r}{s}\right).$$

On vérifiera, enfin, que ψ est un morphisme de K-algèbres.

b) *Unicité du morphisme ψ :* Supposons qu'il existe un morphisme ψ_1 satisfaisant aux mêmes propriétés que ψ ; alors,

$$\begin{aligned}\forall \frac{p}{q} \in K(X)_0, \psi_1\left(\frac{p}{q}\right) &= \psi_1(p) \psi_1\left(\frac{1}{q}\right), \text{ où } \psi_1(p) = p; \\ \frac{1}{q} &= q^{-1} \text{ dans } K[[X]] \implies \psi_1\left(\frac{1}{q}\right) = \psi_1(q^{-1}) = (\psi_1(q))^{-1} = q^{-1}, \\ \text{d'où } \psi_1\left(\frac{p}{q}\right) &= p q^{-1} = \psi\left(\frac{p}{q}\right), \text{ donc } \psi_1 = \psi.\end{aligned}$$

Le morphisme canonique ψ permet d'identifier $K(X)_0$ à $Im \psi$ dans $K[[X]]$; ainsi $K(X)_0$ est une sous-K-algèbre de $K[[X]]$ contenant $K[X]$. $\square$

Définition 7.37. L'algèbre $K(X)_0$ est appelée sous-algèbre des **séries formelles rationnelles** de $K[[X]]$. Pour $\frac{p}{q} \in K(X)_0$, on dit que $\psi\left(\frac{p}{q}\right) = pq^{-1}$ est le **développement en série formelle** de la fraction rationnelle $\frac{p}{q}$.

Exemple : $\sum_{n \geq 0} X^n$ est le développement en série formelle de la fraction $\frac{1}{1-X}$.

Remarque 7.38. :

a) On a $K(X)_0 \subsetneq K[[X]]$, car tout élément de $K[[X]]$ n'est pas le développement en série formelle d'une fraction rationnelle.

Par exemple, dans $\mathbb{R}[[X]]$, $\sum_{n \geq 0} \frac{X^n}{n!} = \exp(X) \notin \mathbb{R}(X)_0$.

b) Dans $K[[X]]$, une série formelle f est rationnelle si et seulement s'il existe un polynôme $q \in K[X]$, tel que $q(0) \neq 0$ et $f q \in K[X]$; ce qui conduit au résultat suivant.

Proposition 7.39. Soit $f = \sum_{n \geq 0} a_n X^n \in K[[X]] \setminus K[X]$; pour que f soit rationnelle, il faut et il suffit qu'il existe deux entiers $d \geq 0$, $m > 0$ et des éléments $\lambda_1, \dots, \lambda_m$ dans K tels que $\lambda_m \neq 0$ et

$$\forall n \in \mathbb{N}, (n + m > d \implies a_{n+m} = \sum_{1 \leq i \leq m} \lambda_i a_{n+m-i}). \quad (7.8)$$

Si ces conditions sont vérifiées par $d, m, \lambda_1, \dots, \lambda_m$, où m est minimal, alors le polynôme $q = 1 - \sum_{1 \leq i \leq m} \lambda_i X^i$ est tel qu'en posant $p := f q$, dans $K[X]$, la fraction rationnelle $\frac{p}{q}$ est irréductible.

Preuve :

a) Supposons $f \in K(X)_0$; il existe alors p et q dans $K[X] \setminus \{0\}$ tels que $q(0) \neq 0$ et $f q = p$. Posons $\deg p = d$ et $\deg q = m$; par hypothèse, $f \notin K[X]$, on a donc, $d \geq 0$ et $m \geq 1$ dans $\mathbb{N}$.

On remarque que l'on peut se ramener au cas où $q(0) = 1$; en effet, si $q(0) = \alpha \neq 0$, en prenant les polynômes $q_1 = \alpha^{-1} q$ et $p_1 = \alpha^{-1} p$, on a $q_1(0) = 1$ et $f q_1 = p_1$.

Nous supposons donc que $q(0) = 1$. On peut alors écrire, dans $K[X]$,

$$q = 1 - \sum_{1 \leq i \leq m} \lambda_i X^i, \text{ avec } \lambda_m \neq 0.$$

Posons d'autre part, $p = \sum_{0 \leq j \leq d} \mu_j X^j$, alors l'égalité $f q = p$ devient :

$$(\sum_{n \geq 0} a_n X^n) (1 - \sum_{1 \leq i \leq m} \lambda_i X^i) = \sum_{0 \leq j \leq d} \mu_j X^j. \quad (7.9)$$

On a $\lambda_m \neq 0$ et le degré du second membre de l'égalité (7.9) est d , on peut donc affirmer que dans le premier membre de (7.9), quel que soit $n \in \mathbb{N}$, tel que $n + m > d$, le coefficient de X^{n+m} est nul ; d'où

$$\forall n \in \mathbb{N}, (n + m > d) \implies a_{n+m} = \sum_{1 \leq i \leq m} \lambda_i a_{n+m-i}.$$

Ainsi les entiers d, m et les éléments $\lambda_1, \dots, \lambda_m$ du corps K vérifient les conditions énoncées dans la proposition.

b) Réciproquement, supposons qu'il existe $d \in \mathbb{N}$, $m \in \mathbb{N}^*$ et $\lambda_1, \dots, \lambda_m$ dans K satisfaisant aux conditions de l'énoncé.

Considérons le polynôme $q := 1 - \sum_{1 \leq i \leq m} \lambda_i X^i$. Les conditions (7.8) impliquent que dans le produit $f q$, le coefficient de X^{n+m} est nul dès que l'on a $n + m > d$; on en déduit que $f q$ est un polynôme de $K[X]$, donc $f \in K(X)_0$ et en posant $p := f q$, on obtient

$$f = p q^{-1} = \psi \left(\frac{p}{q} \right).$$

Montrons que si l'entier m est minimal, alors le polynôme $p = f q$ est premier avec q dans $K[X]$. En effet, supposons $\delta := p \wedge q \neq 1$ dans $K[X]$, donc $\deg \delta > 0$. On en déduit (Prop. 5.43.) qu'il existent des polynômes p_1 et q_1 tels que

$$p = \delta p_1, \quad q = \delta q_1 \text{ et } p_1 \wedge q_1 = 1.$$

Par suite, dans $K[X]$, on a

$$f q_1 = p_1 \text{ et } \deg q_1 < \deg q = m,$$

ce qui incompatible avec la minimalité de m , donc $p \wedge q = 1$. □

Remarque 7.40. :

a) Il existe d'autres critères de rationalité d'une série formelle de $K[[X]]$ (Voir, par exemple, [2]).

b) Les résultats précédents montrent que l'on peut obtenir le développement en série formelle d'une fraction rationnelle $\frac{p}{q} \in K(X)_0$, en effectuant la division suivant les puissances croissantes (Th. 4.52.) du polynôme p par le polynôme q , à "l'ordre infini".

Dans la pratique, on utilise aussi d'autres procédés qui découlent du développement connu de $\frac{1}{1-X}$ (voir les exemples qui suivent).

Exemple 7.41. K étant un corps de caractéristique 0, dans $K(X)$, posons, quel que soit $p \in \mathbb{N}^*$, $f_p = \frac{1}{(1-X)^p}$; alors

$$f_p = \sum_{n \geq 0} C_{p+n-1}^{p-1} X^n. \quad (7.10)$$

Preuve : On démontre la relation (7.10) par récurrence sur p .

Pour $p = 1$, on a $f_1 = \frac{1}{1-X} = \sum_{n \geq 0} X^n$.

Supposons (7.10) vérifiée pour tout entier k ($1 \leq k \leq p-1$), donc

$$f_{p-1} = \sum_{n \geq 0} C_{p+n-2}^{p-2} X^n.$$

$$\begin{aligned} f_p &= \frac{1}{(1-X)^p} = \frac{1}{1-X} f_{p-1} = (\sum_{i \geq 0} X^i) (\sum_{i \geq 0} C_{p+i-2}^{p-2} X^i) \\ &= \sum_{n \geq 0} (\sum_{0 \leq i \leq n} C_{p+i-2}^{p-2}) X^n. \end{aligned}$$

Calculons $\sum_{0 \leq i \leq n} C_{p+i-2}^{p-2}$, sachant que quels que soient p et k dans $\mathbb{N}^*$, on a $C_p^k = C_{p-1}^{k-1} + C_{p-1}^k$ (Cf. Ch. 1).

$$\begin{aligned} \sum_{0 \leq i \leq n} C_{p+i-2}^{p-2} &= (C_{p-2}^{p-2} + C_{p-1}^{p-2}) + C_p^{p-2} + C_{p+1}^{p-2} + \dots + C_{p+n-2}^{p-2}, \\ \text{or, } C_{p-2}^{p-2} &= C_{p-1}^{p-1} \implies C_{p-2}^{p-2} + C_{p-1}^{p-2} = C_{p-1}^{p-1} + C_{p-1}^{p-2} = C_{p-1}^{p-1}, \\ \text{et } C_p^{p-1} + C_{p-1}^{p-2} &= C_{p+1}^{p-1}; \end{aligned}$$

de proche en proche, on obtient $\sum_{0 \leq i \leq n} C_{p+i-2}^{p-2} = C_{p+n-1}^{p-1}$, d'où la relation (7.10). $\square$

Remarque 7.42. :

a) Si $\text{car } K = 0$ et $f = \frac{p}{q} \in K(X)_0$, alors pour la dérivée f' de f , on a

$$f' = \frac{p'q - pq'}{q^2} \in K(X)_0 \quad \text{et} \quad \psi(f') = (\psi(f))',$$

où ψ est le plongement canonique de $K(X)_0$ dans $K[[X]]$.

Plus généralement, pour tout entier $p \geq 1$, la dérivée à l'ordre p de f , notée $f^{(p)}$, vérifie $f^{(p)} \in K(X)_0$ et $\psi(f^{(p)}) = (\psi(f))^{(p)}$.

On peut donc, en particulier, retrouver le développement en série formelle de $\frac{1}{(1-X)^p}$ en

dérivant à l'ordre $p-1$ celui de $\frac{1}{1-X}$.

b) Le résultat de l'exemple 7.41. permet d'écrire, pour tout $a \neq 0$ dans K , le développement en série formelle de

$$\frac{1}{(a-X)^p} = \frac{1}{a^p} (\sum_{n \geq 0} C_{p+n-1}^{p-1} \frac{X^n}{a^n}).$$

En supposant connu le principe de la *décomposition d'une fraction rationnelle en éléments simples* ([2]), on peut trouver le développement en série formelle de tout élément $f \in K(X)_0$, où K est un corps de caractéristique 0, algébriquement clos (Déf. 4.42.).

Exemple 7.43. Développement en série formelle de

$$f = \frac{1}{(1-X^2)(1-X^3)} \in \mathbb{C}(X).$$

1^{ère} méthode :

$$f = \left(\frac{1}{1-X^2}\right)\left(\frac{1}{1-X^3}\right) = (\sum_{p \geq 0} X^{2p})(\sum_{q \geq 0} X^{3q}) = \sum_{n \geq 0} v_n X^n,$$

où v_n désigne le nombre de couples d'entiers (p, q) tels que $2p + 3q = n$.

2^{ème} méthode : On écrit la décomposition de f en éléments simples dans le corps $\mathbb{C}(X)$ (résultat à vérifier par le lecteur) :

j et j^2 étant les racines complexes du polynôme $1 - X^3$, on a

$$\begin{aligned} f &= \frac{1}{(1+X)(1-X)^2(1-jX)(1-j^2X)} \\ &= \frac{1}{4} \frac{1}{1+X} + \frac{1}{6} \frac{1}{(1-X)^2} + \frac{1}{4} \frac{1}{1-X} + \frac{1-j^2}{9} \frac{1}{1-jX} + \frac{1-j}{9} \frac{1}{1-j^2X}. \end{aligned}$$

En regroupant, pour tout $n \in \mathbb{N}$, les termes en X^n , on obtient

$$f = \sum_{n \geq 0} \left(\frac{(-1)^n}{4} + \frac{n+1}{6} + \frac{1}{4} + \frac{1}{9}(s_n - s_{n+2}) \right) X^n,$$

où quel que soit $n \geq 0$, $s_n = j^n + j^{2n}$, donc

$$s_{n+2} = j^{n+2} + j^{2n+4} = j^{n+2} + j^{2n+1};$$

par suite, $n \equiv 0 \pmod{3} \implies s_n = 2$; $n \not\equiv 0 \pmod{3} \implies s_n = -1$.

La comparaison des résultats des deux méthodes donne, pour tout $n \in \mathbb{N}$, le nombre v_n , de couples d'entiers (p, q) tels que $2p + 3q = n$:

$$\begin{aligned} n = 3m &\implies v_n = \frac{1}{4}(1 + (-1)^m) + \frac{1}{6}(3m+1) + \frac{1}{3} \\ n = 3m+1 &\implies v_n = \frac{1}{4}(1 + (-1)^{m+1}) + \frac{1}{6}(3m+2) - \frac{1}{3} \\ n = 3m+2 &\implies v_n = \frac{1}{4}(1 + (-1)^m) + \frac{m+1}{2}. \end{aligned}$$

5. Structure d'espace métrique de $A[[X]]$

A. Norme et distance dans $A[[X]]$

Pour tout $f \in A[[X]]$, posons $|f| := 2^{-\omega(f)}$, avec la convention $2^{-\infty} = 0$.

$$\begin{aligned} \text{L'application} \quad A[[X]] &\longrightarrow \mathbb{R} \\ f &\longmapsto |f| \end{aligned}$$

vérifie les propriétés suivantes ; quels que soient f, g dans $A[[X]]$,

i) $|f| \geq 0$ et $(|f| = 0 \iff f = 0)$,

ii) $|f + g| \leq \sup(|f|, |g|)$,

iii) $|fg| \leq |f| |g|$.

On remarque que ii) $\implies |f + g| \leq |f| + |g|$, donc l'application $f \mapsto |f|$ définit une **norme** sur $A[[X]]$, d'où l'on déduit une notion de **distance** dans $A[[X]]$, notée d , telle que quels que soient les séries formelles f et g ,

$$d(f, g) = |f - g| = 2^{-\omega(f-g)}.$$

$A[[X]]$ est ainsi muni d'une **structure d'espace métrique**.

B. Etude de l'espace métrique $A[[X]]$

Définition 7.44. Soit $\{u_\lambda\}_{\lambda \in \mathbb{N}}$ une suite d'éléments de $A[[X]]$.

a) On dit que la suite $\{u_\lambda\}_{\lambda \in \mathbb{N}}$ **converge** vers une série formelle $f = \sum_{n \geq 0} a_n \in A[[X]]$, si pour tout $\varepsilon > 0$ dans $\mathbb{R}$, il existe $N_\varepsilon \in \mathbb{N}$ tel que

$$\forall \lambda \in \mathbb{N}, (\lambda \geq N_\varepsilon \implies |f - u_\lambda| \leq \varepsilon).$$

Dans ce cas, on écrira $f = \lim u_\lambda$.

b) On dit que la suite $\{u_\lambda\}_{\lambda \in \mathbb{N}}$ est une **suite de Cauchy** si pour tout $\varepsilon > 0$ dans $\mathbb{R}$, il existe $N_\varepsilon \in \mathbb{N}$ tel que

$$\forall \lambda, \mu \in \mathbb{N}, (\lambda, \mu \geq N_\varepsilon \implies |u_\lambda - u_\mu| \leq \varepsilon).$$

Proposition 7.45. $A[[X]]$ est un espace métrique complet (c'est-à-dire que toute suite de Cauchy converge).

Preuve : Soit $\{u_\lambda\}_{\lambda \in \mathbb{N}}$ une suite de Cauchy dans $A[[X]]$ telle que

$$\forall \lambda \in \mathbb{N}, u_\lambda = \sum_{i \in \mathbb{N}} a_{\lambda,i} X^i, \text{ où } (a_{\lambda,i})_{i \in \mathbb{N}} \in A^{\mathbb{N}}.$$

Soit n fixé dans $\mathbb{N}$; prenons $\varepsilon = 2^{-n}$; il existe alors $N_n \in \mathbb{N}$ tel que

$$\forall \lambda, \mu \in \mathbb{N}, (\lambda, \mu \geq N_n \implies |u_\lambda - u_\mu| \leq 2^{-n}), \quad (7.11)$$

$$\text{d'où } \forall \lambda, \mu \in \mathbb{N}, (\lambda, \mu \geq N_n \implies 2^{-\omega(u_\lambda - u_\mu)} \leq 2^{-n}). \quad (7.12)$$

Par suite, pour tout entier $\lambda \geq N_n$ dans $\mathbb{N}$, on a $\omega(u_\lambda - u_{N_n}) > n$, donc

$$\forall \lambda \in \mathbb{N}, (\lambda \geq N_n \implies \forall i (0 \leq i \leq n), a_{\lambda,i} - a_{N_n,i} = 0). \quad (7.13)$$

En choisissant, pour tout $n \in \mathbb{N}$, le plus petit entier positif N_n vérifiant la condition (7.11), on définit une suite $\{N_n\}_{n \in \mathbb{N}}$ telle que, d'après (7.13), quels que soient n et λ dans $\mathbb{N}$,

$$\lambda \geq N_n \implies a_{\lambda,n} = a_{N_n,n}. \quad (7.14)$$

Considérons alors $f = \sum_{i \geq 0} a_{N_i,i} X^i = (a_{N_0,0}, a_{N_1,1}, \dots, a_{N_i,i}, \dots)$.

Posons, pour tout $n \in \mathbb{N}$, $\mu_n := \max\{N_i, 1 \leq i \leq n\}$; les résultats (7.13) et (7.14) impliquent, quels que soient $(n, \lambda) \in \mathbb{N} \times \mathbb{N}$,

$$\lambda \geq \mu_n \implies \forall i (0 \leq i \leq n), a_{\lambda,i} = a_{N_i,i},$$

$$\text{d'où } \lambda \geq \mu_n \implies \omega(u_\lambda - f) > n \implies |u_\lambda - f| \leq 2^{-n}.$$

Or, pour tout $\varepsilon > 0$ dans $\mathbb{R}$, il existe $n \in \mathbb{N}$ vérifiant $2^{-n} \leq \varepsilon$ et d'après ce qui précède, pour un tel entier n , il existe $\mu_n \in \mathbb{N}$ tel que

$$\forall \lambda \geq \mu_n, |u_\lambda - f| \leq 2^{-n} \leq \varepsilon.$$

On en conclut que $f = \lim u_\lambda$. □

6. Séries formelles à n indéterminées sur A , $n > 1$

A. A-algèbre des séries formelles à n indéterminées

1. On généralise la construction de l'algèbre des séries formelles faite dans le cas $n = 1$, en munissant le A -module à gauche $A^{\mathbb{N}^n}$ d'une multiplication interne. On a

$$f \in A^{\mathbb{N}^n} \iff f = (a_i)_{i \in \mathbb{N}^n}, \text{ où } \forall i = (i_1, i_2, \dots, i_n) \in \mathbb{N}^n, a_i \in A.$$

La multiplication dans $A^{\mathbb{N}^n}$ est définie par l'application

$$(f = (a_i)_{i \in \mathbb{N}^n}, g = (b_i)_{i \in \mathbb{N}^n}) \mapsto fg = (c_i)_{i \in \mathbb{N}^n}$$

$$\text{où } c_{(i_1, i_2, \dots, i_n)} = \sum_{j_r + k_r = i_r, 1 \leq r \leq n} a_{(j_1, j_2, \dots, j_n)} b_{(k_1, k_2, \dots, k_n)}.$$

On vérifie que $A^{\mathbb{N}^n}$ est alors un *anneau unitaire, commutatif* et la structure de A -module de $A^{\mathbb{N}^n}$ est compatible avec la multiplication interne, c'est-à-dire :

$$\alpha(fg) = (\alpha f)g = f(\alpha g).$$

Ainsi $A^{\mathbb{N}^n}$ est une **A-algèbre commutative**.

2. Par un changement de notation semblable à celui qui a été explicité dans le cas de la construction de l'anneau de polynômes $A[X_1, X_2, \dots, X_n]$, on est conduit à écrire tout élément $f = (a_i)_{i \in \mathbb{N}^n}$ de $A^{\mathbb{N}^n}$ sous la forme

$$f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \text{ où } i = (i_1, i_2, \dots, i_n). \quad (7.15)$$

Comme dans le cas $n = 1$, l'écriture (7.15) est une expression *formelle*, car le signe $\sum$ ne désigne pas, en général, une somme finie ; une infinité d'éléments a_i pouvant être non nuls dans A .

Les X_i , ($1 \leq i \leq n$) étant les **indéterminées**, l'algèbre $A^{\mathbb{N}^n}$ est notée $A[[X_1, X_2, \dots, X_n]]$ et appelée **algèbre des séries formelles à n indéterminées sur A** .

Remarque 7.46. :

a) Comme pour l'algèbre des polynômes $A[X_1, X_2, \dots, X_n]$, l'algèbre $A[[X_1, X_2, \dots, X_n]]$ est indépendante du nom donné à chaque indéterminée et de l'ordre dans lequel on les considère.

b) On admettra ici l'existence des isomorphismes de A -algèbres suivants

$$A[[X_1, \dots, X_n]] \simeq A[[X_1, \dots, X_{n-1}]][[X_n]]$$

et plus généralement,

$$\forall j (1 \leq j \leq n), A[[X_1, \dots, X_n]] \simeq A[[X_1, \dots, \hat{X}_j, \dots, X_n]][[X_j]].$$

c) Comme dans le cas de l'algèbre des polynômes (Rem. 4.56.), on identifie de façon naturelle A et, plus généralement, $A[[X_1, \dots, X_m]]$, $1 \leq m \leq n$, à une sous-algèbre de $A[[X_1, \dots, X_n]]$.

D'autre part, $A^{(\mathbb{N}^n)}$ est une sous-algèbre de $A^{\mathbb{N}^n}$, d'où les inclusions

$$A \subsetneq A[[X_1, \dots, X_n]] \subsetneq A[[X_1, \dots, X_n]].$$

B. Propriétés de l'anneau $A[[X_1, \dots, X_n]]$

Plusieurs propriétés démontrées dans le cas $n = 1$, se généralisent *par récurrence*, au cas $n > 1$, d'où les résultats suivants.

- 1) A partir du Cor. 7.7., on obtient, quel que soit $n \geq 1$,
 $A \text{ int\`egre} \implies A[[X_1, \dots, X_n]] \text{ int\`egre}.$
 2) Du Th. 7.23., on d\`eduit qu'une s\`erie formelle

$$f = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \text{ o\`u } i = (i_1, i_2, \dots, i_n)$$

est inversible dans $A[[X_1, \dots, X_n]]$ si et seulement si le coefficient $a_0 = a_{0,0,\dots,0}$ est inversible dans A .

- 3) Le Th. 7.32. implique, pour tout $n \geq 1$,
 $A \text{ noeth\'erien} \implies A[[X_1, \dots, X_n]] \text{ noeth\'erien}.$

On en d\`eduit, en particulier, que si K est un corps, alors $K[[X_1, \dots, X_n]]$ est noeth\'erien.

- 4) Avec le Th. 7.30., on montre que, pour tout $n \geq 1$,

$$\begin{aligned} A \text{ est un anneau local} &\implies A[[X_1, \dots, X_n]] \text{ est un anneau local.} \\ \text{donc, } K \text{ est un corps} &\implies K[[X_1, \dots, X_n]] \text{ est un anneau local.} \end{aligned}$$

- 5) Nous admettrons le r\'esultat suivant.

Th\'eor\`eme 7.47. Si K est un corps, alors pour tout $n \geq 1$, $K[[X_1, \dots, X_n]]$ est un anneau factoriel.

On sait que $K[[X]]$ est un domaine principal (Th. 7.29.), c'est donc un anneau factoriel (Th.5.90.). Pour $n > 1$, le Th. 7.47. peut \^etre d\'emonstr\'e en utilisant le "Th\'eor\`eme de pr\'eparation de Weierstrass" [12].



7. Exercices

- 1) a) V\'erifier que $1 + X$ et $\sum_{n \geq 0} 2^n X^n$ sont inversibles dans $\mathbb{Z}[[X]]$ et trouver leurs inverses.
 b) Montrer que le polyn\^ome $2 + 3X + X^2$ est irr\'eductible dans $\mathbb{Z}[[X]]$ et non irr\'eductible dans $\mathbb{Z}[X]$.
- 2) Soit $s = \sum_{n \geq 0} a_n X^n$ dans $\mathbb{Z}[[X]] \setminus \{0\}$. On dira que $d \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ est un p.g.c.d. des coefficients de s , si
- $\forall n \in \mathbb{N}, d | a_n.$
 - $(d' \in \mathbb{Z}^* \text{ et } \forall n \in \mathbb{N}, d' | a_n) \implies d' | d.$
- Une s\'erie formelle $s \in \mathbb{Z}[[X]]$, sera dite *primitive* si 1 est un p.g.c.d. des coefficients de s .
 Montrer que, dans $\mathbb{Z}[[X]]$, le produit de deux s\'eries formelles primitives est une s\'erie formelle primitive.
- 2°) On dira qu'une s\'erie formelle $s \in \mathbb{Z}[[X]]$ est *rationnelle* si elle est le d\'eveloppement en s\'erie formelle d'une fraction rationnelle $\frac{f(X)}{g(X)} \in \mathbb{Q}(X)$. On \\'ecrira dans ce cas, $s = \frac{f}{g}$.
- Etant donn\'e une s\'erie rationnelle, non nulle, $s = \frac{f}{g}$ dans $\mathbb{Z}[[X]]$, montrer que l'on peut supposer f et g \`a coefficients entiers et tels que $f \wedge g = 1$ dans $\mathbb{Z}[X]$. S'il en est ainsi, d\'emontrer qu'il existe un entier $a \in \mathbb{Z}$ et des polyn\^omes u et v dans $\mathbb{Z}[X]$ tels que $u(X)f(X) + v(X)g(X) = a$.
 - Prouver que $\frac{a}{g(X)}$ admet un d\'eveloppement en s\'erie formelle dans $\mathbb{Z}[[X]]$.
- On pose $\frac{a}{g(X)} = \sum_{n \geq 0} c_n X^n$. On suppose que $c \in \mathbb{Z}^*$ est un p.g.c.d. des $c_n, n \geq 0$, et on note d un p.g.c.d. des coefficients du polyn\^ome $g(X)$.

- Prouver que $\frac{a}{dc} = \pm 1$.
- Montrer que $\frac{f(X)}{d} \in \mathbb{Z}[X]$.
- En déduire que dans $\mathbb{Z}[[X]]$, toute série formelle *rationnelle* est le développement d'une fraction rationnelle $\frac{p(X)}{q(X)} \in \mathbb{Q}(X)$, où l'on peut choisir p et q dans $\mathbb{Z}[X]$, tels que $q(0) = 1$.

3) Autre démonstration du théorème 7.32. (A noethérien $\implies A[[X]]$ noethérien).

A étant un anneau unitaire, commutatif, soit σ le morphisme de $A[[X]]$ dans A tel que $\sigma(\sum_{n \geq 0} a_n X^n) = a_0$.

Soit P un idéal premier, non nul de $A[[X]]$; on pose $P_0 := \sigma(P)$.

1°) Vérifier que si P est de type fini dans $A[[X]]$, alors P_0 est un idéal de type fini dans A .

2°) Réciproquement, on suppose que $P_0 = \sigma(P)$ est un idéal de type fini dans A et le but de ce qui suit est de prouver que l'idéal premier P est de type fini dans $A[[X]]$.

Soit $\{b_1, b_2, \dots, b_k\}, k \in \mathbb{N}^*$, une famille génératrice de P_0 dans A .

a) On considère le cas où $X \in P$; montrer que $\{b_1, b_2, \dots, b_k, X\}$ engendre l'idéal P .

b) On suppose que $X \notin P$. Vérifier que pour tout $i (1 \leq i \leq k)$, on peut choisir $f_i \in A[[X]]$, tel que $\sigma(f_i) = b_i$.

En s'inspirant de la preuve du théorème 7.34., démontrer que l'idéal premier P est engendré par $\{f_1, f_2, \dots, f_k\}$.

3°) En utilisant le théorème 2.85., retrouver le résultat du théorème 7.32.

4) A étant un anneau unitaire, commutatif, on considère dans $A[[X]]$, la partie multiplicative $S_X := \{X^n, n \in \mathbb{N}\}$. L'anneau localisé de $A[[X]]$ par S_X est noté $A((X))$.

1°) Montrer que tout élément $f \in A((X))$ peut s'écrire

$$f = \sum_{i \in \mathbb{Z}} a_i X^i, \text{ où } \forall i \in \mathbb{Z}, a_i \in A$$

$$\text{et } \exists r \in \mathbb{Z} \text{ tel que } a_r \neq 0 \text{ et } a_i = 0, \forall i (i < r).$$

En déduire que $A((X))$ est une A -algèbre contenant $A[[X]]$. Les éléments de $A((X))$ sont appelés **séries de Laurent** à coefficients dans A .

$A((X))$ est, par définition, l'algèbre des séries de Laurent sur A .

2°) Justifier les propriétés suivantes.

i) A intègre $\implies A((X))$ intègre et $A((X)) \subseteq \text{Fr} A[[X]]$.

ii) A noethérien $\implies A((X))$ noethérien.

iii) A est un D.P. $\implies A((X))$ factoriel.

Dans i), $\text{Fr} A[[X]]$ désigne le corps des fractions du D.I. $A[[X]]$.

3°) K désigne un corps.

a) Prouver que $K((X))$ est un corps et que $K((X)) = \text{Fr} K[[X]]$.

b) Trouver l'inverse de $\sum_{i \geq -5} X^i$ dans $K((X))$.

5) A désigne un anneau commutatif, unitaire.

1°) Vérifier que toute partie multiplicative S de A est une partie multiplicative de $A[[X]]$ et que $S^{-1}(A[[X]]) \subseteq (S^{-1}A)[[X]]$.

Pour tout domaine d'intégrité D , on note $\text{Fr} D$ le corps des fractions de D .

On suppose, dans toutes les questions qui suivent, que A est un D.I.; on pose $A^* = A \setminus \{0\}$ et $K = \text{Fr} A$.

2°) $(A^*)^{-1}A[[X]]$ désignant le localisé de $A[[X]]$ par A^* , vérifier les inclusions suivantes

$$(A^*)^{-1}A[[X]] \subseteq K[[X]] \tag{7.16}$$

$$\text{Fr} A[[X]] \subseteq K((X)), \tag{7.17}$$

où $K((X))$ est le corps des séries de Laurent sur K (Cf. Ex. 4, ci-dessus).

3°) Le but de cette question est de prouver (avec les hypothèses et les notations précédentes) que les trois conditions suivantes sont équivalentes.

$$i) K[[X]] = (A^*)^{-1}A[[X]],$$

$$ii) K((X)) = FrA[[X]],$$

$$iii) \forall (a_i)_{i \in \mathbb{N}} \text{ où, pour tout } i \in \mathbb{N}, a_i \in A^*, \text{ on a } \bigcap_{i \in \mathbb{N}} a_i A \neq (0).$$

a) Montrer que $i) \implies ii)$.

b) En vue de prouver que $ii) \implies iii)$, on considère une suite $(a_i)_{i \in \mathbb{N}}$ d'éléments *non nuls* de A et dans $K = FrA$, on pose, pour tout $n \in \mathbb{N}$,

$$c_n := (a_0 a_1 \dots a_n)^{-1}.$$

Soit $c := \sum_{n \geq 0} c_n X^n$, dans $K[[X]]$.

- Montrer que l'hypothèse $ii)$ implique qu'il existe une série formelle $b \neq 0$, dans $A[[X]]$, telle que $bc \in A[[X]]$ et vérifier que l'on peut toujours se ramener au cas où $\omega(b) = 0$.

- Compte tenu de ce qui précède, on suppose $bc \in A[[X]]$, où $b = \sum_{i \geq 0} b_i X^i$, avec $b_0 \neq 0$ dans A . On pose $bc := \sum_{m \geq 0} d_m X^m$.

Pour tout $m \in \mathbb{N}$, calculer d_m en fonction des b_i et a_i , $0 \leq i \leq m$.

En déduire que $b_0 \in a_m A$, quel que soit $m \in \mathbb{N}$; en conclure que $ii) \implies iii)$.

c) Il s'agit de prouver que $iii) \implies i)$. Soit $q = \sum_{n \geq 0} q_n X^n$ dans $K[[X]]$. Pour tout $n \in \mathbb{N}$, justifier l'existence de $s_n \in A^*$ tel que $s_n q_n \in A$. En appliquant l'hypothèse $iii)$ à la suite $(s_n)_{n \in \mathbb{N}}$, prouver que $iii) \implies i)$.

4°) Montrer que si A est un anneau factoriel, alors les inclusions (7.16) et (7.17) de la question 2°) sont, nécessairement, des inclusions strictes.

- 6) A étant un anneau unitaire, *non commutatif*, on définit, respectivement, l'ensemble des polynômes, des séries formelles et des séries de Laurent, à une indéterminée sur A , comme suit.

$$A[X] = \{ \sum_{0 \leq i \leq n} a_i X^i ; n \in \mathbb{N} \text{ et } \forall i (0 \leq i \leq n), a_i \in A \},$$

$$A[[X]] = \{ \sum_{i \in \mathbb{N}} a_i X^i ; \forall i \in \mathbb{N}, a_i \in A \},$$

$$A((X)) = \{ \sum_{i \in \mathbb{Z}} a_i X^i ; \forall i \in \mathbb{Z}, a_i \in A \text{ et } \exists r \in \mathbb{Z}, \text{ t.q. } a_r \neq 0, a_i = 0, \forall i < r \}.$$

1°) On définit formellement, dans chacun des trois ensembles ci-dessus, une addition et une multiplication, comme dans le cas où l'anneau A est commutatif.

Vérifier que $A[X], A[[X]], A((X))$ sont alors munis d'une structure d'anneau unitaire *non commutatif*.

2°) Montrer que si H est un anneau à division (ou corps gauche), il en est de même de $H((X))$.

On remarquera, en particulier, que si $\mathbb{H}$ est le corps (gauche) des quaternions réels (Ch. 3), alors $\mathbb{H}((X))$ est un corps gauche contenant $\mathbb{H}$.

- 7) A désignant un anneau unitaire, commutatif, on note $M_n(A)$ l'anneau unitaire, *non commutatif*, des matrices carrées d'ordre $n > 1$, sur A .

Moyennant les résultats de l'exercice 6 précédent, démontrer l'existence des isomorphismes d'anneaux unitaires, suivants :

$$M_n(A)[X] \simeq M_n(A[X]) \quad \text{et} \quad M_n(A)[(X)] \simeq M_n(A[[X]]).$$



Chapitre 8

Polynômes symétriques

Dans tout ce chapitre, A désigne un domaine d'intégrité.

Toutes les propriétés de l'algèbre des polynômes, $A[X_1, \dots, X_n], n \geq 1$, développées au Chapitre 4, sont supposées connues.

1. Ordre lexicographique dans $A[X_1, \dots, X_n], n > 1$

Remarque 8.1. Lorsque $n = 1$, il est facile d'ordonner les monômes de $A[X]$ suivant leur *degré* ; il s'agit d'un ordre induit par celui des entiers naturels ; ainsi un polynôme de $A[X]$ peut s'écrire comme la somme de ses monômes ordonnés suivant les *puissances décroissantes ou croissantes* de X .

Dans le cas $n > 1$, il est nécessaire aussi, de définir un ordre dans l'ensemble des monômes de $A[X_1, \dots, X_n]$, permettant d'écrire un polynôme comme somme de ses monômes ordonnés suivant cet ordre.

Définition 8.2. Etant donné, dans $A[X_1, X_2, \dots, X_n], n \geq 1$, deux monômes non nuls

$$m = aX_1^{i_1}X_2^{i_2}\dots X_n^{i_n} \text{ et } m' = bX_1^{j_1}X_2^{j_2}\dots X_n^{j_n},$$

on dit m est **plus haut** que m' si le *premier élément non nul* de la suite d'entiers

$$(i_1 - j_1), (i_2 - j_2), \dots, (i_n - j_n)$$

est *positif*. Dans ce cas, on pourra écrire, symboliquement, $m > m'$.

Les monômes m et m' seront dits de **même hauteur** si $i_k = j_k$, quel que soit $k (1 \leq k \leq n)$.

De plus, on convient de dire que tout monôme constant non nul est *plus haut* que le monôme nul ; on vérifie alors que la relation binaire définie ci-dessus, dans l'ensemble des monômes de $A[X_1, X_2, \dots, X_n], n \geq 1$, est une relation d'ordre, qu'on appelle **ordre lexicographique**.

On remarquera que pour $n = 1$, l'ordre lexicographique coïncide avec l'ordre habituellement considéré dans l'ensemble des monômes de $A[X]$.

Exemple 8.3. Dans $A[X_1, X_2, X_3]$, on a

$$X_1^2X_2X_3 > X_1X_2^2X_3 > X_1X_3^3.$$

Définition 8.4. Pour un polynôme $f \neq 0$ dans $A[X_1, X_2, \dots, X_n], n \geq 1$, le monôme le *plus haut*, parmi ceux dont il est la somme, est appelé le **monôme directeur** de f ; on le notera $MD(f)$.

Proposition 8.5. A étant un domaine d'intégrité, pour deux polynômes non nuls f et g dans $A[X_1, X_2, \dots, X_n], n \geq 1$, on a

$$MD(fg) = MD(f)MD(g).$$

Preuve : La propriété est vraie pour $n = 1$. Pour $n > 1$, on raisonne par récurrence sur n . Considérons les polynômes non nuls f et g dans $A[X_2, \dots, X_n][X_1]$:

$$\begin{aligned} f &= \phi_r(X_2, \dots, X_n)X_1^r + \phi_{r-1}(X_2, \dots, X_n)X_1^{r-1} + \dots + \phi_0(X_2, \dots, X_n) \\ g &= \psi_s(X_2, \dots, X_n)X_1^s + \psi_{s-1}(X_2, \dots, X_n)X_1^{s-1} + \dots + \psi_0(X_2, \dots, X_n). \end{aligned}$$

Pour tout $i(1 \leq i \leq r)$ et tout $j(1 \leq j \leq s)$, ϕ_i et ψ_j sont des polynômes de $A[X_2, \dots, X_n]$. Dans $MD(fg)$, X_1 figure avec l'exposant le plus grand possible, d'où

$$MD(fg) = X_1^{r+s} MD(\phi_r) MD(\psi_s).$$

L'hypothèse de récurrence entraîne

$$\begin{aligned} MD(\phi_r \psi_s) &= MD(\phi_r) MD(\psi_s); \\ MD(fg) &= X_1^{r+s} MD(\phi_r) MD(\psi_s) \\ &= X_1^r MD(\phi_r) X_1^s MD(\psi_s) = MD(f) MD(g). \end{aligned}$$

□

2. Polynômes symétriques dans $A[X_1, \dots, X_n], n > 1$

A. Notion de polynôme symétrique

Notons $\mathcal{S}_n$ le groupe des permutations de l'ensemble $\{1, 2, \dots, n\}$, appelé *groupe symétrique de degré n* (Cf. [11], Ch. 1 et 3).

A tout $\sigma \in \mathcal{S}_n$ et tout polynôme $f \in A[X_1, \dots, X_n]$, on associe le polynôme que l'on notera f_σ , dans $A[X_1, \dots, X_n]$, tel que

$$f_\sigma(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)}). \quad (8.1)$$

Quels que soient σ, τ dans $\mathcal{S}_n$, on a

$$\begin{aligned} f_{\tau \circ \sigma}(X_1, \dots, X_n) &= f(X_{\tau \circ \sigma(1)}, \dots, X_{\tau \circ \sigma(n)}) \\ &= (f_\sigma)_\tau(X_1, \dots, X_n) \end{aligned}$$

et pour l'élément unité e du groupe $\mathcal{S}_n$, $f_e = f$.

On en déduit que le groupe $\mathcal{S}_n$ opère sur $A[X_1, \dots, X_n]$ par l'application

$$\begin{aligned} \mathcal{S}_n \times A[X_1, \dots, X_n] &\longrightarrow A[X_1, \dots, X_n] \\ (\sigma, f) &\longmapsto f_\sigma. \end{aligned}$$

Remarque 8.6. Quel que soit $\sigma \in \mathcal{S}_n$, pour tout polynôme constant a et tout $i(1 \leq i \leq n)$, on a $a_\sigma = a$ et $(X_i)_\sigma = X_{\sigma(i)}$.

Définition 8.7. Un polynôme $f \in A[X_1, \dots, X_n]$ est dit **symétrique** si

$$\forall \sigma \in \mathcal{S}_n, \quad f_\sigma = f. \quad (8.2)$$

Remarque 8.8. :

a) D'après la remarque 8.6., tout polynôme constant est un polynôme symétrique.

b) La relation (8.2) montre qu'un polynôme $f \in A[X_1, \dots, X_n]$ est symétrique si c'est un **invariant** (ou élément **fixe**) de $A[X_1, \dots, X_n]$, dans l'action du groupe $\mathcal{S}_n$ ([11], p.187).

On vérifie facilement le résultat suivant.

Proposition 8.9. *L'ensemble des polynômes symétriques de $A[X_1, \dots, X_n]$ forme une sous- A -algèbre de $A[X_1, \dots, X_n]$.*

Proposition 8.10. :

$$1) \text{ Pour tout } \sigma \in \mathcal{S}_n, \text{ l'application } \Phi_\sigma : A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_n] \\ f \longmapsto f_\sigma$$

est un automorphisme de A -algèbres.

$$2) \text{ L'application } \Phi : \mathcal{S}_n \longrightarrow \text{Aut}_A A[X_1, \dots, X_n] \\ \sigma \longmapsto \Phi_\sigma$$

est un morphisme injectif de groupes.

Preuve :

1) L'application Φ_σ , induite par l'action du groupe $\mathcal{S}_n$ sur $A[X_1, \dots, X_n]$, est une *permutation* de l'ensemble $A[X_1, \dots, X_n]$ ([11], Ch. 5).

D'autre part, quels que soient f, g dans $A[X_1, \dots, X_n]$ et $a \in A$, on vérifie que, pour tout $\sigma \in \mathcal{S}_n$, on a

$$\begin{aligned} \Phi_\sigma(f+g) &= \Phi_\sigma(f) + \Phi_\sigma(g) \\ \Phi_\sigma(fg) &= (\Phi_\sigma(f))(\Phi_\sigma(g)) \\ \Phi_\sigma(af) &= a\Phi_\sigma(f), \end{aligned}$$

donc Φ_σ est un morphisme de A -algèbres et par suite, Φ_σ est un automorphisme.

2) L'application Φ est un morphisme de groupes ([11], prop. 5.3) ; vérifions que Φ est *injectif*.

$$\begin{aligned} \sigma \in \text{Ker } \Phi &\iff \Phi_\sigma = \text{id}_{A[X_1, \dots, X_n]} \\ &\iff \forall f \in A[X_1, \dots, X_n], \Phi_\sigma(f) = f, \\ &\iff \forall i (1 \leq i \leq n), \Phi_\sigma(X_i) = X_{\sigma(i)} = X_i, \\ &\iff \sigma = e \text{ (élément unité de } \mathcal{S}_n). \end{aligned}$$

□

Remarque 8.11. :

a) Φ étant injectif, le sous-groupe $\text{Im } \Phi$ de $\text{Aut}_A A[X_1, \dots, X_n]$ est isomorphe au groupe $\mathcal{S}_n$.

b) La propriété universelle de l'anneau $A[X_1, \dots, X_n]$ (Th. 4.57.) montre que pour tout $\sigma \in \mathcal{S}_n$, l'automorphisme Φ_σ est l'unique endomorphisme de $A[X_1, \dots, X_n]$ tel que pour tout $i (1 \leq i \leq n)$, $\Phi_\sigma(X_i) = X_{\sigma(i)}$.

[On applique le théorème 4.57., avec $B = A[X_1, \dots, X_n]$, l'injection canonique φ de A dans B et pour tout $i (1 \leq i \leq n)$, $\beta_i = X_{\sigma(i)}$.]

Exemple 8.12. : Exemples classiques dans $A[X_1, \dots, X_n], n > 1$.

1) **Les sommes des puissances $k^{\text{èmes}}$ des X_i , pour tout $k \in \mathbb{N}$:**

$$S_k = X_1^k + X_2^k + \dots + X_n^k.$$

Les sommes S_k sont appelées **sommes de Newton**.

2) **Les polynômes de Wronski, pour tout $k \in \mathbb{N}$:**

$$W_k = \sum_{i_1+i_2+\dots+i_n=k} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \text{ où } i_j \in \mathbb{N}, \forall j (1 \leq j \leq n).$$

3) Le discriminant des X_i , $1 \leq i \leq n$:

$$D = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

4) Les polynômes symétriques élémentaires des X_i , $1 \leq i \leq n$,

$$\begin{aligned}\Sigma_1 &= X_1 + X_2 + \cdots + X_n \\ \Sigma_2 &= X_1 X_2 + X_1 X_3 + \cdots + X_1 X_n + X_2 X_3 + \cdots + X_{n-1} X_n, \\ &\vdots \\ \Sigma_n &= X_1 X_2 \cdots X_n.\end{aligned}$$

D'une façon générale, pour tout k ($1 \leq k \leq n$), on a

$$\Sigma_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k},$$

où $(i_1, i_2, \dots, i_k)$ décrit l'ensemble des C_n^k combinaisons de $\{1, 2, \dots, n\}$ telles que $1 \leq i_1 < i_2 < \cdots < i_k \leq n$.

Remarque 8.13. :

a) Si Z désigne une $(n+1)^{\text{ème}}$ indéterminée, dans $A[X_1, X_2, \dots, X_n][Z]$, le polynôme

$$p(Z) = (Z - X_1)(Z - X_2) \cdots (Z - X_n) \text{ s'écrit}$$

$$p(Z) = Z^n - \Sigma_1 Z^{n-1} + \Sigma_2 Z^{n-2} - \cdots + (-1)^k \Sigma_k Z^{n-k} + \cdots + (-1)^n \Sigma_n.$$

où les Σ_k , $1 \leq k \leq n$, sont les polynômes symétriques élémentaires des X_i , $1 \leq i \leq n$.

b) Le Théorème fondamental (Th. 8.14.) montrera que les polynômes symétriques élémentaires jouent un rôle primordial dans l'algèbre des polynômes symétriques, à coefficients dans un domaine d'intégrité.

B. Théorème fondamental

Théorème 8.14. *L'anneau A étant un D.I., pour tout polynôme symétrique $f \in A[X_1, \dots, X_n]$, il existe un unique polynôme ϕ à n indéterminées sur A tel que*

$$f(X_1, X_2, \dots, X_n) = \phi(\Sigma_1, \Sigma_2, \dots, \Sigma_n), \quad (8.3)$$

où les Σ_k , $1 \leq k \leq n$, sont les polynômes symétriques élémentaires des X_i , $1 \leq i \leq n$.

1. Lemmes préliminaires

Lemme 8.15. *Pour un polynôme symétrique $f \in A[X_1, X_2, \dots, X_n]$, on a*

$$MD(f) = aX_1^{k_1} X_2^{k_2} \cdots X_n^{k_n} \implies k_1 \geq k_2 \geq \cdots \geq k_n. \quad (8.4)$$

Preuve : Supposons qu'il existe un couple d'entiers (i, j) vérifiant $1 \leq i < j \leq n$ et $k_i < k_j$. Le polynôme f étant symétrique, s'il contient le monôme $MD(f)$ ci-dessus, il contient aussi le monôme

$$\begin{aligned}\mu &= aX_1^{k_1} \cdots X_{i-1}^{k_{i-1}} X_j^{k_i} \cdots X_{j-1}^{k_{j-1}} X_i^{k_j} \cdots X_n^{k_n} \\ &= aX_1^{k_1} \cdots X_{i-1}^{k_{i-1}} X_i^{k_j} \cdots X_{j-1}^{k_{j-1}} X_j^{k_i} \cdots X_n^{k_n};\end{aligned}$$

alors, $k_j - k_i > 0$ implique que le monôme μ est plus haut que le monôme $MD(f)$, d'où une contradiction. □

Lemme 8.16. Soit $\Sigma_1, \Sigma_2, \dots, \Sigma_n$ les polynômes symétriques élémentaires en $X_1, \dots, X_n$; si pour tout $(l_1, l_2, \dots, l_n) \in \mathbb{N}^n$, on pose $l = \sum_{1 \leq i \leq n} l_i$, alors dans $A[X_1, \dots, X_n]$, on a

$$MD(\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}) = X_1^l X_2^{l-l_1} \dots X_n^{l_n}.$$

De plus, $\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}$, considéré dans $A[X_1, \dots, X_n]$, est un polynôme symétrique, homogène de degré $l_1 + 2l_2 + \dots + nl_n$.

Preuve :

$$\begin{aligned} MD(\Sigma_1^{l_1}) &= MD(X_1 + \dots + X_n)^{l_1} = X_1^{l_1} \\ MD(\Sigma_2^{l_2}) &= MD(X_1 X_2 + \dots + X_{n-1} X_n)^{l_2} = X_1^{l_2} X_2^{l_2} \\ &\vdots \\ MD(\Sigma_k^{l_k}) &= MD(X_1 \dots X_k + \dots + X_{n-k} \dots X_n)^{l_k} = X_1^{l_k} X_2^{l_k} \dots X_k^{l_k} \\ &\vdots \\ MD(\Sigma_n^{l_n}) &= X_1^{l_n} \dots X_n^{l_n}, \end{aligned}$$

d'où, en utilisant la proposition 8.5.,

$$MD(\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}) = X_1^{l_1} X_2^{l-l_1} \dots X_n^{l_n}.$$

Pour tout $k, 1 \leq k \leq n$, Σ_k est un polynôme symétrique, homogène de degré k dans $A[X_1, \dots, X_n]$, donc le polynôme $\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}$ est symétrique, homogène et de même degré que le monôme $MD(\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n})$, c'est-à-dire

$$\begin{aligned} l + (l - l_1) + \dots + l_n &= (l_1 + \dots + l_n) + \dots + (l_k + \dots + l_n) + \dots + l_n \\ &= l_1 + 2l_2 + \dots + kl_k + \dots + nl_n. \end{aligned} \quad \square$$

Définition 8.17. Les hypothèses et les notations étant celles du lemme 8.16., l'entier $l_1 + 2l_2 + \dots + nl_n$ est appelé le **poids** de $\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}$.

Pour tout polynôme $\phi(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$, le **poids** de ϕ est le maximum des poids des monômes dont il est la somme.

Remarque 8.18. : Conséquences du lemme 8.16. :

a) Si $k_1 \geq k_2 \geq \dots \geq k_n$, dans $\mathbb{N}^*$, alors

$$MD(\Sigma_1^{k_1-k_2} \Sigma_2^{k_2-k_3} \dots \Sigma_{n-1}^{k_{n-1}-k_n} \Sigma_n^{k_n}) = X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}. \quad (8.5)$$

L'égalité (8.5) s'obtient en appliquant le lemme 8.16, avec, pour tout $i (1 \leq i \leq n-1)$, $l_i = k_i - k_{i+1}$ et $l_n = k_n$. On en déduit que

$$\text{poids}(\Sigma_1^{k_1-k_2} \Sigma_2^{k_2-k_3} \dots \Sigma_n^{k_n}) = k_1 + k_2 + \dots + k_n.$$

b) Avec les notations du lemme 8.16. on a

$$\text{poids}(\Sigma_1^{l_1} \Sigma_2^{l_2} \dots \Sigma_n^{l_n}) = 0 \iff l_i = 0, \forall i (1 \leq i \leq n).$$

2. Preuve du théorème 8.14. (Théorème fondamental)

Soit f un polynôme symétrique dans $A[X_1, \dots, X_n]$.

- Existence du polynôme ϕ vérifiant (8.3)

Si $f = 0$, il suffit de prendre $\phi = 0$; on suppose donc $f \neq 0$ et on raisonne par récurrence sur la hauteur du monôme directeur de f . Supposons

$$MD(f) = aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}, \text{ où } a \in A^*.$$

Si pour tout i ($1 \leq i \leq n$), on a $k_i = 0$, alors $MD(f) = a$, donc $f = a$. Le théorème est vérifié en prenant $\phi = a$.

Si f est non constant, supposons le théorème vrai pour tout polynôme symétrique de $A[X_1, \dots, X_n]$, dont le monôme directeur est *moins haut* que celui de f .

La relation (8.5) implique

$$MD(f) = MD(a\Sigma_1^{k_1-k_2}\Sigma_2^{k_2-k_3}\dots\Sigma_n^{k_n}).$$

Considérons alors le polynôme

$$g(X_1, \dots, X_n) := f(X_1, \dots, X_n) - a\Sigma_1^{k_1-k_2}\Sigma_2^{k_2-k_3}\dots\Sigma_n^{k_n}.$$

On a $MD(g) < MD(f)$. Par suite, compte tenu de l'hypothèse de récurrence, il existe un unique polynôme ψ à n indéterminées sur A tel que

$$g(X_1, \dots, X_n) = \psi(\Sigma_1, \dots, \Sigma_n);$$

$$\text{d'où, } f(X_1, \dots, X_n) = \psi(\Sigma_1, \dots, \Sigma_n) + a\Sigma_1^{k_1-k_2}\Sigma_2^{k_2-k_3}\dots\Sigma_n^{k_n}.$$

En notant $\phi(\Sigma_1, \dots, \Sigma_n)$ le second membre de l'égalité précédente, on a la relation (8.3).

- *Unicité du polynôme ϕ vérifiant (8.3)*

Supposons que par une autre méthode, on ait trouvé un polynôme θ à n indéterminées sur A tel que

$$f(X_1, \dots, X_n) = \theta(\Sigma_1, \dots, \Sigma_n). \quad (8.6)$$

Démontrons que $\theta = \phi$. Supposons $\theta \neq \phi$, alors

$$\phi(\Sigma_1, \dots, \Sigma_n) - \theta(\Sigma_1, \dots, \Sigma_n) = \delta(\Sigma_1, \dots, \Sigma_n),$$

où δ est un polynôme *non nul* dans $A[\Sigma_1, \dots, \Sigma_n]$.

Cependant, en exprimant les Σ_k , $1 \leq k \leq n$, en fonction des X_i , $1 \leq i \leq n$, on obtient, compte tenu des relations (8.3) et (8.6),

$$\delta(\Sigma_1, \dots, \Sigma_n) = d(X_1, \dots, X_n) = f(X_1, \dots, X_n) - f(X_1, \dots, X_n) = 0. \quad (8.7)$$

où d est donc le polynôme nul dans $A[X_1, \dots, X_n]$.

Démontrons que δ est nécessairement le polynôme nul dans $A[\Sigma_1, \dots, \Sigma_n]$.

En effet, $\delta \neq 0$ peut s'écrire comme une somme de monômes non nuls ordonnés suivant l'ordre décroissant de leurs poids :

$$\delta = \Sigma_{1 \leq j \leq r} a_j \Sigma_1^{l_{j,1}} \Sigma_2^{l_{j,2}} \dots \Sigma_n^{l_{j,n}}, \quad (8.8)$$

les a_j , $1 \leq j \leq r$, étant *non nuls* dans A .

D'après le lemme 8.16., dans le développement de δ en fonction des X_i , chaque monôme $a_j \Sigma_1^{l_{j,1}} \Sigma_2^{l_{j,2}} \dots \Sigma_n^{l_{j,n}}$ donne, dans $d(X_1, \dots, X_n)$, une composante homogène de degré égal à son poids : $l_{j,1} + 2l_{j,2} + \dots + nl_{j,n}$. Par suite,

$$d = 0 \implies a_j = 0, \forall j (1 \leq j \leq r) \implies \delta = 0,$$

donc $\theta = \phi$. □

C. Recherche pratique du polynôme ϕ connaissant f

Remarque 8.19. La démonstration du théorème 8.14. fournit, théoriquement, un algorithme pour trouver ϕ connaissant f , mais les calculs deviennent vite inextricables lorsque le nombre des indéterminées augmente.

La méthode peut être simplifiée en remarquant que tout polynôme symétrique est la

somme de ses composantes homogènes ; ainsi, en utilisant le théorème 8.20. ci-dessous, on se ramènera à la recherche du polynôme ϕ , associé à un polynôme f symétrique et homogène.

Théorème 8.20. *A étant un D.I., si $f \in A[X_1, X_2, \dots, X_n]$ est un polynôme symétrique de degré total d , alors l'unique polynôme ϕ tel que $f(X_1, \dots, X_n) = \phi(\Sigma_1, \dots, \Sigma_n)$ est de poids d .*

Preuve : Ecrivons $f(X_1, \dots, X_n) = \sum_{1 \leq i \leq r} h_i(X_1, \dots, X_n)$, où les $h_i(X_1, \dots, X_n)$, $1 \leq i \leq r$, sont les composantes homogènes du polynôme symétrique f . Chaque h_i est donc un polynôme symétrique et homogène ; posons $d_i := \deg h_i$. Le degré total de f étant d , on peut supposer

$$d = d_1 > d_2 > \dots > d_r.$$

Pour tout i ($1 \leq i \leq r$), il existe (Th. 8.14.) un unique polynôme ϕ_i vérifiant

$$h_i(X_1, \dots, X_n) = \phi_i(\Sigma_1, \dots, \Sigma_n). \quad (8.9)$$

$$\text{Posons} \quad \phi_i(\Sigma_1, \dots, \Sigma_n) = \sum_{1 \leq j \leq k_i} a_j \Sigma_1^{l_{j,1}} \dots \Sigma_n^{l_{j,n}}. \quad (8.10)$$

h_i est homogène de degré d_i , donc d'après le lemme 8.16., dans l'égalité (8.10), chaque monôme $a_j \Sigma_1^{l_{j,1}} \dots \Sigma_n^{l_{j,n}}$ est de poids d_i , d'où

$$\forall j (1 \leq j \leq k_i), \quad l_{j,1} + 2l_{j,2} + \dots + nl_{j,n} = d_i.$$

Compte tenu de l'unicité du polynôme ϕ , on a nécessairement,

$$\phi(\Sigma_1, \dots, \Sigma_n) = \sum_{1 \leq i \leq r} \phi_i(\Sigma_1, \dots, \Sigma_n)$$

et $\text{poids}(\phi) = \max\{\text{poids}(\phi_i), 1 \leq i \leq r\} = d_1 = d$. □

Conséquence : Etant donné un polynôme f symétrique dans $A[X_1, \dots, X_n]$, pour trouver le polynôme ϕ défini dans le théorème 8.14., il faut écrire f comme somme de ses composantes homogènes et déterminer les polynômes ϕ_i , donc les coefficients a_j intervenant dans le second membre de la relation (8.10). Ce calcul se fait parfois en substituant aux indéterminées des éléments particuliers de A , comme dans l'exemple 2) ci-dessous.

Exemple 8.21. : Calcul du discriminant D (Cf. Exemple 8.12.), dans les cas $n = 2$ et $n = 3$, lorsque $A = \mathbb{Z}$.

1) $n = 2$ Il est immédiat que

$$D = (X_1 - X_2)^2 = \Sigma_1^2 - 4\Sigma_2.$$

2) $n = 3$

$$D = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2. \quad (8.11)$$

D est symétrique, homogène de degré 6 dans $\mathbb{Z}[X_1, X_2, X_3]$. Posons :

$$D = \sum_{1 \leq j \leq k} a_j \Sigma_1^{l_{j,1}} \Sigma_2^{l_{j,2}} \Sigma_3^{l_{j,3}}. \quad (8.12)$$

Il faut trouver l'entier k et, pour chaque entier j ($1 \leq j \leq k$), le coefficient a_j dans $\mathbb{Z}$, ainsi que le triplet d'entiers naturels $(l_{j,1}, l_{j,2}, l_{j,3})$.

L'expression (8.12) de D permet de calculer son monôme directeur :

$$MD(D) = X_1^4 X_2^2;$$

par suite, quel que soit j , $1 \leq j \leq k$,

$$l_{j,1} + 2l_{j,2} + 3l_{j,3} = 6 \quad (8.13)$$

et dans tout autre monôme intervenant dans le développement de D , l'exposant de X_1 est nécessairement inférieur ou égal à 4, d'où

$$l_{j,1} + l_{j,2} + l_{j,3} \leq 4. \quad (8.14)$$

Les relations (8.13) et (8.14) étant indépendantes de l'entier j , notons (l_1, l_2, l_3) un triplet recherché ; on trouve alors que les seules valeurs possibles pour (l_1, l_2, l_3) sont les suivantes :

$$(3, 0, 1), (2, 2, 0), (1, 1, 1), (0, 3, 0), (0, 0, 2).$$

On en déduit

$$D = a\Sigma_1^3\Sigma_3 + b\Sigma_1^2\Sigma_2^2 + c\Sigma_1\Sigma_2\Sigma_3 + d\Sigma_2^3 + e\Sigma_3^2. \quad (8.15)$$

Pour $X_3 = 0$, on obtient

$$D = (X_1 - X_2)^2 X_1^2 X_2^2 = b\Sigma_1^2\Sigma_2^2 + d\Sigma_2^3, \quad (8.16)$$

où Σ_1 et Σ_2 sont les polynômes symétriques élémentaires en X_1 et X_2 .

L'égalité des monômes directeurs des deux membres de (8.16) donne

$$X_1^4 X_2^2 = b X_1^4 X_2^2, \text{ donc } b = 1.$$

En faisant alors, $X_1 = X_2$ dans la relation (8.16), on obtient

$$0 = 4X_1^6 + dX_1^6, \text{ par suite } d = -4.$$

D'autre part, le lecteur vérifiera les calculs suivants :

$$(X_1 = X_2 = 1, X_3 = -2) \implies e = -27$$

$$(X_1 = X_2 = 2, X_3 = -1) \implies a = -4$$

$$(X_1 = X_2 = X_3 = 1) \implies c = 18,$$

$$\text{d'où } D = -4\Sigma_1^3\Sigma_3 + \Sigma_1^2\Sigma_2^2 + 18\Sigma_1\Sigma_2\Sigma_3 - 4\Sigma_2^3 - 27\Sigma_3^2.$$

Pour certains polynômes symétriques, d'autres méthodes pourront être utilisées, en particulier, par l'application des Formules de Newton développées dans le paragraphe suivant.

3. Formules de Newton

Les notations utilisées sont celles des Exemples 8.12.

Théorème 8.22. *A étant un D.I., dans $A[X_1, \dots, X_n]$, $n \geq 1$, on a pour tout entier k ($1 \leq k \leq n$),*

$$S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} - \dots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k k \Sigma_k = 0; \quad (8.17)$$

pour tout entier $l > n$,

$$S_l - \Sigma_1 S_{l-1} + \Sigma_2 S_{l-2} - \dots + (-1)^n \Sigma_n S_{l-n} = 0. \quad (8.18)$$

Les relations (8.17) et (8.18) sont appelées **Formules de Newton**.

Preuve : Soit Z une $(n+1)^{\text{ème}}$ indéterminée ; dans $A[X_1, \dots, X_n][Z]$, on considère le polynôme $p(Z) = \prod_{1 \leq i \leq n} (Z - X_i)$, donc

$$p(Z) = Z^n - \Sigma_1 Z^{n-1} + \dots + (-1)^{n-1} \Sigma_{n-1} Z + (-1)^n \Sigma_n. \quad (8.19)$$

Pour tout i , $1 \leq i \leq n$, on a $p(X_i) = 0$, autrement dit :

$$X_i^n - \Sigma_1 X_i^{n-1} + \cdots + (-1)^{n-1} \Sigma_{n-1} X_i + (-1)^n \Sigma_n = 0. \quad (8.20)$$

La somme, pour $1 \leq i \leq n$, des premiers membres des égalités (8.20) donne

$$S_n - \Sigma_1 S_{n-1} + \Sigma_2 S_{n-2} - \cdots + (-1)^{n-1} \Sigma_{n-1} S_1 + (-1)^n n \Sigma_n = 0,$$

c'est-à-dire la formule (8.17), pour $k = n$.

Pour $l > n$, on considère $Z^{l-n} p(Z)$; pour $1 \leq i \leq n$, on a $X_i^{l-n} p(X_i) = 0$, donc $X_i^{l-n} (X_i^n - \Sigma_1 X_i^{n-1} + \cdots + (-1)^{n-1} \Sigma_{n-1} X_i + (-1)^n \Sigma_n) = 0$, d'où

$$X_i^l - \Sigma_1 X_i^{l-1} + \cdots + (-1)^{n-1} \Sigma_{n-1} X_i^{l-n+1} + (-1)^n \Sigma_n X_i^{l-n} = 0. \quad (8.21)$$

En effectuant, comme plus haut, la somme, pour $1 \leq i \leq n$, des premiers membres des égalités (8.21), on obtient la formule (8.18).

Pour $k = 1$, la formule (8.17) est satisfaite, puisque $S_1 = \Sigma_1$; il reste à prouver la relation (8.17) pour $1 < k < n$.

On raisonne par récurrence sur le nombre n des indéterminées. Fixons l'entier k tel que $1 < k < n$ et supposons la relation (8.17) vérifiée pour $n-1$ indéterminées. On remarque que pour tout i ($1 \leq i \leq n-1$), on a

$$\begin{aligned} \Sigma_i(X_1, \dots, X_{n-1}) &= \Sigma_i(X_1, \dots, X_{n-1}, 0), \\ S_i(X_1, \dots, X_{n-1}) &= S_i(X_1, \dots, X_{n-1}, 0). \end{aligned}$$

En exprimant le premier membre de la relation (8.17) en fonction des indéterminées $X_1, \dots, X_{n-1}, X_n$ on obtient un polynôme symétrique et homogène de degré k , que nous désignerons par $h(X_1, \dots, X_{n-1}, X_n)$.

L'hypothèse de récurrence implique $h(X_1, \dots, X_{n-1}, 0) = 0$.

On en déduit que $h(X_1, \dots, X_{n-1}, X_n)$ est divisible par X_n ; mais $h(X_1, \dots, X_{n-1}, X_n)$ est symétrique dans $A[X_1, \dots, X_n]$, par suite ce polynôme est divisible par tout X_i , $1 \leq i \leq n-1$. Or, h est homogène de degré $k < n$, donc il ne peut être divisible par le produit $X_1 X_2 \dots X_n$, d'où nécessairement,

$$h(X_1, \dots, X_{n-1}, X_n) = 0.$$

Ce qui prouve la relation (8.17) pour $1 < k < n$. □

Premières applications des formules de Newton

1) Calcul des S_k en fonction des Σ_j , dans $A[\Sigma_1, \dots, \Sigma_n]$.

Les Formules de Newton nous donnent :

$$\begin{aligned} S_1 &= \Sigma_1 \\ S_2 &= S_1 \Sigma_1 - 2 \Sigma_2 = \Sigma_1^2 - 2 \Sigma_2 \\ S_3 &= S_2 \Sigma_1 - S_1 \Sigma_2 + 3 \Sigma_3 = \Sigma_1^3 - 3 \Sigma_1 \Sigma_2 + 3 \Sigma_3. \end{aligned}$$

Ainsi, de proche en proche, on calcule les S_k , pour $1 \leq k \leq n$, et les S_l pour $l > n$, en fonction des Σ_j , $1 \leq j \leq n$.

2) Calcul des Σ_j en fonction des S_k dans $K[S_1, \dots, S_n]$, où K est un corps de caractéristique 0.

En appliquant les Formules de Newton, on obtient

$$\begin{aligned}\Sigma_1 &= S_1 \\ \Sigma_2 &= \frac{1}{2}S_1^2 - \frac{1}{2}S_2 \\ \Sigma_3 &= \frac{1}{6}S_1^3 - \frac{1}{2}S_1S_2 + \frac{1}{3}S_3.\end{aligned}$$

De proche en proche, on peut calculer les Σ_j , $1 \leq j \leq n$, en fonction des S_k , $1 \leq k \leq n$. Du théorème fondamental 8.14., on déduit le corollaire suivant.

Corollaire 8.23. *A étant un D.I., de caractéristique 0, si $K = FrA$, alors pour tout polynôme symétrique $f \in A[X_1, \dots, X_n]$, il existe un polynôme g à n indéterminées sur K tel que*

$$f(X_1, \dots, X_n) = g(S_1, \dots, S_n). \quad (8.22)$$

Preuve : $K = FrA$ désigne le corps des fractions de A (Déf. 5.2.). On note que $car A = 0$ implique $car K = 0$. D'après le Théorème 8.14., il existe un unique polynôme ϕ , à n indéterminées sur A , tel que

$$f(X_1, \dots, X_n) = \phi(\Sigma_1, \dots, \Sigma_n).$$

En exprimant les Σ_j , $1 \leq j \leq n$, en fonction des S_k , $1 \leq k \leq n$, dans $K[S_1, \dots, S_n]$, on obtient le polynôme g défini par

$$g(S_1, \dots, S_n) := \phi(\Sigma_1(S_1, \dots, S_n), \dots, \Sigma_n(S_1, \dots, S_n)).$$

Le polynôme g est à coefficients dans K et vérifie à la relation (8.22). □

3) Relations entre les coefficients et les racines d'un polynôme de $K[X]$, où K est un corps supposé algébriquement clos (Déf. 4.42).

Soit $f \in K[X]$ tel que $\deg f = n \geq 1$. Le corps K étant algébriquement clos, le polynôme f a n racines dans K , distinctes ou confondues, que l'on notera $\alpha_1, \alpha_2, \dots, \alpha_n$ (Cf. Th. 4.38); alors

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i \implies f(X) = a_n \prod_{1 \leq i \leq n} (X - \alpha_i). \quad (8.23)$$

Considérons les polynômes symétriques élémentaires en $\alpha_1, \dots, \alpha_n$ et posons, pour tout k ($1 \leq k \leq n$),

$$\Sigma_k := \Sigma_k(\alpha_1, \dots, \alpha_n).$$

En développant les expressions de $f(X)$ apparaissant dans (8.23), on obtient

$$\begin{aligned}f(X) &= a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \\ &= a_n (X^n - \Sigma_1 X^{n-1} + \Sigma_2 X^{n-2} - \dots + (-1)^{n-1} \Sigma_{n-1} X + (-1)^n \Sigma_n).\end{aligned}$$

Par hypothèse $\deg f = n \geq 1$, d'où $a_n \neq 0$. En identifiant les coefficients des X^k , pour $0 \leq k \leq n$, dans les deux expressions de $f(X)$, ci-dessus, on obtient les relations suivantes, appelées **Relations entre les coefficients et les racines** du polynôme f .

Dans K on identifie a_n^{-1} à $\frac{1}{a_n}$, d'où

$$\Sigma_1 = -\frac{a_{n-1}}{a_n}, \quad \Sigma_2 = \frac{a_{n-2}}{a_n}, \quad \dots, \quad \Sigma_n = (-1)^n \frac{a_0}{a_n},$$

donc, pour tout $k (1 \leq k \leq n)$,

$$\Sigma_k = \Sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}. \quad (8.24)$$

Remarque 8.24. Si l'on se donne n éléments $\alpha_1, \dots, \alpha_n$, dans K , tels que

$$\forall i, 1 \leq i \leq n, \Sigma_i(\alpha_1, \dots, \alpha_n) = \lambda_i,$$

alors $\alpha_1, \dots, \alpha_n$ sont les racines du polynôme

$$X^n - \lambda_1 X^{n-1} + \lambda_2 X^{n-2} - \dots + (-1)^n \lambda_n.$$

Exemple 8.25. Les notations sont celles utilisées dans le cas général.

1) Pour $f(X) = aX^2 + bX + c$ dans $\mathbb{C}[X]$, $a \neq 0$, on (re)trouve

$$\Sigma_1 = \alpha_1 + \alpha_2 = -\frac{b}{a}, \quad \alpha_1 \alpha_2 = \frac{c}{a}.$$

2) Soit $f(X) = X^3 + pX + q$ dans $\mathbb{C}[X]$. Les formules (8.24) donnent

$$\Sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0,$$

$$\Sigma_2 = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = p,$$

$$\Sigma_3 = \alpha_1 \alpha_2 \alpha_3 = -q.$$

4. Fractions rationnelles symétriques

A désignant un D.I., soit $A(X_1, \dots, X_n)$ le corps des fractions du domaine d'intégrité $A[X_1, \dots, X_n]$, c'est à dire le corps des fractions rationnelles à coefficients dans A .

A. Notion de fraction rationnelle symétrique

On rappelle que

$$f \in A(X_1, \dots, X_n) \iff f(X_1, \dots, X_n) = \frac{p(X_1, \dots, X_n)}{q(X_1, \dots, X_n)}, \quad (8.25)$$

où p et q sont des polynômes dans $A[X_1, \dots, X_n]$, $q \neq 0$.

$\frac{p}{q}$ est un représentant de f dans le corps $A(X_1, \dots, X_n)$ et pour tout autre représentant $\frac{r}{s}$ de f , on a $ps = qr$ dans $A[X_1, \dots, X_n]$.

$\mathcal{S}_n$ désignant le groupe symétrique dont les éléments sont les permutations de $\{1, 2, \dots, n\}$, on vérifiera que la correspondance

$$\begin{aligned} \mathcal{S}_n \times A(X_1, \dots, X_n) &\longrightarrow A(X_1, \dots, X_n) \\ (\sigma, f = \frac{p}{q}) &\longmapsto f_\sigma := \frac{p_\sigma}{q_\sigma} \end{aligned}$$

est une application définissant une action du groupe $\mathcal{S}_n$ sur $A(X_1, \dots, X_n)$.

Définition 8.26. Une fraction rationnelle $f = \frac{p}{q} \in A(X_1, \dots, X_n)$, $n > 1$, est **symétrique** si

$$\forall \sigma \in \mathcal{S}_n, \quad f_\sigma = f.$$

Remarque 8.27. Soit $f = \frac{p}{q}$ dans $A(X_1, \dots, X_n)$, alors

$$(\forall \sigma \in \mathcal{S}_n, f_\sigma = f \text{ et } p_\sigma = p) \implies \forall \sigma \in \mathcal{S}_n, q_\sigma = q. \quad (8.26)$$

$$(\forall \sigma \in \mathcal{S}_n, f_\sigma = f \text{ et } q_\sigma = q) \implies \forall \sigma \in \mathcal{S}_n, p_\sigma = p. \quad (8.27)$$

$$(\forall \sigma \in \mathcal{S}_n, p_\sigma = p \text{ et } q_\sigma = q) \implies \forall \sigma \in \mathcal{S}_n, f_\sigma = f. \quad (8.28)$$

Théorème 8.28. Pour toute fraction rationnelle f , symétrique dans $A(X_1, \dots, X_n)$, il existe un représentant $\frac{p}{q}$, où p et q sont des polynômes symétriques dans $A[X_1, \dots, X_n]$.

Preuve : Soit $\frac{p}{q}$ un représentant de f , tel que le degré total de q est *minimal*. Démontrons que le polynôme q est symétrique.

On suppose q non symétrique ; donc il existe au moins une transposition $\tau \in \mathcal{S}_n$ telle que $q_\tau \neq q$; alors

$$f_\tau = f \iff \frac{p_\tau}{q_\tau} = \frac{p}{q} \iff qp_\tau = pq_\tau;$$

$$qp_\tau = pq_\tau \iff q(p_\tau - p) = p(q_\tau - q).$$

Compte tenu de l'hypothèse $q_\tau \neq q$, la dernière égalité implique

$$\frac{p_\tau - p}{q_\tau - q} = \frac{p}{q} = f.$$

Comme on a $\tau \neq id$, il existe un unique couple d'entiers (i, j) tel que $1 \leq i < j \leq n$ et $\tau(i) = j$; alors

$$p_\tau - p = p(X_1, \dots, X_j, \dots, X_i, \dots, X_n) - p(X_1, \dots, X_i, \dots, X_j, \dots, X_n).$$

En substituant X_i à X_j dans $p_\tau - p$ on obtient 0; on en déduit que $(X_j - X_i)$ divise $p_\tau - p$ dans l'anneau $A[X_1, \dots, X_n]$. On prouverait de même que $q_\tau - q$ est divisible par $(X_j - X_i)$. Par suite, il existe des polynômes p_1 et q_1 dans $A[X_1, \dots, X_n]$ tels que

$$p_\tau - p = (X_j - X_i)p_1 \text{ et } q_\tau - q = (X_j - X_i)q_1.$$

On en déduit que $f = \frac{p_1}{q_1}$, où le degré total de q_1 est strictement inférieur au degré total de q , ce qui contredit la *minimalité* du degré total de q ; donc le polynôme q est symétrique. La fraction $f = \frac{p}{q}$ étant symétrique par hypothèse, d'après la relation (8.27), le polynôme p est symétrique, d'où le théorème énoncé. $\square$

Théorème 8.29. Quelle que soit la fraction rationnelle f , symétrique dans $A(X_1, \dots, X_n)$, il existe une fraction rationnelle ϕ à n indéterminées sur A telle que

$$f(X_1, \dots, X_n) = \phi(\Sigma_1, \dots, \Sigma_n).$$

Preuve : Etant donné une fraction rationnelle $f = \frac{p}{q}$, symétrique dans $A(X_1, \dots, X_n)$, on peut supposer (Th. 8.28.) que les polynômes p et q sont symétriques dans $A[X_1, \dots, X_n]$. Il existe alors (Th. 8.14), des polynômes φ et ψ à n indéterminées sur A tels que

$$\begin{aligned} p(X_1, \dots, X_n) &= \varphi(\Sigma_1, \dots, \Sigma_n), \\ q(X_1, \dots, X_n) &= \psi(\Sigma_1, \dots, \Sigma_n). \end{aligned}$$

En posant $\phi := \frac{\varphi}{\psi}$, on obtient $f(X_1, \dots, X_n) = \phi(\Sigma_1, \dots, \Sigma_n)$. $\square$

B. Applications des fractions rationnelles symétriques

1. Généralisation des Formules de Newton

Pour tout $k \in \mathbb{Z}$, on définit, dans $A(X_1, \dots, X_n)$, les fractions rationnelles S_k telles que

$$S_k = \sum_{1 \leq i \leq n} X_i^k.$$

Proposition 8.30. Pour tout $k \in \mathbb{N}$, on a

$$S_{n-k} - \Sigma_1 S_{n-k-1} + \dots + (-1)^l \Sigma_l S_{n-k-l} + \dots + (-1)^n \Sigma_n S_{-k} = 0. \quad (8.29)$$

Preuve : Comme dans la démonstration du Th. 8.22., on utilise le polynôme $p(Z)$ de $A[X_1, \dots, X_n][Z]$ tel que

$$p(Z) = \prod_{1 \leq i \leq n} (Z - X_i) = Z^n - \Sigma_1 Z^{n-1} + \dots + (-1)^n \Sigma_n.$$

Pour tout i ($1 \leq i \leq n$), $p(X_i) = 0$, donc pour tout $k \in \mathbb{N}$,

$$X_i^{-k} (X_i^n - \Sigma_1 X_i^{n-1} + \Sigma_2 X_i^{n-2} - \dots + (-1)^n \Sigma_n) = 0. \quad (8.30)$$

La somme des égalités (8.30), pour $1 \leq i \leq n$, donne la relation (8.29)

$$S_{n-k} - \Sigma_1 S_{n-k-1} + \dots + (-1)^l \Sigma_l S_{n-k-l} + \dots + (-1)^n \Sigma_n S_{-k} = 0$$

qui permet de calculer S_{-k} pour tout entier $k > 0$. □

Exemple 8.31. :

Pour $n = 3$ et $k = 1$, la relation (8.5) s'écrit :

$$S_2 - \Sigma_1 S_1 + \Sigma_2 S_0 - \Sigma_3 S_{-1} = 0;$$

alors ($S_2 = \Sigma_1^2 - 2\Sigma_2$, $S_1 = \Sigma_1$, $S_0 = 3$) $\implies S_{-1} = \frac{\Sigma_2}{\Sigma_3}$.

Pour $n = 3$ et $k = 2$, on obtient

$$S_1 - \Sigma_1 S_0 + \Sigma_2 S_{-1} - \Sigma_3 S_{-2} = 0, \text{ d'où}$$

$$S_{-2} = \frac{\Sigma_2 S_{-1} - 2\Sigma_1}{\Sigma_3} = \frac{\Sigma_2^2 - 2\Sigma_1 \Sigma_3}{\Sigma_3^2}.$$

2. Fonctions rationnelles numériquement symétriques des racines d'un polynôme

K désigne un corps ; pour tout F non nul dans le corps $K(X_1, \dots, X_n)$ des fractions rationnelles à n indéterminées sur K , on considère un représentant $\frac{p}{q}$ irréductible, c'est-à-dire tel que $p \wedge q = 1$, dans l'anneau de polynômes $K[X_1, \dots, X_n]$.

A tout $F = \frac{p}{q} \in K(X_1, \dots, X_n)$ on associe l'application $\tilde{F}$ définie par

$$\tilde{F} : K^n \longrightarrow K$$

$$(x_1, \dots, x_n) \longmapsto \tilde{F}(x_1, \dots, x_n) = \frac{\tilde{p}(x_1, \dots, x_n)}{\tilde{q}(x_1, \dots, x_n)}.$$

Définition 8.32. Compte tenu des hypothèses et notations ci-dessus,

a) On dit que $\tilde{F}$ est une **fonction rationnelle** de K^n dans K .

b) La fonction rationnelle $\tilde{F}$ est dite **formellement symétrique**, si quels que soient $\sigma \in \mathcal{S}_n$ et $(x_1, \dots, x_n) \in K^n$,

$$\tilde{F}(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \tilde{F}(x_1, \dots, x_n).$$

Notation : Avec les hypothèses ci-dessus, on notera $\tilde{F}_\sigma$ la fonction rationnelle telle que, quel que soit $(x_1, \dots, x_n) \in K^n$,

$$\tilde{F}_\sigma(x_1, \dots, x_n) = \tilde{F}(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Définition 8.33. Etant donné un polynôme $f(X) \in K[X]$, de degré $n \geq 2$, scindé sur K (Déf. 4.46), dont les n racines distinctes ou confondues dans K sont $\alpha_1, \dots, \alpha_n$, on dit qu'une fonction rationnelle $\tilde{F}$ de K^n dans K est **numériquement symétrique** des racines de $f(X)$, si

$$\forall \sigma \in \mathcal{S}_n, \tilde{F}_\sigma(\alpha_1, \dots, \alpha_n) = \tilde{F}(\alpha_1, \dots, \alpha_n). \quad (8.31)$$

Remarque 8.34. Dans le contexte ci-dessus, toute fonction rationnelle *symétrique* de K^n dans K est une fonction *numériquement symétrique* des racines du polynôme $f(X)$, mais la réciproque est fautive, comme le montre l'exemple suivant.

Exemple 8.35. Soit $f(X) = X^3 + pX + q$ dans $\mathbb{C}[X]$. Le polynôme f a trois racines distinctes ou confondues, $\alpha_1, \alpha_2, \alpha_3$, dans $\mathbb{C}$ (Cf. Prop. 4.44.).

Désignons par θ la fonction rationnelle de $\mathbb{C}^3$ dans $\mathbb{C}$ telle que

$$\forall (x_1, x_2, x_3) \in \mathbb{C}^3, \quad \theta(x_1, x_2, x_3) = x_1^2 - x_2x_3.$$

La fonction rationnelle θ n'est pas formellement symétrique en x_1, x_2, x_3 , on a cependant,

$$\theta(\alpha_1, \alpha_2, \alpha_3) = \alpha_1(\alpha_1 + \alpha_2 + \alpha_3) - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3).$$

$$(\alpha_1 + \alpha_2 + \alpha_3 = 0 \text{ et } \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p) \implies \theta(\alpha_1, \alpha_2, \alpha_3) = -p,$$

donc θ est une fonction rationnelle *numériquement symétrique* des racines de f .

Remarque 8.36. θ étant une fraction rationnelle *numériquement symétrique* des racines $\alpha_i, 1 \leq i \leq n$, d'un polynôme $f(X) \in K[X]$, scindé sur K , on peut calculer $\theta(\alpha_1, \dots, \alpha_n)$ en fonction des coefficients de f , sans connaître les racines α_i , mais en utilisant les *Relations entre les coefficients et les racines* du polynôme f .

Proposition 8.37. Si θ est une fonction rationnelle *numériquement symétrique* des racines $\alpha_1, \dots, \alpha_n$ d'un polynôme $f(X)$ de $K[X]$, de degré $n \geq 2$, scindé sur K , alors il existe une fonction rationnelle formellement symétrique Φ de K^n dans K telle que

$$\Phi(\alpha_1, \dots, \alpha_n) = \theta(\alpha_1, \dots, \alpha_n).$$

Preuve : Posons

$$\Phi := \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} \theta_\sigma;$$

alors Φ est une fonction rationnelle formellement symétrique de K^n dans K . Or, par hypothèse,

$$\forall \sigma \in \mathcal{S}_n, \theta_\sigma(\alpha_1, \dots, \alpha_n) = \theta(\alpha_1, \dots, \alpha_n),$$

$$\text{donc } \Phi(\alpha_1, \dots, \alpha_n) = \frac{1}{n!} (n! \theta(\alpha_1, \dots, \alpha_n)) = \theta(\alpha_1, \dots, \alpha_n). \quad \square$$

Exemple 8.38. Reprenons l'exemple 8.35.; on a $f(X) = X^3 + pX + q$ dans $\mathbb{C}[X]$ et $\theta(x_1, x_2, x_3) = x_1^2 - x_2x_3$.

Soit $\Sigma_i, 1 \leq i \leq 3$, les polynômes symétriques élémentaires des racines $\alpha_1, \alpha_2, \alpha_3$ de $f(X)$ dans $\mathbb{C}$, et $S_2 = \sum_{1 \leq i < j \leq 3} \alpha_i \alpha_j$. Avec les notations de la proposition 8.37., on obtient

$$\begin{aligned} \Phi(\alpha_1, \alpha_2, \alpha_3) &= \frac{1}{3!} \sum_{\sigma \in \mathcal{S}_3} \theta_\sigma(\alpha_1, \alpha_2, \alpha_3) = \frac{1}{3} (S_2 - \Sigma_2) = \frac{1}{3} (\Sigma_1^2 - 3\Sigma_2), \\ &= \frac{1}{3} (0 - 3p) = -p = \theta(\alpha_1, \alpha_2, \alpha_3). \end{aligned}$$

On retrouve évidemment le résultat obtenu dans l'exemple 8.35..

5. Résultant - Discriminant

A. Introduction

K étant un corps algébriquement clos (Déf. 4.42), on se propose de résoudre le problème suivant.

Problème : Trouver une condition nécessaire et suffisante pour que deux polynômes f et g , non constants et distincts dans $K[X]$, aient au moins une racine commune.

Remarque 8.39. Si f et g ont une racine commune $\alpha \in K$, alors $X - \alpha$ est un diviseur commun à f et g dans $K[X]$ (Cf. Ch. 4).

Par suite, f et g ont au moins une racine commune dans K , si et seulement si leur $p.g.c.d.$, dans l'anneau $K[X]$ (Ch. 5), est de degré strictement positif.

Proposition 8.40. K étant un corps algébriquement clos, pour que deux polynômes non constants f et g de $K[X]$, de degrés respectifs m et n , aient au moins une racine commune, il faut et il suffit qu'il existe des polynômes h et k , non nuls dans $K[X]$, tels que

$$\deg h \leq m-1, \quad \deg k \leq n-1 \quad \text{et} \quad hg = kf. \quad (8.32)$$

Preuve :

a) Supposons les conditions (8.1) vérifiées. Soit $\alpha_i, 1 \leq i \leq m$, les racines, distinctes ou confondues, de f dans K ; alors,

$$\forall i (1 \leq i \leq m), \quad (X - \alpha_i) \text{ divise } h(X)g(X);$$

$$\text{d'où : } (\deg h \leq m-1) \implies (\exists i (1 \leq i \leq m) \text{ tel que } (X - \alpha_i) \text{ divise } g(X)),$$

donc f et g ont au moins une racine commune.

b) Réciproquement, supposons que f et g aient une racine commune $\alpha \in K$; alors, si d est un $p.g.c.d.$ de f et g dans $K[X]$, on a nécessairement $\deg d \geq 1$ et il existe des polynômes non nuls h et k dans $K[X]$, vérifiant

$$f = dh, \quad g = dk \quad \text{et} \quad \deg h < \deg f, \quad \deg k < \deg g.$$

Dans l'anneau intègre $K[X]$,

$$fg = dhg = dkf \implies hg = kf.$$

Les conditions (8.1) sont donc satisfaites par les polynômes h et k . □

B. Résultant de deux polynômes

Les hypothèses et les notations étant celles de la proposition 8.40., posons

$$\begin{aligned} f(X) &= \sum_{0 \leq i \leq m} a_i X^i, & g(X) &= \sum_{0 \leq i \leq n} b_i X^i, \\ h(X) &= \sum_{0 \leq i \leq m-1} \lambda_i X^i, & k(X) &= \sum_{0 \leq i \leq n-1} \mu_i X^i. \end{aligned}$$

En supposant l'existence des polynômes h et k , l'identification des coefficients des puissances de X dans les deux membres de l'égalité $fk = gh$ donne les relations suivantes :

$$\begin{array}{rcl} a_m \mu_{n-1} & = & b_n \lambda_{m-1} \\ a_{m-1} \mu_{n-1} + a_m \mu_{n-2} & = & b_{n-1} \lambda_{m-1} + b_n \lambda_{m-2} \\ \vdots & & \vdots \\ a_0 \mu_1 + a_1 \mu_0 & = & b_0 \lambda_1 + b_1 \lambda_0 \\ a_0 \mu_0 & = & b_0 \lambda_0 \end{array}$$

On peut ramener l'ensemble des relations ci-dessus à un système de $n+m$ équations linéaires à coefficients dans le corps K , à $n+m$ inconnues, considérées dans l'ordre suivant :

$$\mu_{n-1}, \mu_{n-2}, \dots, \mu_0 \text{ et } -\lambda_{m-1}, -\lambda_{m-2}, \dots, -\lambda_0.$$

Le système obtenu, que nous appellerons (S) , est *homogène*.

Par suite il existe des polynômes h et k , non nuls dans $K[X]$, vérifiant (8.32), si et seulement si le système (S) a une solution *non nulle*, ce qui équivaut à la condition : $\det(S) = 0$.

Définition 8.41. Le déterminant du système (S) , considéré ci-dessus, est appelé le **résultant** (ou **déterminant de Sylvester**) des polynômes non nuls f et g donnés dans $K[X]$; on le note $R(f, g)$.

$$R(f, g) = \begin{vmatrix} a_m & 0 & 0 & \dots & 0 & b_n & 0 & 0 & \dots & 0 \\ a_{m-1} & a_m & 0 & \dots & 0 & b_{n-1} & b_n & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \vdots \\ a_1 & \ddots & \ddots & \ddots & a_m & b_1 & \ddots & \ddots & \ddots & b_n \\ a_0 & \ddots & \ddots & \ddots & a_{m-1} & b_0 & b_1 & \ddots & \ddots & b_{n-1} \\ 0 & \ddots & \ddots & \ddots & \vdots & 0 & b_0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 & a_1 & 0 & \ddots & \ddots & b_1 \\ 0 & \ddots & \ddots & \ddots & a_0 & 0 & 0 & \dots & 0 & b_0 \end{vmatrix}$$

La proposition 8.40. et la notion de résultant conduisent à l'énoncé suivant.

Théorème 8.42. K étant un corps algébriquement clos, deux polynômes non constants f et g de $K[X]$ ont au moins une racine commune si et seulement si leur résultant, $R(f, g)$, est nul.

Remarque 8.43. :

a) Le problème, considéré dans l'introduction de ce paragraphe et qui a conduit à la notion de résultant, peut être envisagé lorsque le corps K n'est pas algébriquement clos, à condition que les polynômes f et g soient scindés sur K (Déf. 4.46.); dans ce cas, le théorème 8.4. reste valable.

b) Un p.g.c.d. de f et g dans $K[X]$ étant noté $f \wedge g$, le résultat du Th. 8.42. équivaut à

$$f \wedge g = 1 \iff R(f, g) \neq 0.$$

c) L'expression du résultant $R(f, g)$ sous la forme du déterminant écrit précédemment montre que

$$R(g, f) = \pm R(f, g).$$

Exemple 8.44. On considère des polynômes dans $\mathbb{C}[X]$.

1) $f = a_1X + a_0$, $g = b_1X + b_0$, tels que $a_1b_1 \neq 0$.

$$R(f, g) = \begin{vmatrix} a_1 & b_1 \\ a_0 & b_0 \end{vmatrix} = a_1b_0 - b_1a_0,$$

donc $R(f, g) = 0 \iff \frac{a_0}{a_1} = \frac{b_0}{b_1}$ (résultat prévisible!).

2) $f = a_1X + a_0$, $g = b_2X^2 + b_1X + b_0$, avec $a_1b_2 \neq 0$.

$$R(f, g) = \begin{vmatrix} a_1 & 0 & b_2 \\ a_0 & a_1 & b_1 \\ 0 & a_0 & b_0 \end{vmatrix} = a_1^2b_0 + a_0^2b_2 - a_1a_0b_1.$$

d'où $R(f, g) = 0 \iff g(-\frac{a_0}{a_1}) = 0$.

3) $f = a_2X^2 + a_1X + a_0$, $g = b_2X^2 + b_1X + b_0$, avec $a_2b_2 \neq 0$.

$$R(f, g) = \begin{vmatrix} a_2 & 0 & b_2 & 0 \\ a_1 & a_2 & b_1 & b_2 \\ a_0 & a_1 & b_0 & b_1 \\ 0 & a_0 & 0 & b_0 \end{vmatrix} = (a_2b_0 - a_0b_2)^2 - (a_2b_1 - a_1b_2)(a_1b_0 - a_0b_1).$$

$$R(f, g) = 0 \iff (a_2b_0 - a_0b_2)^2 = (a_2b_1 - a_1b_2)(a_1b_0 - a_0b_1).$$

4) $f = X^4 + X^3 + X + a + 1$, $g = aX^3 + X + a$, dans $\mathbb{C}[X]$.

$$R(f, g) = \begin{vmatrix} 1 & 0 & 0 & a & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & a & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & a & 0 \\ 1 & 0 & 1 & a & 1 & 0 & a \\ a+1 & 0 & 0 & 0 & a & 1 & 0 \\ 0 & a+1 & 1 & 0 & 0 & a & 1 \\ 0 & 0 & a+1 & 0 & 0 & 0 & a \end{vmatrix}$$

$$R(f, g) = a^7 + 2a^4 + 3a^3 + a^2 + a + 1.$$

Les polynômes f et g ont une racine commune si et seulement si $R(f, g) = 0$, donc il existe au plus 7 valeurs distinctes du paramètre a dans $\mathbb{C}$, pour lesquelles f et g ont au moins une racine commune.

C. Calcul de $R(f, g)$ en fonction des racines de f et de g

L'expression du déterminant $R(f, g)$, écrit dans la Déf. 8.41., montre que le résultant de f et g peut être considéré comme un polynôme en les indéterminées $\{a_i\}_{0 \leq i \leq m}$ et $\{b_j\}_{0 \leq j \leq n}$ qui sont, respectivement, les coefficients des polynômes f et g . On en déduit, d'après les règles de calcul des déterminants, que $R(f, g)$ est alors, un polynôme

homogène et de degré n en $a_m, a_{m-1}, \dots, a_0$,

homogène et de degré m en $b_n, b_{n-1}, \dots, b_0$.

Dans l'algèbre de polynômes $K[a_m, a_{m-1}, \dots, a_0, b_n, b_{n-1}, \dots, b_0]$, posons

$$R(f, g) := p(a_m, a_{m-1}, \dots, a_0, b_n, b_{n-1}, \dots, b_0). \quad (8.33)$$

En écrivant dans le corps K , $\frac{a_i}{a_m}$ (resp. $\frac{b_j}{b_n}$) à la place de $a_m^{-1}a_i$, $0 \leq i \leq m$ (resp. $b_n^{-1}b_j$, $0 \leq j \leq n$), on obtient :

$$R(f, g) = a_m^n b_n^m p(1, \frac{a_{m-1}}{a_m}, \dots, \frac{a_0}{a_m}, 1, \frac{b_{n-1}}{b_n}, \dots, \frac{b_0}{b_n}). \quad (8.34)$$

Soit $\Sigma_1, \dots, \Sigma_m$ (resp. $\Sigma'_1, \dots, \Sigma'_n$) les fonctions symétriques élémentaires des racines de f , notées $\alpha_1, \dots, \alpha_m$ (resp. de g , notées $\beta_1, \dots, \beta_n$).

Les relations entre les coefficients et les racines d'un polynôme donnent

$$\begin{aligned}\Sigma_1 &= -\frac{a_{m-1}}{a_m}, \Sigma_2 = \frac{a_{m-2}}{a_m}, \dots, \Sigma_m = (-1)^m \frac{a_0}{a_m}; \\ \Sigma'_1 &= -\frac{b_{n-1}}{b_n}, \Sigma'_2 = \frac{b_{n-2}}{b_n}, \dots, \Sigma'_n = (-1)^n \frac{b_0}{b_n}.\end{aligned}$$

D'autre part, dans $K[X]$ on a

$$f(X) = a_m \prod_{1 \leq i \leq m} (X - \alpha_i), \quad g(X) = b_n \prod_{1 \leq j \leq n} (X - \beta_j). \quad (8.35)$$

Ecrivons $f(X) = a_m f_1(X)$ et $g(X) = b_n g_1(X)$, où

$$\begin{aligned}f_1(X) &= \prod_{1 \leq i \leq m} (X - \alpha_i) = X^m - \Sigma_1 X^{m-1} + \Sigma_2 X^{m-2} - \dots + (-1)^m \Sigma_m, \\ g_1(X) &= \prod_{1 \leq j \leq n} (X - \beta_j) = X^n - \Sigma'_1 X^{n-1} + \Sigma'_2 X^{n-2} - \dots + (-1)^n \Sigma'_n.\end{aligned}$$

La relation (8.34), appliquée aux polynômes f_1 et g_1 , s'écrit

$$R(f_1, g_1) = p(1, -\Sigma_1, \dots, (-1)^m \Sigma_m, 1, -\Sigma'_1, \dots, (-1)^n \Sigma'_n); \quad (8.36)$$

alors $R(f, g) = a_m^n b_n^m R(f_1, g_1)$ implique

$$R(f, g) = 0 \iff R(f_1, g_1) = 0.$$

$$\text{Or, } R(f_1, g_1) = 0 \iff \exists (i, j), 1 \leq i \leq m, 1 \leq j \leq n, \text{ tel que } \alpha_i = \beta_j,$$

$$\text{donc, } R(f_1, g_1) = 0 \implies (\alpha_i - \beta_j) \text{ divise } R(f_1, g_1) \text{ dans } K.$$

Mais la relation (8.36) montre que $R(f_1, g_1)$ est un polynôme symétrique en $\alpha_1, \dots, \alpha_m$, d'une part, et en $\beta_1, \dots, \beta_n$, d'autre part. On en déduit que, dans K , $R(f_1, g_1)$ est divisible par le produit $\prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j)$. En comparant les degrés en $\alpha_1, \dots, \alpha_m$ et en $\beta_1, \dots, \beta_n$, de $R(f_1, g_1)$ et du produit $\prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j)$, et en considérant le coefficient de $(\alpha_1 \alpha_2 \dots \alpha_m)^n$ dans $R(f_1, g_1)$ et dans $\prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j)$, on obtient

$$R(f_1, g_1) = \prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j).$$

Par suite,

$$R(f, g) = a_m^n b_n^m \prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j). \quad (8.37)$$

Théorème 8.45. *K étant un corps algébriquement clos, le résultant de deux polynômes f et g de $K[X]$, de degrés respectifs $m \geq 1$ et $n \geq 1$, tels que*

$$\begin{aligned}f &= \sum_{0 \leq i \leq m} a_i X^i = a_m (X - \alpha_1) \dots (X - \alpha_m), \\ g &= \sum_{0 \leq j \leq n} b_j X^j = b_n (X - \beta_1) \dots (X - \beta_n),\end{aligned}$$

peut s'exprimer comme suit :

$$R(f, g) = a_m^n \prod_{1 \leq i \leq m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{1 \leq j \leq n} f(\beta_j). \quad (8.38)$$

Ce résultat est une conséquence directe de la relation (8.37).

Remarque 8.46. :

a) Les relations (8.37) et (8.38) confirment le Théorème 8.42.

b) Le théorème 8.45. peut s'appliquer lorsque l'un (et un seul) des polynômes f ou g est constant, non nul. Supposons, par exemple,

$$f = a \neq 0 \text{ dans } K, \text{ donc } \deg f = m = 0 \text{ et } \deg g = n \geq 1.$$

La fonction polynôme $\tilde{a}$ étant l'application constante telle que $\tilde{a}(\alpha) = a$ pour tout $\alpha \in K$ (Cf. Ch.4), la seconde expression du résultant donnée dans la relation (8.38) implique

$$R(a, g) = a^n.$$

D. Discriminant d'un polynôme

K désigne toujours un corps algébriquement clos.

Remarque 8.47. Soit $f \in K[X]$ tel que $\deg f \geq 2$ et soit f' son polynôme dérivé. D'après la remarque 8.30., les polynômes f et f' ont une racine commune si et seulement si, dans l'anneau $K[X]$, leur *p.g.c.d.*, noté $f \wedge f'$, est de degré strictement positif, ce qui équivaut à dire que f et f' ne sont pas premiers entre eux, donc $f \wedge f' \neq 1$.

Proposition 8.48. K étant un corps algébriquement clos, soit $f \in K[X]$ tel que $\deg f \geq 2$; si f' est le polynôme dérivé de f , alors les conditions suivantes sont équivalentes :

- 1) Le polynôme f a au moins une racine multiple ;
- 2) $f \wedge f' \neq 1$;
- 3) Les polynômes f et f' ont au moins une racine commune.

Preuve :

1) $\iff$ 2) : Si f a une racine multiple $\alpha \in K$, alors $(X - \alpha)^2$ divise $f(X)$ dans $K[X]$; donc il existe un polynôme non nul $g(X) \in K[X]$ tel que

$$f(X) = (X - \alpha)^2 g(X),$$

$$\text{d'où } f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X).$$

Par suite $(X - \alpha)$ est un diviseur commun à f et f' , donc, dans l'anneau $K[X]$, f et f' ont un *p.g.c.d.* de degré strictement positif, d'où $f \wedge f' \neq 1$.

Réciproquement, supposons $f \wedge f' \neq 1$ et posons $d = f \wedge f'$. On a $\deg d \geq 1$, donc il existe $\alpha \in K$ tel que, dans $K[X]$, on ait

$$(X - \alpha) | d, \text{ d'où } (X - \alpha) | f \text{ et } (X - \alpha) | f'.$$

On en déduit l'existence de g non nul dans $K[X]$, tel que

$$f(X) = (X - \alpha)g(X) \text{ d'où } f' = g + (X - \alpha)g';$$

or par hypothèse, $(X - \alpha)$ divise f' ; par suite, $(X - \alpha)$ divise aussi g , d'où $(X - \alpha)^2 | f$.

Ainsi l'hypothèse $f \wedge f' \neq 1$ entraîne que f a au moins une racine multiple.

2) $\iff$ 3) est conséquence de la notion de *p.g.c.d.* dans $K[X]$ (Rem. 8.30.). □

La proposition 8.48., entraîne le résultat utile suivant :

Corollaire 8.49. Un polynôme non constant $f \in K[X]$ n'a que des racines simples si et seulement si $f \wedge f' = 1$.

Définition 8.50. Etant donné un polynôme non constant $f \in K[X]$, on appelle **discriminant** de f , le résultant de f et de son polynôme dérivé f' . On le notera $\Delta(f)$; donc

$$\Delta(f) = R(f, f').$$

Comme conséquence du Th. 8.42. et de la Prop. 8.48., on obtient :

Théorème 8.51. *K étant un corps algébriquement clos, si $f \in K[X]$ et $\deg f \geq 2$, alors le polynôme f a au moins une racine multiple si et seulement si $\Delta(f) = 0$.*

Exemple 8.52. dans $\mathbb{C}[X]$.

1) $f(X) = aX^2 + bX + c$, avec $a \neq 0$; $f'(X) = 2aX + b$, d'où

$$\Delta(f) = R(f, f') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = a(4ac - b^2).$$

La condition $a \neq 0$ implique

$$\Delta(f) = 0 \iff 4ac - b^2 = 0 \quad (\text{résultat connu !}).$$

2) $f(X) = X^3 + pX + q$ implique $f'(X) = 3X^2 + p$, d'où

$$\Delta(f) = R(f, f') = \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{vmatrix} = 4p^3 + 27q^2.$$

En supposant $\Delta(f) = 0$, désignons par α la racine multiple de f dans $\mathbb{C}$. On sait que α est une racine commune à f et f' (Prop. 8.48.). L'expression de $f'(X)$ nous donne

$$f'(\alpha) = 0 \iff \alpha^2 = -\frac{p}{3}.$$

Si $p \neq 0$, alors

$$4p^3 + 27q^2 = 0 \implies p = -\frac{27q^2}{4p^2};$$

par suite, $\alpha^2 = -\frac{p}{3} = \frac{9q^2}{4p^2}$. On vérifie que seul $\alpha = -\frac{3q}{2p}$ est racine du polynôme f et c'est une racine double de f .

Si $p = 0$, on a $f'(X) = 3X^2$ et

$$\Delta(f) = 0 \iff 27q^2 = 0 \iff q = 0.$$

Dans ce cas, $f(X) = X^3$ et 0 est racine triple de f .

Proposition 8.53. *Soit $f(X) = \sum_{0 \leq i \leq n} a_i X^i \in K[X]$, $n = \deg f \geq 1$, K étant un corps algébriquement clos (sinon, f est supposé scindé sur K). Si $\alpha_1, \dots, \alpha_n$ sont les racines de f dans K , alors*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \quad (8.39)$$

Preuve : Les hypothèses impliquent $f(X) = a_n \prod_{1 \leq i \leq n} (X - \alpha_i)$, d'où

$$f'(X) = a_n \sum_{1 \leq i \leq n} \left(\prod_{1 \leq j \leq n, j \neq i} (X - \alpha_j) \right) = \sum_{1 \leq i \leq n} \frac{f(X)}{X - \alpha_i}.$$

On calcule alors $\Delta(f)$ à partir de la relation (8.38) :

$$\Delta(f) = R(f, f') = a_n^{n-1} \prod_{1 \leq i \leq n} f'(\alpha_i) \text{ et } f'(\alpha_i) = a_n \left(\prod_{1 \leq j \leq n, j \neq i} (\alpha_i - \alpha_j) \right);$$

$$\Delta(f) = a_n^{2n-1} \prod_{1 \leq i \leq n} (\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_n)$$

$$= a_n^{2n-1} \prod_{1 \leq i \leq n} (-1)^{i-1} (\alpha_1 - \alpha_i) \dots (\alpha_{i-1} - \alpha_i)(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_n);$$

$$\Delta(f) = a_n^{2n-1} (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2, \text{ d'où la relation (8.39).}$$

□

Remarque 8.54. La relation (8.39) justifie l'appellation de *discriminant* de f donné à $\Delta(f)$, la notion de *discriminant* des X_i , $1 \leq i \leq n$, ayant été définie (Exemple 8.12.) par

$$D = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

6. Applications

A. Problème général d'élimination

Il s'agit d'une généralisation du problème qui a conduit à la notion de résultant.

Etant donné un corps K de caractéristique 0, algébriquement clos (en général, $K = \mathbb{C}$), et des fractions rationnelles (donc éventuellement des polynômes) $q_1, q_2, \dots, q_r$, $r \geq 1$, dans $K(X_1, \dots, X_n)$, $n \geq 1$, le problème consiste à *trouver une condition nécessaire et suffisante (portant sur les coefficients des q_k , $1 \leq k \leq r$) pour qu'il existe au moins un élément $(\alpha_1, \dots, \alpha_n)$ dans K^n tel que*

$$\forall k (1 \leq k \leq r), q_k(\alpha_1, \dots, \alpha_n) = 0.$$

Définition 8.55. Résoudre le problème précédent, c'est **éliminer** $\alpha_1, \dots, \alpha_n$ entre les r relations

$$q_k(\alpha_1, \dots, \alpha_n) = 0.$$

Lorsque la condition trouvée est réalisée, on peut chercher à déterminer les solutions communes $(\alpha_1, \dots, \alpha_n)$ aux r équations $q_k(X_1, \dots, X_n) = 0$.

Exemple classique : Etant donné un polynôme $f \in K[X]$, de degré $n \geq 1$, trouver une condition nécessaire et suffisante pour que les racines, $\alpha_1, \dots, \alpha_n$ (distinctes ou confondues) de f dans K , vérifient r relations données :

$$q_k(\alpha_1, \dots, \alpha_n) = 0, \quad 1 \leq k \leq r,$$

où les q_k sont dans $K(X_1, \dots, X_n)$.

Signalons que dans le cas d'un tel problème, en général on ne connaît pas explicitement les racines du polynôme $f = \sum_{0 \leq i \leq n} a_i X^i$, de degré $n \geq 1$; on est alors amené à éliminer les $\alpha_1, \dots, \alpha_n$ entre les $n + r$ relations :

$$\Sigma_i(\alpha_1, \dots, \alpha_n) = (-1)^i \frac{a_{n-i}}{a_n}, \quad 1 \leq i \leq n,$$

$$q_k(\alpha_1, \dots, \alpha_n) = 0, \quad 1 \leq k \leq r.$$

Exemple 8.56. Soit $f(X) = X^3 + aX^2 + bX + c$ dans $\mathbb{C}[X]$ où l'on suppose $abc \neq 0$.

Trouver une condition nécessaire et suffisante pour que a, b, c soient les racines du polynôme f .

D'après les *Relations entre les coefficients et les racines* d'un polynôme et la remarque 8.24. les nombres complexes a, b, c sont racines de f si et seulement si les égalités suivantes sont satisfaites :

$$\Sigma_1 = a + b + c = -a \quad (8.40)$$

$$\Sigma_2 = ab + ac + bc = b \quad (8.41)$$

$$\Sigma_3 = abc = -c. \quad (8.42)$$

La condition nécessaire et suffisante recherchée résulte donc de l'élimination de a, b, c entre les trois relations ci-dessus.

$$(8.1) \implies b + c = -2a, \text{ d'où,}$$

$$(8.2) \implies bc = b - a(b + c) = b + 2a^2.$$

$$(8.3) \implies ab = -1, \text{ car on a supposé } abc \neq 0.$$

$$bc = b + 2a^2 \implies abc = -c = ab + 2a^3 = -1 + 2a^3,$$

$$\text{d'où } \underline{c = 1 - 2a^3} \text{ et } b + c = -2a \implies \underline{b = 2a^3 - 2a - 1}.$$

$$\text{Par suite, } ab = -1 \implies \underline{2a^4 - 2a^2 - a + 1 = 0}.$$

Ainsi a, b, c sont les racines du polynôme f si et seulement si a est racine, dans $\mathbb{C}$, du polynôme

$$g(X) = 2X^4 - 2X^2 - X + 1 = (X - 1)(2X^3 + 2X^2 - 1)$$

et pour chaque racine a de g dans $\mathbb{C}$, b et c sont déterminés en fonction de a , par les égalités trouvées plus haut.

En particulier, pour $a = 1$, on a $b = c = -1$ et

$$f(X) = X^3 + X^2 - X - 1 = (X + 1)^2(X - 1).$$

Le polynôme g ayant 4 racines distinctes dans $\mathbb{C}$ (car $g \wedge g' = 1$), le problème proposé admet 4 solutions $(a, b, c) \in \mathbb{C}^3$.

B. Transformation des équations polynômiales

1. Notion d'équation transformée



Soit $f(X)$ un polynôme de $K[X]$, de degré $n \geq 1$, où K est un corps de caractéristique 0 et algébriquement clos (sinon, on suppose f scindé sur K), les solutions de l'équation polynômiale $f(X) = 0$ sont les racines $\alpha_1, \dots, \alpha_n$ (distinctes ou confondues) de f dans K .

Etant donné une fraction rationnelle $F(X) = \frac{p(X)}{q(X)}$ dans $K(X) \setminus K$ n'admettant aucun des $\alpha_i, 1 \leq i \leq n$, pour pôle ($\forall i (1 \leq i \leq n), q(\alpha_i) \neq 0$), posons, dans $K[X]$,

$$g(X) := \prod_{1 \leq i \leq n} (X - F(\alpha_i)). \quad (8.43)$$

Définition 8.57. Compte tenu des hypothèses et des notations ci-dessus, l'équation polynômiale $g(X) = 0$ est appelée **équation transformée par F** , de l'équation $f(X) = 0$.

L'équation $g(X) = 0$ est de même degré que l'équation initiale $f(X) = 0$ et ses solutions sont les $F(\alpha_i), 1 \leq i \leq n$.

Remarque 8.58. :

a) Quel que soit λ non nul dans K , l'équation $\lambda g(X) = 0$ est aussi une équation transformée de $f(X) = 0$, par F .

b) Si α_i est une racine de f , d'ordre k_i , alors $F(\alpha_i)$ est une racine de g , d'ordre au moins égal à k_i .

2. Détermination d'une équation transformée

On conserve les mêmes notations que plus haut.

a) Utilisation des polynômes symétriques des racines de f

En posant $\lambda_{n-k} := \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} F(\alpha_{i_1})F(\alpha_{i_2}) \dots F(\alpha_{i_k})$, on a

$$g(X) = X^n - \lambda_{n-1}X^{n-1} + \dots + (-1)^k \lambda_{n-k}X^{n-k} + \dots + (-1)^n \lambda_0. \quad (8.44)$$

Les λ_i , $1 \leq i \leq n$, sont des polynômes symétriques des racines α_i de f , donc les coefficients du polynôme g s'expriment en fonction des coefficients de f .

Exemple 8.59. $f(X) = X^3 + aX^2 + bX + c$ dans $\mathbb{C}[X]$ et $F(X) = X^2$.

En notant α_i , $1 \leq i \leq 3$, les racines de f dans $\mathbb{C}$, l'équation transformée par F de $f(X) = 0$ est $g(X) = 0$, dont les solutions sont les α_i^2 ; on dit que $g(X) = 0$ est l'équation aux carrés des racines de f .

Comme dans la relation (8.44), on écrit

$$g(X) = X^3 - \lambda_2 X^2 + \lambda_1 X - \lambda_0.$$

Calculons les λ_i en fonction des coefficients de f , en notant Σ_i , $1 \leq i \leq 3$, les polynômes symétriques élémentaires des α_i , et pour tout entier $k \neq 0$, S_k les sommes des puissances $k^{\text{èmes}}$ des α_i , $i = 1, 2, 3$.

$$\lambda_2 = \sum_{1 \leq i \leq 3} \alpha_i^2 = S_2 = \Sigma_1^2 - 2\Sigma_2 = a^2 - 2b.$$

$$\lambda_1 = \sum_{1 \leq i < j \leq 3} \alpha_i^2 \alpha_j^2 = \frac{1}{2}(S_2^2 - S_4).$$

$$S_4 = S_3 \Sigma_1 - S_2 \Sigma_2 + S_1 \Sigma_3 \quad (\text{Formule de Newton})$$

$$= (a^2 - 2b)^2 - 2b^2 + 4ac, \quad \text{d'où}$$

$$\lambda_1 = \frac{1}{2}[(a^2 - 2b)^2 - (a^2 - 2b)^2 + 2b^2 - 4ac] = b^2 - 2ac.$$

$$\lambda_0 = (\alpha_1 \alpha_2 \alpha_3)^2 = \Sigma_3^2 = c^2, \quad \text{d'où}$$

$$g(X) = X^3 - (a^2 - 2b)X^2 + (b^2 - 2ac)X - c^2.$$

b) Utilisation de la notion de résultant

Proposition 8.60. Avec les mêmes hypothèses générales que précédemment, l'équation

transformée de $f(X) = 0$ par $F(X) = \frac{p(X)}{q(X)}$, où $p \wedge q = 1$ dans $K[X]$, s'écrit

$$g(Y) = 0,$$

$g(Y)$ étant, à un scalaire multiplicatif, non nul, près, le résultant de $f(X)$ et $Yq(X) - p(X)$, considérés comme des polynômes de $K(Y)[X]$.

Preuve : On sait que le résultant de $f(X)$ et $Yq(X) - p(X)$ est un polynôme symétrique en les coefficients de ces polynômes, c'est donc un élément de $K[Y]$.

Posons $f(X) = \sum_{0 \leq i \leq n} a_i X^i$, $\deg f = n \geq 1$; en notant $\alpha_1, \dots, \alpha_n$ les racines de f dans K , on a (Th. 8.45.)

$$R(f(X), Yq(X) - p(X)) = a_n^d \prod_{1 \leq i \leq n} (Yq(\alpha_i) - p(\alpha_i)),$$

où d désigne le degré du polynôme $Yq(X) - p(X)$ dans $K(Y)[X]$.

On en déduit que

$$R(f(X), Yq(X) - p(X)) = \mu \prod_{1 \leq i \leq n} (Y - \frac{p(\alpha_i)}{q(\alpha_i)}),$$

où $\mu = a_n^d \prod_{1 \leq i \leq n} q(\alpha_i)$ est non nul dans K , donc

$$g(Y) = \mu^{-1} R(f(X), Yq(X) - p(X))$$

et $g(Y) = 0 \iff R(f(X), Yq(X) - p(X)) = 0$. □

Remarque 8.61. Le résultat ci-dessus fournit un moyen simple pour obtenir une équation polynômiale transformée.

3. Exemples classiques de transformations

Dans $\mathbb{C}[X]$, soit $f(X) = \sum_{0 \leq i \leq n} a_i X^i$, tel que $\deg f = n \geq 1$.

1) Transformation par translation : $F(X) = X + a$, où $a \in \mathbb{C}^*$.

A un coefficient multiplicatif près, le résultant de $f(X)$ et $Y - (X + a)$, dans $\mathbb{C}[Y]$, est $f(Y - a)$; d'où l'équation transformée de $f(X) = 0$, par F :

$$g(Y) = f(Y - a) = 0.$$

Par exemple, en prenant $a = \frac{a_{n-1}}{na_n}$, on obtient $g(Y) = f(Y - \frac{a_{n-1}}{na_n})$, dont la somme des racines est

$$\Sigma'_1 = \Sigma_1 - \frac{a_{n-1}}{a_n} = 0.$$

Ce procédé permet, en particulier, de ramener toute équation du type

$$f(X) = aX^3 + bX^2 + cX + d = 0,$$

à l'équation transformée, dite *canonique*, de la forme

$$g(Y) = Y^3 + pY + q = 0,$$

obtenue en prenant $F(X) = X + \frac{b}{3a}$.

2) Transformation par homothétie : $F(X) = \lambda X$, où $\lambda \in \mathbb{C}^*$.

L'équation transformée est dans ce cas,

$$g(Y) = f\left(\frac{Y}{\lambda}\right) = 0.$$

Pour $\lambda = -1$, on obtient l'équation aux opposés des racines de f .

3) Equation aux inverses des racines de f : $F(X) = \frac{1}{X}$.

On suppose $f(0) \neq 0$. Le résultant des polynômes $f(X)$ et $YX - 1 = Y(X - \frac{1}{Y})$, dans $\mathbb{C}(Y)$, est égal au signe près (Th. 8.45.), à $Y^n f(\frac{1}{Y})$, d'où l'équation transformée

$$g(Y) = a_0 Y^n + a_1 Y^{n-1} + \dots + a_{n-1} Y + a_n = 0. \quad (8.45)$$

4) Transformation par homographie : $F(X) = \frac{aX + b}{cX + d}$, avec $c \neq 0$, $ad - bc \neq 0$, et

$$f\left(-\frac{d}{c}\right) \neq 0.$$

Cette transformation généralise celle du cas précédent, qui correspond à $a = 0$, $b = 1$, $c = 1$, $d = 0$.

Dans le cas général, l'unique racine du polynôme $Y(cX + d) - (aX + b)$, dans $\mathbb{C}(Y)$, est $\frac{b - dY}{cY - a}$; on en déduit (Th. 8.45.) que le résultant de $f(X)$ et $Y(cX + d) - (aX + b)$ est, au signe près,

$$(cY - a)^n f\left(\frac{b - dY}{cY - a}\right),$$

d'où l'équation transformée

$$g(Y) = a_n(b - dY)^n + a_{n-1}(b - dY)^{n-1}(cY - a) + \dots + a_0(cY - a)^n = 0.$$

La transformation homographique est bijective, par suite l'ordre de multiplicité de toute racine de f est conservé ; c'est-à-dire que si α_i , $1 \leq i \leq n$, est une racine de f , d'ordre k_i ,

alors $\frac{\alpha_i + b}{c\alpha_i + d}$ est une racine de $g(Y)$, de même ordre k_i .

5) Equation aux carrés des racines de f : $F(X) = X^2$.

Déterminons le résultant de $f(X)$ et $X^2 - Y$, considérés comme polynômes de $\mathbb{C}(Y)[X]$.

On admettra ici, qu'il existe nécessairement un corps K tel que

$$\mathbb{C} \subset \mathbb{C}(Y) \subseteq K,$$

dans lequel le polynôme $X^2 - Y$ a deux racines opposées, que l'on notera z et $-z$ (Voir Vol. 2, Extensions de Corps). Dans $K[X]$, on a

$$X^2 - Y = (X - z)(X + z) \text{ donc, dans } K, Y = z^2.$$

Par suite, dans K , le résultant des polynômes $f(X)$ et $X^2 - Y$ est égal, au signe près (Th. 8.45.), à $f(z)f(-z)$.

D'autre part, il existe des polynômes h et k dans $\mathbb{C}[X] \subset K[X]$ tels que

$$\begin{aligned} f(X) &= \sum_{0 \leq i \leq n} a_i X^i = h(X^2) + Xk(X^2), \quad \text{d'où} \\ f(z)f(-z) &= (h(z^2) - zk(z^2))(h(z^2) + zk(z^2)) \\ &= (h(z^2))^2 - z^2(k(z^2))^2. \end{aligned}$$

On en conclut que l'équation aux carrés des racines de f est

$$g(Y) = (h(Y))^2 - Y(k(Y))^2 = 0. \quad (8.46)$$

Reprenons l'exemple 8.59., pour lequel $f(X) = X^3 + aX^2 + bX + c$; alors,

$$f(X) = aX^2 + c + X(X^2 + b).$$

En appliquant la formule (8.6), on obtient

$$\begin{aligned} g(Y) &= (aY + c)^2 - Y(Y + b)^2 = 0 \\ &= -Y(Y^2 + 2bY + b^2) + (a^2Y^2 + 2acY + c^2) = 0 \\ &= -(Y^3 - (a^2 - 2b)Y^2 + (b^2 - 2ac)Y - c^2) = 0. \end{aligned}$$

On retrouve ainsi le résultat de l'exemple 8.59., par une méthode plus rapide.

7. Exercices

1) 1°) Dans $\mathbb{C}[X_1, X_2, X_3]$, calculer

$$\begin{aligned} A &= X_1^2 X_2 + X_1 X_2^2 + X_1^2 X_3 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2, \\ B &= (2X_1 - X_2 - X_3)(2X_2 - X_3 - X_1)(2X_3 - X_1 - X_2), \end{aligned}$$

en fonction des polynômes symétriques élémentaires Σ_i , $1 \leq i \leq 3$.

2°) Dans $\mathbb{C}[X_1, \dots, X_4]$, calculer

$$P = (X_1 X_2 + X_3 X_4)(X_1 X_3 + X_2 X_4)(X_1 X_4 + X_2 X_3)$$

en fonction des Σ_i , $1 \leq i \leq 4$.

- 2) Dans $\mathbb{C}(X_1, \dots, X_n)$, $n > 1$, on considère

$$F := \sum_{i \neq j} \frac{X_i}{X_j^2}, \quad 1 \leq i \leq n, \quad 1 \leq j \leq n.$$

Les polynômes symétriques élémentaires et les sommes de Newton des X_i sont respectivement notés Σ_j , pour $1 \leq j \leq n$ et S_k , pour tout $k \in \mathbb{Z}$.

Vérifier que F peut s'exprimer en fonction de Σ_1, S_{-1}, S_{-2} . En déduire, dans le cas $n = 3$, l'expression de F en fonction des Σ_j , $1 \leq j \leq 3$.

- 3) Soit $f(X) = X^4 + X^2 + \lambda X + 2$ dans $\mathbb{C}[X]$.

On note α_i , $1 \leq i \leq 4$, les racines (distinctes ou confondues) de f dans $\mathbb{C}$.

Déterminer λ dans $\mathbb{C}$ pour que $\alpha_1 \alpha_2 = 1$.

Calculer alors les quatre racines α_i de f .

- 4) Dans $\mathbb{C}[X]$, on considère les polynômes

$$f(X) = X^3 + 2aX^2 + (a^2 + 1)X + 1 \text{ et } g(X) = X^2 + aX + 1.$$

Déterminer a dans $\mathbb{C}$, pour que f et g aient au moins une racine commune.

Répondre à la question par les deux méthodes suivantes :

a) en calculant le p.g.c.d. de f et g dans $\mathbb{C}[X]$;

b) en calculant le résultant $R(f, g)$ dans $\mathbb{C}$.

Pour a répondant à la question, préciser les racines de f et de g .

- 5) Soit $f(X) = X^n - 1$, $n > 1$, dans $\mathbb{C}[X]$.

On rappelle que les racines de f , dans $\mathbb{C}$, sont les $z_k = \exp \frac{2k\pi i}{n}$, $1 \leq k \leq n$.

1°) Pour tout $p \in \mathbb{N}$, soit $S_p = \sum_{1 \leq k \leq n} z_k^p$. Prouver que

$$S_p = n \iff p \equiv 0 \pmod{n};$$

$$S_p = 0 \iff p \not\equiv 0 \pmod{n}.$$

2°) Montrer que, quels que soient les nombres complexes α et β , on a

$$\prod_{1 \leq k \leq n} (\alpha + \beta z_k) = \alpha^n + (-1)^{n-1} \beta^n.$$

3°) Prouver que pour tout $\theta \in \mathbb{R}$, on a

$$\prod_{1 \leq k \leq n} (z_k^2 - 2z_k \cos \theta + 1) = 2(1 - \cos n\theta).$$

- 6) Etant donné un entier $n > 1$, on considère dans $\mathbb{C}$, les éléments

$$z_k = \exp \frac{2k\pi i}{n}, \quad 1 \leq k \leq n.$$

1°) Quel est le polynôme $f(X)$ de $\mathbb{C}[X]$, dont les racines sont les

$$z_k = \exp \frac{2k\pi i}{n}, \quad 1 \leq k \leq n-1?$$

2°) Déterminer l'équation polynomiale $g(Y) = 0$, ayant pour racines les

$$y_k = \frac{1}{1 - z_k}, \quad 1 \leq k \leq n-1.$$

En déduire $P := \prod_{1 \leq k \leq n-1} \frac{1}{1 - z_k}$.

- 7) Soit $f(X) = X^3 + pX + q$ dans $\mathbb{C}[X]$.

On note α_i , $1 \leq i \leq 3$, les racines (distinctes ou confondues) de f dans $\mathbb{C}$.

Etant donné $j \in \mathbb{C}$ tel que $j^3 = 1$ et $j \neq 1$, on pose

$$\theta(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1 + j\alpha_2 + j^2\alpha_3)^3.$$

1°) Calculer, en fonction de p et q , les sommes de Newton S_2 et S_3 des α_i , $1 \leq i \leq 3$, ainsi que

$$m := \sum_{(i,k)} \alpha_i^2 \alpha_k, \quad i \neq k \text{ dans } \{1, 2, 3\}.$$

2°) Soit S_3 le groupe des permutations de $\{1, 2, 3\}$. Pour tout $\sigma \in S_3$, on pose

$$\theta_\sigma(\alpha_1, \alpha_2, \alpha_3) = \theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \alpha_{\sigma(3)}).$$

a) Prouver que lorsque σ décrit S_3 , $\theta_\sigma(\alpha_1, \alpha_2, \alpha_3)$ ne prend au plus que deux valeurs dans $\mathbb{C}$, que l'on notera θ_1 et θ_2 ; si on pose $\theta_1 = \theta(\alpha_1, \alpha_2, \alpha_3)$, préciser l'expression de θ_2 en fonction des α_i , $1 \leq i \leq 3$.

b) Déterminer le polynôme du second degré de $\mathbb{C}[X]$, dont les racines sont θ_1 et θ_2 . Calculer θ_1 et θ_2 en fonction de p et q .

c) Pour $k = 1, 2$, on note λ_k une racine cubique de θ_k . Vérifier que, quel que soit le choix de la racine cubique λ_k , $k = 1, 2$, le triplet $(\alpha_1, \alpha_2, \alpha_3)$ est solution du système

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1 + j\alpha_2 + j^2\alpha_3 = \lambda_1 \\ \alpha_1 + j^2\alpha_2 + j\alpha_3 = \lambda_2 \end{cases}$$

Calculer les α_i en fonction de p et q .

3°) On suppose $f(X) = X^3 + pX + q$ dans $\mathbb{R}[X]$. On pose $\Delta := 4p^3 + 27q^2$.

Vérifier les propriétés suivantes :

a) Si $\Delta = 0$, alors f a au moins une racine multiple et dans tous les cas ($p \neq 0$ ou $p = 0$), les racines de f sont réelles; les calculer.

b) Si $\Delta > 0$, f a une seule racine réelle; que peut-on dire des deux autres racines?

c) Si $\Delta < 0$, f a trois racines réelles distinctes.

8) Dans cet exercice, on utilise la notion de déterminant de Vandermonde (Voir un cours d'Algèbre Linéaire).

Soit $f(X) \in \mathbb{C}[X]$, un polynôme unitaire, de degré $n \geq 1$, tel que

$$f(X) = \sum_{0 \leq i \leq n} a_i X^i = \prod_{1 \leq i \leq n} (X - \alpha_i),$$

les α_i étant les racines (distinctes ou confondues) de f dans $\mathbb{C}$.

Soit $V(\alpha_1, \alpha_2, \dots, \alpha_n)$ le déterminant de Vandermonde des α_i ; on rappelle que

$$V(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j).$$

On désigne par M la matrice carrée dont le déterminant est $V(\alpha_1, \alpha_2, \dots, \alpha_n)$ et on note tM la matrice transposée de M .

1°) Calculer $\det(M^t M)$; en déduire que

$$\begin{vmatrix} n & S_1 & \dots & S_{n-1} \\ S_1 & S_2 & \dots & S_n \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-1} & S_n & \dots & S_{2n-2} \end{vmatrix} = D(\alpha_1, \alpha_2, \dots, \alpha_n),$$

où, pour tout entier $k \geq 1$, $S_k = \sum_{1 \leq i \leq n} \alpha_i^k$ et $D(\alpha_1, \alpha_2, \dots, \alpha_n)$ est le discriminant des α_i (Cf. Exemple 8.12.).

2°) a) Calculer $D(\alpha_1, \alpha_2, \dots, \alpha_n)$ en fonction des S_i , pour $n = 2$ et $n = 3$.

b) Pour $n = 2$ et $f(X) = X^2 - a_1X + a_2$, exprimer $D(\alpha_1, \alpha_2)$ en fonction de a_1 et a_2 .

c) Pour $n = 3$ et $f(X) = X^3 - a_1X^2 + a_2X - a_3$, exprimer $D(\alpha_1, \alpha_2, \alpha_3)$ en fonction de a_1, a_2, a_3 .

9) Soit $f(X) = X^3 - a_1X^2 + a_2X - a_3$ dans $\mathbb{R}[X]$.

1°) a) Justifier l'affirmation suivante : le polynôme f a trois racines (distinctes ou confondues) dans $\mathbb{C}$.

b) Vérifier que si $\alpha \in \mathbb{C}$ est une racine de f , alors $\bar{\alpha}$ (l'imaginaire conjugué de α) est aussi une racine f . En déduire que f a au moins une racine réelle.

2°) On pose (Cf. Ex. 8 précédent)

$$D := -4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^2 - 27a_3^2.$$

a) Vérifier que f a une racine multiple si et seulement si $D = 0$ et montrer que dans ce cas, les racines de f sont toutes réelles.

b) On suppose $D \neq 0$. Prouver que f a alors, trois racines réelles distinctes ou une seule racine réelle, suivant que l'on a $D > 0$ ou $D < 0$.

10) K désigne un corps algébriquement clos de caractéristique 0. Soit f et g dans $K[X]$ tels que $\deg f = m \geq 1$, $\deg g = n \geq 1$.

1°) Prouver que f et g ont au moins une racine commune si et seulement si, dans l'espace vectoriel $K[X]$, les $m+n$ vecteurs

$$X^{n-1}f, X^{n-2}f, \dots, Xf, f, X^{m-1}g, X^{m-2}g, \dots, Xg, g$$

forment une famille liée.

2°) On pose $f = \sum_{1 \leq i \leq m} a_i X^i$, $g = \sum_{1 \leq i \leq n} b_i X^i$.

Le résultant $R(f, g)$ est alors le déterminant d'ordre $m+n$ sur K , décrit dans la définition 8.41.

On désigne par $L_1, L_2, \dots, L_{m+n-1}, L_{m+n}$ les vecteurs-lignes du déterminant $R(f, g)$ et on écrit symboliquement



$$R(f, g) = \begin{vmatrix} L_1 \\ L_2 \\ \vdots \\ L_{m+n-1} \\ L_{m+n} \end{vmatrix}$$

En tenant compte des inclusions $K \subset K[X] \subset K(X)$, on peut considérer que $R(f, g)$ est un déterminant à coefficients dans le corps $K(X)$.

Remplaçons alors, dans le déterminant $R(f, g)$, le vecteur-ligne L_{m+n} par le vecteur-ligne

$$L := \sum_{1 \leq i \leq m+n} X^{m+n-i} L_i,$$

les vecteurs-lignes L_i , $1 \leq i \leq m+n-1$, restant inchangés.

a) Vérifier que

$$R(f, g) = \begin{vmatrix} L_1 \\ L_2 \\ \vdots \\ L_{m+n-1} \\ L \end{vmatrix}$$

b) Montrer que le vecteur-ligne L s'identifie au vecteur

$$(X^{n-1}f, X^{n-2}f, \dots, Xf, f, X^{m-1}g, X^{m-2}g, \dots, Xg, g).$$

de l'espace-vectoriel $(K(X))^{m+n}$.

En développant le déterminant $R(f, g)$ suivant la ligne L , prouver qu'il existe des polynômes u et v , dans $K[X]$, tels que

$$R(f, g) = u(X)f(X) + v(X)g(X).$$

Vérifier que si $R(f, g) \neq 0$, alors les polynômes u et v sont uniques.

11) Soit K un corps algébriquement clos de caractéristique 0; $K^* := K \setminus \{0\}$.

1°) Soit f et g , dans $K[X]$, tels que $\deg f = m \geq 0$, $\deg g = n \geq 0$, m et n n'étant pas simultanément nuls (Rem. 8.46.).

Dans le cas où $mn \neq 0$, on pose

$$f(X) = a \prod_{1 \leq i \leq m} (X - \alpha_i), \quad g(X) = b \prod_{1 \leq j \leq n} (X - \beta_j).$$

On note $R(f, g)$ le résultant de f et g .

a) On suppose $\deg g = n \neq 0$; calculer

$$R(a, g), \text{ où } a \in K^* \text{ et } R((X - \alpha), g), \text{ où } \alpha \in K.$$

b) Prouver que $R(g, f) = (-1)^{mn} R(f, g)$.

c) Soit h un polynôme non constant de $K[X]$; démontrer que, dans le cas où $mn \neq 0$, on a

$$R(fg, h) = R(f, h) R(g, h).$$

Prouver que si $\deg g = n \neq 0$ et $\lambda \in K^*$, alors

$$R(\lambda g, h) = R(\lambda, h) R(g, h).$$

2°) Soit p un polynôme unitaire de $K[X]$, de degré $d \geq 1$.

Pour tout polynôme $q \in K[X]$, on note $\bar{q}$ la classe de q modulo (p) , où (p) désigne l'idéal de $K[X]$ engendré par p .

a) Vérifier que $\frac{K[X]}{(p)}$ est un K -espace vectoriel dont on précisera la dimension.

b) A tout polynôme $u \in K[X]$, on associe la correspondance

$$\theta_u: \frac{K[X]}{(p)} \rightarrow \frac{K[X]}{(p)}, \quad \bar{q} \mapsto \overline{uq}.$$

Montrer que pour tout $u \in K[X]$, θ_u est une application (préciser θ_u , lorsque $u \in (p)$) et que θ_u est un endomorphisme du K -espace vectoriel $\frac{K[X]}{(p)}$.

c) Prouver que, quels que soient les polynômes u et v dans $K[X]$, on a

3°) On reprend les hypothèses et les notations du 1°), en supposant le polynôme g non constant et unitaire. On associe alors, à tout polynôme $u \in K[X]$, l'endomorphisme θ_u de $\frac{K[X]}{(g)}$, défini comme dans le 2°).

a) Démontrer que

$$\forall a \in K^*, R(a, g) = \det \theta_a;$$

$$\text{et } \forall \alpha \in K, R((X - \alpha), g) = \det \theta_{X - \alpha}.$$

b) Prouver que, pour tout couple de polynômes (f, g) satisfaisant aux hypothèses du 1°), où l'on suppose g non constant et unitaire, on a

$$R(f, g) = \det \theta_f.$$

12) Soit $f(X)$, dans $\mathbb{C}[X]$ tel que $\deg f = n \geq 1$ et $f(0) \neq 0$. On pose

$$f(X) = \sum_{1 \leq i \leq n} a_i X^i, \text{ avec } a_n \neq 0 \text{ et } a_0 \neq 0.$$

Soit $g(X) = 0$, l'équation aux inverses des racines de f (Cf. rel. 8.45). On dira que $f(X) = 0$ est une équation réciproque, s'il existe λ , non nul dans $\mathbb{C}$, tel que

$$f(X) = \lambda g(X).$$

1°) Montrer que l'équation $f(X) = 0$ est réciproque si et seulement si $\lambda = \pm 1$. On dit alors que $f(X) = 0$ est une équation réciproque

de *première espèce*, si $\lambda = 1$, de *seconde espèce*, si $\lambda = -1$.

2°) Etant donné une équation réciproque, $f(X) = 0$, de degré $n > 1$, vérifier les propriétés suivantes.

a) Si $f(X) = 0$ est de *seconde espèce*, alors, quelle que soit la parité de n , on a $f(1) = 0$ et si $f(X) = (X-1)q(X)$, alors $q(X) = 0$ est une équation réciproque de *première espèce*.

b) Si $f(X) = 0$ est de *première espèce* et si n est *impair*, alors on a $f(-1) = 0$ et l'égalité $f(X) = (X+1)q(X)$ implique que l'équation $q(X) = 0$ est réciproque de *première espèce* et de degré *pair*.

En conclure que la résolution de toute équation réciproque peut être ramenée à celle d'une équation réciproque de *première espèce* et de degré *pair*, n'ayant ni 1, ni -1 comme racines.

3°) On considère une équation réciproque $f(X) = 0$ n'ayant ni 1, ni -1 comme racines, de *première espèce*, et de degré $n = 2m \geq 2$.

a) Vérifier que, dans $\mathbb{C}[X]$, $f(X)$ s'écrit sous la forme

$$f(X) = a_{2m}X^{2m} + a_{2m-1}X^{2m-1} + \dots + a_{m+1}X^{m+1} \\ + a_mX^m + a_{m+1}X^{m-1} + \dots + a_{2m-1}X + a_{2m},$$

avec $a_{2m} \neq 0$.

b) On pose

$$\varphi(X) := a_{2m}\left(X^m + \frac{1}{X^m}\right) + a_{2m-1}\left(X^{m-1} + \frac{1}{X^{m-1}}\right) + \dots \\ + a_{m+1}\left(X + \frac{1}{X}\right) + a_m.$$

Montrer que pour $\alpha \in \mathbb{C}^*$, on a $f(\alpha) = 0 \iff \varphi(\alpha) = 0$.

c) On pose $Y := X + \frac{1}{X}$ et pour tout entier $k > 1$, $P_k := X^k + \frac{1}{X^k}$.

Vérifier que pour tout $k > 1$, P_k est un polynôme de degré k dans $\mathbb{C}[Y]$, que l'on peut déterminer par la formule de récurrence

$$P_k = YP_{k-1} - P_{k-2},$$

à partir de $P_0 = 2$ et $P_1 = Y$.

En déduire qu'il existe, dans $\mathbb{C}[Y]$, un polynôme $\phi(Y)$ de degré m , tel que pour tout $\beta \in \mathbb{C}$ vérifiant $\phi(\beta) = 0$, les racines du polynôme $X^2 - \beta X + 1$ sont des racines de l'équation $f(X) = 0$, inverses l'une de l'autre.

On dit que l'équation $\phi(Y) = 0$ est la *résolvante* de l'équation $f(X) = 0$.

4°) Etant donné une équation réciproque $f(X) = 0$, satisfaisant aux hypothèses de la question 3°), retrouver la résolvante $\phi(Y) = 0$, en déterminant, par la méthode du résultant, l'équation transformée de $f(X) = 0$ par $F(X) = X + \frac{1}{X}$.

5°) En appliquant les résultats des questions 2°) et 3°), exprimer à l'aide de radicaux, les racines dans $\mathbb{C}$ du polynôme $X^5 - 1$ (on calculera d'abord, $\cos \frac{2k\pi}{5}$ et $\sin \frac{2k\pi}{5}$ pour $k = 1$ et $k = 2$).

13) Soit $f(X) = X^4 + aX^3 + bX^2 + cX + d$ dans $\mathbb{C}[X]$, tel que $f(0) \neq 0$ et $f(1) \neq 0$.

On note $g(X) = 0$ l'équation transformée de $f(X) = 0$ par $F(X) = \frac{X}{X-1}$.

1°) Ecrire le polynôme $g(X)$ (ses coefficients étant exprimés en fonction de a, b, c, d).

2°) On dira que l'équation $f(X) = 0$ est invariante par la transformation $F(X)$, s'il existe ρ , non nul dans $\mathbb{C}$, tel que $g(X) = \rho f(X)$.

Trouver toutes les équations du type $f(X) = 0$, invariantes par la transformation $F(X)$.

3°) Montrer que l'équation $f(X) = 0$ est invariante par $F(X)$ si et seulement s'il existe s et s' , non nuls dans $\mathbb{C}$, tels que

$$f(X) = (X^2 - sX + s)(X^2 - s'X + s').$$

4°) Vérifier que l'équation

$$X^4 - 3X^3 + X^2 + 4X - 2 = 0$$

est invariante par la transformation $F(X) = \frac{X}{X-1}$ et la résoudre en utilisant le résultat du 3°).





Appendice A

Propriétés arithmétiques de $\mathbb{Z}$

On suppose connue, la construction de l'anneau $\mathbb{Z}$ des **entiers rationnels**, à partir de l'ensemble des **entiers naturels** muni des opérations usuelles d'addition et de multiplication [42].

1. Rappels

a) L'anneau $\mathbb{Z}$ des entiers rationnels est unitaire, commutatif, intègre ; c'est donc un *domaine d'intégrité* (Déf. 1.21.).

b) L'ensemble $\mathbb{Z}$ est muni d'une relation d'ordre total induite par l'ordre naturel de $\mathbb{N}$.

$$\mathbb{N} = \{n \in \mathbb{Z} ; n \geq 0\} \quad ; \quad \mathbb{Z} \setminus \mathbb{N} = \{n \in \mathbb{Z} ; n < 0\}.$$

$\mathbb{N}$ est l'ensemble des entiers rationnels dits **positifs** ou **nuls** et $\mathbb{Z} \setminus \mathbb{N}$ est l'ensemble des entiers rationnels dits **négatifs**.

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Toute partie non vide, *bornée* de $\mathbb{N}$ a un plus grand élément.

c) A tout $n \in \mathbb{Z}$, on associe sa **valeur absolue**, notée $|n|$, telle que

$$|n| = n, \text{ si } n \geq 0 \quad \text{et} \quad |n| = -n, \text{ si } n < 0.$$

Quels que soient m et n dans $\mathbb{Z}$, on a

$$|m| = |n| \iff m = \pm n.$$

$$|mn| = |m||n| \quad \text{et} \quad |m+n| \leq |m| + |n|.$$

Rappel de notations : $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

$\mathbb{N}^*$ est l'ensemble des entiers rationnels **strictement positifs**.

2. Divisibilité dans $\mathbb{Z}$. Notion de nombre premier

Définition A.1. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.

a) On dit que **b divise a** dans $\mathbb{Z}$, s'il existe $c \in \mathbb{Z}$ tel que **$a = bc$** .

b) Ecrire **$a = bc$** dans $\mathbb{Z}$, c'est effectuer une **factorisation** de a en un produit de deux **facteurs** b et c . Dans ce cas, on dit que, dans $\mathbb{Z}$, b et c sont des **diviseurs** de a ou que a est un **multiple** de b et de c .

c) Pour tout $a \in \mathbb{Z}^*$, a et $-a$ sont dits **associés** dans $\mathbb{Z}$.

Remarque A.2. :

a) Quel que soit $a \in \mathbb{Z}$, 1 et -1 divisent a .

b) *Notations* : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. On écrira symboliquement

$b|a$, pour exprimer que b divise a ;

$b \nmid a$ pour exprimer que b ne divise pas a .

Par exemple, $3 \mid 12$, $-6 \mid 18$, $4 \nmid 15$.

c) Dans $\mathbb{Z}$, $b \mid a \iff -b \mid a$.

Propriétés élémentaires de la divisibilité dans $\mathbb{Z}$:

Le lecteur vérifiera sans peine les résultats suivants :

Proposition A.3. Pour a, b, c , dans $\mathbb{Z}^*$:

- 1) $a \mid a$.
- 2) $a \mid b \implies |a| \leq |b|$.
- 3) $(a \mid b \text{ et } b \mid a) \iff a = \pm b$.
- 4) $(a \mid b \text{ et } b \mid c) \implies a \mid c$.
- 5) $(a \mid b \text{ et } a \mid c) \implies a \mid (b + c)$.

Remarque A.4. :

a) La réciproque de la propriété 5), ci-dessus, est fausse. Par exemple, $7 \mid 21$; or, si l'on écrit $21 = 6 + 15$, on a $7 \nmid 6$ et $7 \nmid 15$.

b) La relation de divisibilité est une relation dite de **préordre**.

En effet, dans la proposition A.3., les lignes 1) et 4) expriment, respectivement, que la divisibilité est *réflexive* et *transitive*; 3) montre qu'elle n'est *ni symétrique*, *ni antisymétrique*.

c) En général, un entier $a \in \mathbb{Z}^*$ a plusieurs diviseurs distincts, autres que 1 et a , et on peut écrire plusieurs factorisations de a . Par exemple :

$$132 = 2 \times 66 = 4 \times 33 = 2 \times 3 \times 22 \\ 132 = 2 \times 2 \times 3 \times 11.$$

Dans la dernière factorisation, chaque facteur est tel qu'il n'a pas d'autre diviseur positif que 1 et lui-même, ce qui motive la définition suivante.

Définition A.5. Un entier $p \in \mathbb{Z}$ est dit **premier** si $|p| > 1$ et p n'a pas d'autre diviseur que ± 1 et $\pm p$.

Remarque A.6. :

a) Dans l'anneau $\mathbb{Z}$, p premier $\iff -p$ premier.

On conviendra d'appeler **nombre premier**, un entier *premier et positif* dans $\mathbb{Z}$.

Compte tenu de cette convention, un entier p est premier dans $\mathbb{Z}$ si et seulement si $|p|$ est un nombre premier.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ... sont des nombres premiers.

b) Les nombres premiers jouent un rôle fondamental dans l'anneau $\mathbb{Z}$, puisque tout entier, autre que 0 et ± 1 , est un produit d'éléments premiers (Voir plus loin le Théorème de Factorisation Unique). Nous utiliserons cette propriété pour prouver que l'ensemble des nombres premiers est infini (Théorème d'Euclide).

c) Les nombres premiers continuent de susciter un vif intérêt en Théorie des Nombres. Les problèmes qui les concernent sont généralement assez faciles à formuler, mais très difficiles à résoudre; ils se rattachent essentiellement à deux types de questions :

Comment reconnaître qu'un entier est premier ?

Comment se répartissent les nombres premiers ?

A ce jour, plusieurs problèmes posés depuis fort longtemps n'ont pas encore été totalement élucidés ([52] ; [33]).

3. Division et congruences dans $\mathbb{Z}$

A. Division dans $\mathbb{Z}$

Théorème A.7. Etant donné $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que $0 \leq r < |b|$ et $a = bq + r$.

Preuve : On considère les entiers de la forme $a - x|b|$, où $x \in \mathbb{Z}$. Posons

$$M = \{a - x|b| \geq 0; x \in \mathbb{Z}\}.$$

Vérifions que M n'est pas vide, en prouvant que $a + |a||b| \geq 0$. En effet,

$$b \neq 0 \implies |b| \geq 1,$$

$$\text{d'où, } a + |a||b| \geq -|a| + |a||b| = |a|(|b| - 1) \geq 0.$$

M étant une partie non vide de $\mathbb{N}$ il existe un plus petit entier $r \in M$. Écrivons $r = a - k|b|$, où $k \in \mathbb{Z}$; alors

$$a = k|b| + r.$$

Montrons que $0 \leq r < |b|$. On a $0 \leq r$, car $r \in M$. D'autre part, $r \geq |b|$ impliquerait

$$0 \leq a - (k+1)|b| < r,$$

d'où une contradiction avec la minimalité de r dans M .

Si $b > 0$, on pose $q = k$; si $b < 0$, on pose $q = -k$. Dans chaque cas, on obtient

$$a = bq + r \quad ; \quad 0 \leq r < |b|. \quad (\text{A.1})$$

Il reste à prouver l'unicité du couple (q, r) . Supposons $(q', r') \neq (q, r)$ dans $\mathbb{Z} \times \mathbb{Z}$, vérifiant les relations (0.1); on a : $b(q - q') = r' - r$.

Si $q' \neq q$, on a nécessairement $r' \neq r$, puisque l'anneau $\mathbb{Z}$ est intègre. Supposons $r' > r$; alors

$$\begin{aligned} (0 \leq r < |b| \text{ et } 0 \leq r' < |b|) &\implies (r' - r) < |b|; \\ \text{mais } (b(q - q') = r' - r) &\implies r' - r \geq |b|, \end{aligned}$$

d'où une contradiction. □

On note que $b|a \iff r = 0$.

Définition A.8. Avec les notations précédentes, q et r sont appelés, respectivement, **quotient** et **reste** de la division de a par b dans $\mathbb{Z}$.

B. Congruences dans $\mathbb{Z}$

On rappelle ([11], Ch. III) que pour tout entier $n \in \mathbb{N}$, la relation binaire $\mathcal{R}$ définie dans $\mathbb{Z}$ par

$$x \mathcal{R} y \iff (x - y) \in n\mathbb{Z}$$

est une relation d'équivalence appelée **congruence modulo n** .

L'ensemble quotient $\mathbb{Z}/\mathcal{R}$ est noté $\mathbb{Z}/(n)$ ou $\mathbb{Z}/n\mathbb{Z}$.

On écrit : $x \equiv y \pmod{n}$ pour exprimer que x est *congru* à y modulo n .

Pour $n = 0$, $\mathbb{Z}/(0)$ s'identifie à $\mathbb{Z}$.

Pour tout $x \in \mathbb{Z}$, on note $\bar{x}$ la classe de congruence de x modulo n :

$$\bar{x} = \{y \in \mathbb{Z}; \exists q \in \mathbb{Z}, y = x + qn\}.$$

Supposons $n > 0$. Etant donné $x \in \mathbb{Z}$, en effectuant la division de x par n , on obtient un unique couple d'entiers rationnels (q, r) tel que

$$x = qn + r \quad \text{et} \quad 0 \leq r < n.$$

Par suite, pour tout $x \in \mathbb{Z}$, il existe un unique $r \in \mathbb{N}$ tel que $0 \leq r < n$ et $\bar{x} = \bar{r}$ dans $\mathbb{Z}/n\mathbb{Z}$.

On en déduit que

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\};$$

donc $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n .

On vérifie ([11], Ch. III) que la congruence modulo n est compatible avec l'addition et la multiplication de l'anneau $\mathbb{Z}$; autrement dit :

Proposition A.9. Dans $\mathbb{Z}$, pour $n > 0$,

$$(x \equiv x' \pmod{n} \text{ et } y \equiv y' \pmod{n}) \text{ implique } \\ x + y \equiv x' + y' \pmod{n} \text{ et } xy \equiv x'y' \pmod{n}.$$

En particulier, quel que soit $a \in \mathbb{Z}$,

$$x \equiv y \pmod{n} \implies (a + x \equiv a + y \pmod{n} \text{ et } ax \equiv ay \pmod{n}).$$

On peut alors définir une addition et une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par

$$\overline{x} + \overline{y} = \overline{x+y} \text{ et } \overline{x}\overline{y} = \overline{xy}.$$

$\mathbb{Z}/n\mathbb{Z}$ est ainsi muni d'une structure d'anneau induite par celle de $\mathbb{Z}$ (Voir Ch. 1, Exemple 1.12).

Pour $n = 1$, l'anneau $\mathbb{Z}/\mathbb{Z}$ est nul.

Pour $n > 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est unitaire et commutatif ; $\overline{0}$ et $\overline{1}$ sont, respectivement, élément neutre pour l'addition et la multiplication.

4. Factorisation unique dans $\mathbb{Z}$

Dans un premier temps, nous considérons le problème de la factorisation unique, pour les entiers $n > 1$.



A. Théorème Fondamental de l'Arithmétique

Théorème A.10. Tout entier $n > 1$ peut s'écrire de façon unique, à l'ordre près des facteurs, comme un produit de nombres premiers :

$$n = p_1 p_2 \dots p_r,$$

avec $r \geq 1$, dans $\mathbb{N}$ et p_i premier positif, quel que soit i ($1 \leq i \leq r$).

Preuve : Soit $n > 1$ dans $\mathbb{Z}$;

si n est premier, la propriété est vérifiée avec $r = 1$;

si n n'est pas premier, alors n admet au moins un diviseur positif autre que 1 et n , on peut donc écrire $n = n_1 n_2$, avec $1 < n_1 < n$ et $1 < n_2 < n$. On raisonne alors, par récurrence sur n , en supposant la propriété vraie pour tout entier m tel que $1 < m < n$.

L'hypothèse de récurrence implique que n_1 et n_2 sont produits de nombres premiers, par suite, il en est de même pour n . Il reste à prouver l'unicité de la factorisation de n .

Supposons $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, où, n n'étant pas premier, on a $r > 1$ et $s > 1$ dans $\mathbb{N}$ et les p_i , ($1 \leq i \leq r$), q_j , ($1 \leq j \leq s$), sont des nombres premiers.

1^{er} cas : il existe i et j tels que $p_i = q_j$.

On peut supposer, par exemple, $p_1 = q_1$. L'intégrité de $\mathbb{Z}$ permet d'écrire :

$$n' = p_2 p_3 \dots p_r = q_2 q_3 \dots q_s; \quad \text{d'où } 1 < n' < n.$$

L'hypothèse de récurrence implique l'unicité de la factorisation de n' , à l'ordre près des facteurs ; par suite on a $s = r$ et il existe une permutation σ des entiers $2, \dots, r$, telle que

$$\forall i \ (2 \leq i \leq r), \quad p_i = q_{\sigma(i)},$$

d'où l'unicité de la factorisation de n , à l'ordre près des facteurs.

2^{ème} cas : $p_i \neq q_j$, quel que soit (i, j) , ($1 \leq i \leq r$, $1 \leq j \leq s$).

On a en particulier, $p_1 \neq q_1$; supposons $p_1 < q_1$.

$$s > 1 \implies 0 < p_1 q_2 \dots q_s < n = q_1 q_2 \dots q_s.$$

Posons $m = n - p_1 q_2 \dots q_s$; alors,

$$m = (q_1 - p_1) q_2 \dots q_s = p_1 (p_2 \dots p_r - q_2 \dots q_s). \quad (\text{A.2})$$

$$s > 1 \implies 1 < m < n.$$

L'hypothèse de récurrence implique que m se factorise de façon unique, à l'ordre près des facteurs, en un produit de nombres premiers. Les égalités (0.2) montrent que le nombre premier p_1 est un facteur de m ; or on a $p_1 \neq q_j$, quel que soit j ($2 < j < s$), par suite, p_1 divise nécessairement $(q_1 - p_1)$. On en déduit que p_1 divise q_1 ; mais p_1 et q_1 étant premiers, positifs dans $\mathbb{Z}$, on a $p_1 = q_1$, ce qui est contraire à l'hypothèse. Le second cas envisagé est donc impossible. $\square$

B. Théorème de Factorisation Unique dans $\mathbb{Z}$

Théorème A.11. *Tout entier $n \in \mathbb{Z}$, tel que $n \neq 0$ et $n \neq \pm 1$, se factorise de façon unique, à l'ordre près des facteurs, en un produit d'éléments premiers de $\mathbb{Z}$.*

Preuve :

Si $n > 0$, on applique le théorème précédent.

Si $n < 0$, $n = -n'$, avec $n' > 0$ et si une factorisation de n' en éléments premiers positifs de $\mathbb{Z}$ s'écrit :

$$n' = p_1 p_2 \dots p_r, \quad \text{alors} \quad n = (-p_1) p_2 \dots p_r,$$

d'où le résultat. $\square$

Théorème A.12. : Théorème d'Euclide

L'ensemble des nombres premiers est infini.

Preuve : Soit $\mathcal{P}$ l'ensemble des nombres premiers, c'est-à-dire, d'après notre convention, l'ensemble des éléments premiers positifs de $\mathbb{Z}$. $\mathcal{P}$ est une partie non vide de $\mathbb{N}$, donc totalement ordonnée par l'ordre induit par celui de $\mathbb{N}$; on peut écrire les nombres premiers par ordre croissant :

$$p_1 < p_2 < \dots < p_{n-1} < p_n \dots$$

où $p_1 = 2, p_2 = 3, p_3 = 5$, etc. ; p_n désigne le $n^{\text{ième}}$ nombre premier.

Soit $N = p_1 p_2 \dots p_n + 1$; d'après le Théorème Fondamental de l'Arithmétique, N est un produit de nombres premiers.

Soit p un diviseur premier (positif) de N ; on a nécessairement $p \neq p_i$, quel que soit i ($1 \leq i \leq n$), donc $p > p_n$.

On en conclut qu'étant donné un nombre premier quelconque dans $\mathcal{P}$, il en existe un autre qui est strictement plus grand; donc $\mathcal{P}$ est infini. $\square$

Remarque A.13. Il existe d'autres preuves du Théorème d'Euclide (Cf.[28], [52]).

C. Conséquences du Théorème de Factorisation Unique

Comme plus haut, on désigne par $\mathcal{P}$, l'ensemble des nombres premiers.

Proposition A.14. *Soit $n \neq 0$ dans $\mathbb{Z}$; alors, quel que soit $p \in \mathcal{P}$, il existe $\alpha \in \mathbb{N}$, tel que $p^\alpha | n$ et $p^{\alpha+1} \nmid n$.*

Preuve : Supposons $n > 0$ et soit $p \in \mathcal{P}$. Si $p \nmid n$, alors, $\alpha = 0$ convient.

Si $p \mid n$, on considère l'ensemble suivant :

$$E_p(n) = \{k \in \mathbb{N} ; p^k \mid n\}.$$

Par hypothèse, $1 \in E_p(n)$, donc $E_p(n)$ est une partie de $\mathbb{N}$, non vide et non réduite à 0. De plus, dans $\mathbb{N}$ on a

$$(p^k \mid n \implies p^k \leq n) \quad \text{et} \quad (p^k < p^{k+1}, \forall k \in \mathbb{N}).$$

On en déduit que l'ensemble $E_p(n)$ est borné dans $\mathbb{N}$; par suite, il existe un plus grand élément dans $E_p(n)$, que nous notons α ; alors,

$$p^\alpha \mid n \quad \text{et} \quad (p^{\alpha+1} \notin E_p(n) \implies p^{\alpha+1} \nmid n).$$

Si $n < 0$, on applique la propriété démontrée ci-dessus à $n' = |n|$ et

$$(p^\alpha \mid n', p^{\alpha+1} \nmid n') \implies (p^\alpha \mid n, p^{\alpha+1} \nmid n).$$

□

Définition A.15. Etant donné $n \in \mathbb{Z}^*$ et $p \in \mathcal{P}$, l'entier $\alpha \geq 0$ tel que $p^\alpha \mid n$ et $p^{\alpha+1} \nmid n$, est appelé la **valuation p-adique de n** . On écrira :

$$\alpha = v_p(n).$$

Proposition A.16. Tout $n \in \mathbb{Z}^*$ s'écrit

$$n = \pm \prod_{p \in \mathcal{P}} p^{v_p(n)}, \quad (\text{A.3})$$

où les $v_p(n)$ sont presque tous nuls dans $\mathbb{N}$, c'est-à-dire, nuls sauf un nombre fini d'entre eux.

Preuve : Si $n = \pm 1$, alors $v_p(n) = 0$, pour tout $p \in \mathcal{P}$.

Supposons $n \neq \pm 1$. D'après le Théorème de Factorisation Unique,

$$n = \pm p_1 p_2 \dots p_r, \quad r \in \mathbb{N}, \quad p_i \in \mathcal{P}, \quad \forall i (1 \leq i \leq r);$$

en regroupant les p_i qui sont égaux, on obtient :

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

où les $p_i, (1 \leq i \leq k)$, sont deux à deux *distincts* dans $\mathcal{P}$ et $\alpha_i = v_{p_i}(n)$, quel que soit $i (1 \leq i \leq k)$. □

5. p.g.c.d. et p.p.c.m. dans $\mathbb{Z}$. Théorème de Bezout

A. Notion de p.g.c.d. et p.p.c.m. dans $\mathbb{Z}$

Remarque A.17. Soit m et n dans $\mathbb{Z}^*$; alors,

$$a) \quad m = \pm 1 \iff v_p(n) = 0, \quad \forall p \in \mathcal{P}.$$

$$b) \quad m \mid n \iff 0 \leq v_p(m) \leq v_p(n), \quad \forall p \in \mathcal{P}.$$

Notations : Quels que soient m et n dans $\mathbb{Z}^*$ et $p \in \mathcal{P}$, posons :

$$\mu_p = \inf(v_p(m), v_p(n)) \quad ; \quad \nu_p = \sup(v_p(m), v_p(n)) \quad (\text{A.4})$$

$$d = \prod_{p \in \mathcal{P}} p^{\mu_p} \quad ; \quad l = \prod_{p \in \mathcal{P}} p^{\nu_p}. \quad (\text{A.5})$$

Exemple A.18. Pour $m = 84 = 2^2 \times 3 \times 7$ et $n = 18 = 2 \times 3^2$,

$$d = 2 \times 3 = 6 \quad \text{et} \quad l = 2^2 \times 3^2 \times 7 = 252.$$

Compte tenu des remarques A.17., on vérifie que les entiers *strictement positifs* d et l définis par les relations (A.5) satisfont aux propriétés suivantes :

Proposition A.19. :

- 1) $d|m$ et $d|n$;
 1') $\forall c \in \mathbb{Z}^*, (c|m \text{ et } c|n) \implies c|d$.
 2) $m|l$ et $n|l$;
 2') $\forall k \in \mathbb{Z}^*, (m|k \text{ et } n|k) \implies l|k$.

Remarque A.20. : Conséquences de la proposition A.19. :

D'après 1'), pour $c \in \mathbb{Z}^*$, $(c|m \text{ et } c|n) \implies |c| \leq d$.

D'après 2'), pour $k \in \mathbb{Z}^*$, $(m|k \text{ et } n|k) \implies l \leq |k|$.

Si $\delta \in \mathbb{Z}^*$ vérifie, comme d , les conditions 1) et 1'), alors $\delta = \pm d$.

En effet, en appliquant 1) et 1') à δ et d , on obtient :

$$(\delta|m \text{ et } \delta|n) \implies \delta|d; (d|m \text{ et } d|n) \implies d|\delta,$$

d'où $\delta = \pm d$.

De façon analogue, on montre que si $\lambda \in \mathbb{Z}^*$ vérifie, comme l , les conditions 2) et 2'), alors $\lambda = \pm l$.

Les remarques A.20. justifient les définitions suivantes.

Définition A.21. Etant donné m et n dans $\mathbb{Z}^*$,

- a) Tout entier $\delta \in \mathbb{Z}^*$, vérifiant les conditions 1) et 1'), est appelé **plus grand commun diviseur** de m et n (p.g.c.d. de m et n).
 b) Tout entier $\lambda \in \mathbb{Z}^*$, vérifiant les conditions 2) et 2'), est appelé **plus petit commun multiple** de m et n (p.p.c.m. de m et n).

Remarque A.22. L'étude précédente a montré que pour tout couple d'entiers non nuls (m, n) , il existe un p.g.c.d. et un p.p.c.m., uniques au signe près.

Compte tenu des notations (A.4), les entiers d et l définis par les relations (A.5), sont les p.g.c.d. et p.p.c.m. positifs de m et n .

Notations : Pour m et n donnés dans $\mathbb{Z}^*$, un p.g.c.d. (resp. un p.p.c.m.) de m et n sera désigné par $m \wedge n$ (resp. $m \vee n$).

Remarque A.23. On sait que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $k\mathbb{Z}$, où $k \in \mathbb{N}$ ([11], Ch. III). On en déduit que tout idéal de l'anneau $\mathbb{Z}$ (Déf. 1.42.) est aussi de cette forme, donc est principal (Déf. 2.5.).

Pour tout $n \in \mathbb{Z}^*$, $-n\mathbb{Z} = n\mathbb{Z}$ et $(k \in n\mathbb{Z} \iff n|k)$.

Proposition A.24. Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$; pour d et l dans $\mathbb{N}^*$, on a

a) $d = m \wedge n \iff m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

b) $l = m \vee n \iff m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$.

Preuve : On rappelle que $m\mathbb{Z} + n\mathbb{Z}$ est l'idéal de l'anneau $\mathbb{Z}$ engendré par m et n (Déf. 2.1.) et que

$$m\mathbb{Z} + n\mathbb{Z} = \{am + bn; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}.$$

a) Supposons $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

$$(m \in d\mathbb{Z} \text{ et } n \in d\mathbb{Z}) \iff (d|m \text{ et } d|n).$$

D'autre part, pour $c \in \mathbb{Z}^*$,

$$(c|m \text{ et } c|n) \iff (m \in c\mathbb{Z} \text{ et } n \in c\mathbb{Z}),$$

$$\text{donc } (c|m \text{ et } c|n) \implies m\mathbb{Z} + n\mathbb{Z} \subseteq c\mathbb{Z},$$

d'où $d\mathbb{Z} \subseteq c\mathbb{Z}$, c'est-à-dire $c|d$. On en conclut que $d = m \wedge n$.

Réciproquement, supposons $d = m \wedge n$ et $d > 0$, alors

$$(d|m \text{ et } d|n) \implies m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}.$$

D'autre part, tout idéal de $\mathbb{Z}$ étant principal, il existe ici, $c \in \mathbb{N}^*$ tel que

$$m\mathbb{Z} + n\mathbb{Z} = c\mathbb{Z}. \text{ On en déduit que } c\mathbb{Z} \subseteq d\mathbb{Z}, \text{ donc } d \text{ divise } c; \text{ or,}$$

$$m\mathbb{Z} + n\mathbb{Z} = c\mathbb{Z} \implies (c|m \text{ et } c|n) \implies c|d,$$

puisque $d = m \wedge n$. Les entiers c et d étant strictement positifs, on en conclut que $c = d$, donc $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$.

b) Supposons $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$;

$$l \in m\mathbb{Z} \cap n\mathbb{Z} \implies (m|l \text{ et } n|l).$$

$$\text{Pour } k \in \mathbb{Z}^*, (m|k \text{ et } n|k) \implies k \in m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z};$$

d'où $l|k$ et par suite, $l = m \vee n$.

Réciproquement, supposons $l = m \vee n$,

$$(m|l \text{ et } n|l) \implies l\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}.$$

$$\text{Pour } k \in m\mathbb{Z} \cap n\mathbb{Z}, (m|k \text{ et } n|k) \implies l|k,$$

puisque $l = m \vee n$; par suite,

$$m\mathbb{Z} \cap n\mathbb{Z} \subseteq l\mathbb{Z}, \text{ d'où } m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}. \quad \square$$

Remarque A.25. : Les hypothèses et les notations étant celles de la Prop. A.24., on a

$$d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} \iff \exists (a, b) \in \mathbb{Z} \times \mathbb{Z}, \text{ tel que } d = am + bn. \quad (\text{A.6})$$

Dans le second membre de cette relation, le couple (a, b) n'est pas unique. En effet,

$$d = m \wedge n \implies \exists (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}, \text{ tel que } m = \alpha d, n = \beta d;$$

d'où $\beta m = \alpha n$; par suite, pour tout $k \in \mathbb{Z}$, on peut écrire

$$d = am + bn = (\alpha + k\beta)m + (b - k\alpha)n. \quad (\text{A.7})$$

De la Prop. A.24., on déduit alors la propriété suivante qui sera utilisée plus loin (Preuve de la Prop. A.38.).

Corollaire A.26. Soit $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m \nmid n$ et $n \nmid m$. Si $d = m \wedge n$ et $d > 0$, il existe alors $(u, v) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que

$$d = um - vn.$$

Preuve : Les hypothèses impliquent $d < m$ et $d < n$ dans $\mathbb{N}^*$.

Par suite, pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant la relation (0.6), on a

$$d = am + bn \text{ avec } ab < 0.$$

En effet, $(a > 0, \text{ et } b > 0)$, impliquerait $(d > m \text{ et } d > n)$.

Si $a > 0$ et $b < 0$, on prend $u = a$ et $v = -b$.

Si $a < 0$ et $b > 0$, on utilise la relation (A.7) en prenant un entier $k > 0$ tel que $a + k\beta > 0$, alors,

$$(a + k\beta)(b - k\alpha) < 0 \implies (b - k\alpha) < 0.$$

Dans ce cas, on pose $u = a + k\beta$ et $v = -(b - k\alpha)$. $\square$

Proposition A.27. Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$; si d et l sont, respectivement, p.g.c.d. et p.p.c.m. de m et n dans $\mathbb{Z}$, alors

$$mn = \pm dl.$$

Preuve : D'après la Prop. A.16., il existe un entier $s > 0$, des nombres premiers distincts $p_1, p_2, \dots, p_s$ et des entiers α_i, β_i dans $\mathbb{N}$ tels que

$$m = \pm \prod_{1 \leq i \leq s} p_i^{\alpha_i} \quad ; \quad n = \pm \prod_{1 \leq i \leq s} p_i^{\beta_i}.$$

Quel que soit i ($1 \leq i \leq s$), posons

$$\mu_i = \inf(\alpha_i, \beta_i) \quad ; \quad \nu_i = \sup(\alpha_i, \beta_i);$$

on a alors, $d = \pm \prod_{1 \leq i \leq s} p_i^{\mu_i}$ et $l = \pm \prod_{1 \leq i \leq s} p_i^{\nu_i}$.

Pour tout i ($1 \leq i \leq s$), on a, soit $\alpha_i \leq \beta_i$, soit $\beta_i \leq \alpha_i$, d'où

$$\mu_i = \alpha_i \quad \text{et} \quad \nu_i = \beta_i, \quad \text{ou bien,} \quad \mu_i = \beta_i \quad \text{et} \quad \nu_i = \alpha_i;$$

par suite, $p_i^{\mu_i + \nu_i} = p_i^{\alpha_i + \beta_i}$, d'où $mn = \pm dl$. $\square$

Remarque A.28. La recherche des p.g.c.d. par l'algorithme d'Euclide sera développée au Chapitre 5, dans un contexte plus général.

B. Éléments premiers entre eux dans $\mathbb{Z}$. Théorème de Bezout

Définition A.29. Deux entiers non nuls dans $\mathbb{Z}$ sont dits **premiers entre eux**, s'ils n'ont pas d'autres diviseurs communs que 1 et -1 .

Proposition A.30. Pour $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$, les conditions suivantes sont équivalentes :

- 1) m et n sont premiers entre eux.
- 2) $1 = m \wedge n$.
- 3) $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$.
- 4) $mn = m \vee n$.
- 5) $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$.
- 6) $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$ (isomorphisme d'anneaux).

L'équivalence des propriétés 1) à 5) découle directement de la définition A.29. et des propositions A.24. et A.27..

Pour l'équivalence entre 5) et 6), on considère l'application

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto (\sigma(x), \pi(x)) \end{aligned}$$

où σ et π sont, respectivement, les surjections canoniques

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \quad ; \quad \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

([11] Th. 3.29.)

Théorème A.31. : Théorème de Bezout

Deux entiers m et n , non nuls dans $\mathbb{Z}$, sont premiers entre eux si et seulement s'il existe a et b dans $\mathbb{Z}$, tels que

$$am + bn = 1. \quad (\text{A.8})$$

En effet, pour m et n dans $\mathbb{Z}^*$, la condition (A.6) est équivalente à la condition 3) de la proposition A.28.

La relation (A.8) est appelée **Relation de Bezout**.

Théorème A.32. : Théorème de Gauss

Pour a, b, c non nuls dans $\mathbb{Z}$:

$$(a|b \text{ et } a \wedge b = 1) \implies a|c.$$

Preuve : Appliquons le théorème de Bezout ;

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z} \times \mathbb{Z} ; ua + vb = 1,$$

d'où $uac + vbc = c$, par suite d'après la proposition A.3., 5),

$$(a|uac \text{ et } a|vbc) \implies a|c. \quad \square$$

On remarque que la propriété est fautive si a et b ne sont pas premiers entre eux. Par exemple, $6|12$, mais $6 \nmid 3$ et $6 \nmid 4$.

Corollaire A.33. Dans $\mathbb{Z}^*$,

$$(p \text{ premier et } p|bc) \implies p|b \text{ ou } p|c.$$

Preuve : Les seuls diviseurs de p étant $\pm p$ et ± 1 , on a nécessairement,

$$p \wedge b = p \text{ ou } p \wedge b = 1.$$

Si $p \wedge b = p$, alors $p|b$; dans le cas où $p \wedge b = 1$, d'après le théorème de Gauss, on a $p|c$.

□

Théorème A.34. Soit a non nul dans $\mathbb{Z}$ et $n > 1$ dans $\mathbb{N}$; alors φ désignant la fonction d'Euler, on a

$$a \wedge n = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Preuve : On rappelle ([11], Ch. III) que $\varphi(n)$ est le cardinal de l'ensemble des entiers k tels que $1 \leq k < n$ et $k \wedge n = 1$.

Si G_n désigne le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, alors (Ch. 1, Prop. 1.13.),

$$G_n = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} ; a \wedge n = 1\};$$

donc le groupe G_n est d'ordre $\varphi(n)$; par suite, pour $a \in \mathbb{Z}$,

$$a \wedge n = 1 \implies \bar{a} \in G_n \implies \bar{a}^{\varphi(n)} = \bar{1},$$

c'est-à-dire, $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Corollaire A.35. : Petit théorème de Fermat

Etant donné $a \in \mathbb{Z}$; pour tout nombre premier p , on a

$$a^p \equiv a \pmod{p}.$$

Preuve : On peut supposer $a \neq 0$.

1) Si $p|a$, alors

$$a \equiv 0 \pmod{p} \implies a^p \equiv 0 \pmod{p},$$

d'où $a^p \equiv a \pmod{p}$.

2) Si $p \nmid a$, comme p est premier, on a nécessairement $a \wedge p = 1$.

D'autre part $\varphi(p) = p - 1$, alors l'application du théorème précédent donne

$$a^{p-1} \equiv 1 \pmod{p}, \text{ d'où l'on déduit (Prop. A.9.) :}$$

$$a^p \equiv a \pmod{p}. \quad \square$$

Théorème A.36. : Théorème de Wilson

Soit $p \geq 2$ dans $\mathbb{N}$; alors

$$p \text{ premier} \iff (p-1)! \equiv -1 \pmod{p}.$$

Preuve : Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps (Cor. 1.14) et ses $p-1$ éléments non nuls sont les $p-1$ racines du polynôme $X^{p-1} - \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit que

$$X^{p-1} - \bar{1} = (X - \bar{1})(X - \bar{2}) \cdots (X - \overline{p-1}).$$

En identifiant les termes constants dans les deux membres de l'égalité précédente, on obtient $-\bar{1} = \overline{(p-1)!}$, donc

$$(p-1)! \equiv -1 \pmod{p}.$$

Réciproquement, supposons $(p-1)! \equiv -1 \pmod{p}$; dans $\mathbb{Z}/p\mathbb{Z}$ on a $\bar{1}\bar{2}\cdots\overline{p-1} = -\bar{1}$.

On en conclut que tout élément non nul de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est inversible, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps; par suite

$$(1 \leq k < p) \implies k \wedge p = 1,$$

ce qui implique p premier. □

Les propriétés suivantes seront utiles, en particulier, dans l'étude des corps finis (Cf. Extensions de Corps).

Proposition A.37. Pour a, b, n dans $\mathbb{N}^*$, $a > 1$, on a

$$(a^s - 1) | (a^n - 1) \iff s | n.$$

Preuve :

1°) Supposons que s divise n , donc il existe $d \in \mathbb{N}^*$ tel que $n = sd$, d'où $a^n = (a^s)^d$.

$$a^n - 1 = (a^s)^d - 1 = (a^s - 1)(a^{s(d-1)} + a^{s(d-2)} + \dots + 1),$$

donc $a^s - 1$ divise $a^n - 1$.

2°) Réciproquement, on suppose que $a^s - 1$ divise $a^n - 1$, dans $\mathbb{N}$; cette hypothèse implique $(a^s - 1) \leq (a^n - 1)$, d'où $a^s \leq a^n$; alors,

$$(a > 1 \text{ et } a^s \leq a^n) \implies s \leq n.$$

Effectuons la division de n par s : il existe des entiers q et r tels que

$$n = sq + r, \quad 0 \leq r < s \text{ et } q \geq 0, \text{ car } 0 < s \leq n.$$

$$\text{Si } r \neq 0, \text{ alors, } a^n - 1 = a^{sq+r} - 1 = (a^s)^q a^r - 1;$$

$$\text{donc } a^n - 1 = ((a^s)^q - 1)a^r + a^r - 1.$$

On en déduit que

$$(a^s - 1) | (a^n - 1) \implies (a^s - 1) | (a^r - 1).$$

$$\text{Or, } (a > 1, 0 \leq r < s) \implies a^s - 1 > a^r - 1,$$

d'où une contradiction, donc $r = 0$ et $s | n$. □

Proposition A.38. Soit a, m, n dans $\mathbb{N}^*$, $a > 1$; alors pour $d > 0$ dans $\mathbb{Z}$,

$$d = m \wedge n \iff a^d - 1 = (a^m - 1) \wedge (a^n - 1).$$

Preuve :

1°) Supposons $d = m \wedge n$. La proposition précédente implique

$$(a^d - 1) | (a^m - 1) \text{ et } (a^d - 1) | (a^n - 1).$$

Il reste à prouver que tout diviseur commun à $(a^m - 1)$ et $(a^n - 1)$ divise $(a^d - 1)$. D'après la proposition A.24,

$$d = m \wedge n \iff d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}.$$

Par hypothèse, d, m, n sont dans $\mathbb{N}^*$ et on a nécessairement $d \leq m$ et $d \leq n$. On peut alors trouver (Cor. A.26.) u et v dans $\mathbb{N}^*$ tels que

$$d = um - vn.$$

L'égalité ci-dessus implique

$$a^{um} - 1 = a^{vn+d} - 1 = a^d(a^{vn} - 1) + a^d - 1.$$

D'après la proposition 0.28 il existe b et c dans $\mathbb{N}^*$ tels que

$$a^{um} - 1 = (a^m - 1)b \quad \text{et} \quad a^{vn} - 1 = (a^n - 1)c.$$

On en déduit :

$$a^d - 1 = (a^m - 1)b + a^d(a^n - 1)c;$$

donc tout diviseur commun à $(a^m - 1)$ et $(a^n - 1)$ divise $(a^d - 1)$; par suite

$$a^d - 1 = (a^m - 1) \wedge (a^n - 1).$$

2°) On suppose, réciproquement, que $a^d - 1$ est p.g.c.d. de $a^m - 1$ et $a^n - 1$. Par ailleurs, soit $\delta > 0$ dans $\mathbb{Z}$, un p.g.c.d. de m et n ; d'après la première partie de la démonstration, $a^\delta - 1$ est p.g.c.d. de $a^m - 1$ et $a^n - 1$. Compte tenu de l'unicité au signe près d'un p.g.c.d.,

$$(a^d - 1 > 0 \text{ et } a^\delta - 1 > 0) \implies a^d - 1 = a^\delta - 1,$$

d'où $d = \delta$. □

Corollaire A.39. Pour a, m, n dans $\mathbb{N}^*$, $a > 1$,

$$m \wedge n = 1 \iff a - 1 = (a^m - 1) \wedge (a^n - 1).$$

C. Généralisation

Les notions de *p.g.c.d.* et *p.p.c.m.* se généralisent à un nombre fini quelconque d'entiers rationnels non nuls (voir Ch. 5).

Les deux propositions qui suivent seront démontrées au Chapitre 5, dans un cadre plus général.

Proposition A.40. Dans $\mathbb{Z}^*$, les opérations *p.g.c.d.* et *p.p.c.m.* sont associatives, c'est-à-dire que pour des entiers non nuls m_1, m_2, m_3 , on a

$$(m_1 \wedge m_2) \wedge m_3 = m_1 \wedge (m_2 \wedge m_3); \quad (\text{A.9})$$

$$(m_1 \vee m_2) \vee m_3 = m_1 \vee (m_2 \vee m_3). \quad (\text{A.10})$$

Proposition A.41. Soit $m_1, \dots, m_k$ dans $\mathbb{Z}^*$; on pose $m = m_1 m_2 \dots m_k$; alors les conditions suivantes sont équivalentes :

1) Les m_i , ($1 \leq i \leq k$), sont deux à deux premiers entre eux.

2) $\bigcap_{1 \leq i \leq k} m_i \mathbb{Z} = m \mathbb{Z}$.

3) $\mathbb{Z}/m_1 \mathbb{Z} \times \mathbb{Z}/m_2 \mathbb{Z} \times \dots \times \mathbb{Z}/m_k \mathbb{Z} \simeq \mathbb{Z}/m \mathbb{Z}$.

Ces résultats se déduisent de l'associativité des *p.g.c.d.* (Prop. A.40.) et des relations 5) et 6) de la proposition A.30.



Appendice B

Produit tensoriel

Dans cet appendice, on définit la notion de *produit tensoriel* de modules sur un anneau unitaire, *commutatif* et on en donne les propriétés essentielles qui pourront être utilisées dans différents chapitres de ce livre (et dans le Vol. 2, Extensions de Corps).

Dans ce qui suit, A désigne un anneau unitaire, commutatif et, sauf indication contraire, les A -modules considérés seront des A -modules à gauche.

Notation On écrira souvent $M \in {}_A\text{Mod}$, pour exprimer que M est un A -module à gauche.

L'anneau A étant commutatif, pour deux A -modules à gauche M et N , $\text{Hom}_A(M, N)$ est un A -module à gauche et $\text{End}_A(M)$ est une A -algèbre unitaire non commutative (Cf. Ch. 3).

1. Produit tensoriel de deux A -modules

A. Applications bilinéaires



Définition B.1. Soit M, N, P trois A -modules à gauche ; une application $h : M \times N \longrightarrow P$ est dite **bilinéaire sur A** si, quels que soient x, x' dans M , y, y' dans N et $a \in A$, on a

$$i) \quad h(x + x', y) = h(x, y) + h(x', y) \quad (\text{B.1})$$

$$ii) \quad h(x, y + y') = h(x, y) + h(x, y') \quad (\text{B.2})$$

$$iii) \quad h(ax, y) = h(x, ay) = ah(x, y). \quad (\text{B.3})$$

On note $\text{Bil}_A(M \times N, P)$ l'ensemble des applications A -bilinéaires de $M \times N$ dans P .

Proposition B.2. L'anneau A étant unitaire et commutatif, $\text{Bil}_A(M \times N, P)$ est un A -module à gauche.

Preuve :

a) On définit une addition dans $\text{Bil}_A(M \times N, P)$ telle que pour tout couple (h_1, h_2) d'applications bilinéaires, on ait

$$\forall (x, y) \in M \times N, \quad (h_1 + h_2)(x, y) = h_1(x, y) + h_2(x, y).$$

On vérifie que, relativement à cette addition, $\text{Bil}_A(M \times N, P)$ est un groupe abélien, dont l'élément 0 est l'application nulle de $M \times N$ dans P .

b) Pour tout $a \in A$ et tout $h \in \text{Bil}_A(M \times N, P)$, on note ah l'application :

$$\begin{aligned} ah : M \times N &\longrightarrow P \\ (x, y) &\longmapsto ah(x, y) = a(h(x, y)). \end{aligned}$$

On vérifie que ah est A -bilinéaire ; en effet, quels que soient x, x' dans M , y, y' dans N et a, b dans A , on a

$$\begin{aligned} ah(x+x', y) &= a(h(x+x'), y) = a(h(x, y) + h(x', y)) \\ &= ah(x, y) + ah(x', y); \end{aligned}$$

de même, $ah(x, y+y') = ah(x, y) + ah(x, y')$ et d'autre part,

$$\begin{aligned} ah(bx, y) &= a(h(bx, y)) = a(h(x, by)) = a(bh(x, y)) \\ &= abh(x, y). \end{aligned}$$

L'anneau A étant commutatif, on a $ab = ba$, d'où

$$ah(bx, y) = bah(x, y) = b(ah(x, y)),$$

donc $ah \in \text{Bil}_A(M \times N, P)$.

On vérifie, alors, que le groupe abélien $\text{Bil}_A(M \times N, P)$ est un A -module à gauche. $\square$

B. Construction du produit tensoriel de deux A -modules

1. Problème

La construction du produit tensoriel de deux A -modules M et N répond au problème suivant :

Trouver un A -module T et une application $\theta \in \text{Bil}_A(M \times N, T)$ tels que, quels que soient le A -module P et l'application $h \in \text{Bil}_A(M \times N, P)$, il existe un unique $f \in \text{Hom}_A(T, P)$ tel que $f \circ \theta = h$; c'est-à-dire que le diagramme suivant commute

$$\begin{array}{ccc} M \times N & \xrightarrow{\theta} & T \\ & \searrow h & \downarrow \exists! f \\ & & P \end{array}$$

Le but de ce qui suit est de montrer que pour M et N donnés, il existe, à un isomorphisme près, un unique couple (T, θ) répondant à la question. Le A -module T sera appelé *produit tensoriel sur A des A -modules M et N* .

2. Existence d'un couple (T, θ)

Compte tenu des hypothèses et des notations ci-dessus, considérons le A -module libre F ayant pour base l'ensemble $M \times N$ (Cf. Ch. 3). Soit α l'injection canonique de $M \times N$ dans F . La propriété universelle du couple (F, α) (Th. 3.67.) implique que, quels que soient le A -module P et l'application $h \in \text{Bil}_A(M \times N, P)$, il existe un unique $g \in \text{Hom}_A(F, P)$ tel que $g \circ \alpha = h$, d'où le diagramme commutatif suivant :

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha} & F \\ & \searrow h & \downarrow \exists! g \\ & & P \end{array}$$

Mais, en général, l'injection canonique α n'est pas bilinéaire ; on a par exemple, pour x, x' dans M et y dans N ,

$$\alpha(x+x', y) = (x+x', y) \neq (x, y) + (x', y), \quad \text{en général.}$$

Le couple (F, α) ne répond donc pas au problème posé.

On considère alors le sous-module S de F engendré par l'ensemble de tous les éléments s'écrivant sous l'une des formes (B.4) ou (B.5) suivantes :

$$(ax + a'x', y) - a(x, y) - a'(x', y) \quad (\text{B.4})$$

$$(x, by + b'y') - b(x, y) - b'(x, y') \quad (\text{B.5})$$

pour x, x' dans M , y, y' dans N , et a, a', b, b' dans A .

Soit π la surjection canonique de F sur le module quotient F/S .

Posons $T = F/S$ et $\theta = \pi \circ \alpha$ et démontrons que le couple (T, θ) est une solution au problème posé dans 1.

- L'application θ est A-bilinéaire ; en effet, quels que soient x, x' dans M , y, y' dans N et a dans A ,

$$\begin{aligned} (\text{B.4}) \implies \theta(x+x', y) &= \pi(x+x', y) = \pi(x, y) + \pi(x', y) \\ &= \theta(x, y) + \theta(x', y) \end{aligned}$$

$$\begin{aligned} (\text{B.5}) \implies \theta(x, y+y') &= \pi(x, y+y') = \pi(x, y) + \pi(x, y') \\ &= \theta(x, y) + \theta(x, y'). \end{aligned}$$

$$\begin{aligned} (\text{B.4}) \implies \theta(ax, y) &= \pi(ax, y) = a\pi(x, y) \\ &= a\theta(x, y) \end{aligned}$$

$$\begin{aligned} (\text{B.5}) \implies \theta(x, ay) &= \pi(x, ay) = a\pi(x, y) \\ &= a\theta(x, y). \end{aligned}$$

- Vérifions que $S \subseteq \text{Ker } g$. Il suffit de montrer que les générateurs du sous-module S sont dans $\text{Ker } g$. Pour tout (x, y) dans $M \times N$,

$$g \circ \alpha = h \implies g(x, y) = h(x, y).$$

Soit z un générateur de S de la forme (B.4), alors

$$g(z) = h(ax + a'x', y) - ah(x, y) - a'h(x', y)$$

et la bilinéarité de h implique $g(z) = 0$. On vérifie de même que pour un générateur z de S de la forme (B.5), on a encore $g(z) = 0$.

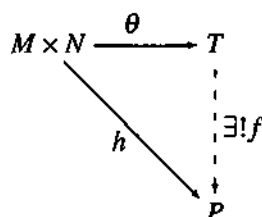
D'après la propriété universelle du couple $(F/S, \pi)$ (Th. 2.31.), la condition $S \subseteq \text{Ker } g$ entraîne l'existence d'un unique $f \in \text{Hom}_A(F/S, P)$ tel que $f \circ \pi = g$:

$$\begin{array}{ccc} F & \xrightarrow{\pi} & F/S \\ & \searrow g & \downarrow \exists! f \\ & & P \end{array}$$

donc $f \circ \pi \circ \alpha = g \circ \alpha = h$.

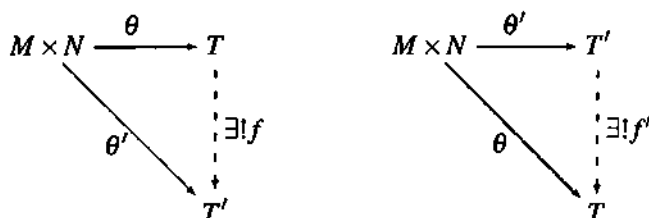
En posant, comme plus haut, $T = F/S$ et $\theta = \pi \circ \alpha$, on obtient que, quels que soient le A-module P et l'application $h \in \text{Bil}_A(M \times N, P)$, il existe un unique $f \in \text{Hom}_A(T, P)$ tel

que $f \circ \theta = h$, d'où le diagramme commutatif :



3. Unicité du couple (T, θ) , à un isomorphisme près

Supposons (T', θ') vérifiant la même propriété que le couple (T, θ) , relativement aux A -modules M et N donnés. On a donc les deux diagrammes commutatifs suivants :



alors, de $f \circ \theta = \theta'$ et $f' \circ \theta' = \theta$, on déduit :

$$f' \circ f \circ \theta = \theta \quad \text{et} \quad f \circ f' \circ \theta' = \theta'.$$

Or $\text{id}_T \circ \theta = \theta$, par suite, la propriété imposée, par construction, au couple (T, θ) implique $f' \circ f = \text{id}_T$; on a de même $f \circ f' = \text{id}_{T'}$, donc f est un isomorphisme de A -modules de T sur T' et $f' = f^{-1}$.

Notation définitive : Le A -module T , appelé **produit tensoriel sur A des A -modules M et N** , est noté $M \otimes_A N$.

L'application A -bilinéaire θ est notée $\otimes$ et pour $(x, y) \in M \times N$, on écrit alors

$$\theta(x, y) = x \otimes y.$$

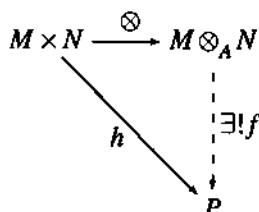
4. Propriété universelle du produit tensoriel

La construction du produit tensoriel $M \otimes_A N$ et la preuve de son unicité, à un isomorphisme près, démontrent le résultat suivant :

Théorème B.3. Propriété universelle

Pour deux A -modules à gauche M et N , il existe, à un isomorphisme près, un unique couple $(M \otimes_A N, \otimes)$, où $M \otimes_A N$ est un A -module à gauche et $\otimes \in \text{Bil}_A(M \times N, M \otimes_A N)$, pour lequel, quels que soient le A -module P et l'application $h \in \text{Bil}_A(M \times N, P)$, il existe un unique morphisme $f \in \text{Hom}_A(M \otimes_A N, P)$ vérifiant $f \circ \otimes = h$.

Le Th. B.3., exprime l'existence et la commutativité du diagramme suivant :



Remarque B.4. Le A-module $M \otimes N$ est engendré par l'ensemble des éléments $x \otimes y$, où $(x, y) \in M \times N$.

En effet, compte tenu des notations utilisées dans la construction du produit tensoriel, on a $M \otimes_A N = F/S$, où F est le A-module libre de base $M \times N$. Par suite, $M \otimes_A N$ est engendré par les éléments

$$\pi \circ \alpha(x, y) = \theta(x, y) = x \otimes y, \quad \text{où } (x, y) \in M \times N.$$

De plus, dans F/S , quels que soient $(x, y) \in M \times N$ et $a \in A$, on a

$$\pi(a(x, y)) = \pi(ax, y) = \pi(x, ay).$$

Par suite, un élément quelconque t du A-module $M \otimes_A N$ s'écrit

$$t = \sum_{1 \leq i \leq n} x_i \otimes y_i, \quad \text{où } n \in \mathbb{N}^* \text{ et } \forall i (1 \leq i \leq n), (x_i, y_i) \in M \times N.$$

En conséquence, tout morphisme de A-modules f défini sur $M \otimes_A N$ sera déterminé par la donnée des $f(x \otimes y)$, pour tous les éléments $(x, y) \in M \times N$.

C. Propriétés du produit tensoriel

Proposition B.5. Pour deux A-modules à gauche M et N , on a

$$M \otimes_A N \simeq N \otimes_A M \quad (\text{isomorphisme de A-modules}).$$

Preuve : Soit h l'application de $M \times N$ dans $N \otimes_A M$ telle que pour tout $(x, y) \in M \times N$,

$$h(x, y) = y \otimes x.$$

On vérifie que h est A-bilinéaire ; d'après le Th. B.3., il existe un unique morphisme $f \in \text{Hom}_A(M \otimes_A N, N \otimes_A M)$ tel que $f \circ \theta = h$, donc pour tout générateur $x \otimes y$ du A-module $M \otimes_A N$, on a

$$f(x \otimes y) = y \otimes x.$$

De la même façon, en considérant l'application h' de $N \times M$ dans $M \otimes_A N$ telle que $h'(y, x) = x \otimes y$, on obtient $f' \in \text{Hom}_A(N \otimes_A M, M \otimes_A N)$ tel que $f' \circ \theta = h'$, d'où pour tout générateur $y \otimes x$ de $N \otimes_A M$,

$$f'(y \otimes x) = x \otimes y.$$

Par suite, $f' \circ f = \text{id}_{M \otimes_A N}$ et $f \circ f' = \text{id}_{N \otimes_A M}$, donc f est un isomorphisme pour lequel $f^{-1} = f'$. $\square$

Proposition B.6. Quels que soient $M \in {}_A\text{Mod}$ et $n > 0$ dans $\mathbb{N}$, on a

$$A^n \otimes_A M \simeq M^n \quad (\text{isomorphisme de A-modules}).$$

Preuve : Considérons le couple (M^n, u) , où u est l'application

$$\begin{aligned} u : A^n \times M &\longrightarrow M^n \\ ((a_i)_{1 \leq i \leq n}, x) &\longmapsto (a_i x)_{1 \leq i \leq n}. \end{aligned}$$

Montrons que le couple (M^n, u) vérifie la propriété universelle du produit tensoriel du A-module à gauche A^n par M (Th B.3.).

Etant donné $P \in {}_A\text{Mod}$ et $h \in \text{Bil}_A(A^n \times M, P)$, considérons l'application

$$\begin{aligned} f : M^n &\longrightarrow P \\ (x_i)_{1 \leq i \leq n} &\longmapsto \sum_{1 \leq i \leq n} h(e_i, x_i), \end{aligned}$$

où $\{e_i\}_{1 \leq i \leq n}$ est la base canonique du A-module à gauche libre A^n ; alors

$$\begin{aligned} (f \circ u)((a_i)_{1 \leq i \leq n}, x) &= f((a_i x)_{1 \leq i \leq n}) = \sum_{1 \leq i \leq n} h(e_i, a_i x) \\ &= h(\sum_{1 \leq i \leq n} a_i e_i, x) = h((a_i)_{1 \leq i \leq n}, x), \end{aligned}$$

d'où $f \circ u = h$. De plus on vérifie facilement l'unicité du morphisme de A -modules f qui rend le diagramme suivant commutatif :

$$\begin{array}{ccc} A^n \times M & \xrightarrow{u} & M^n \\ & \searrow h & \downarrow f \\ & & P \end{array}$$

L'unicité, à un isomorphisme près, du produit tensoriel des A -modules à gauche A^n et M implique $M^n \simeq A^n \otimes_A M$.

Compte tenu de la proposition B.5., on a aussi $M^n \simeq M \otimes_A A^n$ et en particulier, $M \simeq A \otimes_A M \simeq M \otimes_A A$. □

Proposition B.7. *Quels que soient les A -modules à gauche M, N, P , on a*
 $Hom_A(M \otimes_A N, P) \simeq Bil_A(M \times N, P)$ *(isomorphisme de A -modules).*

Preuve : D'après la propriété universelle du produit tensoriel, les applications

$$\begin{aligned} \varphi : Bil_A(M \times N, P) &\longrightarrow Hom_A(M \otimes_A N, P) \\ h &\longmapsto f, \quad \text{tel que } f \circ \otimes = h, \\ \psi : Hom_A(M \otimes_A N, P) &\longrightarrow Bil_A(M \times N, P) \\ f &\longmapsto f \circ \otimes \end{aligned}$$

sont inverses l'une de l'autre, donc φ est une bijection et $\psi = \varphi^{-1}$.

Montrons d'autre part, que ψ est un morphisme de A -modules à gauche. En effet, soit f_1 et f_2 dans $Hom_A(M \otimes_A N, P)$, alors

$$\psi(f_1 + f_2) = (f_1 + f_2) \circ \otimes,$$

et pour tout $(x, y) \in M \times N$,

$$\begin{aligned} ((f_1 + f_2) \circ \otimes)(x, y) &= (f_1 + f_2)(x \otimes y) \\ &= f_1(x \otimes y) + f_2(x \otimes y) \\ &= \psi(f_1)(x, y) + \psi(f_2)(x, y). \end{aligned}$$

d'où $\psi(f_1 + f_2) = \psi(f_1) + \psi(f_2)$.

De plus, pour $f \in Hom_A(M \otimes_A N, P)$, on a, quels que soient $a \in A$ et $(x, y) \in M \times N$,

$$\begin{aligned} (\psi(af))(x, y) &= af(x \otimes y) = a(f(x \otimes y)) \\ &= a(\psi(f))(x, y), \end{aligned}$$

d'où $\psi(af) = a(\psi(f))$. □

Corollaire B.8. *Quels que soient les A -modules à gauche M, N, P , on a*
 $Hom_A(M \otimes_A N, P) \simeq Hom_A(M, Hom_A(N, P))$.

Preuve : D'après la Prop. B.7., il suffit de montrer que les A -modules $Bil_A(M \times N, P)$ et $Hom_A(M, Hom_A(N, P))$ sont isomorphes.

Soit $h \in Bil_A(M \times N, P)$; pour tout $x \in M$, l'application

$$\begin{aligned} h_x : N &\longrightarrow P \\ y &\longmapsto h_x(y) := h(x, y) \end{aligned}$$

est A-linéaire, donc $h_x \in \text{Hom}_A(N, M)$.

D'autre part, pour $f \in \text{Hom}_A(M, \text{Hom}_A(N, P))$, l'application

$$\begin{aligned} M \times N &\longrightarrow P \\ (x, y) &\longmapsto f(x)(y) \end{aligned}$$

est A-bilinéaire. On considère alors les applications :

$$\begin{aligned} \phi : \text{Bil}_A(M \times N, P) &\longrightarrow \text{Hom}_A(M, \text{Hom}_A(N, P)) \\ h &\longmapsto \phi_h \end{aligned}$$

telle que pour tout $x \in M$ et tout $y \in N$,

$$\phi_h(x)(y) = h_x(y) = h(x, y);$$

$$\begin{aligned} \psi : \text{Hom}_A(M, \text{Hom}_A(N, P)) &\longrightarrow \text{Bil}_A(M \times N, P) \\ f &\longmapsto \psi_f \end{aligned}$$

telle que, pour quel que soit $(x, y) \in M \times N$,

$$\psi_f(x, y) = f(x)(y).$$

On vérifie que les applications ϕ et ψ sont A-linéaires et inverses l'une de l'autre, donc ϕ est un isomorphisme de A-modules et $\phi^{-1} = \psi$. $\square$

Proposition B.9. : Associativité du produit tensoriel.

Quels que soient M, N, P dans ${}_A\text{Mod}$, on a

$$(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P).$$

Preuve : Soit h_1 l'application de $(M \otimes_A N) \times P$ dans $M \otimes_A (N \otimes_A P)$ telle que

$$\forall (x, y, z) \in M \times N \times P, \quad h_1((x \otimes y), z) = x \otimes (y \otimes z).$$

h_1 est A-bilinéaire, donc il existe un unique morphisme de A-modules f rendant le diagramme suivant commutatif

$$\begin{array}{ccc} (M \otimes_A N) \times P & \xrightarrow{\otimes} & (M \otimes_A N) \otimes P \\ & \searrow h_1 & \downarrow \exists! f \\ & & M \otimes_A (N \otimes_A P) \end{array}$$

$$\text{d'où, } \forall (x, y, z) \in M \times N \times P, f((x \otimes y) \otimes z) = x \otimes (y \otimes z).$$

De même, avec l'application A-bilinéaire h_2 de $M \times (N \otimes_A P)$ dans $(M \otimes_A N) \otimes P$ telle que

$$\forall (x, y, z) \in M \times N \times P, h_2(x, y \otimes z) = (x \otimes y) \otimes z,$$

on obtient un unique morphisme de A-modules

$$g : M \otimes_A (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes P$$

tel que quel que soit $(x, y, z) \in M \times N \times P$,

$$g(x \otimes (y \otimes z)) = (x \otimes y) \otimes z.$$

Par suite, $f \circ g = \text{id}_{M \otimes_A (N \otimes_A P)}$ et $g \circ f = \text{id}_{(M \otimes_A N) \otimes P}$, d'où le résultat énoncé. $\square$

Remarque B.10. :

a) L'isomorphisme f mis en évidence dans la démonstration précédente permet d'identifier les A-modules $(M \otimes_A N) \otimes_A P$ et $M \otimes_A (N \otimes_A P)$ que l'on désignera par $M \otimes_A N \otimes_A P$.

On écrira alors, pour (x, y, z) dans $M \times N \times P$,

$$(x \otimes y) \otimes z = x \otimes (y \otimes z) = x \otimes y \otimes z.$$

b) L'associativité du produit tensoriel permet de définir, par récurrence, le produit tensoriel d'un nombre fini quelconque de A -modules.

2. Produit tensoriel de morphismes de A -modules

Proposition B.11. Soit M, M', N, N' des A -modules à gauche ; étant donné $f \in \text{Hom}_A(M, M')$ et $g \in \text{Hom}_A(N, N')$, il existe un unique morphisme noté $f \otimes g$, dans $\text{Hom}_A(M \otimes N, M' \otimes N')$, tel que pour tout générateur $(x \otimes y)$ de $M \otimes N$,

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y).$$

Preuve : On considère l'application $h : M \times N \rightarrow M' \otimes_A N'$ telle que

$$\forall (x, y) \in M \times N, h(x, y) = f(x) \otimes g(y).$$

La linéarité des morphismes f et g , ainsi que la bilinéarité de l'application $\otimes$ impliquent que h est bilinéaire. D'après la propriété universelle du produit tensoriel $M \otimes N$, il existe alors un unique $t \in \text{Hom}_A(M \otimes N, M' \otimes_A N')$ tel que le diagramme suivant commute

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_A N \\ & \searrow h & \downarrow \exists! t \\ & & M' \otimes_A N' \end{array}$$

donc $t \circ \otimes = h$. Le morphisme t est noté $f \otimes g$ et appelé **produit tensoriel des morphismes f et g** . On en déduit le résultat énoncé. $\square$

Proposition B.12. Etant donné M, M', M'', N, N', N'' , dans ${}_A \text{Mod}$,

1) Quels que soient $f \in \text{Hom}_A(M, M')$, $g \in \text{Hom}_A(M', M'')$, $h \in \text{Hom}_A(N, N')$ et $k \in \text{Hom}_A(N', N'')$, on a

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h). \quad (\text{B.6})$$

2) Pour f_1, f_2 dans $\text{Hom}_A(M, M')$ et $g \in \text{Hom}_A(N, N')$, on a

$$(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g. \quad (\text{B.7})$$

3) Si $f \in \text{Hom}_A(M, M')$ et g_1, g_2 sont dans $\text{Hom}_A(N, N')$, alors

$$f \otimes (g_1 + g_2) = f \otimes g_1 + f \otimes g_2. \quad (\text{B.8})$$

Démonstration laissée au lecteur.

Corollaire B.13. Quels que soient M, M', N, N' dans ${}_A \text{Mod}$,

$$(M \simeq M' \text{ et } N \simeq N') \implies M \otimes_A N \simeq M' \otimes_A N'.$$

Preuve : Soit ϕ et ψ des isomorphismes de A -modules de M sur M' et N sur N' , respectivement, alors $\phi \otimes \psi \in \text{Hom}_A(M \otimes_A N, M' \otimes_A N')$ et

$$\phi^{-1} \otimes \psi^{-1} \in \text{Hom}_A(M' \otimes_A N', M \otimes_A N).$$

D'après le théorème précédent, on a

$$\begin{aligned} (\phi^{-1} \otimes \psi^{-1}) \circ (\phi \otimes \psi) &= (\phi^{-1} \circ \phi) \otimes (\psi^{-1} \circ \psi) \\ &= \text{id}_M \otimes \text{id}_N = \text{id}_{M \otimes_A N}. \end{aligned}$$

On a de même $(\phi \otimes \psi) \circ (\phi^{-1} \otimes \psi^{-1}) = \text{id}_{M' \otimes_A N'}$, donc $\phi \otimes \psi$ est un isomorphisme de A-modules et $\phi^{-1} \otimes \psi^{-1} = (\phi \otimes \psi)^{-1}$. $\square$

Proposition B.14. $\{M_i\}_{i \in I}$ et $\{N_j\}_{j \in J}$ étant deux familles non vides de A-modules à gauche, alors,

$$(M = \bigoplus_{i \in I} M_i \text{ et } N = \bigoplus_{j \in J} N_j) \implies M \otimes_A N \simeq \bigoplus_{(i,j) \in I \times J} M_i \otimes_A N_j.$$

Preuve : Soit $\{q_i\}_{i \in I}$ et $\{p_i\}_{i \in I}$ (resp. $\{q'_j\}_{j \in J}$ et $\{p'_j\}_{j \in J}$) les injections et projections canoniques associées à la somme directe des $M_i, i \in I$ (resp. $N_j, j \in J$) (Cf. Ch. 3). Pour tout $(i, j) \in I \times J$, on a

$$(p_i \otimes p'_j) \circ (q_i \otimes q'_j) = (p_i \circ q_i) \otimes (p'_j \circ q'_j) = \text{id}_{M_i} \otimes \text{id}_{N_j} = \text{id}_{M_i \otimes_A N_j}.$$

D'autre part, pour tous les couples $(i, k), i \neq k$ et $(j, l), j \neq l$ dans $I \times J$,

$$(p_i \otimes p'_j) \circ (q_k \otimes q'_l) = (p_i \circ q_k) \otimes (p'_j \circ q'_l) = 0.$$

Compte tenu de la propriété qui caractérise une somme directe de A-modules (Ex. 7, Ch. 5), pour montrer que $M \otimes_A N$ est un A-module isomorphe à $\bigoplus_{(i,j) \in I \times J} M_i \otimes_A N_j$, il reste à prouver que pour tout $z \in M \otimes_A N$, on a

$$z = \sum_{(i,j) \in I \times J} ((q_i \otimes q'_j) \circ (p_i \otimes p'_j))(z).$$

Il suffit de montrer cette propriété pour les générateurs du A-module $M \otimes_A N$, c'est-à-dire pour les éléments $x \otimes y$, où $(x, y) \in M \times N$.

Soit $x = (x_i)_{i \in I}$ dans M et $y = (y_j)_{j \in J}$ dans N . On sait que x et y sont à support fini (Cf. Ch. 3) ; on peut écrire

$$x = \sum_{i \in I} q_i(x_i) \quad \text{et} \quad y = \sum_{j \in J} q'_j(y_j),$$

$$\text{d'où} \quad x \otimes y = \sum_{(i,j) \in I \times J} q_i(x_i) \otimes q'_j(y_j) = \sum_{(i,j) \in I \times J} (q_i \otimes q'_j)(x_i \otimes y_j);$$

alors, pour tout $(i, j) \in I \times J$, $(p_i \otimes p'_j)(x \otimes y) = x_i \otimes y_j$; par suite,

$$x \otimes y = \sum_{(i,j) \in I \times J} (q_i \otimes q'_j) \circ (p_i \otimes p'_j)(x \otimes y). \quad \square$$

Corollaire B.15. Soit $F \neq 0$ un A-module à gauche libre de base $\{e_i\}_{i \in I}$ et $N \in {}_A\text{Mod}$; alors tout élément de $F \otimes_A N$ s'écrit de façon unique :

$$\sum_{i \in I} e_i \otimes y_i, \quad \text{où les } y_i \text{ sont presque tous nuls dans } N.$$

(Même propriété pour $N \otimes_A F$.)

Preuve : Il suffit de prouver la propriété pour les générateurs $x \otimes y$ du A-module $F \otimes_A N$.

Soit $(x, y) \in F \times N$; $x \in F$ implique $x = \sum_{i \in I} a_i e_i$, où les a_i sont presque tous nuls dans A.

$$x \otimes y = (\sum_{i \in I} a_i e_i) \otimes y = \sum_{i \in I} (e_i \otimes a_i y).$$

En posant, pour tout $i \in I$, $y_i = a_i y$, on obtient

$$x \otimes y = \sum_{i \in I} (e_i \otimes y_i), \quad (\text{B.9})$$

où les y_i sont presque tous nuls dans N .

Démontrons l'unicité de l'écriture d'un générateur $x \otimes y$ de $F \otimes_A N$, sous la forme (B.9).

D'après la propriété précédente, on a

$$F = \bigoplus_{i \in I} A e_i \implies F \otimes_A N \simeq \bigoplus_{i \in I} (A e_i \otimes N).$$

D'autre part, pour tout $i \in I$, on a $Ae_i \simeq A$; le Cor. B.13. et la Prop. B.6. impliquent alors

$$Ae_i \otimes_A N \simeq A \otimes_A N \simeq N.$$

On en déduit que l'application $\phi : F \otimes_A N \longrightarrow N^{(I)}$, telle que pour tout $i \in I$ et tout $y_i \in N$, $\phi(e_i \otimes y_i) = y_i$ définit un isomorphisme de A -modules. En conséquence,

$$\sum_{i \in I} (e_i \otimes y_i) = 0 \iff \forall i \in I, e_i \otimes y_i = 0 \iff \forall i \in I, y_i = 0,$$

d'où l'unicité de l'expression de $x \otimes y$ sous la forme (B.9). $\square$

Corollaire B.16. Si M et N sont deux A -modules à gauche libres de bases respectives $\{e_i\}_{i \in I}$ et $\{f_j\}_{j \in J}$, alors $M \otimes_A N$ est un A -module libre de base $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$.

Preuve : D'après le Cor. B.15., tout $z \in M \otimes_A N$ s'écrit de façon unique : $z = \sum_{i \in I} e_i \otimes y_i$, où les y_i sont presque tous nuls dans N .

Mais dans N , tout y_i s'écrit de façon unique : $y_i = \sum_{j \in J} a_{ij} f_j$, où les a_{ij} sont presque tous nuls dans A ; par suite

$$z = \sum_{i \in I} (e_i \otimes \sum_{j \in J} a_{ij} f_j) = \sum_{(i,j) \in I \times J} a_{ij} (e_i \otimes f_j).$$

Ainsi les éléments $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$ engendrent le A -module à gauche $M \otimes_A N$; montrons qu'ils forment une famille libre sur A . Compte tenu des hypothèses et des résultats précédents, on a

$$\begin{aligned} \sum_{(i,j) \in I \times J} a_{ij} (e_i \otimes f_j) = 0 &\iff \sum_{i \in I} (e_i \otimes \sum_{j \in J} a_{ij} f_j) = 0 \\ &\iff \forall i \in I, \sum_{j \in J} a_{ij} f_j = 0 \\ &\iff \forall (i, j) \in I \times J, a_{ij} = 0. \end{aligned}$$

On en conclut que $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$ est une base du A -module $M \otimes_A N$. $\square$

Corollaire B.17. Soit K est un corps. Si E et F sont des K -espaces vectoriels, alors $E \otimes_K F$ est un K -espace vectoriel et si E et F sont de dimension finie, on a

$$\dim_K(E \otimes_K F) = (\dim_K E)(\dim_K F).$$

Ce résultat est une conséquence directe du corollaire précédent.

3. Produit tensoriel et suites exactes

Théorème B.18. Etant donné une suite exacte de A -modules à gauche de la forme :

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0, \quad (\text{B.10})$$

pour tout A -module à gauche N , les deux suites ci-dessous sont exactes :

$$M' \otimes_A N \xrightarrow{f \otimes 1_N} M \otimes_A N \xrightarrow{g \otimes 1_N} M'' \otimes_A N \longrightarrow 0 \quad (\text{B.11})$$

$$N \otimes_A M' \xrightarrow{1_N \otimes f} N \otimes_A M \xrightarrow{1_N \otimes g} N \otimes_A M'' \longrightarrow 0. \quad (\text{B.12})$$

Preuve : 1_N désigne l'application id_N . La méthode de démonstration étant la même, pour les suites (B.11) et (B.12), considérons (B.11). L'hypothèse implique $g \circ f = 0$; alors,

$$(g \circ f) \otimes 1_N = 0 = (g \otimes 1_N) \circ (f \otimes 1_N), \quad \text{entraîne}$$

$$\text{Im}(f \otimes 1_N) \subseteq \text{Ker}(g \otimes 1_N). \quad (\text{B.13})$$

D'après la propriété universelle du module quotient $M \otimes_A N / \text{Im}(f \otimes 1_N)$, il existe alors, un unique morphisme de A -modules u tel que le diagramme suivant commute

$$\begin{array}{ccc} M \otimes_A N & \xrightarrow{\pi} & M \otimes_A N / \text{Im}(f \otimes 1_N) \\ & \searrow g \otimes 1_N & \downarrow \exists! u \\ & & M'' \otimes_A N \end{array}$$

c'est-à-dire, $u \circ \pi = g \otimes 1_N$, où π est la surjection canonique.

Démontrons que u est un isomorphisme ; pour cela on construit le morphisme v inverse de u . Par hypothèse, le morphisme g est surjectif, donc pour tout $x'' \in M''$, il existe $x \in M$ tel que $g(x) = x''$; on considère alors la correspondance suivante :

$$\begin{aligned} \phi : M'' \times N &\longrightarrow M \otimes_A N / \text{Im}(f \otimes 1_N) \\ (g(x), y) &\longmapsto \pi(x \otimes y) \end{aligned}$$

Vérifions que ϕ est une application. Soit x et x_1 dans M tels que $x'' = g(x) = g(x_1)$, alors $\pi(x \otimes y) - \pi(x_1 \otimes y) = \pi((x - x_1) \otimes y)$.

Or $(x - x_1) \in \text{Ker } g = \text{Im } f$; de plus f est injectif, donc il existe un unique $x' \in M'$ tel que $(x - x_1) = f(x')$, d'où

$$(x - x_1) \otimes y = f(x') \otimes y = (f \otimes 1_N)(x' \otimes y).$$

Compte tenu de l'inclusion (13), on a $\pi((x - x_1) \otimes y) = 0$, donc ϕ est une application de $M'' \times N$ sur l'ensemble des générateurs du A -module $M \otimes_A N / \text{Im}(f \otimes 1_N)$. D'autre part, on vérifie facilement que ϕ est bilinéaire, par suite, d'après la propriété universelle du produit tensoriel $M'' \otimes_A N$, il existe un unique morphisme v qui rend le diagramme suivant commutatif :

$$\begin{array}{ccc} M'' \times N & \xrightarrow{\otimes} & M'' \otimes_A N \\ & \searrow \phi & \downarrow \exists! v \\ & & M \otimes_A N / \text{Im}(f \otimes 1_N) \end{array}$$

La relation $v \circ \otimes = \phi$ implique que pour tout générateur $x'' \otimes y$ du A -module $M'' \otimes_A N$, on a $v(x'' \otimes y) = \pi(x \otimes y)$, où $g(x) = x''$, par suite,

$$\begin{aligned} (u \circ v)(x'' \otimes y) &= (u \circ \pi)(x \otimes y) \\ &= (g \otimes 1_N)(x \otimes y) = x'' \otimes y, \end{aligned}$$

et pour tout générateur $\pi(x \otimes y)$ du A -module $M \otimes_A N / \text{Im}(f \otimes 1_N)$ on a

$$\begin{aligned} (v \circ u)(\pi(x \otimes y)) &= v((u \circ \pi)(x \otimes y)) \\ &= v \circ (g \otimes 1_N)(x \otimes y) \\ &= v(g(x) \otimes y) = \phi(g(x), y) \\ &= \pi(x \otimes y). \end{aligned}$$

On en conclut que $u \circ v = 1_{M \otimes_A N}$ et $v \circ u = 1_{M \otimes_A N / \text{Im}(f \otimes 1_N)}$, donc u est un isomorphisme et $v = u^{-1}$, d'où

$$M'' \otimes_A N \simeq M \otimes_A N / \text{Im}(f \otimes 1_N)$$

Or, $u \circ \pi = g \otimes 1_N$, u est un isomorphisme, π est surjectif, donc $g \otimes 1_N$ est surjectif et

$$M'' \otimes_A N \simeq M \otimes_A N / \text{Ker}(g \otimes 1_N),$$

$$\text{d'où } M \otimes_A N / \text{Im}(f \otimes 1_N) \simeq M \otimes_A N / \text{Ker}(g \otimes 1_N).$$

En tenant compte de l'inclusion (B.13), on obtient l'égalité :

$$\text{Im}(f \otimes 1_N) = \text{Ker}(g \otimes 1_N);$$

on en déduit que la suite (B.11) est exacte. $\square$

Remarque B.19. Soit M, M', N , dans ${}_A \text{Mod}$; si $f \in \text{Hom}_A(M', M)$ est injectif, les morphismes $f \otimes 1_N$ et $1_N \otimes f$ ne sont pas nécessairement injectifs.

En effet, prenons, par exemple, $M = M' = \mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$ et $f: \mathbb{Z} \rightarrow \mathbb{Z}$ tel que, pour tout $x \in \mathbb{Z}$, $f(x) = 2x$; alors le morphisme de $\mathbb{Z}$ -modules $f \otimes 1_N$ n'est pas injectif, car pour tout générateur $x \otimes y$ de $\mathbb{Z} \otimes N$, on a

$$(f \otimes 1_N)(x \otimes y) = f(x) \otimes y = 2x \otimes y = x \otimes 2y = 0.$$

On a cependant la propriété suivante :

Proposition B.20. M et M' étant des A -modules à gauche, si F est un A -module à gauche libre, alors pour tout morphisme injectif $f \in \text{Hom}_A(M, M')$, les morphismes $f \otimes 1_F$ et $1_F \otimes f$ sont injectifs.

Preuve : Vérifions, par exemple, que $\text{Ker}(1_F \otimes f) = (0)$.

Soit $\{e_i\}_{i \in I}$ une base de F et $z \in F \otimes_A M$ tel que $(1_F \otimes f)(z) = 0$. D'après le Cor. B.15., z s'écrit de façon unique :

$$z = \sum_{i \in I} e_i \otimes x_i, \text{ les } x_i \text{ étant presque tous nuls dans } M,$$

d'où $(1_F \otimes f)(z) = \sum_{i \in I} e_i \otimes f(x_i) = 0$. Toujours selon l'écriture unique d'un élément de $F \otimes_A M'$, on a

$$\sum_{i \in I} e_i \otimes f(x_i) = 0 \implies \forall i \in I, f(x_i) = 0.$$

f étant injectif, on a $x_i = 0$, pour tout $i \in I$, d'où $z = 0$. $\square$

Définition B.21. Un A -module à gauche P est dit **plat**, si quels que soient les A -modules à gauche M et M' , on a, pour tout $f \in \text{Hom}_A(M, M')$,

$$f \text{ injectif} \implies f \otimes 1_P \text{ et } 1_P \otimes f \text{ injectifs.}$$

Remarque B.22. :

a) Selon la Prop. B.20., tout A -module libre est plat, mais la réciproque est fautive ([5]).

b) Si K est un corps, tout K -espace vectoriel est un K -module plat.

4. Restriction et extension des scalaires

A. Restriction des scalaires

Soit A et B deux anneaux unitaires commutatifs ; alors la donnée d'un morphisme d'anneaux unitaires $f \in \text{Hom}(A, B)$ permet de munir tout B -module à gauche N d'une structure de A -module à gauche, la multiplication externe, à opérateurs dans A , étant définie par l'application

$$A \times N \longrightarrow N$$

$$(a, x) \longmapsto ax := f(a)x.$$

Définition B.23. Compte tenu des notations précédentes, on dit que le A-module N est obtenu, à partir du B-module N , par **restriction des scalaires**.

En particulier, la donnée de $f \in \text{Hom}(A, B)$ définit sur B une structure A-module, grâce à l'application

$$\begin{aligned} A \times B &\longrightarrow B \\ (a, b) &\longmapsto ab := f(a)b. \end{aligned}$$

Proposition B.24. Dans le contexte précédent, si N est un B-module de type fini et si B , en tant que A-module à gauche, est de type fini, alors N est un A-module à gauche de type fini.

Démonstration laissée au lecteur.

B. Extention des scalaires

A et B étant deux anneaux unitaires, commutatifs, soit M un A-module à gauche. On suppose B muni d'une structure de A-module à gauche définie, comme plus haut, par la donnée d'un morphisme $f \in \text{Hom}(A, B)$.

Le produit tensoriel $B \otimes_A M$ peut alors être muni d'une structure de B-module à gauche, grâce à l'application

$$\begin{aligned} B \times (B \otimes_A M) &\longrightarrow B \otimes_A M \\ (b, b' \otimes x) &\longmapsto b(b' \otimes x) := bb' \otimes x, \end{aligned}$$

où $b' \otimes x$ est un générateur quelconque du A-module $B \otimes_A M$.

Définition B.25. Compte tenu des hypothèses et notations précédentes, on dit que le B-module $B \otimes_A M$ est obtenu à partir de M , par **extention des scalaires**.

Proposition B.26. Dans le contexte précédent, si M est un A-module de type fini, alors $(B \otimes_A M)$ est un B-module de type fini.

En effet, si $\{x_1, x_2, \dots, x_n\}$ engendre le A-module M , alors $\{1_B \otimes x_i\}_{1 \leq i \leq n}$ engendre le B-module $(B \otimes_A M)$.

5. Produit tensoriel de A-algèbres

Remarque B.27. Soit R une A-algèbre. L'application

$$\begin{aligned} \alpha : R \times R &\longrightarrow R \\ (x, y) &\longmapsto xy \end{aligned}$$

qui définit la multiplication de l'anneau unitaire R est A-bilinéaire ; par suite (Th. B.3.), il existe un unique morphisme $\beta \in \text{Hom}_A(R \otimes_A R, R)$ tel que

$$\forall (x, y) \in R \times R, \quad \beta(x \otimes y) = xy.$$

D'autre part, l'élément unité 1_R de R détermine le morphisme de A-modules

$$\begin{aligned} u :_A A &\longrightarrow R \\ a &\longmapsto a 1_R; \end{aligned}$$

on en déduit que R est isomorphe aux A -modules $A \otimes_A R$ et $R \otimes_A A$ par

$$\begin{aligned} \mu : A \otimes_A R &\longrightarrow R & \text{et} & & \mu' : R \otimes_A A &\longrightarrow R \\ a \otimes x &\longmapsto ax & & & x \otimes a &\longmapsto xa. \end{aligned}$$

d'où le diagramme commutatif suivant

$$\begin{array}{ccccc} A \otimes_A R & \xrightarrow{\mu} & R & \xleftarrow{\mu'} & R \otimes_A A \\ \downarrow u \otimes id_R & & \downarrow id_R & & \downarrow id_R \otimes u \\ R \otimes_A R & \xrightarrow{\beta} & R & \xleftarrow{\beta} & R \otimes_A R \end{array}$$

Réciproquement, si M est un A -module à gauche et s'il existe des morphismes de A -modules $\beta : M \otimes_A M \longrightarrow M$ et $u : A \longrightarrow M$ tels que le diagramme suivant commute

$$\begin{array}{ccccc} A \otimes_A M & \xrightarrow{\mu} & M & \xleftarrow{\mu'} & M \otimes_A A \\ \downarrow u \otimes id_M & & \downarrow id_M & & \downarrow id_M \otimes u \\ M \otimes_A M & \xrightarrow{\beta} & M & \xleftarrow{\beta} & M \otimes_A M \end{array}$$

alors M est muni d'une structure de A -algèbre dont la multiplication interne est définie par l'application

$$\begin{aligned} M \times M &\longrightarrow M \\ (x, y) &\longmapsto xy := \beta(x \otimes y). \end{aligned}$$

L'élément unité de l'anneau M est alors $u(1_A)$.

Produit tensoriel de deux A -algèbres

Soit R et S deux A -algèbres ; posons $T = R \otimes_A S$ et montrons que l'on munir le A -module T d'une structure de A -algèbre.

Considérons l'application

$$\begin{aligned} \lambda : R \times S \times R \times S &\longrightarrow T \\ (x, y, x', y') &\longmapsto xx' \otimes yy'. \end{aligned}$$

λ est linéaire par rapport à chacune des composantes x, y, x', y' ; d'après la propriété universelle du produit tensoriel généralisé à un nombre fini quelconque de A -modules, il existe un unique morphisme

$$\begin{aligned} \beta : R \otimes_A S \otimes_A R \otimes_A S &\longrightarrow T \\ x \otimes y \otimes x' \otimes y' &\longmapsto xx' \otimes yy'. \end{aligned}$$

On a $R \otimes_A S \otimes_A R \otimes_A S = T \otimes T$. D'autre part, R et S sont des A -algèbres ; d'après la remarque B.27. en utilisant le morphisme

$$\begin{aligned} u : A &\longrightarrow T = R \otimes_A S \\ a &\longmapsto a(1_R \otimes 1_S), \end{aligned}$$

on munit le A-module T d'une structure de A-algèbre, dont la multiplication interne est définie par

$$\begin{aligned} T \times T &\longrightarrow T \\ (x \otimes y, x' \otimes y') &\longmapsto xx' \otimes yy' \end{aligned}$$

et l'élément unité est $u(1_A) = 1_R \otimes 1_S$.

Ainsi le produit tensoriel de deux A-algèbres est une A-algèbre.





Bibliographie

- [1] Arnaudès J.M., Bertin J., *Groupes, Algèbres et Géométrie*, T.1, Ellipses, 1993.
- [2] Arnaudès J.M., Fraysse H., *Cours de Mathématiques-I, Algèbre*, Dunod, 1987.
- [3] Arnold J.T., *Prime ideals in Power series rings*, Preprint, Virginia Polytechnic Institute and State University.
- [4] Artin M., *Algebra*, Prentice Hall, 1991.
- [5] Atiyah M.F., Macdonald I.G., *Introduction to Commutative Algebra*, Wesley Publishing Company, 1969.
- [6] Auslander M., Buchsbaum D., *Groups, Rings, Modules*, Harper and Row, 1974.
- [7] Bhattacharya P.B., Jain S.K., Nagpaul S.R., *Basic Abstract Algebra*, Cambridge University Press, 1986.
- [8] Blanchard A., *Les corps non commutatifs*, P.U.F., 1972.
- [9] Bourbaki N., *Algèbre*, Ch. 1 à 3, Hermann, 1970.
- [10] Bouvier A. et George M., *Dictionnaire des Mathématiques*, P.U.F. 1979.
- [11] Calais J., *Éléments de Théorie des groupes*, P.U.F., 1984 (3^{ème} éd., 1998)
- [12] Chenciner A., *Courbes algébriques planes*, Publication mathématique de l'Université de Paris VII, 1979.
- [13] Chih-Han Sah, *Abstract algebra*, Academic Press 1967.
- [14] Cohn P.M., *Algebra, Vol. 1*, John Wiley and Sons, 1974.
- [15] Cohn P.M., *Algebra, Vol. 2*, John Wiley and Sons, 1977.
- [16] Comtet L., *Analyse Combinatoire*, t.1, t.2, P.U.F., 1970.
- [17] Dixmier J., *Topologie Générale*, P.U.F., 1981.
- [18] Eisenbud D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.
- [19] Ellis G., *Rings and Fields*, Carendon Press, 1992.
- [20] Faith C., *Algebra : Rings, Modules and categories, I*, Springer-Verlag, 1973.
- [21] Francinon S., Gianella H., *Exercices de mathématiques pour l'Agrégation, Algèbre I*, Masson, 1995.
- [22] Fresnel J., *Algèbre des Matrices*, Hermann, 1997.
- [23] Fulton W., *Algebraic Curves*, Benjamin, Inc., 1969.
- [24] Gilmer R., *A note on the quotient field of the domain $D[[X]]$* , Proc. Amer. Math. Soc. 18 (1967), 1138-1140.
- [25] Gilmer R., *Multiplicative ideal theory*, Marcel Dekker, 1972.
- [26] Godement R., *Cours d'Algèbre*, Hermann, 1966.
- [27] Gray M., *A Radical approach to Algebra*, Addison-Wesley Publ. Comp. 1970.
- [28] Hardy G.H. and Wright E.M., *An introduction to the Theory of Numbers*, Oxford, 1962.
- [29] Hartley B., Hawkes T.O., *Rings, Modules and Linear algebra*, Chapman and Hall, 1970.
- [30] Hellegouarch Y., *Invitation aux mathématiques de Fermat-Wiles*, Masson, 1997.
- [31] Herstein I.N., *Topics in Algebra*, Xerox College Publishing, 1964.

- [32] Hungerford T.H., *Algebra*, Holt, Rinehart and Winston, Inc., 1974.
- [33] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 2^{ème} Ed. 1992.
- [34] Jacobson N., *Basic Algebra I*, W.H. Freeman and Company, 1974.
- [35] Jacobson N., *Basic Algebra II*, W.H. Freeman and Company, 1980.
- [36] Kaplansky I., *Commutative Rings*, The University of Chicago Press, 2^{ème} Ed. 1974.
- [37] Kunz E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.
- [38] Lafon J.P., *Les formalismes fondamentaux de l'Algèbre Commutative*, Hermann, 1974.
- [39] Lang S., *Algebra*, Addison-Wesley, 1967.
- [40] Leichtname E., Schauer X., *Exercices corrigés de mathématiques, t. 1, Algèbre I*, Ellipses 1988.
- [41] Lelong-Ferrand J., Arnaudis J.M., *Cours de mathématiques, t. 1, Algèbre*, Dunod, 1971.
- [42] Lesieur L., Meyer Y., Joulain C., Lefebvre J., *Algèbre générale*, Armand Colin, 1975.
- [43] Mc Coy N.H., *The Theory of Rings*, The Macmillan Comp., 1968.
- [44] Mac Lane S., Birkhoff G., *Algèbre, t. 1, t. 2*, Gauthier-Villars, 1970, 1978.
- [45] Merindol J.Y., *Symbole de Legendre et résultant*, Revue de mathématiques spéciales, Vuibert, mai-juin 1997.
- [46] Naudin P., Quitté C., *Algorithmique algébrique*, Masson, 1992.
- [47] Parent D.P., *Exercices de Théorie des nombres*, Bordas, 1978.
- [48] Perrin D., *Cours d'Algèbre*, Ellipses, 1996.
- [49] Queysanne M., *Algèbre*, Armand Colin, 1964.
- [50] Ramis E., Deschamps C., Odoux J., *Cours de Mathématiques Spéciales, 1 : Algèbre*, Masson, 1974.
- [51] Ribenoim, P., *Algebraic Numbers*, Wiley-Interscience, 1972.
- [52] Ribenoim P., *Nombres Premiers : mystères et records*, P.U.F., 1994.
- [53] Ruaud J.F., Warusfel A., *Exercices de Mathématiques pour l'Agrégation, Algèbre 3*, Masson, 1995.
- [54] Samuel P., *Anneaux Factoriels*, Soc. Math. de Sao Paulo, 1963, p. 61.
- [55] Samuel P., *Théorie Algébrique des Nombres*, Hermann, 1967.
- [56] Schubert H., *Categories*, Springer-Verlag, 1972.
- [57] Stewart I.N. and Tall D.O., *Algebraic Number Theory*, Chapman and Hall, 1979.
- [58] Stewart I., *Galois Theory*, Chapman and Hall, 1973.
- [59] Tauvel P., *Mathématiques Générales pour l'Agrégation*, Masson, 1993.
- [60] Van der Waerden B.L., *Algebra*, vol. 1 et 2, Frederick Ungar, 1970.
- [61] Warner S., *Modern Algebra*, Dover Publications, Inc., 1990.
- [62] Zariski O., Samuel P., *Commutative Algebra*, vol. I, Van Nostrand Reinhold Comp., 1958.
- [63] Zariski O., Samuel P., *Commutative Algebra*, vol. II, Springer-Verlag, 1960.

Index

A

algèbre (A-algèbre), 3.81.

anneau, 1.1.

- artinien, Ex. 17, Ch. 2.
- booléen, 2.95.
- commutatif, 1.1.
- à division, 1.6.
- euclidien, 5.70.
- factoriel, 5.87.
- intègre, 1.21.
- local, 2.73.
- noethérien, 2.81.
- nul, 1.1.
- principal, 2.8.
- quotient, 2.27.
- total de fractions, 6.7.
- unitaire, 1.1.

annulateur,

- d'une partie d'un anneau, 1.44.
- d'une partie d'un A-module, 3.4.

associé (élément —) 5.11.

automorphisme,

- d'anneaux, 1.63.
- de A-modules, 3.34.

B

base (d'un A-module libre), 3.62.

Bezout (théorème de —) A.31.,

et 5.48.

(relation de —) A.31.

et 5.50.

bimodule, 3.2.

Boole (anneau de —) Ex. 15, Ch. 1.

C

caractéristique, 1.68.

centre d'un anneau, 1.32.

coefficient (d'un polynôme), 4.10.

— directeur, 4.10.

composante homogène, 4.67.

condition,

- de chaîne ascendante, 2.79.
- maximale 2.79.

congruence (dans $\mathbb{Z}$), A.9.

contenu, 5.100.

copie d'un A-module, rel. (3.7)

corps, 1.7.

- algébriquement clos, 4.42.
- commutatif, 1.6.
- de fractions, 5.2.
- gauche, 1.6.
- des quaternions, 1.17.
- résiduel, 2.78.

D

degré (d'un polynôme), 3.58.

- partiel, 4.61.
- total, 4.63.

dénombrable (ensemble —), 3.58.

développement en série formelle,

7.37.

discriminant, 8.12.

— d'un polynôme, 8.50.

diviseur,

- dans $\mathbb{Z}$, A.1.
- dans un anneau, 5.9.
- de zéro, 1.19.

division

- dans $\mathbb{Z}$, A.7.
- euclidienne, 5.71.
- euclidienne des polynômes, 4.33.

- suivant les puissances croissantes, 4.52.

domaine,

- d'intégrité, 1.21.
- principal, 2.7.
- pseudo-bezoutien, Ex. 28, Ch. 5.

E

Eisenstein (critère d'—), 5.112.

élément

- inversible, 1.9.
- irréductible, 5.16.
- premier, 5.20.
- régulier, 6.2.
- unité, 1.1

élimination (problème d'—), 8.55.

endomorphisme,

- de A-algèbres, 3.85.
- d'anneaux, 1.49.
- de A-modules, 3.27.

épimorphisme d'anneaux, Ex. 16,
Ch. 1.

équivalence, 5.14.

Euclide,

- (théorème d'—), A.12.
- (algorithme d'—), Ch. 5.

extension des scalaires, B.25.

F

facteur direct, 3.25.

factorisation (dans $\mathbb{Z}$), A.1.

Fermat (petit théorème de —), A.35.

fidèle (A-module —), 3.10.

fonction,

- polynôme, 4.21.
- rationnelle 8.32.
- formellement symétrique, 8.32.
- numériquement symétrique, 8.33.

formule,

- du binôme, 1.4.
- d'interpolation de Lagrange, Ex. 13., Ch. 5.

fraction, 5.1.

- rationnelle, 5.4.
- rationnelle symétrique, 8.26.

G

Gauss (anneau des entiers de —),
1.31.
(théorème de —), A.32.
et 5.45.

H

Hamilton W., 3.98.

Hilbert (théorème de—), 4.72.

I

idéal, 1.42.

- irréductible, Ex. 16, Ch. 2.
- maximal, 2.60.
- premier, 2.50.
- primaire, Ex. 15, Ch. 2.
- principal, 2.5.
- propre, 1.45.
- de type fini, 2.5.

idéaux,

- copremiers, 2.42.
- étrangers, 2.42.

idempotent (élément —), 1.28.

image,

- d'un morphisme, 1.52.
- homomorphe, 1.55.

inductif (ensemble —), 2.69.

indéterminée, 4.2.

isomorphisme,

- d'anneaux, 1.61.
- de A-modules, 3.34.

J

Jacobson (radical de —), 2.90.

L

localisé,

- d'un anneau, 6.3.
- d'un A-module, 6.27.

M

module (A-module), 3.1.

- libre, 3.62.
- monogène, 3.18.
- noétérien, 3.75.
- plat, B.21.
- quotient, 3.37.
- de type fini, 3.18.

monôme, 4.10. et 4.55.

- directeur, 8.4.

monomorphisme d'anneaux,

Ex. 16, Ch. 1.

morphisme,

- de A-algèbres, 3.85.
- d'anneaux 1.49.
- d'anneaux unitaires, 1.51.
- de A-modules, 3.27.
- nul, 1.57.

N

Newton,

- formules de —, 8.22.
- sommes de —, 8.12.

nilpotent (élément —), 1.26.

nilidéal, 2.94.

nilradical, 2.87.

nombre premier, A.5.

nombres décimaux, 6.7.

norme (d'un quaternion), 3.95.

noyau (d'un morphisme), 1.52.

O

ordre,

- lexicographique, 8.2.
- de multiplicité d'une racine, 4.41.
- d'une série formelle, 7.4.

P

partie multiplicative (Ex. 10, Ch. 2),
et 6.1.

- saturée, Ex. 11, Ch. 2.

p.g.c.d., 5.27.

p.p.c.m., 5.51.

poids d'un polynôme à n ind., 8.17.

polynôme,

- à une indéterminée, 4.2.
- à n indéterminées, 4.55.
- composé, 4.15.
- constant, 4.10.
- dérivé, 4.24.
- dérivé à l'ordre k , 4.30.
- homogène, 4.67.
- primitif, 5.102.
- scindé, 4.46.
- symétrique, 8.7.

préordre, 5.14.

produit d'idéaux, 2.11.

produit direct,

- d'anneaux, 1.74.
- de A-modules, 3.44.

propriété universelle,

- d'un anneau quotient, 2.31.
- d'un anneau de polynômes à une indéterminée, 4.6.
- d'un anneau de polynômes à n indéterminées, 4.57.
- du corps des fractions d'un D.I., 5.5.
- du localisé d'un anneau, 6.9.
- d'un A-module libre, 3.67.
- d'un module quotient, 3.39.

- d'un produit direct d'anneaux, 1.81.
- d'un produit direct de A-modules, 3.46.
- d'un produit tensoriel, B.3.
- d'une somme directe de A-modules, 3.52.

Q

- quaternion, 1.17.
- pur, 3.91.

R

- racine (d'un polynôme) 4.18.
- simple, 4.41.
 - multiple, 4.41.
- radical d'un idéal, Ex. 14, Ch. 2.
- rang (d'un A-module libre), 3.66.
- relations entre coefficients et racines, d'un polynôme, 8.24.
- restriction des scalaires, B.23.
- résultant, 8.41.

S

- série formelle, 7.1.
- composée, 7.18.
 - rationnelle, 7.37.
- série de Laurent, Ex. 4, Ch. 7.
- somme,
- d'idéaux, 2.12.
 - directe d'idéaux, 2.17.
 - de sous-modules, 3.19.
 - directe de sous-modules, 3.23.
 - directe de A-modules, 3.50.
- sommable (famille), 7.10.
- sous-anneau, 1.29.
- unitaire, 1.34.
 - engendré par une partie, 1.38.
- sous-algèbre, 3.83.
- sous-module, 3.6.
- spectre (premier), 2.59.

- suite exacte, 3.70.
- courte, 3.72.
- supplémentaires (sous-modules —), 3.25.
- support, 3.49.
- support fini (à —) 3.49.
- stathme, 5.70.
- Sylvester (déterminant de —), 8.41.

T

- tensoriel (produit —), App.B.
- théorème,
- de factorisation unique dans $\mathbb{Z}$, A.11.
 - fondamental de l'arithmétique, A.10.
 - d'isomorphisme d'anneaux, 2.34., 2.39., 2.41.
 - d'isomorphisme de A-modules, 3.40., 3.41., 3.43.
- trace (d'un quaternion), 3.95.
- transformée (d'une équation), 8.57.

U

- unité d'un anneau, 1.7.

V

- Vandermonde (déterminant de —), Ex. 8, Ch. 8.
- valuation p-adique dans $\mathbb{Z}$, A.15.

W

- Wedderburn (théorème de —), 1.25.
- Wilson (théorème de —), A.36.

Z

- Zariski (topologie de —), Ex. 18, Ch. 2.
- Zorn (axiome de —), 2.69.





Achevé d'imprimer sur les presses de l'Imprimerie BARNÉOUD

B.P. 44 - 53960 BONCHAMP-LÈS-LAVAL

Dépôt légal : mai 2006 - N° d'imprimeur : 605.004

Imprimé en France

La collection *Mathématiques à l'Université* se propose de mettre à la disposition des étudiants de troisième, quatrième et cinquième années d'études supérieures en mathématiques des ouvrages couvrant l'essentiel des programmes actuels des universités françaises. Certains de ces ouvrages pourront être utiles aussi aux étudiants qui préparent le CAPES ou l'agrégation, ainsi qu'aux élèves des grandes écoles.

Nous avons voulu rendre ces livres accessibles à tous : les sujets traités sont présentés de manière simple et progressive, tout en respectant scrupuleusement la rigueur mathématique. Chaque volume comporte un exposé du cours avec des démonstrations détaillées de tous les résultats essentiels et de nombreux exercices. Les auteurs de ces ouvrages ont tous une grande expérience de l'enseignement des mathématiques au niveau supérieur.

Ce livre, d'abord destiné aux étudiants de licence et de maîtrise de mathématiques, contient l'essentiel des connaissances de base de la théorie des anneaux commutatifs ; il doit donc intéresser les candidats à l'agrégation de mathématiques et les élèves des classes préparatoires aux grandes écoles scientifiques.

Chaque chapitre est suivi d'exercices ou problèmes qui mettent en relief les principaux résultats du cours ou les complètent.

Josette Calais est Professeur émérite à l'Université de Reims-Champagne-Ardenne. Elle est l'auteur des *Éléments de théorie des groupes*, publié aux Presses Universitaires de France.



ISBN 2-7298-2779-X