

# Algèbre

## Manuscrit Personnel

Stilianos Louca

7 juin 2014

---

### Table des matières

<b>1 Anneaux, idéaux, algèbres</b>	<b>6</b>
1.1 Anneaux	6
1.1.1 Définition : Monoïde	6
1.1.2 Définition : Monoïde produit	6
1.1.3 Définition : Anneau	6
1.1.4 Définition : Anneau produit	7
1.1.5 Définition : Diviseur de zéro	7
1.1.6 Définition : Anneau intègre	7
1.1.7 Définition : Inversibilité	8
1.1.8 Définition : Élément irréductible	8
1.1.9 Définition : Élément nilpotent	8
1.1.10 Définition : Élément central, centre	8
1.1.11 Définition : Sous-anneau	8
1.1.12 Définition : Morphisme d'anneaux	8
1.1.13 Lemme sur l'anneau des endomorphismes	9
1.1.14 Définition : Anneau euclidien	9
1.1.15 Lemme sur la division dans anneaux euclidiens	10
1.1.16 Le morphisme de Frobenius	10
1.2 Idéaux	10
1.2.1 Définition : Idéal	10
1.2.2 Définition : Anneau simple	11
1.2.3 Lemme : Stabilité des idéaux sous morphismes	11
1.2.4 Définition : L'idéal engendré	11
1.2.5 Lemme : Invariance de générateurs sous morphismes	11
1.2.6 Proposition : Représentation de $\langle X \rangle$	11
1.2.7 Définition : Idéal & anneau principal	11
1.2.8 Définition : Idéal de type fini	12
1.2.9 Idéaux engendré par idéaux	12
1.2.10 Lemme : Idéaux des endomorphismes sur un espace vectoriel	12
1.2.11 Définition : Anneau quotient	13
1.2.12 Théorème : Factorisation des morphismes	13
1.2.13 Théorème d'isomorphismes d'anneaux	14
1.2.14 Lemme : Transitivité des quotients	15
1.2.15 Définition : Idéal premier	15
1.2.16 Définition : Topologie de Zariski	16
1.2.17 Définition : Idéal maximal	16
1.2.18 Lemme : Caractérisation des idéaux maximaux	16
1.2.19 Théorème de Krull : Existence des idéaux maximaux	16
1.2.20 Lemme sur idéaux maximaux et premiers	17
1.2.21 Théorème : Idéaux maximaux et anneaux locaux	18
1.2.22 Lemme sur parties multiplicatives	18
1.2.23 Corollaire	18

1.2.24	Exemple : Les fonctions continues	18
1.2.25	Théorème des restes chinois	19
1.3	Anneaux Noetheriens	21
1.3.1	Definition : Anneau Noetherien	21
1.3.2	Théorème : Caractérisation des anneaux noetheriens	21
1.3.3	Lemme : Anneaux quotients des anneaux noetheriens	21
1.4	Algèbres	21
1.4.1	Definition : $R$ -Algèbre	21
1.4.2	Definition : Morphisme de $R$ -algèbres	22
<b>2</b>	<b>Modules</b>	<b>23</b>
2.1	Modules	23
2.1.1	Definition : Opération d'un anneau sur un groupe, module	23
2.1.2	Definition : Module simple	23
2.1.3	Definition : Morphisme d'un module	23
2.1.4	Definition : Module quotient	24
2.1.5	Théorème : Universalité d'un module quotient	25
2.1.6	Lemme : Sous-modules de modules quotients	25
2.1.7	Le théorème d'isomorphismes pour modules	26
2.1.8	Corollaire du théorème d'isomorphismes	26
2.1.9	Definition : Sous-module engendré	27
2.1.10	Definition : Module noetherien	27
2.1.11	Théorème : Caractérisation des modules noetheriens	28
2.1.12	Definition : Suite exacte	28
2.1.13	Lemme sur modules de type fini et suites exactes	28
2.1.14	Corollaire sur modules de type fini	29
2.1.15	Lemme sur modules noetheriens et suites exactes	29
2.1.16	Corollaire sur puissances d'anneaux noetheriens	29
2.1.17	Corollaire sur modules de type fini et modules noetheriens	30
2.1.18	Definition : Torsion	30
2.1.19	Definition : Annulateur	31
2.1.20	Exemple : Le corps quotient	31
2.1.21	Definition : Produit direct et somme directe des modules	32
2.1.22	Definition : Somme directe de sous-modules	32
2.2	Modules libres	33
2.2.1	Definition : Base et module libre	33
2.2.2	Definition : Génératrice minimale et système indépendant maximal	33
2.2.3	Lemme : Modules libres de type fini	34
2.2.4	Lemme : Structure des modules libres	34
2.2.5	Lemme : Existence de supplémentaires	34
2.2.6	Corollaire sur morphismes surjectifs	35
2.2.7	Corollaire sur modules quotients libres	35
2.2.8	Lemme : Existence de morphismes de modules	35
2.2.9	Definition : Matrices de morphismes de $A$ -modules	36
2.2.10	Lemme : Bases de corps quotients	36
2.2.11	Théorème : Cardinalité des bases finies	36
2.2.12	Lemme sur bases des sommes directes	37
2.2.13	Lemme : Condition suffisante pour modules libres	37
2.2.14	Exemple d'un $\mathbb{K}[X]$ -module	37
2.2.15	Exemple : Le $\mathbb{Z}$ -module $\mathbb{Z}[p^{-1}]$	38
2.2.16	Exemples de modules libres et non libres	39
2.2.17	Lemme sur espaces vectoriels de dimension finie	39

<b>3</b>	<b>Polynômes et séries formelles</b>	<b>40</b>
3.1	Polynômes	40
3.1.1	Definition : Algèbre	40
3.1.2	Definition : Algèbre graduée	40
3.1.3	Definition : Algèbre quotient	40
3.1.4	Definition : L'anneau des polynômes	40
3.1.5	Théorème : La propriété universelle	41
3.1.6	Corollaire : Morphismes de $A$ -algèbres de $A[S]$	43
3.1.7	Théorème : Produits des algèbres des polynômes	43
3.1.8	Corollaire : Produits d'algèbres des polynômes	44
3.1.9	Definition : L'ordre lexicographique & monômial	44
3.1.10	Definition : Degré des polynômes dans $A[S]$	45
3.1.11	Lemme : Le degré comme morphisme de monoïdes	46
3.1.12	Corollaire sur les polynômes inversibles	46
3.1.13	Definition : Racines et polynôme scindés	47
3.1.14	Théorème : Factorisation de polynômes	47
3.1.15	Corollaire : Factorisation de polynômes	48
3.1.16	Lemme sur polynômes linéairement indépendants	49
3.1.17	Lemme sur bases de polynômes	49
3.2	Idéaux dans $A[S]$	49
3.2.1	Definition : Idéal monômial dans $A[S]$	49
3.2.2	Lemme sur idéaux monômiaux	50
3.2.3	Théorème sur anneaux noetheriens	50
3.2.4	Exemple : $\mathbb{Z}[X]$	51
3.2.5	Corollaire : Théorème de la base de Hilbert	51
3.2.6	Caractérisation d'algèbres de polynômes principaux	52
3.2.7	Fonctions polynomiales	52
3.2.8	Théorème : Fonctions polynomiales sur corps infinis	53
3.2.9	Application : Principe de prolongement des identités algébriques	53
3.2.10	Théorème : Fonctions polynomiales sur corps de type $\mathbb{Z}/p\mathbb{Z}$	54
3.2.11	Théorème : Idéaux dans $A[X]$	54
3.2.12	Lemme : L'anneau $\mathbb{K}[X]$ comme anneau euclidien	54
3.2.13	Lemme : Anneaux quotient dans $\mathbb{K}[X]$	54
3.3	Dérivation de polynômes	54
3.3.1	Definition : Opérateur de différences	54
3.3.2	Lemme sur l'opérateur de différences et polynômes constants	55
3.3.3	Definition : Coefficient binomial	55
3.3.4	Definition : Dérivée d'un polynôme	55
3.3.5	Caractérisation des polynômes constants	56
3.4	Polynômes invariants sous un groupe fini	56
3.4.1	Definition : Groupe linéaire générale	56
3.4.2	Lemme sur l'action des sous-groupes de $GL_n(A)$	56
3.4.3	Exemple : Action du groupe symétrique	56
3.4.4	Partitions et diagrammes de Young	57
3.4.5	Definition : Monômes symétriques	58
3.4.6	Lemme : Engendrement des polynômes symétriques	59
3.4.7	Lemme : Représentation des polynômes symétriques	60
3.4.8	Théorème des polynômes symétriques	60
3.4.9	Algorithme sur la représentation des polynômes symétriques	61
3.4.10	Exemple : Les sommes de Newton	62
3.4.11	Corollaire sur polynômes symétriques et sous-anneaux	63
3.4.12	Exemple : Polygones réguliers dans $\mathbb{C}$	63
3.4.13	Exemple : Caractérisation des polynômes caractéristiques	65
3.4.14	Definition : Polynôme antisymétrique	66
3.4.15	Lemme : Représentation des polynômes antisymétriques	66
3.5	Séries formelles	66
3.5.1	Definition : Algèbre des séries formelles	66

3.5.2	Definition : Valuation d'une série formelle	67
3.5.3	Lemme : La valuation comme morphisme de monoïdes	67
3.5.4	Definition : Famille de séries sommable	67
3.5.5	Definition : Composition des séries formelles	68
3.5.6	Lemme : Inversibilité des séries formelles	68
3.5.7	Corollaire sur séries formelles inversibles par rapport à la multiplication	69
3.5.8	Lemme : Caractérisation des idéaux dans $\mathbb{K}[[X]]$	69
3.5.9	Lemme : Idéaux engendrés dans $\mathbb{K}[[X]]$	69
3.5.10	Lemme sur la valuation	70
3.5.11	Definition : Séries formelles inversibles par rapport à la composition	70
3.5.12	Théorème de la fonction inverse	70
3.5.13	Corollaire sur séries formelles inversibles par rapport à la composition	71
3.5.14	Definition : Dérivée d'une série formelle	72
3.5.15	Propriétés élémentaires de la dérivée	72
3.5.16	Lemme ; Caractérisation des séries formelles constantes	72
3.5.17	Exemple : Inverse de la série exponentielle	72
3.5.18	Lemme sur puissances de polynômes	73
3.5.19	Développement en séries formelles d'une fraction rationnelle	74
3.5.20	Lemme : Le corps des fractions de $\mathbb{K}[[X]]$	74
<b>4</b>	<b>Anneaux factoriels</b>	<b>76</b>
4.1	Préliminaires	76
4.1.1	Definition : Élément irréductible	76
4.1.2	Definition : Éléments associés	76
4.1.3	Definition : Élément premier	76
4.1.4	Definition : Anneau factoriel	77
4.1.5	Lemme de Gauss sur anneaux intègres, principaux	77
4.1.6	Lemme : Chaîne des inclusions de classes des anneaux intègres	77
4.1.7	Caractérisation des anneaux factoriels	78
4.1.8	Corollaire : Factorisation de produits	78
4.1.9	Definition : pgcd et ppcm	78
4.1.10	Théorème de Bachet-Bézout	79
4.2	Factorialité d'algèbres des polynômes	80
4.2.1	Definition : Polynôme primitif	80
4.2.2	Definition : Réduction d'un polynôme	80
4.2.3	Lemme : Caractérisation des polynômes primitifs	80
4.2.4	Lemme de Gauss sur le contenu de polynômes	81
4.2.5	Lemme : Division dans $R[X]$ et $\mathbb{K}[X]$	81
4.2.6	Lemme : Polynômes comme diviseurs	82
4.2.7	Théorème : Factorialité de $A[X_1, \dots, X_n]$	82
4.2.8	Lemme : Division euclidienne dans $\mathbb{K}[X]$	84
4.2.9	Lemme : Changement de <i>variables</i> dans polynômes	84
4.2.10	Le critère d'Eisenstein pour l'irréductibilité dans $\mathbb{Q}[X]$	84
4.2.11	Le critère d'Eisenstein pour le cas général	86
4.2.12	Exemple : Irréductibilité de $X^2 - a$	86
<b>5</b>	<b>Extensions de corps</b>	<b>87</b>
5.1	Préliminaires	87
5.1.1	Definition : Extension d'un corps	87
5.1.2	Lemme : Polynômes premiers entre eux	87
5.1.3	Lemme : Caractéristique d'un anneau intègre	87
5.1.4	Definition : Corps engendré	88
5.1.5	Éléments algébriques	88
5.1.6	Lemme sur la dérivée du polynôme minimal	89
5.1.7	Lemme : Anneaux quotients sur polynômes irréductibles	90
5.2	Morphismes et Automorphismes	90
5.2.1	Definition : $\mathbb{K}$ -morphisme	90
5.2.2	Lemme sur $\mathbb{K}$ -automorphismes de corps	91

5.2.3	Théorème : Éléments algébriques et $\mathbb{K}$ -morphisms $\mathbb{K}[x] \rightarrow \mathbb{E}$ . . . . .	91
5.2.4	Corollaire sur le nombre de $\mathbb{K}$ -morphisms de corps $\mathbb{K}[x] \rightarrow \mathbb{E}$ . . . . .	92
5.2.5	Théorème : Existence du corps de décomposition . . . . .	92
5.2.6	Définition : Corps algébriquement clos . . . . .	93
5.2.7	Théorème : Existence d'une clôture algébrique . . . . .	93
5.2.8	Définition : Polynôme séparable . . . . .	93
5.2.9	Lemme : Separabilité de polynômes irréductibles . . . . .	93
5.2.10	Théorème d'Artin sur l'indépendance des $\mathbb{K}$ -morphisms de corps . . . . .	94
5.2.11	Corollaire sur le nombre des $\mathbb{K}$ -morphisms de corps . . . . .	94
5.2.12	Lemme : Restrictions de morphisms de corps . . . . .	94
5.3	Extensions de corps séparables . . . . .	95
5.3.1	Définition : Extension séparable . . . . .	95
5.3.2	Lemme : Transitivité de la separabilité d'extensions . . . . .	95
5.3.3	Théorème : Caractérisation de la separabilité de $\mathbb{K}[x]/\mathbb{K}$ . . . . .	95
5.3.4	Théorème : Caractérisation de separabilité par simplicité de racines . . . . .	95
5.3.5	Théorème : Génération des extensions séparables . . . . .	96
5.4	Groupes de Galois . . . . .	96
5.4.1	Définition : Groupe de Galois . . . . .	96
5.4.2	Théorème : Correspondance galoisienne . . . . .	96
5.4.3	Théorème : Génération de sous-corps galoisiens . . . . .	97
5.4.4	Théorème : Groupe de Galois d'un polynôme . . . . .	97
5.4.5	Théorème : Action de l'extension galoisienne sur racines . . . . .	97
5.5	Corps finis . . . . .	98
5.5.1	Théorème : $\mathbb{Z}/p\mathbb{Z}$ comme corps . . . . .	98
5.5.2	Théorème : Caractérisation des corps finis . . . . .	98
5.5.3	Théorème : Sous-corps de corps finis . . . . .	99
5.5.4	Lemme sur polynômes dans $\mathbb{F}_p[X]$ . . . . .	99
5.5.5	Exemple : Racines de l'unité et polynômes cyclotomiques . . . . .	100
5.5.6	Théorème : Irréductibilité des polynômes cyclotomiques . . . . .	101
<b>6</b>	<b>Modules sur anneaux principaux, intègres</b> . . . . .	<b>103</b>
6.0.7	Théorème sur sous-modules libres . . . . .	103
6.0.8	Définition : Le groupe linéaire, générale . . . . .	103
6.0.9	Lemme : Extensions à bases . . . . .	104
6.0.10	Théorème de Gauss : Réduction de matrices . . . . .	104
6.0.11	Théorème : Structure des modules de type fini . . . . .	105
<b>A</b>	<b>Annexe</b> . . . . .	<b>106</b>
A.0.12	Lemme : Factorisation des applications linéaires . . . . .	106
A.0.13	Lemme : Représentation des endomorphismes sur espaces vectoriels . . . . .	106
A.0.14	Lemme de Zorn . . . . .	107
<b>B</b>	<b>Symboles</b> . . . . .	<b>108</b>
	Index109 . . . . .	

# 1 Anneaux, idéaux, algèbres

## 1.1 Anneaux

### 1.1.1 Definition: Monoïde

Un **monoïde**  $(S, \circ)$  et un ensemble  $S$  munit d'un loi binaire  $\circ : S \times S \rightarrow S$  associative, avec un élément neutre  $e$ , ça veut dire  $s \circ e = e \circ s = s \forall s \in S$ . Si  $s \circ t = t \circ s \forall s, t \in S$ , on dit  $S$  **commutatif**. En ce cas, on utilise souvent “+” au lieu de “ $\circ$ ” et “0” au lieu de “ $e$ ”.

Une application  $f : S \rightarrow T$  entre deux monoïdes  $(S, \circ)$ ,  $(T, \circ)$  est dit **morphisme de monoïdes** ssi :

- Elle commute avec l'opération du monoïde, c'est-à-dire  $f(s \circ s') = f(s) \circ f(s')$  pour tout  $s, s' \in S$
- Elle préserve les unités, c'est-à-dire  $f(e_S) = e_T$ .

### Remarques :

1. L'élément neutre  $e$  de  $S$  est unique.
2. Soit  $G$  un groupe,  $S$  un monoïde et  $f : G \rightarrow S$  un morphisme de monoïdes. Alors,  $f(G)$  est un groupe et  $f : G \rightarrow f(G)$  un morphisme de groupes.

### Exemples :

- (i) Tout groupe est un monoïde.
- (ii)  $(\mathbb{N}_0, +)$  et  $(\mathbb{R}_+, +)$  sont monoïdes mais pas de groupes.

### 1.1.2 Definition: Monoïde produit

Soit  $(S_i)_{i \in I}$  une famille de monoïdes. Alors, le produit  $\prod_{i \in I} S_i$  munit de la composition composant à composant

$$(s_i)_{i \in I} + (t_i)_{i \in I} := (s_i + t_i)_{i \in I} \quad , \quad s_i, t_i \in S_i$$

est lui même un monoïde et dit **monoïde produit** des  $(S_i)_{i \in I}$ .

### 1.1.3 Definition: Anneau

Un **anneau** (avec élément unité)  $A$  est un ensemble muni de 2 lois  $+, \cdot$  (**addition** et **multiplication**), tel que :

1.  $(A, +)$  est un groupe abélien avec l'élément neutre (**nul**)  $0 \in A$ ,
2.  $(A, \cdot)$  est un monoïde avec l'élément unité  $1 \in A$ , c.a.d.  $a \cdot 1 = 1 \cdot a = a \quad \forall a \in A$  et  $\cdot : A \times A \rightarrow A$  est associative,
3. la multiplication  $\cdot$  est distributive par rapport à l'addition :

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad , \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in A \quad ,$$

On dit  $A$  **commutatif** si sa multiplication est commutative. On dit  $A$  anneau **trivial** si  $0 = 1$ , c'est-à-dire  $A = \{0\}$ .

### Remarques :

- (i) L'élément unité 1 est unique.
- (ii) Il faut  $a \cdot 0 = 0 \cdot a = 0$  pour tout  $a \in A$ .
- (iii) Souvent on note  $ab$  au lieu de  $a \cdot b$ .
- (iv) Pour sous-ensembles  $X, Y \subseteq A$  on note

$$X + Y := \{x + y : x \in X, y \in Y\} \quad , \quad X \cdot Y = \{x \cdot y : x \in X, y \in Y\} \quad .$$

- (v) Tout corps  $\mathbb{K}$  est un anneau.

**Exemples :**

- (i)  $\mathbb{Z}$  et l'espace  $\mathbb{K}[X]$  de polynômes sur un corps  $\mathbb{K}$  sont anneaux.
- (ii)  $\mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$ , où  $n \in \mathbb{N}$ , est un anneau par rapport à la multiplication

$$(k + n\mathbb{Z})(l + n\mathbb{Z}) = kl + n\mathbb{Z} .$$

- (iii) Souvent on parle de l'anneau d'endomorphismes d'une structure. Si  $V$  est un  $\mathbb{K}$ -espace vectoriel, ses endomorphismes  $\text{End}_{\mathbb{K}}(V)$  forment un anneau par rapport à l'addition et à la composition.
- (iv) On considère l'anneau des endomorphismes  $\text{End}(C_n)$  de la groupe cyclique  $C_n$  d'ordre  $n \geq 2$ , engendré par  $c \in C_n$ . Tout endomorphisme  $f : C_n \rightarrow C_n$  est déterminé par  $f(c) \in C_n$  et on a  $f(kc) = kf(c)$ ,  $k \in \mathbb{N}_0$ . Donc on a une correspondance naturelle entre  $C_n$  et  $\text{End}(C_n)$ .

**1.1.4 Définition: Anneau produit**

Soit  $(A_i)_{i \in I}$  une famille des anneaux. Alors on définit l'**anneau produit** comme le produit cartésien  $\prod_{i \in I} A_i$ , en définissant les opérations composante par composante, i.e.

$$(a_i)_{i \in I} + (b_i)_{i \in I} := (a_i + b_i)_{i \in I}$$

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} := (a_i \cdot b_i)_{i \in I} \quad , \quad (a_i), (b_i) \in \prod_{i \in I} A_i .$$

La nul d'anneau produit est  $(0_{A_i})_{i \in I}$ , son élément unité est  $(1_{A_i})_{i \in I}$ .

**1.1.5 Définition: Diviseur de zéro**

Soit  $(A, +, \cdot)$  un anneau. On appelle un élément  $0 \neq a \in A$  un **diviseur de zéro** à gauche (à droite) dans  $A$  s'il existe un  $0 \neq b \in A$  tel que  $a \cdot b = 0$  ( $b \cdot a = 0$ ). En tout autre cas, on dit qu'un élément  $x \in A$  **divise** un autre  $y \in A \setminus \{0\}$  à gauche (à droite), ssi  $y \in xA$  ( $y \in Ax$ ). En cas  $A$  est commutatif on écrit  $x \mid y$ .

**1.1.6 Définition: Anneau intègre**

Un anneau commutatif  $(A, +, \cdot)$  est dit **intègre**<sup>1</sup> (ou **d'intégrité**) si pour  $0 \neq x, y \in A$  on a toujours  $x \cdot y \neq 0$ . Donc,  $A$  est intègre ssi il ne possède pas de diviseurs de zéro.

**Exemples**

1. L'anneau  $\mathbb{Z}/p\mathbb{Z}$  où  $p \in \mathbb{P}$  est premier, est intègre.
2. L'anneau  $\mathbb{Z}/6\mathbb{Z}$  n'est pas intègre, parce que  $(2 + 6\mathbb{Z}) \cdot (3 + 6\mathbb{Z}) = 0 + 6\mathbb{Z}$ .

**Remarques :** On suppose que  $A$  est intègre.

- (i) Si  $x, a, b \in A$  sont tels que  $0 \neq x$  et  $ax = bx$ , alors  $a = b$ .
- (ii) Deux éléments  $x, y \in A$  satisfont  $Ax = Ay$  ssi il existe un inversible (vois 1.1.7)  $a \in A$  tel que  $x = ay$ .

**Preuve :** Supposons que  $Ax = Ay$ . Alors, il existe un  $a \in A$  tel que  $1 \cdot x = a \cdot y$ . Donc  $Aay = Ax = Ay$ , et de même il existe un  $b \in A$  tel que  $bay = 1 \cdot y$ . Donc  $ba = 1$ , c'est-à-dire  $a$  est inversible.

Si inversement  $x = ay$  pour un  $a \in A^\times$ , alors pour tout  $b \in A$  on a  $bx = bay$ , c'est-à-dire  $Ax \subseteq Ay$ . De même, comme  $y = a^{-1}x$  on trouve  $Ay \subseteq Ax$ .

---

1. Anglais : Integral domain.

**1.1.7 Définition: Inversibilité**

Soit  $(A, +, \cdot)$  un anneau. Un élément  $x \in A$  s'appelle **inversible** (ou **unité**), si  $\exists y \in A : xy = yx = 1$ . Cet  $y$  est unique et on écrit  $y = x^{-1}$ . L'ensemble  $A^\times$  des éléments inversibles de  $A$  est un groupe par rapport à la multiplication et on a  $(x_1x_2)^{-1} = x_2^{-1}x_1^{-1}$  pour tout paire  $x_1, x_2 \in A^\times$ . Si  $A^\times = A \setminus \{0\}$  on dit que  $A$  est un **anneau à division**<sup>2</sup>. Si en plus  $A$  est non-trivial, commutatif,  $(A, +, \cdot)$  s'appelle un **corps**<sup>3</sup>.

**Remarques**

- (i) Si  $x \in A^\times$  est inversible et  $a \in A \setminus A^\times$  non-inversible, alors  $ax$  et  $xa$  sont non-inversibles.
- (ii) Si  $A$  est commutatif et  $x, y \in A \setminus A^\times$  non-inversibles, alors  $xy$  est non-inversible.
- (iii) Soit  $(A, +, \cdot)$  un anneau et  $a \in A$ . Alors  $a \in A^\times$  ssi  $Aa = A = aA$ .
- (iv) Tout anneau commutatif à division est intègre.

**Exemple :** Si  $V$  est un  $\mathbb{K}$ -espace linéaire, il est  $\text{End}_{\mathbb{K}}(V)^* = \text{GL}(V)$ .

**1.1.8 Définition: Élément irréductible**

Un élément  $a \in A$  d'un anneau  $(A, +, \cdot)$  est dit **irréductible** si toute sa décomposition en deux facteurs contient exactement un élément inversible.

**1.1.9 Définition: Élément nilpotent**

Un élément  $a \in A$  d'un anneau  $(A, +, \cdot)$  est dit **nilpotent** s'il existe  $n \in \mathbb{N}$  tel que  $a^n = 0$ .

**1.1.10 Définition: Élément central, centre**

Soit  $(A, +, \cdot)$  un anneau. Un élément  $x \in A$  est **central** si  $xy = yx \quad \forall y \in A$ . On note  $Z(A)$  l'ensemble des éléments centraux de  $A$ . On l'appelle le **centre** de  $A$ .

**1.1.11 Définition: Sous-anneau**

Soit  $(A, +, \cdot)$  un anneau. Une partie  $B \subseteq A$  est un **sous-anneau** de  $A$  si  $1 \in B$  et  $B + B \subseteq B$ ,  $B \cdot B \subseteq B$ .

**Exemple :** Le centre  $Z(A)$  d'un anneau  $A$  est un sous-anneau. Si  $A = Z(A)$ , alors  $A$  est commutatif.

**1.1.12 Définition: Morphisme d'anneaux**

Un **morphisme d'anneaux** est une application  $f : A \rightarrow B$  entre deux anneaux  $(A, +, \cdot)$ ,  $(B, +, \cdot)$  telle que :

1.  $f : (A, +) \rightarrow (B, +)$  est un morphisme de groupes,
2.  $f(1_A) = 1_B$ ,
3.  $f(xy) = f(x)f(y)$  pour  $x, y \in A$ .

---

2. Anglais : Division ring.

3. Anglais : Field.



**Remarques :**

- (i) Si  $A$  et  $B$  sont corps, on dit  $f$  un **morphisme de corps**. Noter que tout morphisme de corps est injectif.
- (ii) Si  $f$  est bijective, alors  $f^{-1} : B \rightarrow A$  est un morphisme d'anneaux. On dit que  $f$  est un **isomorphisme**, les anneaux  $A, B$  **isomorphes** et on note  $(A, +, \cdot) \cong (B, +, \cdot)$ .
- (iii) Si  $A, B, C$  sont anneaux et  $f : A \rightarrow B, g : B \rightarrow C$  morphismes d'anneaux, alors  $g \circ f$  est un morphisme d'anneaux aussi.
- (iv) Si  $A, B$  sont anneaux,  $f : A \rightarrow B$  un morphisme d'anneaux et  $\tilde{A} \subseteq A, \tilde{B} \subseteq B$  sous-anneaux, alors  $f(\tilde{A}) \subseteq \tilde{B}$  et  $f^{-1}(\tilde{B}) \subseteq \tilde{A}$  sont sous-anneaux.

**Exemple :** L'anneau  $\mathbb{Z}/n\mathbb{Z}$  est isomorphe à l'anneau  $\text{End}(\mathbb{Z}/n\mathbb{Z})$  par

$$\text{End}(\mathbb{Z}/n\mathbb{Z}) \rightarrow \mathbb{Z}/n\mathbb{Z} \quad , \quad f \mapsto f([1])$$

**1.1.13 Lemme sur l'anneau des endomorphismes**

Soit  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension fini et  $\text{End}_{\mathbb{K}}(V)$  l'anneau des endomorphismes sur  $V$ . Alors

$$Z(\text{End}_{\mathbb{K}}(V)) = \mathbb{K} \cdot \mathbb{1}_V \quad ,$$

où  $\mathbb{1}_V$  est l'identité sur  $V$ .

**Preuve :** Il suffit de montrer  $Z(\text{End}_{\mathbb{K}}(V)) \subseteq \mathbb{K} \cdot \mathbb{1}_V$ . Si  $f, g \in \text{End}_{\mathbb{K}}(V)$  sont tels que  $fg = gf$ , alors  $f$  laisse stable les sous-espaces propres de  $g$  (et vice versa), car si  $gx = \lambda x$  on a  $g(f(x)) = f(g(x)) = \lambda f(x)$ . Si  $D$  est une droite vectorielle,  $D$  est évidemment sous-espace propre d'un endomorphisme. Donc, si  $f$  est central,  $f(D) \subseteq D$  pour toute droite vectorielle  $D \subseteq V$ . En particulier  $f(e_i) = \lambda_i e_i$ , où  $\{e_1, \dots, e_n\}$  est une base de  $V$  et  $\lambda_i \in \mathbb{K}, i = 1, \dots, n$ .

On a aussi, pour quelqu'un  $\lambda \in \mathbb{K}$  :

$$\sum_{i=1}^n \lambda_i e_i = \sum_{i=1}^n f(e_i) = f \left[ \sum_{i=1}^n e_i \right] = \lambda \cdot \sum_{i=1}^n e_i \quad ,$$

qui implique  $\lambda_i = \lambda \forall i = 1, \dots, n$  et donc  $f = \lambda \cdot \mathbb{1}_V$ .

□

**1.1.14 Definition: Anneau euclidien**

Un anneau  $A$  intègre est dit **euclidien** s'il existe une application  $\text{val} : A \setminus \{0\} \rightarrow \mathbb{N}_0$  satisfaisante :

1. Pour  $a, b \in A \setminus \{0\}$  on a toujours  $\text{val}(a) \leq \text{val}(ab)$ .
2. Pour  $(a, b) \in A \times (A \setminus \{0\})$  il existe deux  $q, r \in A$  tels que  $a = bq + r$  et  $\text{val}(r) < \text{val}(b)$  si  $r \neq 0$ . On appelle ce combinaison **une division euclidienne de  $a$  par  $b$** .

On dit une telle application **stathme** (ou **fonction euclidienne** ou **valuation**) sur  $A$ . Si le couple  $q, r$  dans point (2) est toujours unique, on appelle  $A$  euclidien avec **division euclidienne unique**.

**Remarques**

- (i) Comme 1 divise tous les non-nules, axiome (2) implique que  $\text{val}(1)$  est la plus petite valeur de  $\text{val}()$  sur  $A \setminus \{0\}$ .
- (ii) S'il existe une  $\varphi : A \setminus \{0\} \rightarrow \mathbb{N}_0$  satisfaisante l'axiome (2), alors il existe toujours une valuation sur  $A$ , donnée par exemple par

$$\text{val}(a) := \min_{x \in A \setminus \{0\}} \varphi(xa) = \min \text{val}(\langle Ax \rangle \setminus \{0\}) \quad , \quad a \in A \setminus \{0\} \quad .$$

Donc,  $A$  est euclidien ssi il existe une application  $\text{val} : A \setminus \{0\} \rightarrow \mathbb{N}_0$  satisfaisante (2).

- (iii) Souvent on demande que  $\text{val}()$  soit défini sur tout l'anneau et satisfaisante  $\text{val}(0) = 0$ .
- (iv) Si  $a, b, c \in A \setminus \{0\}$  sont tels que  $a = bc$  et  $c \notin A^\times$ , alors  $\text{val}(b) < \text{val}(a)$ .
- (v) Si  $a \in A$  n'est pas inversible, alors  $\text{val}(a) > 0$ .

### Exemples

- (i) Tout corps  $\mathbb{K}$  est euclidien avec division euclidienne unique, en posant  $\text{val}(x) = 1$  pour tout  $x \in \mathbb{K}^\times$ .
- (ii) L'anneau  $\mathbb{Z}$  est euclidien avec division euclidienne unique, en posant  $\text{val}(n) := |n|$  pour  $n \in \mathbb{Z} \setminus \{0\}$ .
- (iii) L'anneau des **entiers de Gauss**  $\mathbb{Z}[i] := \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$  est euclidien avec stathme  $\text{val} : z \mapsto |z|^2$ .

#### 1.1.15 Lemme sur la division dans anneaux euclidiens

Soient  $A, B$  deux anneaux euclidiens avec division euclidienne unique tels que  $A \subseteq B$  et la stathme sur  $A$  est simplement la restriction de la stathme  $\text{val}()$  de  $B$ . Si  $a, b \in A$  et  $q, r \in B$  sont tels que  $a = qb + r$  avec  $\text{val}(r) < \text{val}(b)$  ou  $r = 0$ , alors  $q, r \in A$ .

**Preuve :** Comme  $\text{val}|_A$  est une stathme sur  $A$ , il existe  $\tilde{q}, \tilde{r} \in A$  tels que  $a = \tilde{q}b + \tilde{r}$  et  $\text{val}(\tilde{r}) < \text{val}(b)$  ou  $\tilde{r} = 0$ . Mais par unicité de la division euclidienne dans  $B$ , il faut que  $\tilde{q} = q$  et  $\tilde{r} = r$ , donc  $q, r \in A$ .  $\square$

#### 1.1.16 Le morphisme de Frobenius

Soit  $A$  un anneau commutatif de caractéristique  $p$ , où  $p \in \mathbb{P}$  soit un nombre premier. Alors, l'application

$$A \rightarrow A, \quad x \mapsto x^p$$

est un morphisme d'anneaux, appelé **morphisme de Frobenius**. Si  $A$  est intègre, alors ce morphisme est injectif. Si  $A$  est intègre et fini, il est une bijection, c'est-à-dire un automorphisme.

## 1.2 Ideaux

### 1.2.1 Définition: Ideal

Soit  $(A, +, \cdot)$  un anneau. Un **idéal à gauche**  $I \subseteq A$  (resp. **à droite**) est un sous-groupe additif  $(I, +) \subseteq (A, +)$ , stable par la multiplication à gauche (à droite) :  $AI \subseteq I$  (resp.  $IA \subseteq I$ ).  $I$  est **bilatère** s'il est idéal des 2 côtés, donc  $x \in I, a, b \in A$  implique  $axb \in I$ .

### Remarques :

- (i)  $\{0\}$  et  $A$  sont des idéaux bilatères *triviaux*.
- (ii) Si  $I \subseteq A$  est un idéal (d'un type certain), alors  $I = A$  ssi  $I \cap A^\times \neq \emptyset$ .
- (iii) L'intersection d'une famille d'idéaux (d'un type certain) est encore un idéal de même type.
- (iv) L'anneau  $A$  est un corps ssi il est non-trivial, commutatif et il n'a que les deux idéaux  $\{0\}$  et  $A$ . Ça c'est impliqué par remarque (ii) et la remarque de la définition 1.1.7.

**Exemple :** Considérons l'anneau  $A^{\text{op}}$  (anneau *oppose*) obtenu en modifiant la multiplication par  $a \cdot_{\text{op}} b := b \cdot a$ . Ses idéaux à gauche (resp. à droite) correspondent aux idéaux à droite (resp. à gauche) de  $A$ . Par exemple, l'anneau  $M_n(\mathbb{K})$  des  $n \times n$ -matrices sur le corps  $\mathbb{K}$  est isomorphe à l'anneau oppose  $M_n(\mathbb{K})^{\text{op}}$  avec la correspondance  $M \mapsto M^T, M \in M_n(\mathbb{K})$ .

### 1.2.2 Définition: Anneau simple

Un anneau  $A$  est dit **simple** ssi il ne contient des idéaux bilatères excepté  $\{0\}$  et  $A$ .

### 1.2.3 Lemme : Stabilité des idéaux sous morphismes

Soient  $A, B$  anneaux et  $f : A \rightarrow B$  un morphisme d'anneaux.

1. Si  $J \subseteq B$  est un idéal (d'un type certain),  $f^{-1}(J)$  est un idéal dans  $A$  de même type. En particulier,  $\ker(f) = f^{-1}(\{0\})$  est un idéal bilatère de  $A$ .
2. Si  $I \subseteq A$  est un idéal (d'un type certain),  $f(I)$  est un idéal (du même type) dans l'anneau  $f(A)$ .
3. L'image  $f(A^\times)$  est un sous-groupe du groupe multiplicatif  $(B^\times, \cdot)$ .

### 1.2.4 Définition: L'idéal engendré

Soit  $A$  un anneau et  $X \subseteq A$  une partie quelconque. L'idéal à gauche

$$\langle X \rangle_g := \bigcap_{\substack{X \subseteq I \subseteq A \\ I \text{ idéal à gauche}}} I \quad (1.2.4.1)$$

(resp.  $\langle \cdot \rangle_d$  à droite,  $\langle \cdot \rangle_b$  bilatère) est le plus petit idéal à gauche (à droite, bilatère) contenant  $X$ . On l'appelle l'idéal **engendré**<sup>4</sup> à gauche (à droite, bilatère) par  $X$ .

### 1.2.5 Lemme : Invariance de générateurs sous morphismes

Soient  $A, B$  deux anneaux et  $f : A \rightarrow B$  un morphisme d'anneaux surjectif. Alors :

1. Si  $X \subseteq A$ , il faut  $\langle f(X) \rangle_g = f(\langle X \rangle_g)$ .
2. Si  $Y \subseteq B$ , il faut  $\langle f^{-1}(Y) \rangle_g = f^{-1}(\langle Y \rangle_g)$ .

### 1.2.6 Proposition : Représentation de $\langle X \rangle$

Soit  $A$  un anneau et  $X \subseteq A$  une partie quelconque. Alors l'idéal engendré  $\langle X \rangle_g$  à gauche admet la représentation

$$\langle X \rangle_g = \left\{ \sum_{i=1}^n a_i x_i : a_i \in A, x_i \in X \right\} =: \text{span}_A(X) . \quad (1.2.6.1)$$

**Preuve :** C'est évident que  $\sum_{i=1}^n a_i x_i \in I$  pour tous  $a_i \in A$ ,  $x_i \in X$  et idéal  $I$  contenant  $X$ . D'autre part, l'ensemble à droite du (1.2.6.1) est un idéal à gauche qui contient  $X$ . Donc, l'idéal à gauche engendré par  $X$  est l'ensemble des combinaisons linéaires à gauche d'éléments de  $X$ . □

### 1.2.7 Définition: Idéal & anneau principal

Si  $A$  est un anneau et  $a \in A$ , alors l'idéal à gauche (à droite, bilatère) engendré par  $\{a\}$  est  $Aa := \{xa : x \in A\}$  (resp.  $aA$  et  $AaA$ ). Tout idéal  $I \subseteq A$  (d'un type certaine) qui est engendré par un seul élément, est dit **principal**. Un anneau commutatif  $A$  est dit **principal**<sup>5</sup> si tout son idéal est principal.

---

4. Anglais : Generated ideal.

5. Anglais : Principal ideal ring.

### 1.2.8 Définition: Idéal de type fini

Soit  $(A, +, \cdot)$  un anneau et  $I \subseteq A$  un idéal à gauche. On dit  $I$  un idéal de **type fini** s'il est engendré par un nombre fini d'éléments  $a_1, \dots, a_n \in I$ , c.a.d.

$$I = \langle a_1, \dots, a_n \rangle_g = \sum_{i=1}^n Aa_i \ .$$

**Remarque :** Si  $I \subseteq A$  est un idéal à gauche de type fini et engendré par un système  $X$ , alors on peut choisir un nombre fini d'éléments  $x_1, \dots, x_n \in X$  tel que  $I = \langle x_1, \dots, x_n \rangle_g$ .

### 1.2.9 Idéaux engendré par idéaux

Soit  $(I_j)_{j \in J}$  une famille d'idéaux (d'un type  $t \in \{g, d, b\}$  certain) de l'anneau  $A$ . L'idéal (du même type) engendré par leur union  $\bigcup_{j \in J} I_j$  est l'ensemble

$$\sum_{j \in J} I_j := \left\{ \sum_{j \in J'} a_j \ : \ J' \subseteq J, a_j \in I_j, |J'| < \infty \right\}$$

des sommes finies des éléments des  $I_j$ . En outre, si  $J = \{1, \dots, n\}$  l'idéal engendré par le produit

$$\prod_{j=1}^n I_j := \left\{ \prod_{j=1}^n a_j \ : \ a_j \in I_j \right\} \tag{1.2.9.1}$$

est exactement

$$\left\langle \prod_{j \in J} I_j \right\rangle_t = \left\{ \sum_{i=1}^n b_i \ : \ b_i \in \prod_{j=1}^n I_j, n \in \mathbb{N}_0 \right\} \ .$$

On le dit l'**idéal produit** de  $(I_j)_{j=1}^n$

**Remarque :** Le produit des idéaux est associatif sous génération, c.a.d pour idéaux  $I_1, I_2, I_3$  (d'un type  $t \in \{g, d, b\}$  certain) on a

$$\langle I_1 \cdot \langle I_2 \cdot I_3 \rangle_t \rangle_t = \langle \langle I_1 \cdot I_2 \rangle_t \cdot I_3 \rangle_t \ .$$

### 1.2.10 Lemme : Idéaux des endomorphismes sur un espace vectoriel

Soit  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension  $n \in \mathbb{N}$ . Alors :

1. Pour tout sous-espace vectoriel  $W \subseteq V$ , l'ensemble  $I_W := \{f \in \text{End}_{\mathbb{K}}(V) : f(W) = 0\}$  est un idéal à gauche dans  $\text{End}_{\mathbb{K}}(V)$ .
2. Tout idéal à gauche dans  $\text{End}_{\mathbb{K}}(V)$  est en fait de type (1).
3. Pour tout sous-espace vectoriel  $W \subseteq V$ , l'ensemble  $J_W := \{f \in \text{End}_{\mathbb{K}}(V) : f(V) \leq W\}$  est un idéal à droite dans  $\text{End}_{\mathbb{K}}(V)$ .
4. Tout idéal à droite dans  $\text{End}_{\mathbb{K}}(V)$  est en fait de type (3).
5. Les seuls idéaux bilatères de  $\text{End}_{\mathbb{K}}(V)$  sont  $\{0\}$  et  $\text{End}_{\mathbb{K}}(V)$ .

**Preuve :**

1. C'est évident que  $I_W$  est une sous-groupe additive du  $\text{End}_{\mathbb{K}}(V)$ . En plus, si  $f \in I_W$  et  $g \in \text{End}_{\mathbb{K}}(V)$  on a  $(g \circ f)(W) = g(\{0\}) = \{0\}$ , donc  $I_W$  est un idéal.

2. Soit  $I \subseteq \text{End}_{\mathbb{K}}(V)$  un idéal à gauche et  $W := \bigcap_{f \in I} \ker(f)$ . Car  $I \subseteq I_W$ , il suffit de montrer  $I_W \subseteq I$ . Parce que  $\dim V < \infty$ ,  $W$  est intersection d'un finit nombre de noyaux, donc il y a  $f_1, \dots, f_m \in I$  tels que

$$W = \bigcap_{i=1}^m \ker(f_i) .$$

Chaque  $f \in I_W$  satisfait par définition  $f(W) = \{0\}$ , donc selon A.0.13(1) il y a  $g_1, \dots, g_m \in \text{End}_{\mathbb{K}}(V)$  tels que  $f = \sum_{i=1}^m g_i \circ f_i$ . Mais  $I$  est un idéal à gauche, donc  $f \in I$ .

3. Évident.

4. Soit  $J \subseteq \text{End}_{\mathbb{K}}(V)$  un idéal à gauche et  $W := \bigcup_{f \in J} f(V)$ . Car  $J \subseteq J_W$ , il suffit de montrer  $J_W \subseteq J$ . Par la même argumentation comme (2), il y a  $f_1, \dots, f_m \in J$  tels que

$$W = \bigcup_{i=1}^m f_i(V) .$$

Chaque  $f \in J_W$  satisfait  $f(V) \subseteq W$ , donc par A.0.13(2) il y a  $g_1, \dots, g_m \in \text{End}_{\mathbb{K}}(V)$  tels que  $f = \sum_{i=1}^m f_i \circ g_i$ . Mais  $J$  est un idéal à gauche, donc  $f \in J$ .

5. Supposons que  $W, \widetilde{W} \leq V$  sont sous-espaces vectoriels de  $V$  et  $I := I_W = J_{\widetilde{W}} \subseteq \text{End}_{\mathbb{K}}(V)$  un anneau bilatère défini par eux. Si  $\{0\} \neq I \neq \text{End}_{\mathbb{K}}(V)$ , alors  $\{0\} \subsetneq W, \widetilde{W} \subsetneq V$ . Donc  $V = W \oplus W^c = \widetilde{W} \oplus \widetilde{W}^c$ , avec  $W^c, \widetilde{W}^c \neq \{0\}$ . Bien sûr, il existe une application linéaire  $g : \in \text{End}_{\mathbb{K}}(V)$  telle que

$$g(W) = 0 \quad \wedge \quad g(W^c) \subseteq \widetilde{W}^c \setminus \{0\} ,$$

donc  $g \in I_W$  et  $g \notin J_{\widetilde{W}}$ , une contradiction !

□

### 1.2.11 Définition: Anneau quotient

Soient  $(A, +, \cdot)$  un anneau et  $I \subseteq A$  un idéal bilatère. Alors le groupe abélien quotient

$$A/I := \{a + I : a \in A\}$$

a une structure *naturelle* d'anneau par rapport à la multiplication<sup>6</sup>

$$(a + I) \cdot (b + I) := ab + I \quad , \quad a, b \in A .$$

Son élément zéro est  $0 + I$  est son élément d'unité est  $1 + I$ . En plus, l'application  $\Pi : A \rightarrow A/I$  définie par  $\Pi(a) := a + I$  est un morphisme surjectif d'anneaux. On appelle  $A/I$  **l'anneau quotient** (par rapport à  $I$ ) et  $\Pi$  le **morphisme canonique** (ou **application quotient**) de  $A/I$ .

### 1.2.12 Théorème : Factorisation des morphismes

Soit  $(A, +, \cdot)$  un anneau,  $I \subseteq A$  un idéal bilatère et  $\Pi : A \rightarrow A/I$  le morphisme canonique dans l'anneau quotient  $A/I$ . Alors  $\Pi$  satisfait :

1.  $\ker \Pi = \{0\}$ .
2. Le morphisme  $\Pi$  est *universel* : Soit  $f : A \rightarrow B$  un morphisme d'anneaux avec  $f(I) = \{0\}$ , alors  $f$  *factorise* par  $A/I$ , c.a.d. il existe un unique morphisme  $\bar{f} : A/I \rightarrow B$  d'anneaux tel que  $f = \bar{f} \circ \Pi$ .
3. L'anneau  $A/I$  et le morphisme canonique  $\Pi : A \rightarrow A/I$  est le *seul*<sup>7</sup> paire d'anneau et morphisme qui satisfont  $\Pi(I) = \{0\}$  et (2). Autrement dit, si  $A_1$  est un anneau et  $\Pi_1 : A \rightarrow A_1$  un morphisme tel que  $\Pi_1(I) = \{0\}$  et pour tout morphisme  $f : A \rightarrow B$ ,  $f(I) = \{0\}$  on a  $f = \bar{f} \circ \Pi_1$  pour un unique morphisme  $\bar{f} : A_1 \rightarrow B$ , il faut  $A/I \cong A_1$ . En plus,  $\Pi_1$  est simplement le transport du  $\Pi$  par un isomorphisme certain entre  $A/I$  et  $A_1$ .

6. Cette opération est bien défini, car si  $a + I = a' + I$  et  $b + I = b' + I$  on a  $a' = a + \alpha$  et  $b' = b + \beta$  pour quelques  $\alpha, \beta \in I$ , donc  $a'b' + I = ab + a\beta + \alpha b + I = ab + I$ .

7. À isomorphismes.

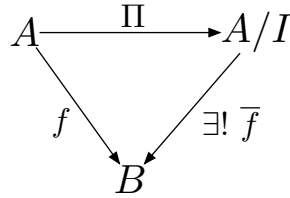


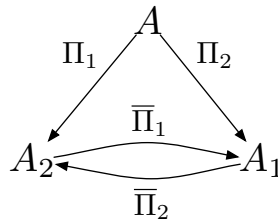
FIGURE 1: Sur la factorisation des morphismes.

**Preuve :**

1. Évident.
2. Définissons  $\bar{f} : A/I \rightarrow B$  comme  $\bar{f}(\Pi(a)) := f(a)$  pour  $a \in A$ . Cette définition a un sens, car  $\Pi$  est surjectif et si  $\Pi(a) = \Pi(b)$ , on a  $a - b \in I$  est donc  $f(a) = f(b)$ . Parce que  $\Pi$  est surjectif,  $\bar{f}$  est unique.
3. Soient  $A_1, A_2$  deux anneaux et  $\Pi_1 : A \rightarrow A_1$ ,  $\Pi_2 : A \rightarrow A_2$  morphismes satisfaisant  $\Pi_1(I) = \Pi_2(I) = \{0\}$  et (2). Alors ils existent morphismes  $\bar{\Pi}_1 : A_2 \rightarrow A_1$ ,  $\bar{\Pi}_2 : A_1 \rightarrow A_2$  tels que  $\Pi_1 = \bar{\Pi}_1 \circ \Pi_2$  et  $\Pi_2 = \bar{\Pi}_2 \circ \Pi_1$ . Donc

$$\bar{\Pi}_1 \circ \bar{\Pi}_2 \circ \Pi_1 = \bar{\Pi}_1 \circ \Pi_2 = \Pi_1$$

et par l'unicité de factorisation  $\Pi_1$  par  $\Pi_1$  lui même, il faut  $\bar{\Pi}_1 \circ \bar{\Pi}_2 = \text{Id}$ . De même on trouve que  $\bar{\Pi}_2 \circ \bar{\Pi}_1 = \text{Id}$ , donc  $\bar{\Pi}_1 : A_2 \rightarrow A_1$  est un isomorphisme avec l'inverse  $\bar{\Pi}_2$ .

FIGURE 2: Sur la preuve du 1.2.12(3). Les facteurs  $\bar{\Pi}_1, \bar{\Pi}_2$  sont des isomorphismes entre  $A_1$  et  $A_2$ .

□

### 1.2.13 Théorème d'isomorphismes d'anneaux

Soient  $A, B$  des anneaux et  $f : A \rightarrow B$  un morphisme d'anneaux. Alors  $f$  incite un isomorphisme

$$\bar{f} : A/\ker(f) \rightarrow f(A) \quad , \quad \bar{f}(a + \ker(f)) := f(a)$$

d'anneaux et donc  $A/\ker(f) \cong f(A)$ .

**Preuve :** L'application  $\bar{f}$  est vraiment bien définie, car si  $a + \ker(f) = b + \ker(f)$  il faut  $f(a) = f(b)$ . C'est bien un morphisme d'anneaux est sûrement surjective. Si  $\bar{f}(a + \ker(f)) = 0_B$  il faut  $a \in \ker(f)$  et donc  $a + \ker(f) = 0_{A/\ker f}$ , donc  $\bar{f}$  est injective. Donc,  $\bar{f}$  est un isomorphisme d'anneaux.

□

**Remarques :**

- (i) Se rappelle que  $\ker(f)$  est un idéal bilatère dans  $A$ . Le morphisme  $\bar{f} : A/\ker(f) \rightarrow f(A)$  est simplement un des deux facteurs de la factorisation comme décrit à 1.2.12(2). En particulier  $f = \bar{f} \circ \Pi$  où  $\Pi : A \rightarrow A/\ker(f)$  est le morphisme canonique de  $A/\ker(f)$ .

- (ii) Soit  $f : A \rightarrow B$  un homomorphisme de groupes surjective. Il y a une bijection entre les sous-groupes de  $B$  et ceux de  $A$  qui contient  $\ker(f)$ . Si  $f$  est un morphisme d'anneaux, il envoie idéaux (d'un type certain) à idéaux (de même type) et vice versa.

**Démonstration :** Au chaque sous-groupe  $U \subseteq A$  qui contient  $\ker(f)$  assigne le sous-groupe  $f(U)$ . Cette attribution est injective, car :

Soit  $f(U_1) = f(U_2)$  pour deux sous-groupes  $\ker(f) \subseteq U_1, U_2 \subseteq A$ . Si  $a_1 \in U_1$ , il faut  $f(a_1) \in f(U_2)$ , donc  $f(a_1) = f(a_2)$  pour quelque'un  $a_2 \in U_2$  et donc  $a_1 \in a_2 + \ker(f) \subseteq a_2 + U_2 \subseteq U_2$ . Ça implique  $U_1 \subseteq U_2$  et par symétrie  $U_2 \subseteq U_1$ .

Cette attribution est surjective, car pour tout sous-groupe  $V \subseteq B$ , le sous-groupe  $f^{-1}(V) \subseteq A$  contient  $\ker(f)$  et par surjectivité de  $f$  satisfait  $f(f^{-1}(V)) = V$ .

Si en plus  $f : A \rightarrow B$  est un morphisme d'anneaux, alors par 1.2.3 il envoie idéaux à idéaux du même type et vice versa.

### 1.2.14 Lemme : Transitivité des quotients

Soit  $(A, +, \cdot)$  un anneau et  $I \subseteq J \subseteq A$  deux idéaux bilatères. Soit  $\Pi_I : A \rightarrow A/I$  l'homomorphisme canonique d'anneau quotient  $A/I$ . Alors  $\Pi_I(J) \subseteq A/I$  est un idéal bilatère de  $A/I$  et on a

$$\boxed{(A/I)/\Pi_I(J) \cong A/J \quad .}$$

**Preuve :** Car  $\Pi_I : A \rightarrow A/I$  est un homomorphisme surjectif, par 1.2.3(2)  $\Pi_I(J)$  est un idéal bilatère de  $f(A) = A/I$ . Soit  $\Pi_J : A/I \rightarrow (A/I)/\Pi_I(J)$  le morphisme d'anneau quotient  $(A/I)/\Pi_I(J)$  et  $\Pi := \Pi_J \circ \Pi_I$ . Par 1.2.13 on a

$$A/\ker \Pi \cong \text{image}(\Pi) = (A/I)/\Pi_I(J) \quad .$$

Bien sûr,  $J \subseteq \ker \Pi$ . Mais aussi d'autre part, on a

$$\ker \Pi = \Pi_I^{-1}(\ker \Pi_J) = \Pi_I^{-1}(\Pi_I(J)) = \{a \in A \mid \exists j \in J : a \in \underbrace{j+I}_{\subseteq J}\} \subseteq J$$

et donc finalement

$$A/J \cong (A/I)/\Pi_I(J) \quad .$$

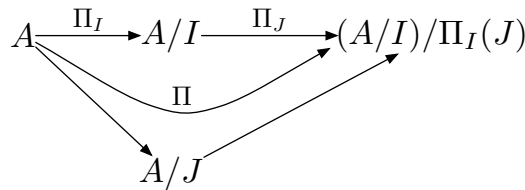


FIGURE 3: Sur la transitivité des anneaux quotients.

□

### 1.2.15 Définition: Idéal premier

Un idéal  $I \subsetneq A$  d'anneau  $(A, +, \cdot)$  est dit **premier**<sup>8</sup> si pour tous  $x, y \in A \setminus I$  on a  $x \cdot y \in A \setminus I$ . On note  $\text{Spec}(A)$  l'ensemble des idéaux premiers de  $A$  et l'appelle **spectre d'anneau**  $A$ .

8. Anglais : Prime ideal.

**Remarques**

- (i) Soit  $I \subseteq A$  un idéal premier et  $X_1, X_2 \subseteq A$  deux parties tels que  $X_1 \cdot X_2 \subseteq I$ . Alors, l'un de ces deux parties est inclus dans  $I$ .
- (ii) Si  $A$  est commutatif, alors un idéal  $I \subsetneq A$  est premier ssi l'anneau quotient  $A/I$  est intègre.
- (iii) Soit  $u : A \rightarrow B$  un morphisme d'anneaux commutatifs. Si  $I_B \subseteq B$  est un idéal premier de  $B$ , alors  $u^{-1}(I_B) \subseteq A$  est un idéal premier de  $A$ .

**Preuve :** On montre que le morphisme induit  $\bar{u} : A/u^{-1}(I_B) \rightarrow B/I_B$  est injectif. Donc  $A/u^{-1}(I_B)$  est intègre comme sous-anneau d'un anneau intègre.

**1.2.16 Définition: Topologie de Zariski**

Soit  $(A, +, \cdot)$  un anneau avec le spectre  $\text{Spec}(A)$ . Pour tout idéal bilatère  $I \subseteq A$  on définit  $Z(I) \subseteq \text{Spec}(A)$  comme l'ensemble des idéaux premiers contenant  $I$ , c.a.d.

$$Z(I) := \{J \in \text{Spec}(A) : I \subseteq J\} \quad .$$

Ces parties satisfont :

- $Z(\{0\}) = \text{Spec}(A)$  et  $Z(A) = \emptyset$ .
- Pour idéaux bilatères  $I, J \subseteq A$  on a  $Z(I) \cup Z(J) = Z(IJ)$ .
- Pour toute famille d'idéaux bilatères  $(I_j)_{j \in J}$  on a  $\bigcap_{j \in J} Z(I_j) = Z\left(\sum_{j \in J} I_j\right)$ .

Ainsi  $\{Z(I) \mid I \subseteq A \text{ idéal bilatère}\}$  est l'ensemble des fermés d'une topologie sur  $\text{Spec}(A)$  appelée **topologie Zariski**. Si  $I \subseteq A$  est un idéal bilatère principal, la fermé  $Z(I)$  est appelé **fermé principal** et l'ouvert  $Z(I)^c := \text{Spec}(A) \setminus Z(I)$  **ouvert principal** de la topologie de Zariski. Tous les ouverts principaux, constituent une base de la topologie de Zariski. Vraiment, pour tout idéal bilatère on peut écrire

$$Z(I) = Z\left(\sum_{a \in I} AaA\right) = \bigcap_{a \in A} \underbrace{Z(AaA)}_{\substack{\text{fermé} \\ \text{principal}}} \quad .$$

**1.2.17 Définition: Idéal maximal**

Un idéal  $I \subsetneq A$  (d'un type certain) d'un anneau  $(A, +, \cdot)$  est dit **maximal dans  $A$** <sup>9</sup> si il n'y a pas d'idéal  $J \subseteq A$  (de même type) tel que  $I \subsetneq J \subsetneq A$ . On note  $\text{Specmax}(A)$  la famille des idéaux maximaux dans  $A$ .

**1.2.18 Lemme : Caractérisation des idéaux maximaux**

Soit  $(A, +, \cdot)$  un anneau commutatif et  $I \subseteq A$  un idéal. Alors  $I$  est maximal ssi l'anneau quotient  $A/I$  est un corps.

**Preuve :** Par remarque 1.2.1(iv),  $A/I$  est un corps ssi il n'a que les deux idéaux  $\{0\}$  et  $A$ . Par remarque 1.2.13(ii) il y a une bijection entre les idéaux de  $A/I$  et les idéaux de  $A$  contenant  $I$ . Donc, si  $I \subseteq A$  est maximal dans  $A$ , ils existent seulement deux tels idéaux et  $A/I$  est un corps. D'autre part, si  $A/I$  est un corps,  $I \subseteq A$  est maximal.

□

**1.2.19 Théorème de Krull : Existence des idéaux maximaux**

Soit  $(A, +, \cdot)$  un anneau est  $I \subsetneq A$  un idéal (d'un type certain). Alors il existe un idéal maximal  $I_m \subseteq A$  (de même type) qui contient  $I$ .

---

9. Anglais : Maximal ideal.



**Preuve :** Soit  $\mathcal{F}$  la famille des idéaux de même type comme  $I$ , inégaux à  $A$ , contenant  $I$ . Car  $I \in \mathcal{F}$  on a  $I \neq \emptyset$ . L'inclusion munit  $\mathcal{F}$  d'un ordre. Soit  $\mathcal{J} \subseteq \mathcal{F}$  un ensemble totalement ordonné. Alors  $J_m := \bigcup_{J \in \mathcal{J}} J$  est un idéal contenant  $I$ , majorant de  $\mathcal{J}$ . Note que  $J_m \neq A$  par remarque 1.2.1(ii). Par le lemme de Zorn A.0.14,  $\mathcal{F}$  a un élément  $I_m$  maximal (maximal contenant  $I$ ). Cet idéal est en fait un idéal maximal.  $\square$

### 1.2.20 Lemme sur idéaux maximaux et premiers

Si  $(A, +, \cdot)$  est un anneau commutatif et  $I \subseteq A$  un idéal maximal, alors  $I$  est un idéal premier. Autrement dit,  $\text{Specmax}(A) \subseteq \text{Spec}(A)$ .

**Preuve par l'absurde :** Soient  $a, b \in A$  tels que  $ab \in I$  et  $a, b \notin I$ . Donc les idéaux

$$I_a := \langle I \cup \{a\} \rangle = I + Aa \quad , \quad I_b := \langle I \cup \{b\} \rangle = I + Ab$$

sont tels que  $I \subsetneq I_a$  et  $I \subsetneq I_b$ . Mais  $I$  est maximal, donc  $I_a = A = I_b$ . Donc

$$A = I_a I_b = \underbrace{II}_{\subseteq I} + \underbrace{IAb}_{\subseteq I} + \underbrace{AaI}_{\subseteq I} + \underbrace{AaAb}_{Aab \subseteq I} \subseteq I \quad ,$$

une contradiction à  $I \neq A$ !

**Autrement :** Soit  $I \subseteq A$  maximal. D'après 1.2.18, l'anneau  $A/I$  est un corps et donc intègre. Donc  $I$  est premier et on retrouve lemme 1.2.20.  $\square$

### Exemples :

- (i) Les idéaux de  $(\mathbb{Z}, +, \cdot)$  sont exactement ses sous-groupes, donc de la forme  $n\mathbb{Z}$  où  $n \in \mathbb{N}_0$ . Les idéaux premiers sont ceux engendrés par les nombres premiers ou nul :

$$\text{Spec}(\mathbb{Z}) = \{p\mathbb{Z} : p \in \mathbb{P}\} \cup \{0\mathbb{Z}\}$$

Les fermés de la topologie de Zariski sont de la forme

$$\mathcal{Z}(n\mathbb{Z}) = \{p\mathbb{Z} : p \in \mathbb{P}, p \mid n\} \quad , \quad n \in \mathbb{N}$$

ou  $\mathcal{Z}(0\mathbb{Z}) = \text{Spec}(\mathbb{Z})$ . Donc, le singleton  $\{0\mathbb{Z}\} \in \text{Spec}(\mathbb{Z})$  n'est pas un point fermé. D'autre part, les idéaux premiers  $p\mathbb{Z}$  avec  $p \in \mathbb{P}$  sont des points fermés de  $\text{Spec}(\mathbb{Z})$ , car  $\mathcal{Z}(p\mathbb{Z}) = \{p\mathbb{Z}\}$ .

Les idéaux maximaux sont

$$\text{Specmax}(\mathbb{Z}) = \{p\mathbb{Z} : p \in \mathbb{P}\} \quad ,$$

inclus dans  $\text{Spec}(\mathbb{Z})$  comme prévu par 1.2.20.

- (ii) Tous les idéaux de  $\mathbb{C}[X]$  sont de la forme  $Q \cdot \mathbb{C}[X]$  où  $Q \in \mathbb{C}[X]$ , c'est-à-dire  $\mathbb{C}[X]$  est principal. Ses idéaux premiers sont exactement l'idéal trivial et ceux engendrés par les polynômes de degré 1 (*premiers*) :

$$\text{Spec}(\mathbb{C}[X]) = \{P \cdot \mathbb{C}[X] : P(x) = (x - a), a \in \mathbb{C}\} \cup \{0\} \quad .$$

En analogie à  $\mathbb{Z}$ , les fermés de la topologie de Zariski sont de la forme

$$\mathcal{Z}(Q \cdot \mathbb{C}[X]) = \{(x - a) \cdot \mathbb{C}[X] : a \in \mathbb{C}, (x - a) \mid Q\} \quad , \quad Q \in \mathbb{C}[X] \setminus \{0\}$$

ou  $\mathcal{Z}(0 \cdot \mathbb{C}[X]) = \text{Spec}(\mathbb{C}[X])$ . donc, le nul  $0 \cdot \mathbb{C}[X]$  n'est pas un point fermé. D'autre part, les idéaux premiers  $P \cdot \mathbb{C}[X]$  avec  $P(x) = (x - a)$ ,  $a \in \mathbb{C}$  sont des points fermés de  $\text{Spec}(\mathbb{C}[X])$ , car  $\mathcal{Z}(P \cdot \mathbb{C}[X]) = \{P \cdot \mathbb{C}[X]\}$ .

### 1.2.21 Théorème : Idéaux maximaux et anneaux locaux

Soit  $(A, +, \cdot)$  un anneau. Les suivantes propriétés sont équivalents :

1.  $A$  possède un idéal à gauche maximal unique.
2.  $A$  possède un idéal à droite maximal unique.
3.  $A \setminus A^\times$  est un idéal bilatère.
4.  $A \setminus A^\times$  est un idéal bilatère maximal.
5.  $A \setminus A^\times$  est un idéal bilatère maximal, unique.

En tout cas, les (uniques) idéaux maximaux à gauche, droite et bilatères sont égaux et on dit  $A$  un anneau **local**<sup>10</sup>. Si en plus  $A$  est commutatif, son idéal maximal (unique) est  $A \setminus A^\times$ .

### 1.2.22 Lemme sur parties multiplicatives

Soit  $(A, +, \cdot)$  un anneau commutatif et  $\emptyset \neq S \subseteq A \setminus \{0\}$  une partie **multiplicatif** c.a.d.  $S \cdot S \subseteq S$ . Alors il existe un idéal premier de  $A$  disjoint de  $S$ .

**Preuve :** Considérons l'ensemble  $\mathcal{E}$  des idéaux dans  $A$  disjoint à  $S$ . Car  $\{0\} \in \mathcal{E}$ , on a  $\mathcal{E} \neq \emptyset$ . L'inclusion munit  $\mathcal{E}$  d'un ordre. Suit  $\mathcal{F} \subseteq \mathcal{E}$  un sous-ensemble totalement ordonné de  $\mathcal{E}$ , donc  $\forall I, J \in \mathcal{F}$  on a  $I \subseteq J$  ou  $J \subseteq I$ . Alors l'ensemble  $H := \bigcup_{I \in \mathcal{F}} I$  est aussi un idéal de  $A$  tel que  $H \cap S = \emptyset$ .

Donc, par le lemme de Zorn, l'ensemble  $\mathcal{F}$  admet au moins un élément maximal  $I_{\max}$ , c.a.d. il n'y a pas d'idéal  $I \supsetneq I_{\max}$  tel que  $I \cap S = \emptyset$ . On va montrer par l'absurde que l'idéal  $I_{\max}$  est premier. Soient  $a, b \in A \setminus I_{\max}$  tels que  $ab \in I_{\max}$ . Donc les idéaux

$$I_a := I_{\max} + Aa \quad , \quad I_b := I_{\max} + Ab$$

sont tels que  $I_{\max} \subsetneq I_a$  et  $I_{\max} \subsetneq I_b$ , donc  $S \cap I_a \neq \emptyset$  et  $S \cap I_b \neq \emptyset$ . Soient  $s_a \in S \cap I_a$  et  $s_b \in S \cap I_b$ , alors

$$s_1 s_2 \in I_a I_b = \underbrace{I_{\max} I_{\max}}_{\subseteq I_{\max}} + \underbrace{I_{\max} Ab}_{\subseteq I_{\max}} + \underbrace{Aa I_{\max}}_{\subseteq I_{\max}} + \underbrace{Aa Ab}_{Aab \subseteq I_{\max}} \subseteq I_{\max}$$

et  $s_1 s_2 \in S$  car  $S$  est multiplicative. Mais ça veut dire  $S \cap I_{\max} \neq \emptyset$ , une contradiction! □

### 1.2.23 Corollaire

Soit  $(A, +, \cdot)$  un anneau commutatif et  $a \in A$ . Alors  $a$  est nilpotent ssi il appartient à tous les idéaux premiers de  $A$ .

**Démonstration :** Sens " $\Rightarrow$ ". Soit  $I \subseteq A$  un idéal premier et  $a \in A$ ,  $n \geq 2$ . Alors  $a^n \in I$  implique  $a^{n-1} \in I$  ou  $a \in I$ , donc en tout cas  $a^{n-1} \in I$ . Parce que  $0 \in I$ , par récursivité tout élément nilpotent est contenu par  $I$ . Sens " $\Leftarrow$ ". Soit  $a \in A$  un élément pas nilpotent, c.a.d.  $a^n \neq 0 \quad \forall n \in \mathbb{N}$ . Considérons l'ensemble multiplicatif  $S := \{a^n : n \in \mathbb{N}\}$ , alors  $\emptyset \neq S \subseteq A \setminus \{0\}$ . Donc, par lemme 1.2.22 il y a un idéal premier  $I \subseteq A$  disjoint de  $S$ . En particulier  $a \notin I$ . □

### 1.2.24 Exemple : Les fonctions continues

Soit  $X$  un espace topologique compacte, de cardinal  $\geq 2$ , connexe, fonctionnellement Hausdorff<sup>11</sup> et  $A := \mathcal{C}(X, \mathbb{R})$  l'anneau des fonctions continues, réelles sur  $X$ . Pour  $x \in X$  on pose  $\mathfrak{R}_x := \{f \in A : f(x) = 0\}$ . Alors :

10. Anglais : Local ring.

11. C.a.d. tous deux points peuvent être séparés par une fonction continue.

1. Les idéaux maximaux de  $A$  sont exactement les ensembles  $\mathfrak{M}_x$ ,  $x \in X$ .
2. L'application  $x \mapsto \mathfrak{M}_x$  entre  $X$  et  $\text{Specmax}(A)$  est une bijection.
3. Tout  $\mathfrak{M}_x$  n'est pas un idéal de type fini.

**Preuve :**

1. La projection  $\delta_x : A \rightarrow \mathbb{R}$  définie par  $\delta_x : f \mapsto f(x)$  est un homomorphisme surjective d'anneaux, avec noyau  $\ker \delta_x = \mathfrak{M}_x$ . Donc par 1.2.13,  $A/\mathfrak{M}_x \cong \mathbb{R}$  pour chaque  $x \in X$ . Car  $\mathbb{R}$  est un corps,  $A/\mathfrak{M}_x$  est un corps et donc par 1.2.18  $\mathfrak{M}_x$  est un idéal maximal.

D'autre part, soit  $\mathfrak{M} \subsetneq A$  un idéal maximal et supposer que  $\mathfrak{M}_x \neq \mathfrak{M} \forall x \in X$ . Car  $\mathfrak{M}$  est maximal, alors pour tout  $x \in X$  il existe  $f \in \mathfrak{M} \setminus \mathfrak{M}_x$ . Définir les ouverts  $U_f := f^{-1}(\mathbb{R} \setminus \{0\})$  pour  $f \in A$ . Alors  $X = \bigcup_{f \in \mathfrak{M}} U_f$  est car  $X$  est compact on peut choisir  $f_1, \dots, f_n \in \mathfrak{M}$  tels que  $X = \bigcup_{i=1}^n U_{f_i}$ . Pose  $g := \sum_{i=1}^n f_i^2$ , alors  $g \in \mathfrak{M}$  et  $g > 0$ , c.a.d.  $g \in \mathfrak{M} \cap A^\times \neq \emptyset$  et donc par 1.2.1(ii) on a  $\mathfrak{M} = A$ . Ça, c'est une contradiction !

2. Évident car pour  $x \neq y \in X$  il y a une  $f \in A$  tel que  $f(x) \neq f(y)$ .
3. Preuve par l'absurde : Supposons au contraire qu'il existe  $f_1, \dots, f_n \in \mathfrak{M}_x$  tels que  $\mathfrak{M}_x = \langle f_1, \dots, f_n \rangle$ . On défini

$$f := \max_{1 \leq i \leq n} |f_i| \in \mathfrak{M}_x \quad .$$

et vois que  $\sqrt{f} \in \mathfrak{M}_x$  aussi. Par assomption il y a  $\alpha_1, \dots, \alpha_n \in A$  tels que  $\sqrt{f} = \sum_{i=1}^n \alpha_i \cdot f_i$  et donc

$$\sqrt{f} \leq \sum_{i=1}^n |\alpha_i| \cdot \underbrace{|f_i|}_{\leq f} \leq f \cdot \sum_{i=1}^n |\alpha_i| \quad .$$

Parce que  $X$  est compacte, les  $\alpha_i \in \mathcal{C}(X)$  sont bornées et donc

$$\sqrt{f} \leq f \cdot \underbrace{\sum_{i=1}^n \|\alpha_i\|_\infty}_c$$

On a par ça trouvé une<sup>12</sup>  $0 \neq f \in \mathfrak{M}_x$  telle que  $\mathfrak{M}_x \ni \sqrt{f} \leq c \cdot f$ .

Cette inégalité implique  $f(y) \geq c^{-2}$  pour tout  $y \in X$  tel que  $f(y) \neq 0$ . Note que  $f(x) = 0$  et  $f \neq 0$ . Donc  $f : X \rightarrow \mathbb{R}$  est une fonction continue dont l'image n'est pas connexe. Ça, c'est une contradiction car  $X$  est connexe.

□

### 1.2.25 Théorème des restes chinois

Soit  $(A, +, \cdot)$  un anneau commutatif et  $(I_i)_{i=1}^n$  une famille d'idéaux deux à deux **étrangers** entre eux, ça veut dire  $I_i + I_j = A \forall i \neq j$ . Alors leur idéal produit (voir 1.2.9) est donné par

$$\left\langle \prod_{i=1}^n I_i \right\rangle = \bigcap_{i=1}^n I_i \quad . \quad (1.2.25.1)$$

Son anneau quotient est isomorphe à l'anneau produit des anneaux quotients individuels :

$$A / \bigcap_{i=1}^n I_i \cong \prod_{i=1}^n A / I_i$$

avec l'isomorphisme

$$\Phi : \left[ a + \bigcap_{i=1}^n I_i \right] \mapsto (a + I_i)_{i=1}^n \quad , \quad a \in A \quad . \quad (1.2.25.2)$$

12. Note que par les propriétés de  $X$  il faut  $\mathfrak{M}_x \neq \{0\}$  et donc  $f \neq 0$ .

**Preuve :** On note  $I := \bigcap_{i=1}^n I_i$ . C'est évident que l'application  $\Phi : A/I \rightarrow \prod_{i=1}^n A/I_i$  de (1.2.25.2) est bien définie et un morphisme d'anneaux. Si  $\Phi(a + I) = (0, \dots, 0)$  il faut  $a \in I_i \forall i$  et donc  $a \in I$ , donc  $\Phi$  est injective. On va montrer par induction que  $\Phi$  est surjectif et  $I = \langle \prod_{i=1}^n I_i \rangle$ .

**Cas  $n = 2$  :** Soit  $n = 2$  et  $I_1 + I_2 = A$ , c.a.d.  $1 \in I_1 + I_2$  et donc  $1 = a_1 + a_2$  pour  $a_i \in I_i$  appropriés. Bien sûr on a  $\langle I_1 I_2 \rangle \subseteq I_1 \cap I_2$ . D'autre part, pour  $x \in I_1 \cap I_2$  on a

$$x = \underbrace{x \cdot a_1}_{\in I_2 I_1} + \underbrace{x \cdot a_2}_{\in I_1 I_2} \in \langle I_1 \cdot I_2 \rangle$$

et donc l'égalité  $\langle I_1 \cdot I_2 \rangle = I_1 \cap I_2$ . Pour la surjectivité du  $\Phi$  il faut montrer que pour  $b_1, b_2 \in A$  il existe un  $a \in A$  tel que  $a + I_i = b_i + I_i$ . Mais vraiment, on a

$$b_1 - b_2 = (b_1 - b_2) \cdot a_1 + (b_1 - b_2) \cdot a_2$$

et donc

$$b_1 = b_2 + \underbrace{(b_1 - b_2) \cdot a_1}_{\in I_1} + (b_1 - b_2) \cdot a_2 .$$

On pose  $a := b_2 + (b_1 - b_2) \cdot a_2$  et trouve d'une part que  $b_1 \in a + I_1$ . D'autre part on a

$$b_2 = a + \underbrace{(b_2 - b_1) \cdot a_2}_{\in I_2} \in a + I_2$$

et donc  $\Phi : A/I_1 \cap I_2 \rightarrow (A/I_1) \times (A/I_2)$  est surjectif.

**Cas  $n \geq 3$  :** On suppose l'affirmation reste vrai pour  $n - 1$ . Soit  $I_1 + I_i = A$  pour  $i \in \{2, \dots, n\}$ , c.a.d.  $a_i + b_i = 1$  pour appropriés  $a_i \in I_1$ ,  $b_i \in I_i$ . On a d'une part

$$1 = \prod_{i=2}^n (a_i + b_i) = \prod_{i=2}^n b_i + \underbrace{\sum \{\text{termes contenant des } a_i\}}_{\in I_1} \in I_1 + \left\langle \prod_{i=2}^n I_i \right\rangle$$

et donc

$$I_1 + \left\langle \prod_{i=2}^n I_i \right\rangle = A . \quad (1.2.25.3)$$

D'autre part, par la hypothèse de récurrence il faut

$$\left\langle \prod_{i=2}^n I_i \right\rangle = \bigcap_{i=2}^n I_i \quad (1.2.25.4)$$

et donc par le cas  $n = 2$  :

$$I_1 \cap \bigcap_{i=2}^n I_i \stackrel{(1.2.25.4)}{=} I_1 \cap \left\langle \prod_{i=2}^n I_i \right\rangle \stackrel{(1.2.25.3)}{\underset{\text{cas } n=2}{=}} \left\langle I_1 \cdot \left\langle \prod_{i=2}^n I_i \right\rangle \right\rangle = \left\langle \prod_{i=1}^n I_i \right\rangle .$$

De plus, on a le chaîne des isomorphismes

$$A / \bigcap_{i=1}^n I_i = A / \left[ I_1 \cap \bigcap_{i=2}^n I_i \right] \stackrel{\text{cas } n=2}{\cong} (A/I_1) \times A / \bigcap_{i=2}^n I_i \stackrel{\text{cas } n-1}{=} (A/I_1) \times \prod_{i=2}^n A/I_i \cong \prod_{i=1}^n A/I_i .$$

Ça finit la preuve. □

### Remarques

(i) L'isomorphie du morphisme (1.2.25.2) est équivalent à la déclaration suivante :

$$\forall b_1, \dots, b_n \in A : \exists a \in A : a \in b_i + I_i \quad \forall i \quad (1.2.25.5)$$

alors  $a$  est unique modulo l'idéal produit  $\langle \prod_{i=1}^n I_i \rangle$ .

(ii) Un cas spécial (en prenant  $A := \mathbb{Z}$  et  $I_i = \mathbb{Z}n_i$ ) du théorème est le suivant : Soient  $n_1, \dots, n_k \in \mathbb{N}$  deux à deux premiers entre eux<sup>13</sup> et  $a_1, \dots, a_k \in \mathbb{Z}$  n'importe quels. Alors, il existe un entier  $x \in \mathbb{Z}$ , unique modulo<sup>14</sup>  $n := \prod_{i=1}^k n_i$ , tel que  $x = a_i \pmod{n_i} \quad \forall i \in \{1, \dots, k\}$ .

13. Noter que par Bézout 4.1.10, pour tout  $i \neq j$  on a donc  $\mathbb{Z}n_i + \mathbb{Z}n_j = \mathbb{Z}$ , c'est-à-dire les  $\mathbb{Z}n_i$  sont deux à deux étrangers.

14. Noter que par remarque 4.1.9(vi) on a  $\bigcap_{i=1}^k \mathbb{Z}n_i = \mathbb{Z} \text{ppcm}(n_1, \dots, n_k) = \mathbb{Z} \prod_{i=1}^k n_i$ .

## 1.3 Anneaux Noetheriens

### 1.3.1 Définition: Anneau Noetherien

Un anneau  $(A, +, \cdot)$  est dit **noetherien** à gauche si tout idéal à gauche  $I \subseteq A$  est de type fini.

#### Exemples

- (i) Tout idéal  $n\mathbb{Z} \subseteq \mathbb{Z}$  de  $\mathbb{Z}$  est principal et donc de type fini. Ainsi,  $\mathbb{Z}$  est noetherien.
- (ii) Tout corps  $\mathbb{K}$  est un anneau noetherien.

### 1.3.2 Théorème : Caractérisation des anneaux noetheriens

Soit  $(A, +, \cdot)$  un anneau. Alors il y a équivalence entre :

1.  $A$  est noetherien.
2. Toute suite croissante  $I_1 \subseteq I_2 \subseteq \dots \subseteq A$  des idéaux à gauche dans  $A$  est finie, ça veut dire  $I_i = I_N \forall i \geq N$  pour un  $N \in \mathbb{N}$  assez grand.
3. Toute famille non-vidée d'idéaux à gauche admet un élément maximal.

#### Preuve :

- 1  $\Rightarrow$  2 :** L'ensemble  $I := \bigcup_{i=1}^{\infty} I_i$  est un idéal dans  $A$ , donc avec un nombre fini de générateurs  $a_1, \dots, a_n$ . Il existe donc un  $N \in \mathbb{N}$  assez grand tel que  $a_1, \dots, a_n \in I_N$ . Donc  $I = I_N$ .
- 2  $\Rightarrow$  3 :** Par l'absurde : Suppose que pour tout idéal  $I \in \mathcal{I}$  dans la famille d'idéaux à gauche  $\mathcal{I}$  il existe un  $I' \in \mathcal{I}$  tel que  $I \subsetneq I'$ . Alors, il existe une suite strictement croissante des idéaux. Ça, c'est une contradiction !
- 3  $\Rightarrow$  1 :** Soit  $I \subseteq A$  un idéal et  $\mathcal{I}$  la famille des idéaux de type fini  $\subseteq I$ . Soit  $J \in \mathcal{I}$  maximal, alors  $J = I$ . Sinon, prends un  $x \in I \setminus J$  et pose  $J' := J + Ax$ . Or  $J \subsetneq J' \in \mathcal{I}$ , une contradiction !

□

### 1.3.3 Lemme : Anneaux quotients des anneaux noetheriens

Soit  $A$  un anneau noetherien et  $I \subseteq A$  un idéal bilatère. Alors l'anneau quotient  $A/I$  est aussi noetherien.

**Preuve :** Considérons le morphisme canonique  $\Pi : A \rightarrow A/I$ , surjectif. Soit  $J \subseteq A/I$  un idéal. Alors  $\Pi^{-1}(J)$  est un idéal dans  $A$  et donc engendré par un nombre fini des éléments  $a_1, \dots, a_n \in A$ . Après 1.2.5(1) on a

$$J = \Pi(\Pi^{-1}(J)) = \Pi(\langle a_1, \dots, a_n \rangle_g) \stackrel{1.2.5(1)}{=} \langle \Pi(a_1), \dots, \Pi(a_n) \rangle_g$$

et  $J$  est donc de type fini.

□

## 1.4 Algèbres

### 1.4.1 Définition: $R$ -Algèbre

Soit  $R$  un anneau commutatif, dit l'**anneau de base**. Une  **$R$ -algèbre** est un couple  $(A, \tau)$  tel que :

1.  $A$  est un anneau (pas forcément commutatif).
2.  $\tau : R \rightarrow Z(A)$  est un morphisme d'anneaux dans le centre  $Z(A)$  de  $A$ .

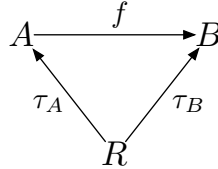
Souvent,  $\tau$  est injectif et alors on identifie  $R$  avec son image dans  $Z(A)$ .

### 1.4.2 Définition: Morphisme de $R$ -algèbres

Soit  $R$  un anneau commutatif et  $(A, \tau_A)$ ,  $(B, \tau_B)$   $R$ -algèbres. Un morphisme d'anneaux  $f : A \rightarrow B$  est dit un **morphisme de  $R$ -algèbres** si

$$f(\tau_A(r)) = \tau_B(r) \quad , \quad r \in R \quad .$$

Si on identifie les images  $\tau_A(r), \tau_B(r)$  par l'élément  $r \in R$ , on peut interpréter l'en dessus comme " $f(r) = r$ ". Si  $f$  est bijective, on dit  $f$  un **isomorphisme de  $R$ -algèbres** et note  $A \cong_R B$ .



**FIGURE 4:** Illustration d'un morphisme de  $R$ -algèbres. Le diagramme commute.

### Exemples

- (i) L'algèbre  $\mathbb{R}^{n \times n}$  des matrices à coefficients dans  $\mathbb{R}$  est une  $\mathbb{R}$ -algèbre par rapport du morphisme injectif

$$\mathbb{R} \hookrightarrow \mathbb{R}^{n \times n} \quad , \quad \alpha \mapsto \begin{pmatrix} \alpha & \dots & 0 \\ & \ddots & \\ 0 & \dots & \alpha \end{pmatrix} .$$

Le morphisme d'anneaux

$$\mathbb{R}^{n \times n} \rightarrow \mathbb{R}^{2n \times 2n} \quad , \quad M \mapsto \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$$

est un morphisme de  $\mathbb{R}$ -algèbres.

- (ii) Soient  $\mathbb{K} \subseteq \mathbb{L}$  deux corps. Alors  $\mathbb{L}$  est *naturellement* une  $\mathbb{K}$ -algèbre par rapport à l'inclusion  $\mathbb{K} \hookrightarrow \mathbb{L}$ .

## 2 Modules

### 2.1 Modules

#### 2.1.1 Definition: Opération d'un anneau sur un groupe, module

Soit  $(A, +, \cdot)$  un anneau (pas forcément commutatif) et  $(G, +)$  un groupe abélien. Une **opération** (à gauche) de l'anneau  $A$  sur le groupe  $G$  est un morphisme d'anneaux

$$\rho : (A, +, \cdot) \rightarrow (\text{End}(G), +, \circ) \quad .$$

Autrement dit,  $\rho$  satisfait pour  $x, y \in G$  et  $a, b \in A$  :

1.  $\rho(a)(x + y) = \rho(a)(x) + \rho(a)(y)$ .
2.  $\rho(a + b)(x) = \rho(a)(x) + \rho(b)(x)$ .
3.  $\rho(a \cdot b)(x) = \rho(a)(\rho(b)(x))$ .
4.  $\rho(1_A) = \text{Id}_G$ .

On appelle  $\rho(a) \in \text{End}(G)$  l'**homothétie** de  $a \in A$  sur  $G$  et note souvent  $\rho(a)(x) =: ax$  pour  $a \in A$ ,  $x \in G$ . On dit  $G$  un  **$A$ -module** à gauche. Un sous-groupe  $G_0 \leq G$  de  $G$  est dit **sous- $A$ -module**, si  $AG_0 \subseteq G_0$ , c.a.d.  $ax \in G_0 \quad \forall x \in G_0, a \in A$ .

**Remarque :** Soit  $(G_i)_{i \in I}$  une famille de sous- $A$ -modules du  $A$ -module  $G$ . Alors, leur intersection  $\bigcap_{i \in I} G_i$  est aussi un sous- $A$ -module.

#### 2.1.2 Definition: Module simple

Soit  $A$  un anneau. Alors, un  $A$ -module  $G$  est dit **simple** ssi il ne contient pas de sous- $A$ -modules excepté  $\{0\}$  et  $G$ .

#### 2.1.3 Definition: Morphisme d'un module

Soit  $(A, +, \cdot)$  un anneau et  $(G, +), (H, +)$  des  $A$ -modules. Un **morphisme de  $A$ -modules** (**application  $A$ -linéaire**) est un morphisme de groupes  $f : G \rightarrow H$  qui commute avec l'opération de  $A$ , ça veut dire  $f(ax) = a(f(x))$  pour  $a \in A$ ,  $x \in G$ .

$$\begin{array}{ccc}
 G & \xrightarrow{f} & H \\
 \uparrow a & & \uparrow a \\
 G & \xrightarrow{f} & H
 \end{array}
 \quad a \in A$$

**FIGURE 5:** Illustration d'une application  $A$ -linéaire entre deux  $A$ -modules. Le diagramme commute.

On note  $\text{Hom}_A(G, H)$  l'ensemble des applications  $A$ -linéaires  $G \rightarrow H$  et

$$\text{End}_A(G) := \text{Hom}_A(G, G) \quad , \quad \text{Aut}_A(G) := \text{End}_A(G) \cap \text{Sym}(G) \quad .$$

On dit que deux  $A$ -modules  $G, H$  sont **isomorphes**, s'il existe un  $A$ -linéaire isomorphisme de groupes, appelé **isomorphisme de  $A$ -modules**, entre les deux. On note  $G \cong_A H$ .

**Remarques :**

- (i) Avec la composition

$$(f_1 + f_2)(x) := f_1(x) + f_2(x), \quad f_1, f_2 \in \text{Hom}_A(G, H), \quad x \in G$$

l'ensemble  $\text{Hom}_A(G, H)$  est muni d'une structure de groupe abélien. Si en plus  $A$  est commutatif, alors

$$(af)(x) := a(f(x)) \quad , \quad f \in \text{Hom}_A(G, H), \quad x \in G, \quad a \in A$$

munit  $\text{Hom}_A(G, H)$  d'une structure de  $A$ -module.

- (ii) Soient  $G_0 \leq G$  et  $H_0 \leq H$  sous- $A$ -modules des  $A$ -modules  $G$  et  $H$  respectivement. Soit  $f : G \rightarrow H$   $A$ -linéaire. Alors  $f(G_0)$  et  $f^{-1}(H_0)$  sont sous- $A$ -modules de  $H$  et  $G$  respectivement.
- (iii) Si  $f : G \rightarrow H$  est un isomorphisme de  $A$ -modules, alors l'inverse  $f^{-1}$  est également. De plus, l'isomorphisme entre  $A$ -modules est une relation d'équivalence.

**2.1.4 Définition: Module quotient**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $N \leq G$  un sous- $A$ -module de  $G$ . Alors, l'anneau  $A$  opère sur le groupe quotient  $G/N$  comme  $a(g + N) := (ag + N)$ ,  $a \in A$ ,  $g \in G$  et munit  $G/N$  d'une structure de  $A$ -module. Le  $A$ -module  $G/N$  est dit **module quotient** de  $G$  sur  $N$ . L'application quotient  $\Pi : G \rightarrow G/N$  donnée par  $g \mapsto g + N$  devient donc un morphisme de  $A$ -modules, s'appelle **morphisme quotient**.

**Exemples**

- (i) Soit  $G$  un  $A$ -module. Si  $A = \mathbb{K}$  est un corps, on retrouve à  $G$  la structure habituelle d'un  $\mathbb{K}$ -espace vectoriel. Les éléments de  $\mathbb{K}$  sont appelés les *scalaires*, les éléments de  $G$  sont appelés les *vecteurs*. Les sous- $\mathbb{K}$ -modules sont exactement les sous-espaces vectoriels. Les morphismes des  $\mathbb{K}$ -modules sont exactement les applications  $\mathbb{K}$ -linéaires entre espaces vectoriels.
- (ii) Tout groupe abélien  $(G, +)$  est un  $\mathbb{Z}$ -module par rapport du loi

$$n \cdot g := \underbrace{g + \cdots + g}_{\times n} \quad , \quad n \in \mathbb{Z}, \quad g \in G \quad .$$

Les sous-groupes sont exactement les sous- $\mathbb{Z}$ -modules et les groupes quotients exactement les modules quotients.

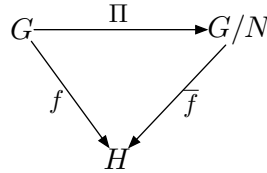
- (iii) Soient  $A, B$  deux anneaux commutatifs et  $\Phi : A \rightarrow B$  un morphisme d'anneaux. Si  $(G, +)$  est un  $B$ -module à gauche, alors l'application  $A \times G \rightarrow G$  définie comme  $(a, g) \mapsto \Phi(a)g$  fait du groupe abélien sous-jacent à  $G$  un  $A$ -module à gauche noté  $\Phi_*G$ . Si  $u \in \text{Hom}_B(G, H)$  est une application  $B$ -linéaire entre deux  $B$ -modules  $G, H$ , alors  $u \in \text{Hom}_A(\Phi_*G, \Phi_*H)$ . La réciproque n'est pas forcément vraie. Prendre par exemple le  $\mathbb{C}$ -module  $G := \mathbb{C}$  et l'inclusion  $\Phi : \mathbb{R} \hookrightarrow \mathbb{C}$ , alors  $G$  est aussi un  $\mathbb{R}$ -module par rapport à l'opération  $\lambda z := \Phi(\lambda)z$ ,  $\lambda \in \mathbb{R}$ ,  $z \in \mathbb{C}$ . Toute application  $\mathbb{C}$ -linéaire  $G \rightarrow H$  est aussi  $\mathbb{R}$ -linéaire. D'autre part, l'opération  $\mathbb{R}$ -linéaire  $z \mapsto z^*$  sur  $G$  n'est pas  $\mathbb{C}$ -linéaire.
- (iv) Tout anneau  $A$  est un  $A$ -module lui-même par rapport au loi de multiplication interne. Ses sous- $A$ -modules sont exactement ses idéaux à gauche. Si  $A$  est simple comme  $A$ -module, alors il est simple comme anneau. Si  $A$  est commutatif, alors l'inverse est aussi vrai.
- (v) Soit  $A$  un anneau,  $I \subseteq A$  un idéal bilatère et  $A/I$  l'anneau quotient, comme défini en 1.2.11. Alors, il existe une *correspondance bijective* entre  $(A/I)$ -modules et  $A$ -modules annihilés par  $I$ . Tout  $(A/I)$ -module  $G$  possède naturellement une structure de  $A$ -module via  $ag := (a + I)g$ ,  $a \in A$ ,  $g \in G$ . D'autre part, si  $H$  est un  $A$ -module tel que  $IH = \{0\}$ , la composition  $(a + I)h := ah$ ,  $a \in A$ ,  $h \in H$  est bien défini et fait de  $H$  un  $(A/I)$ -module. De plus, les deux associations sont compatibles.



**2.1.5 Théorème : Universalité d'un module quotient**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module,  $N \leq G$  un sous- $A$ -module et  $\Pi : G \rightarrow G/N, g \mapsto (g + N)$  le morphisme quotient. Alors :

1.  $\Pi$  est surjectif et satisfait  $\Pi(N) = \{0\}$ .
2.  $\Pi$  est **universal**, c'est-à-dire : Si  $H$  est un  $A$ -module et  $f : G \rightarrow H$   $A$ -linéaire telle que  $f(N) = 0$ , alors il existe une unique  $A$ -linéaire  $\bar{f} : G/N \rightarrow H$  telle que  $f = \bar{f} \circ \Pi$ .
3. Cette  $\bar{f}$  est injective ssi  $\ker(f) = N$ .
4. Si  $G_1$  est un  $A$ -module,  $\Pi_1 : G \rightarrow G_1$   $A$ -linéaire tel que  $\Pi_1(N) = \{0\}$  et satisfaisant (2), alors  $G/N \cong_A G_1$ .



**FIGURE 6:** Sur la universalité du groupe quotient  $G/N$  : Factorisation d'un morphisme  $f$ . Le diagramme commute.

**Preuve :**

1. Trivial.
2. Le preuve serait être proche à la preuve de 1.2.12. Pose  $\bar{f}(g + N) := f(g)$  pour  $g \in G$ , alors  $\bar{f} : G/N \rightarrow H$  est bien défini,  $A$ -linéaire et satisfait  $f = \bar{f} \circ \Pi$ . Unicité suit de la surjectivité de  $\Pi$ .
3. Par supposition on sait déjà que  $N \subseteq \ker(f)$ . Si  $\bar{f}$  est injective, alors  $f(x) = 0$  implique  $\Pi(x) = 0_{G/N}$ , c'est-à-dire  $x \in N$ . Si inversement  $\ker(f) \subseteq N$ , alors  $\bar{f}(x + N) = 0$  implique  $f(x) = 0$  et donc  $x \in N$ , c'est-à-dire  $\ker(\bar{f}) = \{0_{G/N}\}$ .
4. Soient  $G_1, G_2$  deux  $A$ -modules et  $\Pi_1 : G \rightarrow G_1, \Pi_2 : G \rightarrow G_2$  morphismes universels satisfaisant  $\Pi_1(N) = \Pi_2(N) = \{0\}$ . Alors il existe morphismes  $A$ -linéaires  $\bar{\Pi}_1 : G_2 \rightarrow G_1, \bar{\Pi}_2 : G_1 \rightarrow G_2$  tels que  $\Pi_1 = \bar{\Pi}_1 \circ \Pi_2$  et  $\Pi_2 = \bar{\Pi}_2 \circ \Pi_1$ .  
Donc

$$\bar{\Pi}_1 \circ \bar{\Pi}_2 \circ \Pi_1 = \bar{\Pi}_1 \circ \Pi_2 = \Pi_1$$

et par l'unicité de la factorisation de  $\Pi_1$  par  $\Pi_1$  lui même il faut  $\bar{\Pi}_1 \circ \bar{\Pi}_2 = \text{Id}$ . De même on trouve que  $\bar{\Pi}_2 \circ \bar{\Pi}_1 = \text{Id}$ , donc  $\bar{\Pi}_1 : G_2 \rightarrow G_1$  est un isomorphisme de  $A$ -modules avec l'inverse  $\bar{\Pi}_2$ .

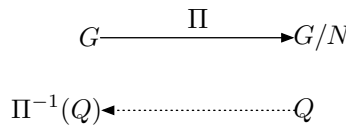
□

**2.1.6 Lemme : Sous-modules de modules quotients**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $N \leq G$  un sous- $A$ -module. Soit  $\Pi : G \rightarrow G/N$  le morphisme quotient dans le module quotient  $G/N$ . Alors, les sous- $A$ -modules du  $G/N$  correspondent via  $\Pi^{-1}$  de manière bijective aux sous-modules de  $G$  contenant  $N$ . De plus

$$(G/N)/Q \cong_A G/\Pi^{-1}(Q) \tag{2.1.6.1}$$

pour tout sous- $A$ -module  $Q \leq G/N$ .

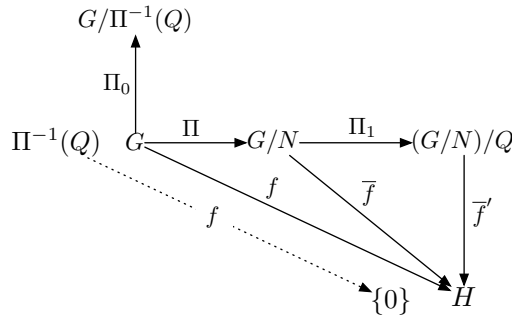


**FIGURE 7:** Sur la correspondance entre sous modules de  $G$  et du module quotient  $G/N$ .

**Preuve :** Soit  $Q \leq G/N$  un sous- $A$ -module de  $G/N$ . Alors, par remarque 2.1.3(ii)  $\Pi^{-1}(Q)$  est un sous- $A$ -module dans  $G$ . Car  $(0 + N) \in Q$  il faut  $N \in \Pi^{-1}(Q)$ . D'autre part, si  $P \leq G$  est un sous- $A$ -module contenant  $N$ , l'image  $\Pi(P) =: P/N$  est un sous- $A$ -module de  $G/N$  et car  $N \subseteq P$  il faut  $\Pi^{-1}(\Pi(P)) = P$  : sinon il existerait un  $g \in G \setminus P$  et  $p \in P$  tels que  $g + N = p + N$ , c'est-à-dire  $g \in p + N \subseteq p + P = P$ , une contradiction ! Finalement, l'application  $Q \rightarrow \Pi^{-1}(Q)$  est injective : Si  $Q_1, Q_2 \leq G/N$  sont sous- $A$ -modules tels que  $\Pi^{-1}(Q_1) = \Pi^{-1}(Q_2)$ , il faut  $Q_1 = Q_2$  car  $\Pi$  est surjective.

Soit  $Q \leq G/N$  un sous- $A$ -module de  $G/N$  et  $\Pi_1 : (G/N) \rightarrow (G/N)/Q$  le morphisme quotient de  $(G/N)/Q$ . Soit  $\Pi_0 : G \rightarrow G/\Pi^{-1}(Q)$  le morphisme quotient de  $G/\Pi^{-1}(Q)$ . Pour prouver l'isomorphisme (2.1.6.1) on va montrer que  $\Pi_1 \circ \Pi : G \rightarrow (G/N)/Q$  satisfait la propriété universelle 2.1.5(2) de  $\Pi_0 : G \rightarrow G/\Pi^{-1}(Q)$  et utilise l'unicité d'universalité 2.1.5(4). Évidemment  $\Pi_1 \circ \Pi(N) = \{0\}$  et  $\Pi_1 \circ \Pi$  est surjective.

Soit or  $f : G \rightarrow H$   $A$ -linéaire telle que  $f(\Pi^{-1}(Q)) = \{0\}$ . Alors  $f(N) = 0$  et on peut trouver une  $A$ -linéaire  $\bar{f} : (G/N) \rightarrow H$  telle que  $f = \bar{f} \circ \Pi$ . Car  $f(\Pi^{-1}(Q)) = \{0\}$  il faut  $\bar{f}(Q) = 0$ . Donc, on peut trouver une  $A$ -linéaire  $\bar{f}' : (G/N)/Q \rightarrow H$  telle que  $\bar{f} = \bar{f}' \circ \Pi_1$ , c'est-à-dire  $f = \bar{f}' \circ \Pi_1 \circ \Pi$ . Car  $\Pi_1 \circ \Pi$  est surjective,  $\bar{f}'$  est unique. Par 2.1.5(4) on a trouvé  $(G/N)/Q \cong_A G/\Pi^{-1}(Q)$ .



**FIGURE 8:** Sur la preuve de l'isomorphisme  $(G/N)/Q \cong_A G/\Pi^{-1}(Q)$ , par factorisation des fonctions  $f : G \rightarrow H$  satisfaisant  $f(\Pi^{-1}(Q)) = \{0\}$ .

□

### 2.1.7 Le théorème d'isomorphismes pour modules

Soient  $(A, +, \cdot)$  un anneau,  $(G, +)$ ,  $(H, +)$   $A$ -modules et  $f : G \rightarrow H$   $A$ -linéaire. Alors  $G/\ker(f) \cong_A f(G)$ .

**Preuve :** Pose  $F(g + \ker(f)) := f(g)$ , alors  $F : G/\ker(f) \rightarrow H$  est bien défini et un isomorphisme de  $A$ -modules.

□

### 2.1.8 Corollaire du théorème d'isomorphismes

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module avec sous- $A$ -modules  $M, N \leq G$ . Alors, on a

$$(M + N)/N \cong_A M/(M \cap N)$$

**Preuve :** Considérons l'application  $A$ -linéaire  $f := \Pi \circ i : M \rightarrow (M + N)/N$  où  $\Pi : (M + N) \rightarrow (M + N)/N$  est le morphisme quotient de  $(M + N)/N$  et  $i : M \rightarrow (M + N)$  l'inclusion de  $M$  dans  $(M + N)$ . Alors  $f$  est surjective et avec noyau  $\ker(f) = i^{-1}(\ker(\Pi)) = M \cap N$ . Donc par le théorème d'isomorphismes on trouve

$$M/M \cap N \cong_A (M + N)/N \quad .$$

□

### 2.1.9 Definition: Sous-module engendré

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$  module et  $X \subseteq G$  n'importe quel partie. Alors, le sous- $A$ -module

$$\text{span}_A(X) := \bigcap_{\substack{X \subseteq G_0 \leq G \\ G_0 \text{ } A\text{-module}}} G_0 = \left\{ \sum_{i=1}^n a_i x_i : a_i \in A, x_i \in X, n \in \mathbb{N}_0 \right\}$$

est le plus petit sous- $A$ -module de  $G$  qui contient  $X$  et s'appelle  **$A$ -module engendré par  $X$** . On dit  $X$  un  **$A$ -générateur de  $G$** . Si  $(G_i)_{i \in I}$  sont sous- $A$ -modules de  $A$ , alors le sous- $A$ -module engendré par leur union est donné par

$$\text{span}_A \left( \bigcup_{i \in I} G_i \right) = \sum_{i \in I} G_i := \left\{ \sum_{k=1}^n g_{i_k} : g_{i_k} \in G_{i_k}, i_k \in I, n \in \mathbb{N}_0 \right\}$$

En particulier, si  $I = \{1, \dots, n\}$  on a

$$\text{span}_A \left( \bigcup_{i=1}^n G_i \right) = G_1 + \dots + G_n .$$

On dit que le module  $G$  est de **type fini** ssi il possède un sous-ensemble fini qui engendre  $G$ . On dit  $G$  **cyclique** s'il est engendré par un seul élément.

### Remarques

- (i) Si  $G, H$  sont des  $A$ -modules,  $X \subseteq G$  un sous-ensemble n'importe quel et  $f : G \rightarrow H$   $A$ -linéaire, alors

$$\text{span}_A f(X) = f[\text{span}_A(X)] . \quad (2.1.9.1)$$

Si en particulier  $G$  est de type fini, alors  $f(G)$  est également.

- (ii) Si  $G$  est un  $A$ -module de type fini et engendré par un système  $X \subseteq G$  n'importe quel, alors il existe un nombre fini d'éléments  $x_1, \dots, x_n \in X$  tel que  $G = \text{span}_A(x_1, \dots, x_n)$ . Pour le voir, soit  $Y \subseteq G$  un générateur fini de  $G$ , alors pour  $y \in Y$  on peut trouver  $a_{yi} \in A, x_{yi} \in X$  tels que  $y = \sum_{i=1}^{n_y} a_{yi} x_{yi}$ . Prends  $\bigcup_{y \in Y} \{x_{y1}, \dots, x_{yn_y}\}$ .
- (iii) Tout  $A$ -module simple est cyclique, car tout  $0 \neq x$  engendre nécessairement tout le module.
- (iv) Toute groupe cyclique est un  $\mathbb{Z}$ -module cyclique.
- (v) Pour tout idéal  $J \subseteq A$  le  $A$ -module  $A/J$  est engendré par la classe  $\bar{1}$  et est donc cyclique.
- (vi) Inversement, tout  $A$ -module cyclique  $G = \text{span}_A\{g\}$  est isomorphe à un quotient  $A/J$  pour un idéal  $J \subseteq A$ . Pour le voir, considérer le morphisme de  $A$ -modules surjectif

$$A \rightarrow G, \quad \alpha \mapsto \alpha \cdot g,$$

et appliquer le théorème d'isomorphismes 2.1.7.

- (vii) De plus, tout  $A$ -module est simple ssi il est isomorphe à un quotient  $A/J$  pour un idéal maximal  $J \subseteq A$ . Pour le voir, se rappeler qu'il existe une association bijective, croissante entre les idéaux de  $A/J$  et les idéaux entre  $J$  et  $A$ .

### 2.1.10 Definition: Module noetherien

Soit  $A$  un anneau et  $G$  un  $A$ -module. Alors,  $G$  est dit **noetherien** ssi tout sous- $A$ -module de  $G$  est de type fini.

**Exemples**

- (i) Tout anneau  $A$  est un  $A$ -module lui-même par rapport à la multiplication. Ses sous-modules sont exactement ses idéaux à gauche. Si  $X \subseteq A$  est quelconque, alors l'idéal à gauche engendré par  $X$  est exactement le sous- $A$ -module engendré par  $X$ . Si  $I \subseteq A$  est un idéal à gauche, alors  $A/I$  est un  $A$ -module, même si  $I$  n'est pas bilatère.
- (ii) Tout anneau  $A$  est noetherien comme anneau ssi il est noetherien comme  $A$ -module. En fait, par 2.1.16 si  $A$  est noetherien comme anneau, tout  $A^n$ ,  $n \in \mathbb{N}$  est un  $A$ -module noetherien.
- (iii) Le  $\mathbb{Z}$ -module  $\mathbb{Z}^n$  est de type fini, car  $\mathbb{Z}^n = \text{span}_{\mathbb{Z}} \{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$ .
- (iv) Le  $\mathbb{Z}$ -module  $\mathbb{Z}/n\mathbb{Z}$  est de type fini, car il est fini lui-même.
- (v) Le  $\mathbb{Z}$ -module  $\mathbb{Q}$  n'est pas de type fini, car tout  $\text{span}_{\mathbb{Z}} \left\{ \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} \right\}$  pour quelques  $p_i, q_i \in \mathbb{Z} \setminus \{0\}$  contient seulement des rationnels du type  $p/q$  où  $q$  est le plus petit multiple commune des  $q_1, \dots, q_n$ .
- (vi) Le  $\mathbb{Z}$ -module  $\mathbb{R}$  n'est pas de type fini. S'il était, il faudrait existe  $r_1, \dots, r_n \in \mathbb{R}$  tels que l'application  $\mathbb{Z}^n \rightarrow \mathbb{R}$ ,  $(k_1, \dots, k_n) \mapsto k_1 r_1 + \dots + k_n r_n$  est surjective. Mais cela est impossible, car  $\mathbb{R}$  est de cardinal plus grand que  $\mathbb{Z}^n$ .

**2.1.11 Théorème : Caractérisation des modules noetheriens**

Soit  $A$  un anneau et  $G$  un  $A$ -module. Alors il y a équivalence entre :

1.  $G$  est un  $A$ -module noetherien.
2. Toute suite croissante  $G_1 \leq G_2 \leq \dots \leq G$  de sous- $A$ -modules de  $G$  est finie, ça veut dire  $G_n = G_N \forall n \geq N$  pour un  $N \in \mathbb{N}$  assez grand.
3. Toute famille non-vide de sous- $A$ -modules admet un élément maximal.

**Preuve :** Analogie à la preuve de théorème 1.3.2 sur anneaux noetheriens.

**2.1.12 Définition: Suite exacte**

Soit  $A$  un anneau. Une **suite exacte** de morphismes de  $A$ -modules est une famille  $(G_n, f_n)_{n \in \mathbb{Z}}$  de  $A$ -modules  $G_n$  et morphismes de  $A$ -modules  $f_n : G_n \rightarrow G_{n+1}$  qui satisfait  $\text{image}(f_n) = \ker(f_{n+1})$ . Souvent tous sauf un nombre fini de modules  $G_1, \dots, G_n$  sont triviales. En ce cas on note

$$0 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} G_n \longrightarrow 0$$

et demande  $\ker(f_1) = \{0\}$ ,  $\text{image}(f_{n-1}) = G_n$  et  $\text{image}(f_k) = \ker(f_{k+1}) \forall k \in \{1, \dots, n-2\}$ .

**2.1.13 Lemme sur modules de type fini et suites exactes**

Soit  $(A, +, \cdot)$  un anneau,  $G_1, G_2, G_3$   $A$ -modules et

$$0 \rightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \rightarrow 0$$

une suite exacte de morphismes de  $A$ -modules. Alors, si  $G_1, G_3$  sont de type fini,  $G_2$  est aussi de type fini.

**Preuve :** Soit  $x_1, \dots, x_n \in G_1$  une famille génératrice de  $G_1$  et  $z_1, \dots, z_m \in G_3$  une famille génératrice de  $G_3$ . Soient  $y_1, \dots, y_m \in G_2$  tels que  $g(y_i) = z_i$ ,  $i \in \{1, \dots, m\}$ , alors la famille  $\{f(x_1), \dots, f(x_n), y_1, \dots, y_m\}$  engendre le module  $G_2$ . □

### 2.1.14 Corollaire sur modules de type fini

Soit  $(A, +, \cdot)$  un anneau,  $G, H$   $A$ -modules et  $f : G \rightarrow H$   $A$ -linéaire telle que  $\ker(f)$  et  $f(G)$  sont  $A$ -modules de type fini. Alors,  $G$  est aussi de type fini.

**Preuve :** Soit  $i : \ker(f) \hookrightarrow G$  l'inclusion de  $\ker(f)$  dans  $G$ . Alors, en appliquant lemme 2.1.13 sur la suite exacte

$$0 \rightarrow \ker(f) \xrightarrow{i} G \xrightarrow{f} f(G) \rightarrow 0 ,$$

on déduit l'affirmation. □

### 2.1.15 Lemme sur modules noetheriens et suites exactes

Soit  $A$  un anneau,  $G_1, G_2, G_3$   $A$ -modules et

$$0 \rightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \rightarrow 0$$

une suite exacte de morphismes de  $A$ -modules. Alors,  $G_1, G_3$  sont noetheriens ssi  $G_2$  est noetherien.

**Preuve :**

**Direction “ $\Leftarrow$ ” :** Supposons que  $G_2$  est noetherien. Soit  $N_1 \leq N_2 \leq \dots \leq G_3$  une suite croissante de sous-modules de  $G_3$ , alors  $g^{-1}(N_1) \leq g^{-1}(N_2) \leq \dots \leq G_2$  est une suite croissante de sous-modules de  $G_2$ . Par 2.1.11 il existe un  $n_0 \in \mathbb{N}$  tel que  $g^{-1}(N_n) = g^{-1}(N_{n_0}) \forall n \geq n_0$ . Donc

$$N_n \xrightarrow{g} g(g^{-1}(N_n)) = g(g^{-1}(N_{n_0})) \xrightarrow{g} N_{n_0} \quad \forall n \geq n_0 ,$$

d'où on déduit que  $G_3$  est noetherien. En façon similaire on montre que  $G_1$  est noetherien.

**Direction “ $\Rightarrow$ ” :** Supposons que  $G_1, G_2$  sont noetheriens. Soit  $N_1 \leq N_2 \leq \dots \leq G_2$  une suite croissante de sous-modules de  $G_2$ , alors  $f^{-1}(N_1) \leq f^{-1}(N_2) \leq \dots \leq G_1$  et  $g(N_1) \leq g(N_2) \leq \dots \leq G_3$  sont suites croissantes de sous-modules de  $G_1$  et  $G_3$  respectivement. Par supposition et théorème 2.1.11, il existe un  $n_0 \in \mathbb{N}$  tel que  $f^{-1}(N_n) = f^{-1}(N_{n_0})$  et  $g(N_n) = g(N_{n_0})$  pour tout  $n \geq n_0$ . Soit  $a \in N_n$ , alors il existe un  $b \in N_{n_0}$  tel que  $g(a) = g(b)$ . Donc  $(a - b) \in \ker(g) = \text{image}(f)$ , c'est-à-dire

$$(a - b) \in f(G_1) \cap N_n = f(f^{-1}(N_n)) = f(f^{-1}(N_{n_0})) = \text{image}(f) \cap N_{n_0} .$$

Note qu'on a utilisé le fait que  $a, b \in N_n$  et  $N_n$  est un sous-module. Donc  $a \in b + N_{n_0} \subseteq N_{n_0}$  et plus général  $N_n \subseteq N_{n_0}$ . Cela complète la preuve. □

**Conséquences :**

- (i) Si  $G$  est un  $A$ -module noetherien,  $H$  un  $A$ -module quelconque et  $f : G \rightarrow H$  un morphisme de  $A$ -modules, alors  $f(G)$  est un sous-module noetherien. Pour le voir considère la suite exacte

$$0 \rightarrow \ker(f) \xrightarrow{\text{inclusion}} G \xrightarrow{f} f(G) \rightarrow 0 .$$

### 2.1.16 Corollaire sur puissances d'anneaux noetheriens

Soit  $A$  un anneau et  $n \in \mathbb{N}$  quelconque. Alors,  $A$  est un anneau noetherien ssi  $A^n$  est un  $A$ -module noetherien.

**Preuve :** On note que  $A$  est noetherien comme anneau ssi il est noetherien comme  $A$ -module.

**Direction “ $\Rightarrow$ ” :** Démonstration par récurrence : Considérons l’inclusion  $i : A \hookrightarrow A^n$ ,  $a \mapsto (a, 0, \dots, 0)$  et la projection  $p : A^n \rightarrow A^{n-1}$ ,  $(a_1, \dots, a_n) \mapsto (a_2, \dots, a_n)$ . Alors la suite

$$0 \longrightarrow A \xrightarrow{i} A^n \xrightarrow{p} A^{n-1} \longrightarrow 0$$

est exacte. Par lemme 2.1.15, si  $A$  et  $A^{n-1}$  sont  $A$ -modules noetheriens, alors  $A^n$  est également.

**Direction “ $\Leftarrow$ ” :** Considérons le sous- $A$ -module  $A \times \{0\} \times \dots \times \{0\} \leq A^n$  qui est isomorphe à  $A$ . Comme tout sous-module d’un module noetherien est lui même noetherien, on conclut l’affirmation.  $\square$

**Remarque :** Voir 6.0.7 pour une affirmation plus forte sur anneaux intègres, principaux.

### 2.1.17 Corollaire sur modules de type fini et modules noetheriens

Soit  $A$  un anneau noetherien et  $G$  un  $A$ -module de type fini. Alors  $G$  est un module noetherien.

**Preuve :** Soit  $\{x_i\}_{i=1}^n$  une famille finie génératrice de  $G$ . Alors le morphisme de  $A$ -modules

$$\sigma : A^n \rightarrow G, \quad \sigma : (a_i)_{i=1}^n \mapsto \sum_{i=1}^n a_i x_i$$

est surjective. Par 2.1.16  $A^n$  est noetherien. Par conséquence 2.1.15(i)  $G$  est noetherien.

**Preuve alternative :** Soit  $G$  engendré par la famille  $(\xi_i)_{i=1}^n$ . Alors, le morphisme de  $A$ -modules  $\Phi : A^n := \prod_{i=1}^n A \rightarrow G$  défini par  $\Phi : (a_i)_{i=1}^n \mapsto \sum_{i=1}^n a_i \xi_i$  est surjectif. Alors, par remarques 2.1.3(ii) et 2.1.9(i) il suffit à montrer que tout sous- $A$ -module de  $A^n$  est du type fini. Le cas  $n = 1$  est d’après exemple 2.1.9(i) et la définition d’un anneau noetherien clair.

Soit  $n \geq 2$  et supposons que l’affirmation est prouvé pour  $(n - 1)$ . Soit  $N \subseteq A^n$  un sous- $A$ -module. Considérons la restriction de la projection  $\Pi : A^n \rightarrow A$ ,  $\Pi : ((a_i)_{i=1}^n) \mapsto a_1$  sur  $N$ . Alors  $\Pi|_N(N) =: J$  est un idéal à gauche et car  $A$  est noetherien, de type fini. D’autre part,  $\ker \Pi|_N \subseteq \ker(\Pi) \hookrightarrow A^{n-1}$ , donc  $\ker \Pi|_N$  est par supposition de type fini. Par 2.1.14 ça implique que  $N$  est de type fini.  $\square$

### 2.1.18 Definition: Torsion

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module. Un élément  $g \in G$  est dit de **torsion** s’il existe  $a \in A \setminus \{0\}$  tel que  $ag = 0$ . On note  $G_{\text{tor}}$  l’ensemble des éléments de torsion de  $G$ . On dit que  $G$  **n’a pas de torsion** si  $G_{\text{tor}} = \{0\}$ . On dit  $G$  **est de torsion** si  $G_{\text{tor}} = G$ .

**Remarques :** On suppose que  $A$  est intègre. Alors :

- (i)  $G_{\text{tor}}$  est un sous-module de  $G$ .
- (ii)  $G/G_{\text{tor}}$  n’a pas de torsion.

### Exemples

1. Le  $\mathbb{Z}$ -module  $\mathbb{Z}^n$  n’a pas de torsion.
2. Pour le  $\mathbb{Z}^n$ -module  $\mathbb{Z}^n$  on a

$$(\mathbb{Z}^n)_{\text{tor}} = \{(k_1, \dots, k_n) \in \mathbb{Z}^n \mid \exists 1 \leq i \leq n : k_i = 0\} \quad .$$

### 2.1.19 Definition: Annulateur

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module. Alors, pour  $g \in G$  on appelle l'ensemble

$$\text{Ann}_A(g) := \{a \in A : ag = 0\}$$

annulateur de  $g$  dans  $A$ .

#### Remarques

1. Un élément  $g \in G$  est de torsion ssi  $\text{Ann}_A(g) \supsetneq \{0\}$ .
2. Tout annulateur  $\text{Ann}_A(g)$  est un idéal à gauche de  $A$ .
3. Si  $V$  est un  $\mathbb{K}$ -espace vectoriel et  $x \in V \setminus \{0\}$ , alors  $\text{Ann}_{\mathbb{K}}(x) = \{0\}$ .
4. Considère l'anneau  $A$  comme  $A$ -module lui même. Alors,  $a \in A \setminus \{0\}$  est diviseur de zéro ssi  $\text{Ann}_A(a) \neq \{0\}$ .

### 2.1.20 Exemple : Le corps quotient

Soit  $(A, +, \cdot)$  un anneau commutatif et  $S \subseteq A$  un sous ensemble multiplicatif<sup>15</sup> contenant l'unité 1. On introduit la relation d'équivalence  $\sim$  sur  $S \times A$  définie par

$$(s, a) \sim (s', a') \Leftrightarrow \exists t \in S : t(s'a - sa') = 0 \quad .$$

On note  $\frac{a}{s}$  la classe d'équivalence de  $(a, s) \in S \times A$  et  $S^{-1}A$  tous ces classes. Note que pour tout  $t \in S$  et  $\frac{a}{s} \in S^{-1}A$  on a  $\frac{ta}{ts} = \frac{a}{s}$ . Les applications

$$+ : S^{-1}A \times S^{-1}A \rightarrow S^{-1}A \quad , \quad \left( \frac{a}{s}, \frac{a'}{s'} \right) \mapsto \frac{a}{s} + \frac{a'}{s'} := \frac{s'a + sa'}{ss'}$$

$$\cdot : S^{-1}A \times S^{-1}A \rightarrow S^{-1}A \quad , \quad \left( \frac{a}{s}, \frac{a'}{s'} \right) \mapsto \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

sont bien définies et munissent  $S^{-1}A$  d'une structure d'anneau dont nul est  $\frac{0}{1}$  ( $= \frac{0}{s} \forall s \in S$ ) et l'unité est  $\frac{1}{1}$ . L'application  $\sigma : A \rightarrow S^{-1}A$ ,  $a \mapsto \frac{a}{1}$  est un morphisme d'anneaux, qui est injectif si  $A$  est intègre et  $0 \notin S$ . En particulier, par exemple 2.1.4(iii) tout  $S^{-1}A$ -module peut être regardé comme  $A$ -module via le transport de  $\sigma$ .

#### Note :

En cas que  $A$  est intègre,  $S := A \setminus \{0\}$  est une partie multiplicatif de  $A$  contenant 1 et  $S^{-1}A =: \text{Quot}(A)$  est un corps, le **corps quotient**<sup>16</sup> de  $A$ . Dans ce cas, pour  $a, b \in A$ ,  $t, s \in A \setminus \{0\}$  on a  $\frac{a}{s} = \frac{b}{t}$  ssi  $ta = sb$ . L'homomorphisme  $\sigma : A \hookrightarrow \text{Quot}(A)$  est un plongement de  $A$  dans son corps quotient.

En fait,  $\text{Quot}(A)$  est le plus petit corps contenant  $A$ , c'est-à-dire si  $A$  est plongé dans un corps  $\mathbb{K}$  via le morphisme d'anneaux  $i : A \hookrightarrow \mathbb{K}$ , alors il existe un morphisme de corps  $\Phi : \text{Quot}(A) \hookrightarrow \mathbb{K}$  tel que  $\Phi \circ \sigma = i$ . Un tel morphisme est donné par  $\Phi\left(\frac{a}{s}\right) := i(a) \cdot i(s)^{-1}$  où  $a \in A$ ,  $s \in A \setminus \{0\}$ . En particulier, si  $A$  est déjà un corps, on a  $A \cong \text{Quot}(A)$ .

Un exemple typique est  $\text{Quot}(\mathbb{Z}) \cong \mathbb{Q}$ .

Soit de plus  $(M, +)$  un  $A$ -module. De la même façon, on introduit sur  $S \times M$  la relation d'équivalence  $\sim$  définie par

$$(s, g) \sim (s', g') \Leftrightarrow \exists t \in S : t(s'g - sg') = 0 \quad .$$

On noté  $\frac{m}{s}$  la classe d'équivalence de  $(s, m) \in S \times M$  et  $S^{-1}M$  tous ces classes. Pareillement, on a  $\frac{tm}{ts} = \frac{m}{s}$  pour tout  $t \in S$ ,  $\frac{m}{s} \in S^{-1}M$ . L'application

$$+ : S^{-1}M \times S^{-1}M \rightarrow S^{-1}M \quad , \quad \left( \frac{m}{s}, \frac{m'}{s'} \right) \mapsto \frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$$

15. C'est-à-dire  $S \cdot S \subseteq S$ .

16. Anglais : Field of Fractions ou Field of Quotients.

est bien défini et fait de  $S^{-1}M$  un groupe abélien. D'autre, l'application

$$\cdot : S^{-1}A \times S^{-1}M \rightarrow S^{-1}M, \quad \left(\frac{a}{s}, \frac{m}{t}\right) \mapsto \frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$$

est bien définie et fait du groupe abélien  $S^{-1}M$  un  $S^{-1}A$ -module. Par le dessus,  $S^{-1}M$  est aussi un  $A$ -module par rapport du loi  $a \cdot \frac{m}{s} := \frac{a}{1} \cdot \frac{m}{s}$  où  $a \in A$ ,  $\frac{m}{s} \in S^{-1}M$ .

L'application  $i : M \rightarrow S^{-1}M$ ,  $m \mapsto \frac{m}{1}$  est un morphisme de  $A$ -modules, qui est injectif si  $A$  est intègre et  $0 \notin S$ . De plus, on peut montrer que  $M$  est trivial ssi  $(A \setminus \mathfrak{M})^{-1}M$  est trivial pour tout idéal maximal  $\mathfrak{M}$  de  $A$ .

### 2.1.21 Définition: Produit directe et somme directe des modules

Soit  $(A, +, \cdot)$  un anneau et  $(G_i)_{i \in I}$  une famille de  $A$ -modules. Alors, leur groupe produit  $\prod_{i \in I} G_i$  possède une structure *naturelle* d'un  $A$ -module avec les lois coordonnées par coordonnées :

$$a(g_i)_{i \in I} := (ag_i)_{i \in I}, \quad a \in A, \quad g_i \in G_i.$$

Avec ce lui, on dit  $\prod_{i \in I} G_i$  le **module produit direct** des  $(G_i)_{i \in I}$ . On note  $\bigoplus_{i \in I} G_i$  la **somme directe** des  $(G_i)_{i \in I}$ , c'est-à-dire le sous- $A$ -module de  $\prod_{i \in I} G_i$  des uplets à support fini :

$$\bigoplus_{i \in I} G_i := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i : |\{i \in I : g_i \neq 0\}| < \infty \right\}.$$

Si  $|I| < \infty$  alors  $\bigoplus_{i \in I} G_i = \prod_{i \in I} G_i$ . Pour  $i \in I$ , la **projection**  $p_i : \prod_{i \in I} G_i \rightarrow G_i$  donnée par  $(g_i)_{i \in I} \mapsto g_i$  est  $A$ -linéaire et surjectif. D'autre part, on a une **injection canonique**  $I_i : G_i \rightarrow \bigoplus_{i \in I} G_i$  donnée par  $g_i \mapsto (0, \dots, 0, g_i, 0, \dots)$ .

### 2.1.22 Définition: Somme directe de sous-modules

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module avec sous- $A$ -modules  $(G_i)_{i \in I}$ . Alors, il existe un morphisme des  $A$ -modules surjectif de  $\bigoplus_{i \in I} G_i$  dans leur somme  $\sum_{i \in I} G_i$  donné par

$$\bigoplus_{i \in I} G_i \rightarrow \sum_{i \in I} G_i, \quad (g_i)_{i \in I} \mapsto \sum_{\substack{i \in I \\ g_i \neq 0}} g_i. \quad (2.1.22.1)$$

La somme  $\sum_{i \in I} G_i$  (vois 2.1.9) est dit **directe** ssi (2.1.22.1) est injectif et donc un isomorphisme de  $A$ -modules. Autrement dit,  $\sum_{i \in I} G_i$  est directe, ssi tout  $x \in \sum_{i \in I} G_i$  est représentable par une unique somme finie des éléments non-nules des  $G_i$ .

Deux sous- $A$ -modules  $K, L$  de  $G$  ont dit **supplémentaires** ssi  $G = K + L$  et la somme est directe.

### Remarques

- (i) Les deux sous- $A$ -modules  $\{0\}$  et  $G$  de  $G$  sont toujours supplémentaires.
- (ii) Si la somme  $\sum_{i \in I} G_i$  est directe, alors  $G_i \cap G_j = \{0\} \quad \forall i \neq j$ .
- (iii) La somme  $\sum_{i \in I} G_i$  est directe ssi pour tout  $0 \neq (g_i)_{i \in I_0} \in \prod_{i \in I_0} G_i$  avec  $I_0 \subseteq I$ ,  $1 \leq |I_0| < \infty$ , on a  $\sum_{i \in I_0} g_i \neq 0$ .
- (iv) Deux sous- $A$ -modules  $K, L \leq G$  sont supplémentaires ssi  $G = K + L$  et  $K \cap L = \{0\}$ .
- (v) Si  $K, L \leq G$  sont deux sous- $A$ -modules supplémentaires, alors  $K \cong_A G/L$ . Pour le voir, considère le morphisme de  $A$ -modules  $f : G \rightarrow G$  défini comme  $f(\varkappa + \lambda) := \varkappa$  pour  $\varkappa \in K$ ,  $\lambda \in L$  et applique le théorème d'isomorphismes 2.1.7.



## 2.2 Modules libres

### 2.2.1 Définition: Base et module libre

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module. Alors, une famille  $(b_i)_{i \in I} \subseteq G$  est dit  **$A$ -linéairement indépendante** (ou **libre**) ssi pour tout  $a_1, \dots, a_n \in A$  et  $i_1, \dots, i_n \in I$  tels que  $a_1 b_{i_1} + \dots + a_n b_{i_n} = 0$ , il faut  $a_k = 0 \forall 1 \leq k \leq n$ . La famille est dit **lié** si elle n'est pas linéairement indépendante. Elle est dit  **$A$ -base** de  $G$  si  $G = \text{span}_A(b_i : i \in I)$  et  $(b_i)_{i \in I}$  est  $A$ -linéairement indépendante. On dit  $G$  **libre** s'il possède une base.

Donné n'importe quel ensemble  $I$  et anneau  $A$ , on peut construire un  $A$ -module libre **sur**  $I$ , noté  $A^{(I)}$ , comme la somme directe

$$A^{(I)} := \bigoplus_{i \in I} A ,$$

où tout  $A$  est regardé comme un  $A$ -module à gauche lui même. En fait, ce module est libre, avec base  $B := (e_i)_{i \in I}$  donnée par  $e_i = (0, \dots, 0, \underset{i}{\uparrow} 1, 0, \dots)$ . Cette base est dit **base canonique** du module libre  $A^{(I)}$ .

### Remarques

- (i) On dit une partie  $B \subseteq G$  **linéairement indépendante** ssi la famille  $(b)_{b \in B}$  est linéairement indépendante.
- (ii) Si  $(b_i)_{i \in I} \subseteq G$  est  $A$ -linéairement indépendante, alors toute sous-famille  $(b_i)_{i \in I_0} \subseteq (b_i)_{i \in I}$  est également.
- (iii) Si deux  $A$ -modules  $G, H$  sont isomorphes via l'isomorphisme  $\Phi : G \rightarrow H$  et  $G$  est libre avec base  $B \subseteq G$ , alors  $H$  est libre avec base  $\Phi(B)$ .
- (iv) Si  $(b_i)_{i \in I}$  est  $A$ -linéairement indépendante, alors  $\text{Ann}_A(b_{i_1} + \dots + b_{i_n}) = \{0\}$  pour tout  $i_1, \dots, i_n \in I$  deux à deux inégales.
- (v) Un système  $B \subseteq G$  est une base du  $A$ -module  $G$  ssi tout élément  $g \in G$  peut être écrit comme combinaison linéaire  $g = \sum_{i=1}^n a_i b_i$  ( $0 \neq a_i \in A$ ,  $n \in \mathbb{N}_0$ ) des éléments distinctes  $b_i \in B$  en façon unique.
- (vi) Un système  $B \subseteq G$  est linéairement indépendant ssi il existe un  $g \in G$  qui peut être écrit comme combinaison linéaire  $g = \sum_{i=1}^n a_i b_i$  ( $0 \neq a_i \in A$ ,  $n \in \mathbb{N}_0$ ) des éléments distinctes  $b_i \in B$  en unique façon.
- (vii) De remarque (vi) on conclut : Si  $B \subseteq G$  est une  $A$ -base de  $G$ , et  $C \subseteq G$  tel que tout  $b \in B$  peut être écrit comme combinaison linéaire unique des éléments de  $C$ , alors  $C$  est aussi une  $A$ -base de  $G$ .
- (viii) Si  $G, H$  sont deux  $A$ -modules et  $G$  libre avec base  $(b_i)_{i \in I}$ , alors toute  $A$ -linéaire  $f : G \rightarrow H$  est déterminé par les images  $f(b_i)$ ,  $i \in I$ .
- (ix) Sous-modules de modules libres ne doivent pas être libres ! Un exemple est donné ci-dessous par 2.2.11(iii).
- (x) Un module de type fini ne doit pas avoir une base finie.
- (xi) Si  $N \leq G$  est un sous- $A$ -module de  $G$  et  $B \subseteq G$  telle que  $\{b + N\}_{b \in B} \subseteq G/N$  est  $A$ -linéairement indépendante, alors  $B$  est  $A$ -linéairement indépendante.

### Exemples :

- (i) Tout  $\mathbb{K}$ -espace vectoriel de dimension finie est un  $\mathbb{K}$ -module libre.
- (ii) Un groupe abélien  $(G, +)$  est libre ssi il est libre comme  $\mathbb{Z}$ -module.
- (iii) On considère un anneau  $(A, +, \cdot)$  commutatif comme  $A$ -module. Alors, toute partie  $X \subseteq A$  de cardinal  $\geq 2$  est liée : Prends  $a \neq b \in X$ , alors  $0 = b \cdot a + (-a) \cdot b$ . Par conséquence, un idéal  $I$  de  $A$  est un  $A$ -module libre ssi  $I$  est engendré par un élément non diviseur de zéro.
- (iv) Soit  $I \subseteq A$  un idéal d'un anneau commutatif  $A$ . Alors, le  $A$ -module  $A/I$  est libre ssi  $I = \{0\}$ .
- (v) Soit  $n \in \mathbb{N}$ , alors tout élément dans  $\mathbb{Z}/n\mathbb{Z}$  possède un  $\mathbb{Z}$ -annulateur non-trivial. Par remarque 2.2.1(iv), ça implique que  $\mathbb{Z}/n\mathbb{Z}$  n'est pas un  $\mathbb{Z}$ -module libre.

### 2.2.2 Définition: Génératrice minimale et système indépendant maximal

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module. Alors, une partie  $B \subseteq G$  est dit :

- **$A$ -génératrice de  $G$  minimale** ssi  $\text{span}_A(B) = G$  et si pour toute  $B_0 \subsetneq B$  on a  $\text{span}_A(B_0) \subsetneq G$ .
- **$A$ -linéairement indépendante maximale dans  $G$**  ssi  $B$  est  $A$ -linéairement indépendante et toute  $B_0 \subseteq G$  avec  $B \subsetneq B_0$  n'est pas  $A$ -linéairement indépendante.

**Remarques :**

- (i) Tout système  $B \subseteq G$  linéairement indépendant est une génératrice de  $\text{span}_A(B)$  minimale.
- (ii) Soit  $B \subseteq G$  linéairement indépendant. Alors,  $B$  est linéairement indépendant maximal dans  $\text{span}_A(B)$ .
- (iii) Toute base de  $G$  est une génératrice de  $G$  minimale et une linéairement indépendante maximale dans  $G$ .
- (iv) Généralement, les notions génératrices minimales, linéairement indépendantes maximales et bases ne coïncident pas. Voir 2.2.16 pour quelques exemples.

**2.2.3 Lemme : Modules libres de type fini**

Soit  $(A, +, \cdot)$  un anneau et  $(G, +)$  un  $A$ -module libre de type fini. Alors, il possède une base finie.

**Preuve :** Soit  $B \subseteq G$  une base de  $G$  et  $G = \text{span}_A \{g_1, \dots, g_n\}$  pour quelques  $g_1, \dots, g_n \in G$ . Alors, pour tout  $i \in \{1, \dots, n\}$  il existe une partie finie  $B_i \subseteq B$  telle que  $g_i \in \text{span}_A(B_i)$ . Par conséquence

$$G = \text{span}_A(g_1, \dots, g_n) = \text{span}_A \left( \bigcup_{i=1}^n B_i \right) ,$$

c'est-à-dire le système fini  $\bigcup_{i=1}^n B_i$  est une base de  $G$ . □

**2.2.4 Lemme : Structure des modules libres**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $(b_i)_{i \in I} \subseteq G$  une famille d'éléments n'importe laquelle. Alors, les suivants sont équivalents :

1. La famille  $(b_i)_{i \in I}$  est une base de  $G$ .
2. Le  $A$ -module  $G$  est isomorphe au  $A$ -module libre  $A^{(I)}$  via un isomorphisme de  $A$ -modules  $\Phi : A^{(I)} \rightarrow G$  tel que  $b_i = \Phi(e_i)$ .
3. Le module  $G$  est la somme directe des sous-modules  $\text{span}_A(b_i)$  engendrés par les  $b_i$  et  $\text{Ann}_A(b_i) = \{0\}$  pour tout  $i \in I$ .

**Preuve :**

**1  $\Rightarrow$  2 :** Définis le morphisme des  $A$ -modules  $\Phi : A^{(I)} \rightarrow G$  comme

$$(a_i)_{i \in I} \mapsto \sum_{\substack{i \in I \\ a_i \neq 0}} a_i b_i .$$

Alors,  $\Phi$  est surjective et injective d'après remarque 2.2.1(v).

**2  $\Rightarrow$  1 :** Par remarque 2.2.1(iii) les  $(b_i)_{i \in I}$  forment une base de  $G$ .

**3  $\Leftrightarrow$  1 :** Par définition 2.1.22  $G$  est la somme directe des  $\text{span}_A(b_i)$ ,  $i \in I$  ssi tout  $x \in G$  est représentable par une unique somme finie des éléments non-nuls des  $(\text{span}_A(b_i))_{i \in I}$ . Par remarque 2.2.1(v) ça c'est vrai ssi  $(b_i)_{i \in I}$  forme une base de  $G$ . □

**2.2.5 Lemme : Existence de supplémentaires**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $M \leq G$  un sous- $A$ -module tel que le  $A$ -module  $G/M$  est libre. Alors,  $M$  possède un supplémentaire libre  $N$  dans  $G$ , isomorphe à  $G/M$ . En particulier, si  $G/M$  possède une base de cardinal  $n$ , alors  $N$  fait également.

**Preuve :** Pour  $g \in G$  soit  $\bar{g} := g + M$  la classe correspondant à  $g$ . Soit  $B \subseteq G$  tel que  $\bar{B} := \{\bar{b}\}_{b \in B}$  est une base de  $G/M$ . Pose  $N := \text{span}_A(B)$ . Note que par remarque 2.2.1(xi),  $B$  est en fait une base de  $N$ . Noter comme cela implique que  $N \cong_A G/M$ . Alors,  $G = N + M$  car tout  $x \in G$  est contenu dans une classe  $\bar{g}$  de  $G/M$ , où

$$\bar{g} = \sum_i a_i \bar{b}_i = \sum_i \overline{a_i b_i} = \overline{\sum_i a_i b_i}$$

pour quelques  $\bar{b}_i \in \bar{B}$ ,  $a_i \in A$ , c'est-à-dire  $x \in \text{span}_A(B) + M$ . On va montrer que la somme  $G = N + M$  est directe. Supposons  $n \in N$ ,  $m \in M$  tels que  $n + m = 0$ , alors  $n = -m \in M$ . Cela implique  $\bar{n} = \bar{0}$ . D'autre part,  $n = \sum_i a_i b_i$  pour un nombre fini des  $a_i \in A$  et  $b_i \in B$  deux à deux inégales, c'est-à-dire  $\bar{n} = \sum_i a_i \bar{b}_i$ . Par supposition les  $\bar{b}_i$  sont linéairement indépendants, donc  $a_i = 0$  et  $n = 0$ . Par conséquence ainsi  $m = 0$ .  $\square$

### 2.2.6 Corollaire sur morphismes surjectifs

Soit  $A$  un anneau,  $G$  un  $A$ -module,  $L$  un  $A$ -module libre et  $\varphi : G \rightarrow L$  un morphisme de  $A$ -modules surjectif. Alors

$$G \cong \ker(\varphi) \oplus L$$

**Preuve :** Par le théorème d'isomorphismes on sait que  $G/\ker(\varphi) \cong_A L$ . Comme  $L$  est libre, par 2.2.5 on sait que  $\ker(\varphi)$  possède un supplément  $\tilde{L}$  dans  $G$ , isomorphe à  $L$ . Donc  $G = \ker(\varphi) \oplus \tilde{L} \cong_A \ker(\varphi) \oplus L$ .  $\square$

### 2.2.7 Corollaire sur modules quotients libres

Soient  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $M \leq G$  un sous- $A$ -module. Si  $M \leq G$  et  $G/M$  sont libres, alors  $G$  est libre.

**Preuve :** Par 2.2.5,  $G$  est la somme directe de deux sous- $A$ -modules libres et par 2.2.12 libre lui même.  $\square$

### 2.2.8 Lemme : Existence de morphismes de modules

Soient  $(A, +, \cdot)$  un anneau,  $G, H$  deux  $A$ -modules,  $(g_i)_{i \in I}$  une base de  $G$  et  $(h_i)_{i \in I} \subseteq H$  quelconque. Alors, il existe un unique morphisme de  $A$ -modules  $f : G \rightarrow H$  tel que  $f(g_i) = h_i \quad \forall i \in I$ . Si de plus  $(h_i)_{i \in I}$  est une base de  $H$ , ce morphisme est en fait un isomorphisme.

**Preuve :** Soit  $\Phi_G : A^{(I)} \rightarrow G$  l'isomorphisme satisfaisant  $\Phi_G(e_i) = g_i$  (vois 2.2.4). Pour  $x \in G$  pose

$$f(x) := \sum_{\substack{i \in I \\ (\Phi_G^{-1}(x))_i \neq 0}} (\Phi_G^{-1}(x))_i \cdot h_i \quad .$$

Alors  $f : G \rightarrow H$  est un morphisme de  $A$ -modules satisfaisant  $f(g_i) = h_i \quad \forall i$ . L'unicité de  $f$  suit de remarque 2.2.1(viii). Si de plus  $(h_i)_{i \in I}$  est une base de  $H$ , soit  $\Phi_H : A^{(I)} \rightarrow H$  l'isomorphisme satisfaisant  $\Phi_H(e_i) = h_i$ . Alors, l'isomorphisme  $f := \Phi_H \circ \Phi_G^{-1}$  satisfait les conditions.  $\square$

**Conséquence :** Les morphismes de  $A$ -modules  $G \rightarrow H$  sont en bijection avec  $H^I$ .

### 2.2.9 Définition: Matrices de morphismes de $A$ -modules

Soient  $(A, +, \cdot)$  un anneau et  $G, H$  deux  $A$ -modules libres avec bases  $(g_i)_{i \in I}$  et  $(h_j)_{j \in J}$  respectivement. Soient  $\Phi_G : A^{(I)} \rightarrow G$  et  $\Phi_H : A^{(J)} \rightarrow H$  les isomorphismes satisfaisant  $\Phi_G(e_i) = g_i$  et  $\Phi_H(e_i) = h_i$  respectivement (voir 2.2.4(2)). Alors, l'uplet  $\Lambda(f) := (\Lambda_{ji}(f))_{i \in I, j \in J}$  donné par

$$\Lambda_{ji}(f) := (\Phi_H^{-1} \circ f \circ \Phi_G(e_i))_j$$

est dit la **matrice** de  $f$  sur les bases  $(g_i)_{i \in I}$  et  $(h_j)_{j \in J}$  respectives de  $G$  et  $H$ . Il est cet uplet unique qui satisfait

$$f(g_i) = \sum_{\substack{j \in J \\ \Lambda_{ji}(f) \neq 0}} \Lambda_{ji}(f) \cdot h_j$$

pour tout  $i \in I$ . Si  $C$  est aussi un  $A$ -module libre avec base  $(c_k)_{k \in K}$  et  $\tilde{f} : H \rightarrow C$   $A$ -linéaire avec matrice  $\Lambda(\tilde{f}) := (\Lambda_{kj}(\tilde{f}))_{j \in J, k \in K}$ , alors  $\tilde{f} \circ f : G \rightarrow C$  a la matrice

$$\Lambda_{ki}(\tilde{f} \circ f) = \sum_{\substack{j \in J \\ \Lambda_{ji}(f) \neq 0 \\ \Lambda_{kj}(\tilde{f}) \neq 0}} \Lambda_{ji}(f) \cdot \Lambda_{kj}(\tilde{f}) . \quad (2.2.9.1)$$

#### Remarques :

- (i) Fait attention à l'ordre des matrices dans (2.2.9.1) en cas que  $A$  est non-commutatif!
- (ii) Si  $f : G \rightarrow H$  est l'isomorphisme donné par lemme 2.2.8, il possède la matrice  $\Lambda_{ji}(f) = \delta_{ij}$ .

### 2.2.10 Lemme : Bases de corps quotients

Soit  $(A, +, \cdot)$  un anneau intègre et  $n \in \mathbb{N}$ . On considère  $A$  plongé dans son corps quotient  $\mathbb{K} := \text{Quot}(A)$  par l'identification  $a \mapsto \frac{a}{1}$ ,  $a \in A$  (vois 2.1.20). Alors, tout  $A$ -base de  $A^n$  est une  $\mathbb{K}$ -base de  $\mathbb{K}^n$ .

**Preuve :** Soit  $C$  une  $A$ -base de  $A^n$ . On note que pour toute famille finie  $\frac{a_1}{s_1}, \dots, \frac{a_m}{s_m} \in \mathbb{K}$  on peut suppose  $s_1 = \dots = s_m$ . Les  $(c_j)_{j \in J}$  sont  $\mathbb{K}$ -linéairement indépendants :

Soient  $\frac{a_1}{s}, \dots, \frac{a_m}{s} \in \mathbb{K}$  n'importe quels tels que  $\sum_{k=1}^m \frac{a_k}{s} \cdot c_k = 0$  pour quelques  $c_1, \dots, c_m \in C$ . Alors,  $\sum_{k=1}^m a_k c_k = 0$ . Mais car  $C$  est  $A$ -linéairement indépendant, il faut  $a_k = 0 \forall k \in \{1, \dots, m\}$ .

De plus,  $C$  engendre tout  $\mathbb{K}^n$ , c'est-à-dire  $\mathbb{K}^n = \text{span}_{\mathbb{K}}(C)$  :

Soit  $x \in \mathbb{K}^n$ , alors il existe  $b \in A \setminus \{0\}$  tel que  $bx \in A^n$ <sup>17</sup>. Donc, il existe  $a_1, \dots, a_m \in A$  et  $c_1, \dots, c_m \in C$  tels que  $\sum_{k=1}^m a_k c_k = bx$  et par conséquent  $x = \sum_{k=1}^m \frac{a_k}{b} \cdot c_k$ .

□

### 2.2.11 Théorème : Cardinalité des bases finies

Soit  $(A, +, \cdot)$  un anneau intègre et  $(G, +)$  un  $A$ -module libre de base finie  $(b_i)_{i=1}^n$ . Alors, toute autre base  $C$  (finie ou infinie) de  $G$  a le même cardinal, c'est-à-dire  $|C| = n$ . On appelle ce cardinal  $n$  le **rang** du module  $G$ .

**Preuve :** D'après lemme 2.2.4  $G$  est isomorphe à  $A^n := \prod_{i=1}^n A$ , qui possède la  $A$ -base canonique  $(e_i)_{i=1}^n$ . Donc par remarque 2.2.1(iii) il suffit de montrer l'affirmation pour le  $A$ -module  $A^n$ . On considère  $A$  plongé dans son corps quotient  $\mathbb{K} := \text{Quot}(A)$  et donc  $A^n \hookrightarrow \mathbb{K}^n$ . D'après lemme 2.2.10 tout  $A$ -base de  $A^n$  est une  $\mathbb{K}$ -base de  $\mathbb{K}^n$ . Comme on sait, toute  $\mathbb{K}$ -base de  $\mathbb{K}^n$  a cardinal  $n$ .

□

17. Si  $x = (\frac{a_i}{s})_{i=1}^n \in \mathbb{K}^n$  on sait que  $sx = (\frac{s a_i}{s})_{i=1}^n = (a_i)_{i=1}^n \in A^n$ .

**Exemples**

- (i) Tout anneau commutatif  $A$  est un  $A$ -module libre de rang 1 : L'élément unité  $\{1\}$  forme une  $A$ -base.
- (ii) Si  $A$  est un anneau commutatif intègre, alors  $A^n$  est un  $A$ -module de rang  $n$ .
- (iii) Considère l'anneau  $A := \mathcal{C}(X)$  d'exemple 1.2.24 et l'idéal  $\mathfrak{M}_x := \{f \in A : f(x) = 0\}$ . Alors, par 1.2.24 le sous- $A$ -module  $\mathfrak{M}_x$  n'est pas de type fini, même si  $A$  est un  $A$ -module libre de rang 1. De plus, par exemple 2.2.1(iii)  $\mathfrak{M}_x$  n'est pas libre, car sinon il serait de type fini.

**2.2.12 Lemme sur bases des sommes directes**

Soit  $(A, +, \cdot)$  un anneau,  $(G, +)$  un  $A$ -module et  $(G_i)_{i \in I}$  une famille des sous- $A$ -modules de  $G$  tels que la somme  $\sum_{i \in I} G_i$  est directe. Soient  $B_i \subseteq G_i$ ,  $i \in I$  sous-parties n'importe quel. Alors :

1. L'union  $\bigcup_{i \in I} B_i$  est  $A$ -linéairement indépendante ssi toute  $B_i$  est  $A$ -linéairement indépendante.
2. L'union  $\bigcup_{i \in I} B_i$  est génératrice de la somme  $\sum_{i \in I} G_i$  ssi toute  $B_i$  est génératrice de  $G_i$ .
3. L'union  $\bigcup_{i \in I} B_i$  est une  $A$ -base de la somme  $\sum_{i \in I} G_i$  ssi toute  $B_i$  est une  $A$ -base de  $G_i$ .
4. Si  $A$  est commutatif,  $I = \{1, \dots, N\}$  et tout  $G_i$  est libre de rang  $n_i$ , alors la somme directe  $\sum_{i=1}^N G_i$  est libre de rang  $\sum_{i=1}^N n_i$ .

**Preuve :** Les affirmations (1) et (2) sont claires. L'affirmation (3) suit de (1) et (2). Assertion (4) suit de (3).  $\square$

**2.2.13 Lemme : Condition suffisante pour modules libres**

Soit  $(A, +, \cdot)$  un anneau commutatif,  $G, H$   $A$ -modules et  $f : G \rightarrow H$  un morphisme de  $A$ -modules. Si  $\ker(f)$  est libre de rang  $m \in \mathbb{N}$  et  $f(G)$  est libre de rang  $n$ , alors  $G$  est libre de rang  $m + n$ .

**Preuve :** Par le théorème d'isomorphisme 2.1.7,  $G/\ker(f) \cong_A f(G)$  et donc  $G/\ker(f)$  est libre de rang  $n$ . Par 2.2.5,  $\ker(f)$  possède un sous- $A$ -module  $N \leq G$  supplémentaire de rang  $n$ , c'est-à-dire  $G = \ker(f) \oplus N$ . Par 2.2.12(4)  $G$  est libre de rang  $m + n$ .  $\square$

**2.2.14 Exemple d'un  $\mathbb{K}[X]$ -module**

Soit  $\mathbb{K}$  un corps,  $\mathbb{K}[X]$  l'anneau des polynômes sur  $\mathbb{K}$ ,  $V$  un  $\mathbb{K}$ -espace vectoriel et  $f \in \text{End}_{\mathbb{K}}(V)$ . Alors le loi de composition

$$\mathbb{K}[X] \times V \rightarrow V, (P, x) \mapsto P(f)x$$

munit le groupe sous-adjoint de  $V$  d'une structure de  $\mathbb{K}[X]$ -module. Les sous- $\mathbb{K}[X]$ -modules de  $V$  sont exactement les sous- $\mathbb{K}$ -espaces vectoriels qui sont  $f$ -invariant.

Si  $V$  est un  $\mathbb{K}$ -espace vectoriel de dimension fini, alors par le théorème de Caley-Hamilton il existe un polynôme  $0 \neq P \in \mathbb{K}[X]$  tel que  $P(f) = 0$ , donc le  $\mathbb{K}[X]$ -module  $V$  est de torsion. De plus, en cette cas  $V$  est un  $\mathbb{K}[X]$ -module de type fini.

Le cas  $\dim V = \infty$  est plus compliqué. Si par exemple  $f = 0$ , alors  $V$  est un  $\mathbb{K}[X]$ -module de torsion mais n'est pas de type fini. Considérons d'autre le module libre  $V = \mathbb{K}^{(\mathbb{N}_0)}$ , c'est-à-dire l'espace vectoriel des suites  $(x_i)_{i \in \mathbb{N}_0}$  à valeurs dans  $\mathbb{K}$  et de support fini, et  $f : V \rightarrow V$  donné par  $f((x_i)_{i \in \mathbb{N}_0}) := (x_{i-1})_{i \in \mathbb{N}}$ . Alors,  $V = \mathbb{K}[X]e_0$  où  $e_0 := (1, 0, \dots)$ , c'est-à-dire  $V$  est de type fini. De plus,  $V$  n'a pas de torsion.

**2.2.15 Exemple : Le  $\mathbb{Z}$ -module  $\mathbb{Z}[p^{-1}]$** 

Soit  $p \in \mathbb{P}$  premier et  $\mathbb{Z}[p^{-1}]$  le sous-ensemble du  $\mathbb{Z}$ -module  $(\mathbb{Q}, +, \cdot)$  définie comme

$$\mathbb{Z}[p^{-1}] := \left\{ \frac{q}{p^n} \mid q \in \mathbb{Z}, n \in \mathbb{N}_0 \right\} = \bigcup_{n=0}^{\infty} \frac{1}{p^n} \mathbb{Z} .$$

Alors :

1. Tout  $p^{-n}\mathbb{Z}$  est un sous- $\mathbb{Z}$ -module de  $\mathbb{Q}$ .
2. Pour  $n < m \in \mathbb{N}_0$  on a

$$\frac{1}{p^n} \mathbb{Z} \subsetneq \frac{1}{p^m} \mathbb{Z} .$$

3. Si  $(n_k)_{k=1}^{\infty} \subseteq \mathbb{N}_0$  sont tels que  $\sup_{k \in \mathbb{N}} n_k = \infty$ , on a

$$\mathbb{Z}[p^{-1}] = \bigcup_{k=1}^{\infty} \frac{1}{p^{n_k}} \mathbb{Z} .$$

4.  $\mathbb{Z}[p^{-1}]$  n'est pas de type fini.
5. Soit  $p \in \mathbb{P} \setminus \{2\}$ . Alors, une sous-partie  $B \subseteq \mathbb{Z}[p^{-1}]$  est génératrice de  $\mathbb{Z}[p^{-1}]$  ssi il existe  $b_1, \dots, b_m \in B$  tels que  $\mathbb{Z} \subseteq \text{span}\{b_k\}_{k=1}^m$  et une suite  $(c_k)_{k=1}^{\infty} \in B$  de la forme  $c_k = \frac{a_k}{p^{n_k}}$ ,  $a_k \in \mathbb{Z}$  avec  $\sup_{k \in \mathbb{N}} n_k = \infty$  et  $a_k, p$  copremiers.
6. Soit  $p \in \mathbb{P} \setminus \{2\}$ . Alors,  $\mathbb{Z}[p^{-1}]$  n'a pas des parties génératrices minimales. En particulier,  $\mathbb{Z}[p^{-1}]$  n'a pas de base.

**Preuve :**

1. Trivial.
2. L'inclusion est triviale. L'inégalité suit du fait que  $\frac{1}{p^m} \notin \frac{1}{p^n} \mathbb{Z}$  car  $p$  est premier.
3. Suit de (2).
4. Suppose que  $\mathbb{Z}[p^{-1}]$ , c'est-à-dire

$$\mathbb{Z}[p^{-1}] = \text{span}_{\mathbb{Z}} \left\{ \frac{q_1}{p^{n_1}}, \dots, \frac{q_m}{p^{n_m}} \right\} \subseteq \text{span}_{\mathbb{Z}} \left\{ \frac{1}{p^{n_1}}, \dots, \frac{1}{p^{n_m}} \right\} .$$

Alors, par (2) il faudrait  $\mathbb{Z}[p^{-1}] \subseteq \frac{1}{q^n} \mathbb{Z}$  où  $n := \max_{1 \leq k \leq m} n_k$ . Mais ça n'est pas possible.

5. **Direction “ $\Rightarrow$ ” :** Soit  $B \subseteq \mathbb{Z}[p^{-1}]$  génératrice. Alors  $1 \in \text{span}_{\mathbb{Z}}(B)$ , c'est-à-dire il existe  $b_1, \dots, b_m \in B$  tels que  $1 \in \text{span}_{\mathbb{Z}}\{b_i\}_{i=1}^m$  et donc  $\mathbb{Z} \subseteq \text{span}_{\mathbb{Z}}\{b_i\}_{i=1}^m$ .

On suppose tous éléments de  $B$  de la forme  $\frac{a}{p^n}$  où  $a$  et  $p$  sont premiers entre eux. Alors, pour tout élément  $\frac{a}{p^n} \in B$  on peut trouver un élément  $\frac{b}{p^m} \in B$  tel que  $m > n$ . Sinon, par (1) et (2) il faudrait  $\text{span}_{\mathbb{Z}}(B) \subseteq p^{-N} \mathbb{Z}$  pour un certain  $N \in \mathbb{N}$  assez grand. Donc, on peut trouver une suite  $\left( \frac{a_k}{p^{n_k}} \right)_{k=1}^{\infty} \subseteq B$  telle que  $a_k, p$  sont premiers entre eux et  $n_k \xrightarrow{k \rightarrow \infty} \infty$ .

**Direction “ $\Leftarrow$ ” :** Soient  $B \subseteq \mathbb{Z}[p^{-1}]$  quelconque et  $b_1, \dots, b_m \in B$ ,  $(c_k)_{k=1}^n \subseteq B$  comme décrit. Alors, pour tout  $c_k = \frac{a_k}{p^{n_k}}$  on a

$$\text{span}\{c_k, b_1, \dots, b_m\} = c_k \mathbb{Z} + \text{span}_{\mathbb{Z}}\{b_k\}_{k=1}^m \supseteq c_k \mathbb{Z} + \mathbb{Z} = \frac{1}{p^{n_k}} \underbrace{[a_k \mathbb{Z} + p^{n_k} \mathbb{Z}]}_{\mathbb{Z}} = \frac{1}{p^{n_k}} \mathbb{Z} . \quad (2.2.15.1)$$

par Bézout 4.1.10

Car  $\sup_{k \in \mathbb{N}} n_k = \infty$ , par (3) ça implique

$$\text{span}_{\mathbb{Z}} \left[ \{c_k\}_{k=1}^{\infty} \cup \{b_k\}_{k=1}^m \right] \stackrel{(2.2.15.1)}{\supseteq} \bigcup_{k=1}^{\infty} \frac{1}{p^{n_k}} \stackrel{(3)}{=} \mathbb{Z}[p^{-1}] .$$

6. Soit  $B \subseteq \mathbb{Z}[p^{-1}]$  une génératrice de  $\mathbb{Z}[p^{-1}]$ . Alors par (5) il existe une sous-partie finie  $B_0 \subsetneq B$  tel que  $\mathbb{Z} \subseteq \text{span}_{\mathbb{Z}}(B_0)$  et une suite  $(c_k)_{k=1}^{\infty} \in B$  de la forme décrit dans (5). Note que la suite  $(c_k)_{k=1}^{\infty}$  contient un nombre infini des éléments deux à deux inégaux. Alors, on peut supprimer un certain  $c_k$  tel que  $c_k \notin B_0$ . On obtient donc encore une suite comme suppose dans (5), qui avec  $B_0$  engendre  $\mathbb{Z}[p^{-1}]$ . Autrement dit,  $B$  n'est pas une génératrice de  $\mathbb{Z}[p^{-1}]$  minimale. Par remarque 2.2.2(iii) ça implique que  $B$  n'est pas une base.  $\square$

### 2.2.16 Exemples de modules libres et non libres

Les exemples ci-dessus montrent que, les notions des bases et modules libres ne satisfont pas les propriétés à lesquelles on est habitué dans espaces vectoriels.

1. Le  $\mathbb{Z}$ -module  $\mathbb{Z}$  est un module libre de rang 1 qui possède familles linéairement indépendantes maximales qui ne sont pas bases. En fait, pour tout  $n \in \mathbb{Z} \setminus \{0, \pm 1\}$  la famille  $\{n\}$  est de ce type, même si elle est de même cardinalité que le rang de  $\mathbb{Z}$ .
2. La famille  $B := \{2, 3\}$  est une génératrice du  $\mathbb{Z}$ -module  $\mathbb{Z}$  minimale, qui n'est pas une base.
3. Le  $\mathbb{Z}$ -module  $\mathbb{Z}$  est un exemple de module, dont les familles génératrices minimales n'ont pas toutes le même cardinal. Prends par exemple les génératrices minimales  $\{1\}$  et  $\{2, 3\}$ .
4. Soit  $A := \mathcal{C}([0, 1])$  l'anneau des fonctions continues sur  $[0, 1]$ . Alors,  $A$  est un exemple d'un  $A$ -module libre, qui possède des sous-modules non-libres, comme  $\mathfrak{A}_x$  pour un  $x \in [0, 1]$ . Vois exemple 2.2.11(iii).
5. Tout corps  $\mathbb{K}$  est un  $\mathbb{K}$ -module libre de rang 1 qui ne possède pas de sous- $\mathbb{K}$ -modules maximales. En fait,  $\{0\}$  et  $\mathbb{K}$  sont les seules sous- $\mathbb{K}$ -modules de  $\mathbb{K}$ .
6. Le sous- $\mathbb{Z}$ -module  $M := \{\bar{0}, \bar{2}\}$  du  $\mathbb{Z}$ -module  $G := \mathbb{Z}/4\mathbb{Z}$  n'admet pas un supplémentaire dans  $G$ . Pour le voir, suppose que  $G = N \oplus M$  pour un sous- $\mathbb{Z}$ -module  $N \leq G$ . Alors  $|N| = 2$ , c'est-à-dire  $N$  est une sous-groupe d'ordre 2. Ça impliquerait que  $N = M$ , une contradiction.

### 2.2.17 Lemme sur espaces vectoriels de dimension finie

Soit  $\mathbb{K}$  un corps infini et  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension finie. Soit  $(V_i)_{i \in I}$  une famille finie de sous-espaces vectoriels de  $V$  telle que  $V = \bigcup_{i \in I} V_i$ . Alors, il existe un  $i \in I$  tel que  $V = V_i$ .

**Preuve :** Soit  $I = \{1, \dots, n\}$ . Les cas  $n = 1$  est clair. Supposons l'affirmation est vrai pour un  $n \in \mathbb{N}$  et que  $V = \bigcup_{i=1}^{n+1} V_i$  pour quelques sous-espaces  $V_i \subsetneq V$ . Par supposition  $V_{n+1} \subsetneq \bigcup_{i=1}^n V_i$ . Prends  $x \in V_{n+1} \setminus \bigcup_{i=1}^n V_i$  et  $y \in V \setminus V_{n+1}$ .

Supposons qu'il existe  $i_0 \in I$  et  $\lambda_1 \neq \lambda_2 \in \mathbb{K}$  tels que  $(x + \lambda_1 y), (x + \lambda_2 y) \in V_{i_0}$ . Alors

$$(x + \lambda_1 y) - (x + \lambda_2 y) = (\lambda_1 - \lambda_2)y \in V_{i_0}$$

et donc  $y \in V_{i_0}$ , donc  $x \in V_{i_0}$ . Cela impliquerait que  $V_{i_0} = V_{n+1}$ , donc  $y \in V_{n+1}$ , une contradiction !

Donc, si  $\lambda_1 \neq \lambda_2 \in \mathbb{K}$  on a toujours  $x + \lambda_k y \in V_{i_{\lambda_k}}$ ,  $k = 1, 2$  avec  $i_{\lambda_1} \neq i_{\lambda_2} \in I$ . Cela est impossible car  $\mathbb{K}$  est infini et  $I$  est fini.  $\square$

### 3 Polynômes et séries formelles

#### 3.1 Polynômes

##### 3.1.1 Définition: Algèbre

Soient  $(R, +, \cdot)$  un anneau commutatif et  $(A, +, *)$  un anneau tel que  $(A, +)$  est un  $R$ -module. Si l'opération de  $R$  sur  $A$  et le **produit extérieur**  $*$  :  $A \times A \rightarrow A$  sont compatibles, c'est-à-dire  $\rho \cdot (a * b) = a * (\rho \cdot b) = (\rho \cdot a) * b$  pour  $a, b \in A$ ,  $\rho \in R$ , on dit  $(A, +, *)$  une  $R$ -**algèbre** ou **algèbre sur**  $R$ . On dit  $R$  l'**anneau base** de l'algèbre. On dit la  $A$ -algèbre  $(A, +, *)$  **commutative** si  $A$  est un anneau commutatif.

Si  $(B, +, *)$  est aussi une  $R$ -algèbre, alors  $f : A \rightarrow B$  est dit **morphisme de  $R$ -algèbres** s'il est un morphisme d'anneaux et un morphisme de  $R$ -modules. Si  $f$  est bijective, on dit  $A$  et  $B$  **isomorphes** et note  $A \cong_R B$ .

##### Remarques :

- (i) Cette définition est équivalente à la définition 1.4.1. Puisque, tout homomorphisme  $\tau : R \rightarrow Z(A)$  induit une opération de  $R$  sur  $A$  par  $(\rho, a) \mapsto \rho \cdot a := \tau(\rho) * a$  où  $\rho \in R$ ,  $a \in A$ , qui munit  $A$  d'une structure de  $R$ -module compatible avec le produit extérieur  $*$ .

Inversement, si  $(A, +, *)$  est une  $R$ -algèbre par définition 3.1.1, alors  $\tau : R \rightarrow Z(A)$  donnée par  $\tau(\rho) := \rho \cdot 1_A$ ,  $\rho \in R$  fait de  $A$  une  $R$ -algèbre de type 1.4.1.

La même équivalence existe entre les définitions 1.4.2 et 3.1.1 des morphismes de  $R$ -algèbres.

- (ii) Souvent,  $R$  est un corps et donc  $(A, +)$  un  $\mathbb{K}$ -espace vectoriel, munit d'un produit extérieur  $*$ .

##### 3.1.2 Définition: Algèbre graduée

Soit  $(R, +, \cdot)$  un anneau commutatif et  $(A, +, *)$  une  $R$ -algèbre. Une **graduation** de  $A$  est une famille de sous- $R$ -modules  $(A_s)_{s \in S}$  de  $A$ , où  $S$  est un monoïde, tels que :

- $A$  est la somme directe des  $A_n$ ,
- Pour  $n, m \in S$  on a  $A_n * A_m \subseteq A_{n+m} \quad \forall n, m \in S$ .

On dit que  $A$  est **graduée** ssi elle est munit d'une structure de **graduation**.

**Exemple :** Toute  $R$ -algèbre peut être dotée d'une graduation en posant  $A_0 := A$  et  $A_n := \{0\} \quad \forall n \in \mathbb{N}$ .

##### 3.1.3 Définition: Algèbre quotient

Soient  $(R, +, \cdot)$  un anneau commutatif et  $(A, +, *)$  une  $R$ -algèbre. Soit  $I \subseteq A$  un idéal bilatère invariant par  $R$ , c'est-à-dire  $RI \subseteq I$ . Alors, la multiplication

$$r \cdot [x] := [rx] \quad \forall r \in R, [x] \in A/I$$

est bien définie et fait de l'anneau quotient  $A/I$  une  $R$ -algèbre. La projection  $A \rightarrow A/I$ ,  $x \mapsto [x]$  est un morphisme de  $R$ -algèbres.

##### 3.1.4 Définition: L'anneau des polynômes

Soit  $(S, +)$  un monoïde commutatif et  $(A, +, \cdot)$  un anneau commutatif (vois 1.1.1), dit l'**anneau base**. On forme le  $A$ -module libre  $A^{(S)}$  sur  $S$  (vois 2.2.1) avec la base canonique  $(e^s)_{s \in S}$  donnée par  $(e^s)_t := \delta_{st}$ ,  $t \in S$ . Tout élément  $f \in A^{(S)}$  peut donc être écrit dans la forme

$$f = \sum_{s \in S} f_s \cdot e^s \quad , \quad f_s \in A$$



en façon unique. On définit sur  $A^{(S)}$  l'opération binaire

$$* : A^{(S)} \times A^{(S)} \rightarrow A^{(S)} \quad , \quad (f * g)_u := \sum_{t+s=u} f_t \cdot g_s \quad , \quad f, g \in A^{(S)} \quad ,$$

dit la **multiplication**. Alors  $*$  est associatif et commutatif, avec élément neutre  $e^0 =: 1$ . De plus,  $*$  commute avec l'opération de  $A$  sur  $A^{(S)}$ , c'est-à-dire  $((a \cdot f) * g) = a \cdot (f * g)$  pour  $f, g \in A^{(S)}$ ,  $a \in A$ . Finalement, elle est distributive par rapport à l'addition, c'est-à-dire  $f * (g + h) = f * g + f * h$  pour  $f, g, h \in A^{(S)}$ . En particulier, pour  $s, t \in S$  on a

$$e^t * e^s = e^{t+s} \quad .$$

On dit l'anneau commutatif  $A[S] := [A^{(S)}, +, *]$  la  $A$ -algèbre des **polynômes des monômes**  $e^s$  ou bien une **algèbre de polynômes sur  $A$** . On dit le plongement  $A \hookrightarrow A[S]$ ,  $a \mapsto ae^0$  **plongement canonique**. On dit un polynôme  $f \in A[S]$  **constant** si  $f$  est de la forme  $f = f_0 \cdot e^0$ .

### Exemples

(i) Pour  $S := (\mathbb{N}_0^n, +)$  on note  $A[\mathbb{N}_0^n] =: A[X_1, \dots, X_n]$ . Pour  $s = (s_1, \dots, s_n) \in \mathbb{N}_0^n$  on note

$$e^s =: X^s =: X_1^{s_1} \cdot \dots \cdot X_n^{s_n}$$

et écrit tout polynôme  $P \in A[X_1, \dots, X_n]$  dans la forme

$$P(X) = \sum_{(s_1, \dots, s_n) \in \mathbb{N}_0^n} P_{s_1, \dots, s_n} \cdot X_1^{s_1} \cdot \dots \cdot X_n^{s_n} \quad .$$

En particulier, on note

$$X_i := X_1^0 \cdot \dots \cdot X_{i-1}^0 \cdot X_i^1 \cdot X_{i+1}^0 \cdot \dots \cdot X_n^0 \quad .$$

(ii) Pour  $S := (\mathbb{Z}^n, +)$ ,  $A[\mathbb{Z}^n] =: A[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$  est l'algèbre des polynômes de Laurent sur l'anneau commutatif  $A$ . Un élément  $P \in A[\mathbb{Z}^n]$  est représenté par la somme

$$P(X) = \sum_{s \in \mathbb{Z}^n} P_s \cdot X_1^{s_1} \cdot \dots \cdot X_n^{s_n} \quad .$$

#### 3.1.5 Théorème : La propriété universelle

Soient  $(A, +, \cdot)$ ,  $(B, +, \cdot)$  anneaux commutatifs,  $(S, +)$  un monoïde commutatif. Soit  $i : A \hookrightarrow A[S]$  le plongement canonique et  $\sigma : (S, +) \rightarrow (A[S], *)$  le morphisme de monoïdes défini par  $\sigma : s \rightarrow e^s$ .

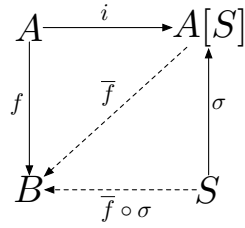
1. Le triplet  $(i, \sigma, A[S])$  possède la propriété **universelle** :

Soit  $f : (A, +, \cdot) \rightarrow (B, +, \cdot)$  un morphisme d'anneaux (de  $A$ -algèbres). Alors,  $f$  peut être prolongée par  $i$ , c'est-à-dire il existe un morphisme d'anneaux (de  $A$ -algèbres<sup>18</sup>)<sup>19</sup>  $\bar{f} : (A[S], +, *) \rightarrow (B, +, \cdot)$  tel que  $f = \bar{f} \circ i$ . En fait, les prolongements  $\bar{f}$  de  $f$  par  $i$  sont en bijection avec les morphismes de monoïdes  $(S, +) \rightarrow (B, \cdot)$  via l'attribution  $\bar{f} \mapsto \bar{f} \circ \sigma$ .

2. Soit  $(C, +, *)$  une  $A$ -algèbre commutative,  $j : A \rightarrow C$  un morphisme de  $A$ -algèbres et  $\tau : (S, +) \rightarrow (C, *)$  un morphisme de monoïdes. Si le triplet  $(j, \tau, C)$  satisfait la même propriété universelle (1) comme  $(i, \sigma, A[S])$ , alors les  $A$ -algèbres  $A[S]$  et  $C$  sont isomorphes.

18. Noter que si  $f : A \rightarrow B$  est un morphisme de  $A$ -algèbres, alors il est unique, donné par  $f : a \mapsto a \cdot 1_B$ .

19. Si  $f$  est un morphisme de  $A$ -algèbres, tout son prolongement comme morphisme d'anneaux est en fait un morphisme de  $A$ -algèbres.



**FIGURE 9:** Sur la propriété universelle de  $A[S]$  : Les prolongements d'un morphisme d'anneaux fixé  $f : A \rightarrow B$  sont en bijection avec les morphismes des monoïdes  $S \rightarrow B$ . Le diagramme ci-dessus commute.

**Preuve :**

- (i) Évidemment, si  $\bar{f} : (A[S], +, *) \rightarrow (B, +, \cdot)$  est un morphisme d'anneaux, la composition  $\bar{f} \circ \sigma : (S, +) \rightarrow (B, \cdot)$  est un morphisme de monoïdes. Soit  $\mu : (S, +) \rightarrow (B, \cdot)$  un morphisme de monoïdes quelconque. Pose

$$\bar{f}(P) := \sum_{s \in S} f(P_s) \cdot \mu(s) \quad , \quad P \in A[S] \quad .$$

Alors, pour  $P, Q \in A[S]$  on trouve

$$\bar{f}(P + Q) = \bar{f}(P) + \bar{f}(Q)$$

$$\bar{f}(e^0) = f(1) \cdot \mu(0) = 1$$

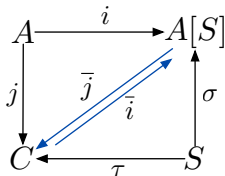
$$\bar{f}(P * Q) = \sum_{s \in S} \sum_{u+v=s} f(P_u) f(Q_v) \mu(s) = \sum_{s,t \in S} f(P_s) f(Q_t) \mu(s+t) = \bar{f}(P) \cdot \bar{f}(Q)$$

c'est-à-dire  $\bar{f} : (A[S], +, *) \rightarrow (B, +, \cdot)$  est vraiment un morphisme d'anneaux qui évidemment satisfait  $f = \bar{f} \circ i$ . Note que si  $f$  est un (le) morphisme de  $A$ -algèbres,  $\bar{f}$  est également<sup>20</sup>. De plus,  $\bar{f} \circ \sigma = \mu$ , d'où on déduit que l'attribution  $\bar{f} \mapsto \bar{f} \circ \sigma$  est une surjection des prolongements de  $f$  dans l'ensemble des monoïdes  $(S, +) \rightarrow (B, \cdot)$ . Il reste donc de montrer l'injectivité de cette attribution. Si  $\bar{f}_0 : A[S] \rightarrow B$  est un autre prolongement de  $f$  satisfaisant  $\mu = \bar{f}_0 \circ \sigma$ , il faut

$$\bar{f}_0(P) = \sum_{s \in S} \bar{f}_0(\underbrace{P_s e^s}_{P_s e^0 * e^s}) = \sum_{s \in S} \underbrace{\bar{f}_0(P_s e^0)}_{\bar{f}_0 \circ i(P_s)} \cdot \underbrace{\bar{f}_0(e^s)}_{\bar{f}_0 \circ \sigma(s)} = \sum_{s \in S} f(P_s) \cdot \mu(s) = \bar{f}(P)$$

pour  $P \in A[S]$ , c'est-à-dire  $\bar{f}_0 = \bar{f}$ .

- (ii) On choisit  $\bar{i} : (C, +, *) \rightarrow (A[S], +, *)$  comme prolongement de  $i$  par  $j$  satisfaisant  $\bar{i} \circ \tau = \sigma$ . De même, on choisit  $\bar{j} : (A[S], +, *) \rightarrow (C, +, *)$  comme prolongement de  $j$  par  $i$  satisfaisant  $\bar{j} \circ \sigma = \tau$ . Alors,  $\bar{i} \circ \bar{j} : (A[S], +, *) \rightarrow (A[S], +, *)$  est un prolongement de  $i$  par  $i$  lui même, satisfaisant  $(\bar{i} \circ \bar{j}) \circ \sigma = \sigma$ . Par unicité de ce prolongement, on déduit  $\bar{i} \circ \bar{j} = \text{Id}_{A[S]}$ . De même on trouve que  $\bar{j} \circ \bar{i} = \text{Id}_C$ . Donc  $\bar{j} : (A[S], +, *) \rightarrow (C, +, *)$  est un isomorphisme de  $A$ -algèbres d'inverse  $\bar{i}$ .



**FIGURE 10:** Sur l'unicité du  $A[S]$  par rapport à son universalité : Si  $(j, \tau, C)$  satisfait la même propriété, alors  $A[S]$  et  $C$  sont  $A$ -algèbres isomorphes.

20. Et nécessairement donné par  $\bar{f}(P) = \sum_s P_s \cdot \mu(s)$ .

□

### 3.1.6 Corollaire : Morphismes de $A$ -algèbres de $A[S]$

Soit  $A$  un anneau commutatif,  $S$  un monoïde,  $\sigma : (S, +) \rightarrow (A[S], *)$  le morphisme de monoïdes donné par  $s \mapsto e^s$ . Soit  $B$  une  $A$ -algèbre commutative. Alors, les morphismes de  $A$ -algèbres  $\bar{f} : (A[S], +, *) \rightarrow (B, +, \cdot)$  sont en bijection avec les morphismes de monoïdes  $(S, +) \rightarrow (B, \cdot)$  via l'association  $\bar{f} \mapsto \bar{f} \circ \sigma$ .

**Preuve :** Toute d'abord, notons que tout morphisme de  $A$ -algèbres  $\bar{f} : A[S] \rightarrow B$  est prolongement du morphisme de  $A$ -algèbres  $\bar{f} \circ i : A \rightarrow B$ , où  $i : A \hookrightarrow A[S]$  est l'inclusion. Mais  $\bar{f} \circ i$  est unique, donné par  $(\bar{f} \circ i)(a) = a \circ 1_B \forall a \in A$  et noté  $f := \bar{f} \circ i$ . Par théorème 3.1.5, les morphismes de monoïdes  $(S, +) \rightarrow (B, \cdot)$  sont en bijection avec les prolongements (morphismes de  $A$ -algèbres) de  $f$  par  $i$  via l'association cité. □

**Exemple :** Considérons le cas  $S = \mathbb{N}_0^n$ . Tout morphisme de monoïdes  $\mu : (\mathbb{N}_0^n, +) \rightarrow (B, \cdot)$  est déterminé par les images  $\mu(e_i)$ ,  $i = 1, \dots, n$  où  $(e_i)_{i=1}^n$  est la base canonique de  $\mathbb{Z}^n$ . En fait, pour tout système  $(b_i)_{i=1}^n \subseteq B$  il existe un unique morphisme  $\mu : S \rightarrow B$  tel que  $\mu(e_i) = b_i$ , c'est-à-dire les morphismes de monoïdes  $(\mathbb{N}_0^n, +) \rightarrow (B, \cdot)$  sont en bijection avec  $B^n$  via l'attribution  $\mu \mapsto (\mu(e_i))_{i=1}^n$ .

D'autre part, par 3.1.6 les morphismes de  $A$ -algèbres  $\bar{f} : A[X_1, \dots, X_n] \rightarrow (B, +, \cdot)$  sont en bijection avec les morphismes de monoïdes  $(\mathbb{N}_0^n, +) \rightarrow (B, \cdot)$  via l'attribution  $\bar{f} \mapsto \bar{f} \circ \sigma$ , donc en bijection avec  $B^n$ . En fait, cette bijection est donnée par l'attribution  $\bar{f} \mapsto (\bar{f}(X_i))_{i=1}^n \in B^n$ . Autrement dit, les morphismes de  $A$ -algèbres  $A[X_1, \dots, X_n] \rightarrow B$  sont caractérisés par leurs images des monômes  $X_1, \dots, X_n$ .

### 3.1.7 Théorème : Produits des algèbres des polynômes

Soient  $(A, +, \cdot)$  un anneau commutatif,  $(S_1, +)$ ,  $(S_2, +)$  monoïdes commutatifs et  $S_1 \times S_2$  leur monoïde produite. Alors

$$A[S_1 \times S_2] \cong_A A[S_1][S_2] \ .$$

c'est-à-dire, il existe un isomorphisme de  $A$ -algèbres entre  $A[S_1 \times S_2]$  et  $A[S_1][S_2]$ .

**Preuve :** Soit  $i : A \hookrightarrow A[S_1 \times S_2]$  le plongement canonique donné par  $i : a \mapsto ae^{(0,0)}$ . Les plongements canoniques  $i_1 : A \hookrightarrow A[S_1]$  et  $i_2 : A[S_1] \hookrightarrow (A[S_1])[S_2]$  munissent  $(A[S_1])[S_2]$  d'une structure de  $A$ -algèbres et d'un plongement canonique  $j := (i_2 \circ i_1) : A \hookrightarrow (A[S_1])[S_2]$ . Soient

$$\sigma_1 : S_1 \rightarrow A[S_1] \ , \ \sigma_2 : S_2 \rightarrow (A[S_1])[S_2] \ , \ \tau : S_1 \times S_2 \rightarrow (A[S_1])[S_2]$$

les morphismes de monoïdes définis par

$$\sigma_1 : s_1 \mapsto e^{s_1} \ , \ \sigma_2 : s_2 \mapsto e^{0_1} e^{s_2} \ , \ \tau : (s_1, s_2) \mapsto e^{s_1} e^{s_2} \ .$$

Par théorème 3.1.5(2) il suffit de montrer que  $(j, \tau, (A[S_1])[S_2])$  satisfait la même propriété universelle comme  $(i, \sigma, A[S_1 \times S_2])$ .

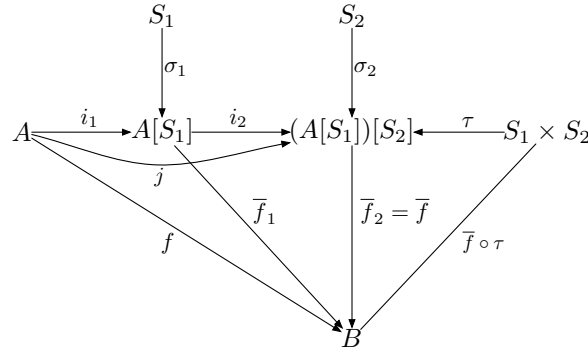
Soit  $f : (A, +, \cdot) \rightarrow (B, +, \cdot)$  un morphisme de  $A$ -algèbres, alors ses prolongements  $\bar{f} : (A[S_1])[S_2] \rightarrow B$  (morphismes de  $A$ -algèbres) via  $j$  sont en bijection avec les uplets  $(\bar{f}_1, \bar{f}_2)$  où  $\bar{f}_1 : A[S_1] \rightarrow B$  est son prolongement par  $i_1$  et  $\bar{f}_2 : (A[S_1])[S_2] \rightarrow B$  est le prolongement de  $\bar{f}_1$  par  $i_2$  : Pour un tel uplet pose  $\bar{f} := \bar{f}_2$ . D'autre part, les prolongements  $\bar{f}_1$  et  $\bar{f}_2$  sont à chaque fois en bijection avec les morphismes de monoïdes  $\mu_1 : S_1 \rightarrow B$  et  $\mu_2 : S_2 \rightarrow B$  via  $\bar{f}_1 \mapsto \bar{f}_1 \circ \sigma_1$  et  $\bar{f}_2 \mapsto \bar{f}_2 \circ \sigma_2$ . Eux, ils sont en bijection avec les morphismes de monoïdes  $\mu : S_1 \times S_2 \rightarrow B$  via

$$(\mu_1, \mu_2) \mapsto \mu_1 \cdot \mu_2 \quad \text{où} \quad (\mu_1 \cdot \mu_2)(s_1, s_2) := \mu_1(s_1) \cdot \mu_2(s_2) \ .$$

Donc, les prolongements  $\bar{f} : (A[S_1])[S_2] \rightarrow B$  sont en bijection avec les morphismes de monoïdes  $\mu : S_1 \times S_2 \rightarrow B$  via

$$\bar{f} \mapsto (\bar{f} \circ i_2 \circ \sigma_1) \cdot (\bar{f} \circ \sigma_2) = (\cdot) = \bar{f} \circ \tau \ .$$

Cela complète la preuve.



**FIGURE 11:** Sur la preuve de théorème 3.1.7. Le diagramme ci-dessus commute. Les prolongements  $\bar{f}$  d'un morphisme  $f : A \rightarrow B$  par  $j$  sont en bijection avec les morphismes de monoïdes  $S_1 \times S_2 \rightarrow B$  via  $\bar{f} \mapsto \bar{f} \circ \tau$ .

□

**Interprétation :** Un isomorphisme  $A[S_1][S_2] \rightarrow A[S_1 \times S_2]$  est donné par

$$\sum_{s_2 \in S_2} \left[ \underbrace{\sum_{s_1 \in S_1} P_{s_1, s_2} X_1^{s_1}}_{\in A[S_1]} \right] X_2^{s_2} \mapsto \sum_{s_2 \in S_2} \left[ \sum_{s_1 \in S_1} P_{s_1, s_2} X_1^{s_1} \right] * X_2^{s_2} = \sum_{(s_1, s_2) \in S_1 \times S_2} P_{s_1, s_2} X_1^{s_1} X_2^{s_2} ,$$

et est dit l'**isomorphisme canonique** entre  $A[S_1][S_2]$  et  $A[S_1 \times S_2]$ . Autrement dit, tout polynôme de *deux indéterminées* est un polynôme d'une indéterminée, dont les coefficients sont eux mêmes polynômes d'une indéterminée. Ou bien dans la langue des algèbres : Toute algèbre de polynômes sur une algèbre de polynômes, est une algèbre de polynômes.

### 3.1.8 Corollaire : Produits d'algèbres des polynômes

Soient  $(A, +, \cdot)$  un anneau commutatif,  $(S_1, +), \dots, (S_n, +)$  monoïdes commutatifs et  $\prod_{i=1}^n S_i$  leur monoïde produite. Alors

$$A \left[ \prod_{i=1}^n S_i \right] \cong_A A \left[ \prod_{i=1}^k S_i \right] \left[ \prod_{i=k+1}^n S_i \right] \cong_A (((A[S_1])[S_2])[S_3]) \dots [S_n] .$$

pour tout  $1 \leq k \leq n$ .

**Preuve :** Suit par induction de théorème 3.1.7.

□

### 3.1.9 Définition: L'ordre lexicographique & monômial

Pour  $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$  on note  $\mathbf{x} <_l \mathbf{y}$  ssi  $\mathbf{x} \neq \mathbf{y}$  et

$$x_k < y_k \quad \text{où} \quad k := \min \{k \in \{1, \dots, n\} : x_k \neq y_k\} .$$

On note  $\mathbf{x} \leq_l \mathbf{y}$  ssi  $\mathbf{x} = \mathbf{y}$  ou  $\mathbf{x} <_l \mathbf{y}$  et dit la relation  $\leq_l$  sur  $\mathbb{R}^n$  l'**ordre lexicographique**.

En utilisant l'ordre lexicographique, on définit sur  $\mathbb{R}^n$  la relation  $\leq$ , dit **ordre monomial** définie par

$$\mathbf{x} \leq \mathbf{y} \quad :\Leftrightarrow \quad (|\mathbf{x}| < |\mathbf{y}|) \vee (|\mathbf{x}| = |\mathbf{y}| \wedge \mathbf{x} \leq_l \mathbf{y}) \quad .$$

où on appelle  $|\mathbf{x}| := \sum_{i=1}^n x_i$  le **degré** de  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ . On écrit  $\mathbf{x} < \mathbf{y}$  ssi  $\mathbf{x} \leq \mathbf{y}$  et  $\mathbf{x} \neq \mathbf{y}$ .

**Exemples :**  $(1, 18) <_l (2, 0)$  et  $(3, 1, 1) <_l (3, 2, 0)$  mais  $(1, 18) > (2, 0)$ .

**Remarques :**

(i) La relation binaire  $\leq_l$  sur  $\mathbb{R}^n$  est un ordre totale, c'est-à-dire, elle est :

- Réflexive :  $\mathbf{x} \leq_l \mathbf{x}$  pour tout  $\mathbf{x} \in \mathbb{R}^n$ .
- Antisymétrique :  $\mathbf{x} \leq_l \mathbf{y} \wedge \mathbf{y} \leq_l \mathbf{x}$  implique  $\mathbf{x} = \mathbf{y}$ .
- Transitive :  $\mathbf{x} \leq_l \mathbf{y} \wedge \mathbf{y} \leq_l \mathbf{z}$  implique  $\mathbf{x} \leq_l \mathbf{z}$ .
- Totale : Pour tout  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$  on a  $\mathbf{x} \leq_l \mathbf{y}$  ou  $\mathbf{y} \leq_l \mathbf{x}$ .

Elle est compatible à l'addition, c'est-à-dire  $\mathbf{x} \leq_l \mathbf{y}$  implique  $\mathbf{x} + \mathbf{z} \leq_l \mathbf{y} + \mathbf{z}$  pour tout  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ .

(ii) De même, la relation  $\leq$  sur  $\mathbb{R}^n$  est un ordre totale, compatible à l'addition. En cas  $n = 1$  on retrouve l'ordre normale de  $\mathbb{R}$ .

(iii) Pour toute  $X \subseteq \mathbb{N}^n$ , il existe un unique plus petit élément par rapport à  $\leq_l$ . De même pour  $\leq$ .

(iv) Pour toute  $X \subseteq \mathbb{R}^n$  finie, il existe un unique plus grand élément par rapport à  $\leq_l$ . De même pour  $\leq$ .

### 3.1.10 Définition: Degré des polynômes dans $A[S]$

Soit  $(A, +, \cdot)$  un anneau commutatif,  $S \subseteq \mathbb{Z}^n$  un sous-monoïde de  $\mathbb{Z}^n$  et  $P \in A[S]$  un polynôme non-nul de la représentation

$$P = \sum_{s \in S} P_s \cdot e^s \quad .$$

où  $s = (s_1, \dots, s_n)$ . Alors, on appelle **degré** de  $P$  la valeur

$$\text{dg}(P) := \max_{\substack{s \in S \\ P_s \neq 0}} |s| \quad \text{où} \quad |s| := \sum_{i=1}^n s_i \quad .$$

Par convention le nul-polynôme n'a pas un degré. On appelle un polynôme  $P$  **homogène de degré**  $n \in \mathbb{N}_0$  s'il est non-nul et de la forme

$$P = \sum_{\substack{s \in S \\ |s|=n}} P_s \cdot e^s \quad .$$

Par convention, on écrit tout polynôme  $P \in A[S]$  non-nul comme

$$P = P_{s_1} e^{s_1} + \dots + P_{s_n} e^{s_n} \quad , \tag{3.1.10.1}$$

où  $P_{s_1}, \dots, P_{s_n} \neq 0$  et  $s_1 > s_2 > \dots > s_n$  et appelle la forme (3.1.10.1) la **représentation canonique** de  $P$ . En cette représentation, on a  $\text{dg}(P) = |s_1|$ . On dit  $P_{s_1} e^{s_1} =: \text{ini}(P)$  le **terme dominant** (ou **forme initiale**) de  $P$  et  $P_{s_1}$  le **coefficient dominant** de  $P$ . On dit  $P$  **unitaire**, ssi  $P_{s_1} = 1$ .

**Remarques :**

(i) Tout monôme  $e^s$  est homogène de degré  $|s|$ .

(ii) Si  $P, Q \in A[S]$  sont homogènes de degré  $\text{dg}(P)$  et  $\text{dg}(Q)$ , alors  $P * Q$  est soit nul soit homogène de degré  $\text{dg}(P) + \text{dg}(Q)$ .

(iii) Le système  $A[S]_n$  des polynômes homogènes de degré  $n$  dans  $A[S]$  (plus nul), forment un sous- $A$ -module de  $A[S]$ . Il possède la forme

$$A[S]_n = \sum_{|s|=n} A e^s$$

où la somme est directe. De cela et lemme 2.2.4(3), on déduit que  $A[S]_n$  est libre de  $A$ -base  $\{e^s : |s| = n\}$ . De plus, c'est facile de voir que

$$A[S] = \sum_{n \in \mathbb{Z}} A[S]_n$$

où la somme est directe. Remarque (ii) se traduit en

$$A[S]_n * A[S]_m \subseteq A[S]_{n+m} \quad \forall n, m \in S \quad ,$$

d'où on déduit que  $A[S]$  est une  $A$ -algèbre graduée (voir def. 3.1.2).

(iv) Suppose que  $S$  contient un élément  $s > 0$ , alors il existe dans  $A[S]$  une suite de polynômes  $(P_n)_{n \in \mathbb{N}}$  telle que  $\text{dg}(P_n) < \text{dg}(P_{n+1}) \forall n$ . Car pour tout  $0 \neq P, Q \in A[S]$  et  $a, b \in A$  on a toujours  $aP + bQ = 0$  ou  $\text{dg}(aP + bQ) \leq \max\{\text{dg}(P), \text{dg}(Q)\}$  (vois 3.1.11), le  $A$ -module  $A[S]$  n'est pas de type fini.

### 3.1.11 Lemme : Le degré comme morphisme de monoïdes

Soit  $(A, +, \cdot)$  un anneau commutatif,  $S \subseteq \mathbb{Z}^n$  un sous-monoïde de  $(\mathbb{Z}^n, +)$  et  $0 \neq P, Q \in A[S]$  n'importe que quels. Alors, on a soit  $P * Q = 0$  soit

$$\text{dg}(P * Q) \leq \text{dg}(P) + \text{dg}(Q) \quad .$$

Si de plus  $A$  est intègre, alors impérativement  $P * Q \neq 0$  et

$$\text{dg}(P * Q) = \text{dg}(P) + \text{dg}(Q) \quad ,$$

c'est-à-dire l'anneau  $A[S]$  est intègre et  $\text{dg} : (A[S] \setminus \{0\}, *) \rightarrow (\mathbb{Z}, +)$  est un morphisme de monoïdes.

**Preuve :** Soient  $0 \neq P, Q \in A[S]$  des représentations canoniques

$$P = P_{s_1} e^{s_1} + \dots + P_{s_n} e^{s_n} \quad , \quad Q = Q_{t_1} e^{t_1} + \dots + Q_{t_m} e^{t_m} \quad .$$

Suppose que leur produit  $P * Q$  est non-nul et de la représentation canonique

$$(P * Q) = (P * Q)_{u_1} \cdot e^{u_1} + \dots + (P * Q)_{u_k} \cdot e^{u_k} \quad .$$

Alors, par la compatibilité de “<” à l'addition on trouve  $u_1 \leq s_1 + t_1$ , d'où on déduit que

$$\text{dg}(P * Q) \leq \text{dg}(P) + \text{dg}(Q) \quad .$$

Si  $A$  est intègre, alors  $(P * Q)_{s_1+t_1} = P_{s_1} \cdot Q_{t_1} \neq 0$ , c'est-à-dire  $P * Q \neq 0$  et

$$\text{dg}(P * Q) = \text{dg}(P) + \text{dg}(Q) \quad .$$

□

### 3.1.12 Corollaire sur les polynômes inversibles

Soit  $A$  un anneau intègre. Alors :

1.  $P \in A[X_1, \dots, X_n]$  est inversible ssi  $P$  est une constante inversible dans  $A$ .
2. Deux polynômes  $P, Q \in A[X_1, \dots, X_n]$  engendrent les mêmes idéaux dans  $A[X_1, \dots, X_n]$  ssi ils sont égales modulo multiplication par  $A^\times$ .

**Preuve :**

1. Supposons  $Q \in A[X_1, \dots, X_n]$  tel que  $P * Q = 1$ . Évidemment  $Q, P \neq 0$ . Alors par 3.1.11

$$0 = \text{dg}(P * Q) = \underbrace{\text{dg}(P)}_{\geq 0} + \underbrace{\text{dg}(Q)}_{\geq 0} ,$$

donc  $\text{dg}(P) = 0 = \text{dg}(Q)$ . Donc  $P = p_0, Q = q_0$  avec  $p_0, q_0 \in A$  tel que  $p_0 q_0 = 1$ , c'est-à-dire  $p_0$  est inversible. Supposons inversement  $P = p_0 \in A^\times$ . Alors évidemment  $P * (p_0^{-1} \cdot X^0) = 1$ .

2. Par 3.1.11 on sait que  $A[X_1, \dots, X_n]$  est intègre. Par remarque 1.1.6(ii) on sait que  $A[X_1, \dots, X_n] * P = A[X_1, \dots, X_n] * Q$  ssi  $P \in A[X_1, \dots, X_n]^\times * Q$ . Par affirmation (1) on sait que  $A[X_1, \dots, X_n]^\times = A^\times$ .

□

### 3.1.13 Définition: Racines et polynôme scindés

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Alors, un polynôme  $P \in A[X_1, \dots, X_n]$  est dit **scindé** s'il est produit de polynômes de degrés 0 et 1. On dit  $(x_1, \dots, x_n) \in A^n$  une **racine** d'un polynôme  $P \in A[X_1, \dots, X_n]$  si  $P(x_1, \dots, x_n) = 0$ .

### 3.1.14 Théorème : Factorisation de polynômes

Soit  $A$  un anneau intègre,  $0 \neq P(X) \in A[X]$  et  $x \in A$  une racine de  $P$ . Alors,  $P$  est de la forme

$$P = (X - x)^\varepsilon * Q \tag{3.1.14.1}$$

pour un  $\varepsilon \in \mathbb{N}$  et un polynôme  $Q \in A[X]$  ne possédant pas  $x$  comme racine. Sous cette condition,  $Q$  et  $\varepsilon$  sont uniques et  $Q$  est de degré  $\text{dg}(Q) = \text{dg}(P) - \varepsilon$ . On appelle  $\varepsilon$  la **multiplicité** de la racine  $x$  dans  $P$ . On dit une racine **simple** si sa multiplicité est égale à 1.

**Preuve d'existence :** Soit  $P$  de la forme  $P = \sum_{i=0}^n p_i \cdot X^i$  avec  $p_n \neq 0$ . Supposons que  $x \in A$  est tel que  $P(x) = 0$ , c'est-à-dire

$$p_0 + p_1 \cdot x^1 + \dots + p_n \cdot x^n = 0 \ . \tag{3.1.14.2}$$

Noter que  $n \geq 1$ . Cherchons un  $Q = \sum_{i=0}^m q_i \cdot X^i \in A[X]$  tel que  $P = (X - x) * Q$ , ça veut dire

$$-xq_0 + \sum_{i=1}^{n-1} (q_{i-1} - q_i \cdot x) \cdot X^i + q_{n-1} \cdot X^n + \sum_{i=n+1}^m b_{i-1} X^i \stackrel{!}{=} \sum_{i=0}^n p_i \cdot X^i \ . \tag{3.1.14.3}$$

Noter que comme  $A$  est intègre, par 3.1.11 il faut que  $\text{dg}(Q) = n - 1$ . La condition (3.1.14.3) est équivalente aux conditions

$$\begin{aligned} q_{n-1} &= p_n \\ q_{i-1} &= p_i + q_i \cdot x \quad \forall i \in \{1, \dots, n-1\} \\ x \cdot q_0 &= -p_0 \end{aligned}$$

Les deux premières possèdent évidemment une solution unique et donnent donc les  $q_0, \dots, q_{n-1}$ . En particulier

$$q_0 = p_1 + q_1 x = (\dots) = p_1 + p_2 x + \dots + p_n x^{n-1} \ . \tag{3.1.14.4}$$

Mais avec (3.1.14.2), cela est compatible à la troisième condition

$$x \cdot q_0 \stackrel{(3.1.14.4)}{=} p_1 x^1 + \dots + p_n x^n \stackrel{(3.1.14.2)}{=} -p_0 \ .$$

On a donc trouver un  $Q \in A[X]$  tel que  $P = Q * (X - x)$ . Si  $x$  est encore une racine de  $Q$ , alors on peut répéter la procédure et arriver à la forme (3.1.14.1). Noter que par 3.1.11 il faut que  $\text{dg}(Q) = \text{dg}(P) - \varepsilon$ .

**Preuve d'unicité :** Supposons  $Q, \tilde{Q} \in A[X]$  et  $\varepsilon, \tilde{\varepsilon} \in \mathbb{N}$  sont tels que

$$Q * (X - x)^\varepsilon = \tilde{Q} * (X - x)^{\tilde{\varepsilon}} ,$$

et  $Q(x), \tilde{Q}(x) \neq 0$ . Supposons  $\varepsilon \geq \tilde{\varepsilon}$ . Alors, comme  $A[X]$  est intègre, il faut que

$$Q * (X - x)^{\varepsilon - \tilde{\varepsilon}} = \tilde{Q} .$$

Comme  $\tilde{Q}(x) \neq 0$ , il faut que  $\varepsilon = \tilde{\varepsilon}$ . Donc, par intégrité de  $A[X]$  nous concluons  $Q = \tilde{Q}$ . □

### 3.1.15 Corollaire : Factorisation de polynômes

Soit  $A$  un anneau intègre et  $0 \neq P \in A[X]$  de degré  $n := \text{dg}(P)$ . Alors,  $P$  possède au maximum  $n$  racines distinctes. De plus, si  $x_1, \dots, x_k \in A$  sont ses racines distinctes, alors il est de la forme

$$P(X) = Q(X) * \prod_{i=1}^k (X - x_i)^{\varepsilon_i} , \quad (3.1.15.1)$$

où  $\varepsilon_1, \dots, \varepsilon_k \in \mathbb{N}$  et  $Q \in A[X]$  ne possède pas de racines dans  $A$ . Sous ses conditions, les  $\varepsilon_i$  et  $Q$  sont uniques. Tout  $\varepsilon_i$  est exactement la multiplicité de la racine  $x_i$  dans  $P$ .

**Preuve d'existence :** Par théorème 3.1.14 il existe un  $\varepsilon_1 \in \mathbb{N}$  et un  $0 \neq Q_1 \in A[X]$  tel que  $P = (X - x_1)^{\varepsilon_1} * Q_1$  et  $Q_1(x_1) \neq 0$ . Pour  $i \in \{2, \dots, n\}$  il faut  $0 = P(x_i) = (x_i - x_1)^{\varepsilon_1} * Q_1(x_i)$ . Comme  $A$  est intègre et  $x_i \neq x_1$ , il faut que les  $x_2, \dots, x_n$  sont les seules racines de  $Q_1$ . On peut donc répéter la même procédure et obtenir par récurrence la forme (3.1.15.1), où  $Q$  ne possède pas de racines dans  $A$ .

**Preuve d'unicité :** Supposons que  $Q, \tilde{Q} \in A[X]$  et  $\varepsilon_i, \tilde{\varepsilon}_i \in \mathbb{N}$  satisfont

$$Q * \prod_{i=1}^k (X - x_i)^{\varepsilon_i} = \tilde{Q} * \prod_{i=1}^k (X - x_i)^{\tilde{\varepsilon}_i} ,$$

et  $Q, \tilde{Q}$  ne possèdent pas de racines dans  $A$ . Comme  $A$  est intègre, on sait que les polynômes

$$Q * \prod_{i=1}^{k-1} (X - x_i)^{\varepsilon_i} , \quad \tilde{Q} * \prod_{i=1}^{k-1} (X - x_i)^{\tilde{\varepsilon}_i} \quad (3.1.15.2)$$

ne possèdent que les racines  $x_1, \dots, x_{k-1}$ . Par théorème 3.1.14, il faut que  $\varepsilon_k = \tilde{\varepsilon}_k$  et les polynômes (3.1.15.2) sont égales. Par récurrence, on montre que  $\varepsilon_i = \tilde{\varepsilon}_i$  pour tout  $i$  et  $Q = \tilde{Q}$ . Noter que pour tout  $l \in \{1, \dots, n\}$ , le polynôme  $Q * \prod_{i \neq l} (X - x_i)$  ne possède pas  $x_l$  comme racine et par la même argumentation  $\varepsilon_l$  est exactement la multiplicité de  $x_l$  dans  $P$ . □

**Remarques :** Soit  $A$  intègre et  $P \in A[X]$ .

- (i) Le polynôme  $P$  est scindé ssi  $Q = \text{const}$  dans la factorisation (3.1.15.1) ci-dessus.
- (ii) Si  $x \in A$  est une racine de  $P$ , alors  $x$  est simple ssi  $P'(x) \neq 0$ .

**Preuve :** Comme  $x$  est racine de  $P$ , on peut écrire  $P = (X - x) * Q$  pour un polynôme  $0 \neq Q \in \mathbb{K}[X]$ . Comme

$$P' = Q + (X - x) * Q' ,$$

on sait que  $x$  est racine simple ssi  $Q(x) \neq 0$  et donc ssi  $P'(x) \neq 0$ .



### 3.1.16 Lemme sur polynômes linéairement indépendants

Soit  $A$  un anneau commutatif,  $n \in \mathbb{N}$  et  $(P_i)_{i \in I} \subseteq A[X_1, \dots, X_n]$  une famille de polynômes avec termes dominants  $P_{i,s_i} X^{s_i}$ . On suppose que les  $(s_i)_{i \in I}$  sont deux à deux inégales et que tout  $P_{i,s_i}$  n'est pas diviseur de zéro. Alors, les  $(P_i)_{i \in I}$  sont  $A$ -linéairement indépendants.

**Preuve :** Claire.

### 3.1.17 Lemme sur bases de polynômes

Soit  $A$  un anneau commutatif,  $n \in \mathbb{N}$  et  $(P_s)_{s \in \mathbb{N}_0^n} \subseteq A[X_1, \dots, X_n]$  une famille de polynômes. On suppose que tout  $P_s \in A[X_1, \dots, X_n]$  possède le terme dominant  $P_{s,s} X^s$  et que  $P_{s,s} \in A^\times$  est inversible. Alors, les  $(P_s)_{s \in \mathbb{N}_0^n}$  forment une base du  $A$ -module  $A[X_1, \dots, X_n]$ .

**Preuve :** Comme tout inversible de  $A$  et non-diviseur de zéro, par 3.1.16 la famille  $(P_s)_{s \in \mathbb{N}_0^n}$  est linéairement indépendant. De plus, comme les coefficients  $P_{s,s}$  sont inversibles, on a

$$\text{span}_A \{P_s\}_{s \in \mathbb{N}_0^n} = \text{span}_A \{P_{s,s}^{-1} \cdot P_s\}_{s \in \mathbb{N}_0^n} ,$$

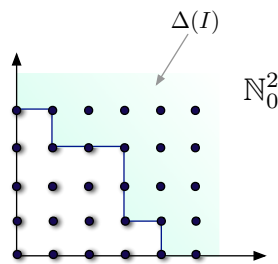
ce qui évidemment contient tout polynôme de  $A[X_1, \dots, X_n]$ . □

## 3.2 Idéaux dans $A[S]$

### 3.2.1 Définition: Idéal monômial dans $A[S]$

Soit  $(A, +, \cdot)$  un anneau commutatif et  $(S, +)$  un monoïde commutatif. Un idéal  $I \subseteq A[S]$  de l'anneau  $(A[S], +, *)$  est dit **monômial**, s'il est engendré par des monômes (de nombre fini ou pas).

**Remarque :** Soit  $I \subseteq A[S]$  un idéal n'importe quel et  $\Delta(I) := \{s \in S : X^s \in I\}$ . Alors,  $\Delta(I) + S = \Delta(I)$ . Si par exemple  $S = \mathbb{N}_0$ , alors il existe un  $n \in \mathbb{N}_0$  tel que  $\Delta(I) = \{n, n+1, \dots\}$ . Si  $S = \mathbb{N}_0^2$ , le *bord* de l'ensemble  $\Delta(I)$  est un escalier montant de la droite vers la gauche (vois figure 12).



**FIGURE 12:** Exemple de la famille  $\Delta(I) := \{s \in \mathbb{N}_0^2 : X^s \in I\}$  pour un idéal  $I \subseteq A[X_1, X_2]$ . On a  $\Delta(I) + \mathbb{N}_0^2 = \Delta(I)$ , c'est-à-dire  $s + \mathbb{N}_0^2 \subseteq \Delta(I)$  pour tout  $s \in \Delta(I)$ .

Or, un idéal monômial  $I \subseteq A[S]$  est un idéal engendré par  $\Delta(I)$ .

### Exemples

- (i) Si  $A$  est un anneau commutatif, alors l'idéal  $\langle X \rangle \subseteq A[X]$  est monomial. L' $A$ -algèbre  $A[X]/\langle X \rangle$  est isomorphe au anneau  $A$  (vu comme  $A$ -algèbre) via l'isomorphisme

$$\sum_{i=0}^n P_i X^i \mapsto P_0 \quad .$$

### 3.2.2 Lemme sur idéaux monômiaux

Soit  $(A, +, \cdot)$  un anneau commutatif et  $S$  un monoïde commutatif. Alors, un idéal  $I \subseteq A[S]$  est monomial ssi pour tout  $P \in I$  de la représentation

$$P = \sum_{i=1}^n P_{s_i} \cdot X^{s_i}$$

où  $P_{s_i} \neq 0 \forall i \in \{1, \dots, n\}$ , les monômes  $X^{s_1}, \dots, X^{s_n}$  appartient aussi à  $I$ .

**Preuve :** Direction " $\Leftarrow$ " est triviale. Direction " $\Rightarrow$ " : Soit  $(X^s)_{s \in S} \subseteq I$  une famille des monômes engendrant l'idéal  $I$ , alors tout  $P \in I$  peut être écrit comme combinaison  $A[S]$ -linéaire finie des monômes de  $(X^s)_{s \in S}$  :

$$P = \sum_{i=1}^n P_i * X^{s_i} \quad , \quad s_i \in S, P_i \in A[S]$$

Pour tout  $i \in \{1, \dots, n\}$  soit

$$P_i = \sum_j P_{i,t_j} \cdot X^{t_j} \quad , \quad P_{i,t_j} \in A$$

une représentation de  $P_i$ , alors

$$P = \sum_{i=1}^n \sum_j P_{i,t_j} \cdot X^{t_j + s_i} \quad .$$

Par définition d'un idéal, on sait que tout  $X^{t_j + s_i}$  est dans  $I$ . Par l'unicité des représentations de polynômes (sauf termes triviales) on en déduit l'affirmation.  $\square$

### 3.2.3 Théorème sur anneaux noetheriens

Soit  $(A, +, \cdot)$  un anneau commutatif noetherien <sup>21</sup> et  $n \in \mathbb{N}$ . Alors  $(A[X_1, \dots, X_n], +, *)$  est un anneau noetherien.

**Preuve :** Par 3.1.8, pour la première affirmation il suffit de montrer que si  $A$  est noetherien, alors  $A[X]$  est également.

Soit  $J \subseteq A[X]$  un idéal, où on suppose sans perdu de généralité que  $J \notin \{\{0\}, A[X]\}$ . Pour tout polynôme  $0 \neq P \in A[X]$  de la forme

$$P = a_0 X^0 + a_1 X^1 + \dots + a_n X^n \quad , \quad a_n \neq 0$$

on considère son terme dominant  $a_n X^n$  et en particulier son coefficient dominant  $\text{ini}(P) := a_n$ . On note

$$\mathcal{J} := \langle \text{ini}(P) : P \in J \rangle \subseteq A$$

l'idéal dans  $A$  engendré par les coefficients dominants  $\text{ini}(P)$ ,  $P \in J$ . Car  $A$  est noetherien,  $\mathcal{J}$  est de type fini, c'est-à-dire engendré par des éléments  $\lambda_1, \dots, \lambda_d \in \mathcal{J}$ . Soient  $(P_i)_{i=1}^d \subseteq J$  tels que tout  $P_i$  possède le terme dominant  $\lambda_i X^{n_i}$  et soit  $n := \sup_{1 \leq i \leq d} n_i$ . Pour  $0 \leq k \leq n$  soit

$$\mathcal{J}_k := \langle \text{ini}(P) : P \in J, \text{dg}(P) = k \rangle \subseteq A$$

21. C'est-à-dire tout son idéal est de type fini.

l'idéal dans  $A$  engendré par les coefficients dominants des polynômes  $P \in J$  de degré  $k$ . Alors, de même comme ci-dessus, on peut trouver des polynômes  $(P_{k,i})_{i=1}^{d_k} \subseteq J$  dont les coefficients dominants  $\text{ini}(P_{k,i}) =: \lambda_{k,i}$  engendrent  $\mathcal{J}_k$ .

On va montrer que l'idéal  $\tilde{\mathcal{J}} \subseteq A[X]$  dans  $A[X]$  engendré par la collection finie

$$\{P_i\}_{i=1}^d \cup \bigcup_{k=0}^n \{P_{k,i}\}_{i=1}^{d_k} ,$$

est en fait égal à  $J$ . On suppose que  $\tilde{\mathcal{J}} \subsetneq J$  et choisit  $P \in J \setminus \tilde{\mathcal{J}}$  de degré minimal. En cas  $\text{dg}(P) \geq n$  on peut écrire son coefficient dominant  $\text{ini}(P)$  comme combinaison  $A$ -linéaire des  $\lambda_1, \dots, \lambda_d$  :

$$\text{ini}(P) = \sum_{i=1}^d a_i \underbrace{\lambda_i}_{\text{ini}(P_i)} , \quad a_i \in A .$$

D'autre part, le polynôme

$$\tilde{P} := P - \underbrace{\sum_{i=1}^d a_i P_i}_{\in \tilde{\mathcal{J}}} * X^{\text{dg}(P) - \text{dg}(P_i)}$$

est aussi dans  $J \setminus \tilde{\mathcal{J}}$ . Mais car son degré est plus petit que  $\text{dg}(P)$ , on a trouvé une contradiction à la minimalité de  $\text{dg}(P)$ . En cas  $k := \text{dg}(P) < n$ , par le même argument on peut écrire  $\text{ini}(P)$  comme combinaison  $A$ -linéaire des  $\lambda_{k,1}, \dots, \lambda_{k,d_k}$  :

$$\text{ini}(P) = \sum_{i=1}^{d_k} a_i \cdot \underbrace{\lambda_{k,i}}_{\text{ini}(P_{k,i})} , \quad a_i \in A .$$

D'autre part, le polynôme

$$\tilde{P} := P - \sum_{i=1}^{d_k} a_i P_{k,i}$$

est dans  $J/\tilde{\mathcal{J}}$  et de degré  $< \text{dg}(P)$ , encore une contradiction. □

### 3.2.4 Exemple : $\mathbb{Z}[X]$

Par théorème 3.2.3 on sait que  $\mathbb{Z}[X]$  est noethérien. On va montrer que  $\mathbb{Z}[X]$  n'est pas principal. On considère l'idéal

$$I := \{P \in \mathbb{Z}[X] : P(0) \in 2\mathbb{Z}\} = \langle 2, X \rangle ,$$

et montre par l'absurde que  $I$  n'est pas principal. Supposons que  $I$  est engendré par un  $P \in I$ . Alors,  $P \mid 2$  et donc  $\text{dg } P = 0$ , c'est-à-dire  $P = p_0 : \text{const} \in \mathbb{Z}$ . De même,  $P \mid X$ , c'est-à-dire il existe un  $Q \in \mathbb{Z}[X]$  tel que  $X = PQ = p_0 Q$ . Donc il existe un  $b \in \mathbb{Z}$  tel que  $p_0 b = 1$ , d'où on déduit  $p_0 \in \{\pm 1\}$ . Donc  $\pm 1 \in I$ , c'est-à-dire  $I = \mathbb{Z}[X]$ . Mais cela est une contradiction !

### 3.2.5 Corollaire : Théorème de la base de Hilbert

Si  $\mathbb{K}$  est un corps et  $n \in \mathbb{N}$ , alors  $\mathbb{K}[X_1, \dots, X_n]$  est un anneau noethérien.

**Preuve :** Suit de théorème 3.2.3 et du fait que tout corps  $\mathbb{K}$  est noethérien. □

### 3.2.6 Caractérisation d'algèbres de polynômes principaux

Soit  $A$  un anneau intègre non-trivial. Alors, les suivantes sont équivalents :

1.  $A$  est un corps.
2. L'anneau  $A[X]$  est principal.
3. L'anneau  $A[X]$  est euclidien.

**Preuve :**

$1 \Rightarrow 2$  : Soit  $\{0\} \neq J \subseteq A[X]$  un idéal et  $0 \neq P \in J$  de degré minimal. Si  $\text{dg}(P) = 0$ , alors  $P = \lambda X^0$  pour un  $0 \neq \lambda \in A$ , c'est-à-dire  $P \in A[X]^\times$  et donc par remarque 1.2.1(ii)  $J = A[X]$  et  $J$  est engendré par  $X^0$ .

On suppose donc que  $\text{dg}(P) > 0$  et va montrer que  $P$  engendre  $J$ . Soit

$$P = P_{s_1} X^{s_1} + \dots + P_{s_n} X^{s_n}$$

la représentation canonique de  $P$ . Soit  $0 \neq Q \in J$  de la représentation canonique

$$Q = Q_{t_1} \cdot X^{t_1} + \dots + Q_{t_m} \cdot X^{t_m} .$$

Alors, car  $\text{dg}(Q) \geq \text{dg}(P)$  il faut  $t_1 \geq s_1$  et donc le polynôme

$$Q - \frac{Q_{t_1}}{P_{s_1}} \cdot X^{t_1-s_1} * P \in J \quad (3.2.6.1)$$

possède degré plus petit que  $t_1 = \text{dg}(Q)$ . Supposant que  $A[X] * P \subsetneq J$ , on pourrait choisir un  $Q \notin A[X] * P$  de degré minimal. Par (3.2.6.1) on trouverait une contradiction.

$2 \Rightarrow 1$  : Par le théorème d'isomorphismes d'anneaux 1.2.13, les anneaux  $A$  et  $A[X]/\langle X \rangle$  sont isomorphes. Donc, par 1.2.18 il suffit de montrer que  $\langle X \rangle$  est un idéal maximal dans  $A[X]$ . Supposons que  $J \subseteq A[X]$  est un idéal dans  $A[X]$  tel que  $\langle X \rangle \subsetneq J \subsetneq A$ . Alors, par hypothèse  $J$  est engendré par un polynôme  $P \in A[X]$ , de la forme  $P = \sum_i p_i X^i$ . En particulier,  $X = Q * P$  pour un  $Q = \sum_i q_i X^i \in A[X]$ . Si  $p_0 = 0$ , alors  $P \in \langle X \rangle$  et donc  $J \subseteq \langle X \rangle$ , une contradiction. Comme

$$X = q_0 p_0 + (q_0 p_1 + q_1 p_0) \cdot X + \sum_{i \geq 1} q_i X^i * \sum_{j \geq 1} p_j X^j ,$$

il faut que  $q_0 p_0 = 0$ . Comme  $A$  est intègre et  $p_0 \neq 0$ , il faut que  $q_0 = 0$ . Donc,  $q_1 p_0 = 1$ , c'est-à-dire  $p_0 \in A^\times$ . Mais comme  $X \in \langle P \rangle$ , on sait que aussi  $p_0 \in \langle P \rangle$ . Mais cela impliquerait  $\langle P \rangle = A[X]$ , une contradiction !

$1 \Rightarrow 3$  : Voir lemme 3.2.12.

$3 \Rightarrow 2$  : Par 4.1.6, tout anneau euclidien est principal.

### 3.2.7 Fonctions polynomiales

Soit  $(A, +, \cdot)$  un anneau commutatif,  $(B, +, \cdot)$  une  $A$ -algèbre et  $n \in \mathbb{N}$ . Alors, pour tout  $b = (b_1, \dots, b_n) \in B^n$  il existe un unique morphisme d'algèbres  $\Phi_b : A[X_1, \dots, X_n] \rightarrow B$  satisfaisant

$$\Phi_b(X_i) = b_i \quad \forall i \in \{1, \dots, n\} .$$

Il est donné par

$$\Phi_b \left[ \sum_{s \in \mathbb{N}_0^n} a_s X^s \right] = \sum_{s \in \mathbb{N}_0^n} a_s \cdot \underbrace{b_1^{s_1} \cdot \dots \cdot b_n^{s_n}}_{=: b^s} .$$

Cette *spécialisation des  $X_i$  en les  $b_i$*  donne pour un  $P = \sum_s p_s X^s \in A[X_1, \dots, X_n]$  fixé n'importe quel une application  $B^n \rightarrow B$  par

$$b \mapsto \Phi_b(P) =: \tilde{P}(b) = \sum_{s \in \mathbb{N}_0^n} p_s \cdot b^s ,$$

appelé **application polynomiale** associée à  $P$ . On note  $\mathcal{F}(B^n, B)$  l'ensemble de toutes applications polynomiales de  $B^n$  dans  $B$ . On munit  $\mathcal{F}(B^n, B)$  de la structure d'une  $A$ -algèbre par les lois

$$(a\tilde{P} + b\tilde{Q})(b) := a\tilde{P}(b) + b\tilde{Q}(b)$$

$$(\tilde{P} \cdot \tilde{Q})(b) := \tilde{P}(b) \cdot \tilde{Q}(b)$$

$$\tilde{P}, \tilde{Q} \in \mathcal{F}(B^n, B), a \in A, b \in B .$$

Note que les compositions ci-dessus satisfont vraiment les axiomes d'une  $A$ -algèbre. L'association

$$[A[X_1, \dots, X_n], +, *] \rightarrow [\mathcal{F}(B^n, B), +, \cdot] , P \mapsto \tilde{P}$$

est un morphisme de  $A$ -algèbres. Le cas plus important est  $B = A$ . On dit un  $a \in A$  **racine** d'un polynôme  $P \in A[X_1, \dots, X_n]$  ssi  $\tilde{P}(a) = 0$  (voir aussi 3.2.7).

**Remarque :**

- (i) En général, le morphisme  $P \mapsto \tilde{P}$  n'est pas injectif. Comme exemple, considère l'anneau  $A := \mathbb{Z}/p\mathbb{Z} =: B$  pour un premier  $p \in \mathbb{P}$ . Alors, le polynôme  $(X^p - X) \in A[X]$  induit la fonction polynomiale  $x \mapsto (x^p - x)$  sur  $A$ . Se rappeler que  $n^{p-1} = 1 \pmod{p}$  pour tout entier  $1 \leq n < p$ .

### 3.2.8 Théorème : Fonctions polynomiales sur corps infinies

Si  $\mathbb{K}$  est un corps infini et  $n \in \mathbb{N}$ , alors le morphisme  $\mathbb{K}[X_1, \dots, X_n] \rightarrow \mathcal{F}(\mathbb{K}^n, \mathbb{K})$ ,  $P \mapsto \tilde{P}$  est injectif et donc bijectif.

**Preuve :** La preuve consiste d'une récurrence sur  $n \in \mathbb{N}$ . On commence par le cas  $n = 1$ . Considère  $P \in \mathbb{K}[X]$  et suppose  $P \neq 0$  mais  $\tilde{P}(x) = 0 \forall x \in \mathbb{K}$ . Alors,  $P$  possède par 3.1.15 au plus  $\text{dg}(P)$  racines dans  $\mathbb{K}$ , une contradiction à l'infinitude de  $\mathbb{K}$ .

On suppose que l'affirmation est vrai pour  $1, \dots, n-1$  et se rappelle que  $\mathbb{K}[X_1, \dots, X_n] \cong \mathbb{K}[X_1, \dots, X_{n-1}][X_n]$ , traduit le fait suivant : Tout  $P \in \mathbb{K}[X_1, \dots, X_n]$  est donné par

$$P = \sum_{s_n \in \mathbb{N}_0} P_s \cdot X_n^{s_n} , P_s \in \mathbb{K}[X_1, \dots, X_{n-1}] .$$

On suppose que  $\tilde{P} = 0$ . Soit  $a = (a_1, \dots, a_{n-1}) \in \mathbb{K}^{n-1}$  quelconque. On forme le polynôme en  $X_n$  :

$$P(a, \cdot) := \sum_{s \in \mathbb{N}_0} \tilde{P}_s(a) \cdot X_n^s \in \mathbb{K}[X_n] .$$

Alors, car  $\tilde{P} = 0$  il faut  $\tilde{P}(a, \cdot) = 0$  qui par suppositions de la récurrence implique  $\tilde{P}_s(a) = 0$  pour tout  $s \in \mathbb{N}_0$ . Cela étant vrai pour tout  $a \in \mathbb{K}^{n-1}$ , c'est-à-dire  $\tilde{P}_s \equiv 0 \forall s$ , par supposition de la récurrence on trouve  $P_s = 0 \forall s \in \mathbb{N}_0$ . Donc  $P = 0$ . □

**Interprétation :** Si  $\mathbb{K}$  est un corps infini, alors il n'existe pas d'équations algébriques non-triviales sur  $\mathbb{K}$ , résolues par tout  $\mathbb{K}$ .

### 3.2.9 Application : Principe de prolongement des identités algébriques

Soit  $\mathbb{K}$  un corps infini. On se donne un polynôme  $0 \neq P \in \mathbb{K}[X_1, \dots, X_n]$  et un polynôme  $G \in \mathbb{K}[X_1, \dots, X_n]$  tel que

$$\tilde{G}(a) = 0 \quad \forall a \in \mathbb{K}^n, \tilde{P}(a) \neq 0 .$$

Alors,  $G = 0$ .

**Preuve :** On a  $\widetilde{P * G} = 0$  et donc par théorème 3.2.8  $P * G = 0$ . Par 3.1.11 on sait que  $\mathbb{K}[X_1, \dots, X_n]$  est intègre. Donc,  $P \neq 0$  implique impérativement  $G = 0$ .  $\square$

### 3.2.10 Théorème : Fonctions polynomiales sur corps de type $\mathbb{Z}/p\mathbb{Z}$

Si  $p \in \mathbb{P}$  est premier,  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  et  $n \in \mathbb{N}$ , alors le noyau du morphisme  $\mathbb{F}_p[X_1, \dots, X_n] \rightarrow \mathcal{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ ,  $P \mapsto \widetilde{P}$  est l'idéal engendré par les polynômes  $X_1^p - X_1, \dots, X_n^p - X_n$ . De plus, la  $\mathbb{F}_p$ -algèbre  $\mathcal{F}(\mathbb{F}_p^n, \mathbb{F}_p)$  est libre de rang  $p^n$ .

### 3.2.11 Théorème : Idéaux dans $A[X]$

Soit  $A$  un anneau commutatif et  $I \subseteq A$  un idéal. Alors l'ensemble des polynômes de  $A[X]$  de coefficients dans  $I$ , noté  $I[X] \subseteq A[X]$ , est un idéal et un sous- $A$ -module de  $A[X]$ . Les  $A$ -algèbres  $(A/I)[X]$  et  $A[X]/I[X]$  sont isomorphes via l'isomorphisme donné par

$$\sum_i \underbrace{[p_i]}_{\in A/I} \cdot X^i \mapsto \underbrace{\left[ \sum_i p_i X^i \right]}_{\in A[X]/I[X]} .$$

### 3.2.12 Lemme : L'anneau $\mathbb{K}[X]$ comme anneau euclidien

Soit  $\mathbb{K}$  un corps. Alors,  $\mathbb{K}[X]$  est un anneau euclidien avec division euclidienne unique par rapport à la stathme  $\text{val} : P \mapsto \text{dg}(P)$ ,  $P \in \mathbb{K}[X]$ .

### 3.2.13 Lemme : Anneaux quotient dans $\mathbb{K}[X]$

Soit  $\mathbb{K}$  un corps et  $Q \in \mathbb{K}[X]$  quelconque, fixé. Alors, l'algèbre quotient  $\mathbb{K}[X]/\langle Q \rangle$  de  $\mathbb{K}[X]$  sur l'idéal engendré par  $Q$ , est un  $\mathbb{K}$ -espace vectoriel de base  $\overline{X}^0, \overline{X}^1, \dots, \overline{X}^{m-1}$ , où  $m := \text{dg}(Q)$  si  $Q \neq 0$  et  $m = \infty$  si  $Q = 0$ .

**Preuve :** Se rappeler que par 3.2.12  $\mathbb{K}[X]$  est euclidien avec stathme  $\text{val} := \text{dg}$ . Le cas  $Q = 0$  est claire, comme  $\mathbb{K}[X]/\langle Q \rangle$  est isomorphe à  $\mathbb{K}[X]$ . Supposons donc  $Q \neq 0$ . Alors, tout polynôme  $P \in \mathbb{K}[X]$  s'écrit comme  $P = B * Q + R$ , où  $\text{dg}(R) < \text{dg}(Q)$  si  $R \neq 0$ . En particulier,  $P \in \langle Q \rangle + \text{span}_{\mathbb{K}} \{X^0, \dots, X^{m-1}\}$ , d'où on déduit que les  $\overline{X}^0, \dots, \overline{X}^{m-1}$  engendrent  $\mathbb{K}[X]/\langle Q \rangle$ . D'autre part, soient  $\varkappa_0, \dots, \varkappa_{m-1}$  tels que  $\sum_{i=0}^{m-1} \varkappa_i \overline{X}^i = 0$ , c'est-à-dire  $\sum_{i=0}^{m-1} \varkappa_i X^i = B * Q$  pour un  $B \in \mathbb{K}[X]$ . Alors  $B = 0$ , car sinon  $\text{dg}(B * Q) = \text{dg}(B) + \text{dg}(Q) \geq m$ , ce qui est impossible. Donc  $\varkappa_0, \dots, \varkappa_{m-1} = 0$ , ça veut dire les  $\overline{X}^0, \dots, \overline{X}^{m-1}$  sont linéairement indépendants.  $\square$

## 3.3 Dérivation de polynômes

### 3.3.1 Définition: Opérateur de différences

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Alors, pour  $i \in \{1, \dots, n\}$  on définit l'**opérateur de différences**

$$\Delta_i : A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n] \quad , \quad (\Delta_i P)(X_1, \dots, X_n) := P(X_1, \dots, X_i + 1, \dots, X_n) - P(X_1, \dots, X_n) \quad .$$

Pour  $n = 1$  on note  $\Delta := \Delta_1$ .

### 3.3.2 Lemme sur l'opérateur de différences et polynômes constantes

Soit  $A$  un anneau commutatif contenant  $\mathbb{Q}$ . Alors, un polynôme  $P \in A[X]$  est constant ssi  $\Delta P = 0$ .

**Preuve :** C'est évident que si  $P$  est constante alors  $\Delta P = 0$ . D'autre part, si  $P$  est de la forme

$$P = \sum_{n=0}^N P_n \cdot X^n \quad ,$$

alors

$$\Delta P = \sum_{n=1}^N P_n \cdot \underbrace{\sum_{k=0}^{n-1} \binom{n}{k} X^k}_{\text{terme dominant } n \cdot X^{n-1}} \quad .$$

Note que  $n \in A$  n'est pas diviseur de zéro. Or, si  $\Delta P = 0$ , alors par lemme 3.1.16 on conclut que  $P_n = 0$  pour tout  $n \in \{1, \dots, N\}$ . Par conséquence  $P = P_0$ . □

### 3.3.3 Définition: Coefficient binomial

Soit  $A$  un anneau commutatif contenant  $\mathbb{Q}$ . Pour  $\alpha \in A$  et  $n \in \mathbb{N}_0$  on définit le **coefficient binomial**

$$\binom{\alpha}{n} := \frac{1}{n!} \alpha(\alpha-1) \dots (\alpha-n+1) \quad .$$

En particulier  $\binom{\alpha}{0} := 1$ . De même on pose

$$\binom{X}{n} := \frac{1}{n!} X(X-1) \dots (X-n+1) \in A[X] \quad .$$

**Remarques :**

(i) Tout  $\binom{X}{n}$  possède le terme dominant  $X^n$ . Par lemme 3.1.17 la famille  $\left(\binom{X}{n}\right)_{n \in \mathbb{N}_0}$  forme une base de  $A[X]$ .

(ii) Pour tout  $n \in \mathbb{N}$  on a

$$\Delta \binom{X}{n} = \binom{X}{n-1} \quad .$$

### 3.3.4 Définition: Dérivée d'un polynôme

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Pour tout  $i \in \{1, \dots, n\}$  il existe une unique application

$$\partial_i : A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]$$

satisfaisant :

1.  $\partial_i$  est  $A$ -linéaire, c'est-à-dire un morphisme de  $A$ -modules.
2.  $\partial_i(X_j) = \delta_{ij}$  pour  $j \in \{1, \dots, n\}$ .
3. Pour  $P, Q \in A[X_1, \dots, X_n]$  on a toujours  $\partial_i(P * Q) = \partial_i(P) * Q + P * \partial_i(Q)$ .

On appelle  $\partial_i(P)$  la **dérivée** du polynôme  $P \in A[X_1, \dots, X_n]$  **par rapport à**  $X_i$ . Les conditions ci-dessus définissent la dérivée comme

$$\partial_i \sum_{s \in \mathbb{N}_0^n} P_s \cdot X_1^{s_1} \cdot \dots \cdot X_n^{s_n} = \sum_{s \in \mathbb{N}_0^n} s_i \cdot P_s \cdot X_1^{s_1} \cdot \dots \cdot X_i^{s_i-1} \cdot \dots \cdot X_n^{s_n} \quad .$$

### 3.3.5 Caractérisation des polynômes constantes

Soit  $A$  un anneau commutatif, satisfaisant au moins une des conditions :

- $A$  est intègre et de caractéristique 0.
- $A$  contient  $\mathbb{Q}$ .

Alors, un polynôme  $P \in A[X_1, \dots, X_n]$  est constant ssi toute dérivée  $\partial_i P$  est nulle.

**Preuve :** Direction “ $\Rightarrow$ ” et triviale. Supposons donc  $\partial_i P = 0$  pour un polynôme  $P$  et tout  $i \in \{1, \dots, n\}$ . En considérons  $P(X_1, \dots, X_n)$  comme polynôme dans  $A[X_1, \dots, X_{n-1}][X_n]$ , on peut par récurrence ramener l’affirmation au cas  $n = 1$ . Considérons donc un polynôme  $P = \sum_{i=0}^n p_i X^i \in A[X]$  de dérivée nulle, c’est-à-dire

$$0 = \frac{dP}{dX} = \sum_{i=1}^n i \cdot a_i \cdot X^{i-1} .$$

Alors, comme  $i \neq 0$  dans  $A$  pour tout  $i \in \{1, \dots, n\}$ , en cas que  $A$  est intègre on conclut que les  $a_1, \dots, a_n$  sont nulles. De même, si  $\mathbb{Q} \subseteq A$  il faut  $a_1, \dots, a_n = 0$ . □

## 3.4 Polynômes invariants sous un groupe fini

### 3.4.1 Définition: Groupe linéaire générale

Pour un anneau commutatif  $(A, +, \cdot)$  on note  $\mathrm{GL}_n(A)$  le groupe des matrices  $n \times n$  inversibles à coefficients dans  $A$ . On considère  $\mathrm{GL}_n(A)$  comme agissant sur  $A[X_1, \dots, X_n]$  via automorphismes de  $A$ -algèbres, qui sont eux mêmes donnés par leur valeurs des  $X_1, \dots, X_n$  :

$$M \cdot X_i := \sum_{j=1}^n (M^{-1})_{ij} \cdot X_j \quad , \quad M \in \mathrm{GL}_n(A) . \quad (3.4.1.1)$$

Note que l’action (3.4.1.1) est vraiment un action à gauche sur  $A[X_1, \dots, X_n]$ .

### 3.4.2 Lemme sur l’action des sous-groupes de $\mathrm{GL}_n(A)$

Soit  $A$  un anneau commutatif,  $n \in \mathbb{N}$  et  $G \leq \mathrm{GL}_n(A)$  un sous-groupe. Alors, le sous-ensemble des polynômes  $G$ -invariants est un sous-algèbre notée  $A[X_1, \dots, X_n]^G$ .

**Preuve :** Par construction, pour tout  $M \in G$  l’action de  $M$  sur  $A[X_1, \dots, X_n]$  est un automorphisme d’algèbres. De cela, on trouve que  $A[X_1, \dots, X_n]^G$  est vraiment un sous- $A$ -module et un sous-anneau. □

### 3.4.3 Exemple : Action du groupe symétrique

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Le groupe symétrique  $\mathrm{Sym}(n)$  se réalise naturellement dans  $\mathrm{GL}_n(A)$  via l’association

$$\sigma \mapsto M_\sigma \quad , \quad (M_\sigma)_{ij} := \delta_{i, \sigma(j)} . \quad (3.4.3.1)$$

Alors, (3.4.3.1) est un monomorphisme de groupes  $\mathrm{Sym}(n) \hookrightarrow \mathrm{GL}_n(A)$ , c’est-à-dire  $M_{\sigma\tau} = M_\sigma \cdot M_\tau$  pour  $\sigma, \tau \in \mathrm{Sym}(n)$ . On considère le groupe  $\mathrm{Sym}(n)$  agissant sur  $A[X_1, \dots, X_n]$  via son plongement dans  $\mathrm{GL}_n(A)$ , c’est-à-dire

$$\sigma \cdot X_i := \sum_{j=1}^n (M_\sigma^{-1})_{ij} X_j = X_{\sigma(i)} \quad , \quad i \in \{1, \dots, n\}$$



et plus généralement

$$\sigma \cdot \sum_{s \in \mathbb{N}_0^n} p_s \cdot X_1^{s_1} \cdots X_n^{s_n} = \sum_{s \in \mathbb{N}_0^n} p_s \cdot X_{\sigma(1)}^{s_1} \cdots X_{\sigma(n)}^{s_n} = \sum_{s \in \mathbb{N}_0^n} p_s \cdot X_1^{s_{\sigma^{-1}(1)}} \cdots X_n^{s_{\sigma^{-1}(n)}} .$$

Autrement dit, si  $P \in A[X_1, \dots, X_n]$  alors  $\sigma P$  a la représentation

$$\sigma P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) ,$$

obtenu par remplacer tout  $X_i$  dans la représentation canonique de  $P(X)$  par  $X_{\sigma(i)}$ . Note que  $\text{Sym}(n)$  agit sur  $\mathbb{R}^n$  comme  $\sigma(s_1, \dots, s_n) := (s_{\sigma^{-1}(1)}, \dots, s_{\sigma^{-1}(n)})$ . On peut donc écrire

$$\sigma \cdot \sum_{s \in \mathbb{N}_0^n} p_s \cdot X^s = \sum_{s \in \mathbb{N}_0^n} p_s \cdot X^{\sigma(s)} = \sum_{s \in \mathbb{N}_0^n} p_{\sigma^{-1}(s)} \cdot X^s . \tag{3.4.3.2}$$

### 3.4.4 Partitions et diagrammes de Young

Soit  $n \in \mathbb{N}$ . On considère l'action du groupe symétrique  $\text{Sym}(n)$  sur  $\mathbb{N}_0^n$ , donnée par

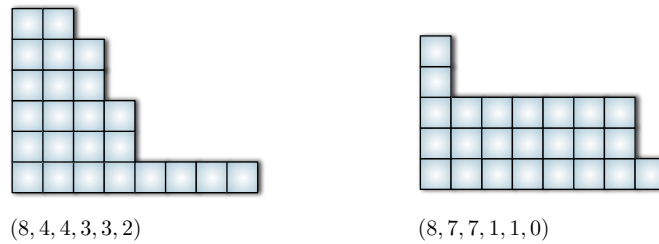
$$\sigma \cdot (s_1, \dots, s_n) := (s_{\sigma^{-1}(1)}, \dots, s_{\sigma^{-1}(n)}) \quad , \quad s_1, \dots, s_n \in \mathbb{N}_0, \sigma \in \text{Sym}(n) .$$

Alors, le stabilisateur d'un  $s \in \mathbb{N}_0^n$  est engendré par les transpositions qui préserve  $s$ . Dans toute orbite  $\text{Orb}_{\text{Sym}(n)}(s)$  de cette action il existe un unique élément  $\lambda = (\lambda_1, \dots, \lambda_n)$  tel que  $\lambda_1 \geq \dots \geq \lambda_n$ . Note que

$$|\lambda| := \lambda_1 + \dots + \lambda_n = s_1 + \dots + s_n = |s| .$$

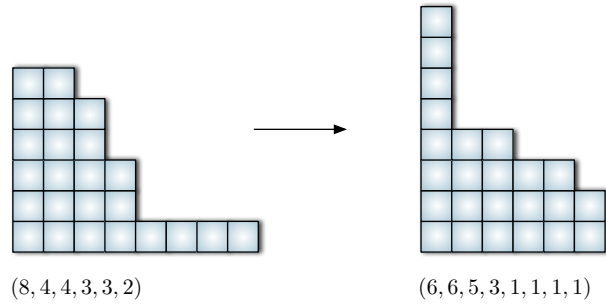
On dit  $\lambda$  une **partition du poids**  $m := |\lambda|$  et écrit souvent  $\lambda = (\lambda_1 \geq \dots \geq \lambda_n)$ . Si on fixe le poids  $m \in \mathbb{N}_0$ , il y a un nombre fini de partitions de  $m$  dans  $\mathbb{N}_0^n$ . On appelle **longueur** d'une partition  $\lambda \in \mathbb{N}_0^n$  le nombre de composants  $\lambda_i$  non-nulles.

Le **diagramme de Young** d'une partition  $\lambda \in \mathbb{N}_0^n$  est un ensemble de cases justifiées à gauche et en bas, dont le nombre de cases de chaque ligne correspond aux éléments de la partition  $\lambda$ . Vois figure 13 ci-dessous pour un exemple.



**FIGURE 13:** Diagrammes de Young pour deux partitions de 24 dans  $\mathbb{N}_0^6$ .

Tout diagramme de Young d'une partition  $\lambda \in \mathbb{N}_0^n$  de  $m \in \mathbb{N}_0$  engendre un autre par changement des deux axes, correspondant à une partition  $\lambda^*$  de  $m$  dans  $\mathbb{N}_0^{\lambda_1}$ , appelée la **partition duale** de  $\lambda$ . Note que  $|\lambda^*| = |\lambda|$  et  $\lambda^{**} = \lambda$ .



**FIGURE 14:** Sur la partition duale : Montré est la partition de 24 dans  $\mathbb{N}_0^6$  et sa duale dans  $\mathbb{N}_0^8$ .

En fait, le composant  $\lambda_i^*$  de  $\lambda^*$  correspond au nombre des composants de  $\lambda$  plus grands ou égaux à  $i$ . En particulier,  $\lambda_1^*$  est la longueur de  $\lambda$ . On note

$$\mathcal{P}_n := \{\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{N}_0^n : \lambda_1 \geq \dots \geq \lambda_n\}$$

l'ensemble des partitions de  $n$  composants et

$$\mathcal{P}_n(m) := \{\lambda \in \mathcal{P}_n : |\lambda| = m\}$$

le sous-ensemble des partitions de  $n$  composants de poids  $m$ . On note

$$\mathcal{P}_n^* := \{\lambda^* : \lambda \in \mathcal{P}_n\} = \{(\mu_1, \dots, \mu_k) \in \mathbb{N}_0^k : n \geq \mu_1 \geq \dots \geq \mu_k, k \in \mathbb{N}\}$$

$$\mathcal{P}_n^*(m) := \{\lambda^* \in \mathcal{P}_n^* : |\lambda| = m\} \quad .$$

#### Remarques :

- (i) Toute partition est maximale dans son orbite par rapport à l'ordre lexicographique (et donc monômial).
- (ii) La plus petite partition dans  $\mathcal{P}_n(m)$  est donnée par

$$\min \mathcal{P}_n(m) = (\underbrace{k+1, \dots, k+1}_{\times r}, \underbrace{k, \dots, k}_{\times (n-r)})$$

où  $m = k \cdot n + r$  avec  $k, r \in \mathbb{N}_0$  et  $0 \leq r < n$ . Le plus grand élément de  $\mathcal{P}_n^*(m)$  est donné par

$$\max \mathcal{P}_n^*(m) = (\underbrace{n, \dots, n}_{\times k}, r) = [\min \mathcal{P}_n(m)]^* \quad .$$

#### 3.4.5 Définition: Monômes symétriques

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . On appelle un polynôme  $P \in A[X_1, \dots, X_n]$  **symétrique** ssi il est invariant sous l'action de  $\text{Sym}(n)$ , c'est-à-dire pour tout  $\sigma \in \text{Sym}(n)$  on a  $\sigma P = P$ . Si  $P$  est de la forme  $P = \sum_s p_s X^s$ , alors  $P$  est symétrique ssi

$$\sum_{s \in \mathbb{N}_0^n} p_{\sigma(s)} \cdot X^s = \sum_{s \in \mathbb{N}_0^n} p_s \cdot X^s \quad \forall \sigma \in \text{Sym}(n) \quad ,$$

c'est-à-dire les coefficients  $p_s$  sont constantes dans les orbites de  $\text{Sym}(n)$ . On note  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$  la  $A$ -algèbre des polynômes symétriques de  $A[X_1, \dots, X_n]$ . Pour toute partition  $\lambda \in \mathbb{N}_0^n$  on note

$$\sum_{s \in \text{Orb}_{\text{Sym}(n)}(\lambda)} X^s =: M_\lambda(X) \in A[X_1, \dots, X_n]$$

le **monôme symétrique complet** associée à  $\lambda \in \mathbb{N}_0^n$ . Par exemple, le monôme symétrique complet associé à  $\lambda = (3, 1, 0)$  est donné par

$$M_\lambda(X) = X_1^3 X_2^1 + X_1^1 X_2^3 + X_2^3 X_3^1 + X_2^1 X_3^3 + X_1^3 X_3^1 + X_1^1 X_3^3 \ .$$

Noter que tout monôme symétrique complet  $M_\lambda$  est un polynôme symétrique, homogène de degré  $|\lambda|$ . Pour tout monôme  $X^s$  dans  $A[X_1, \dots, X_n]$  où  $s \in \mathbb{N}_0^n$ , on appelle le monôme symétrique complet

$$\text{Sym}(X^s) := M_s(X) := \sum_{\tau \in \text{Orb}_{\text{Sym}(n)}(s)} X^\tau$$

la **symétrisation** de  $X^s$ .

Un monôme symétrique complet  $M_\lambda$  est dit un **polynôme symétrique élémentaire de degré  $k$**  si  $\lambda$  est de la forme  $\lambda = (1, \dots, 1, 0, \dots, 0)$ , où  $\lambda$  est de la longueur  $k$ . En ce cas on note  $M_\lambda(X) =: \sigma_k(X)$ . Donc

$$\sigma_k(X) = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k} = \text{Sym}(X_{i_1} \cdots X_{i_k}) \ .$$

En particulier

$$\sigma_0(X) = 1 \ , \ \sigma_1(X) = X_1 + \dots + X_n \ , \ \sigma_n(X) = X_1 \cdots X_n \ .$$

Pour partition  $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots) \in \mathcal{P}_n^*$  (c'est-à-dire  $\lambda_1 \leq n$ ) on note

$$\sigma_\lambda := \sigma_{\lambda_1} \cdots \sigma_{\lambda_n} \ .$$

Noter que les  $\sigma_\lambda$  sont exactement les monômes en les *variables*  $\sigma_1, \dots, \sigma_n$ . En fait, tout monôme  $\sigma_1^{s_1} \cdots \sigma_n^{s_n}$  en  $\sigma_1, \dots, \sigma_n$ , avec  $s \in \mathbb{N}_0^n$ , s'écrit dans la forme

$$\underbrace{(\sigma_n * \dots * \sigma_n)}_{\times s_n} * \underbrace{(\sigma_{n-1} * \dots * \sigma_{n-1})}_{\times s_{n-1}} * \dots * \underbrace{(\sigma_1 * \dots * \sigma_1)}_{\times s_1} = \sigma_\lambda$$

où

$$\lambda = \underbrace{(n, \dots, n)}_{\times s_n} \underbrace{(n-1, \dots, n-1)}_{\times s_{n-1}} \dots \underbrace{(1, \dots, 1)}_{\times s_1} \in \mathcal{P}_n^* \ .$$

Noter que le degré de  $\sigma_\lambda(X)$  (comme polynôme dans  $A[X_1, \dots, X_n]$ ) est exactement le poids  $|\lambda|$ .

### 3.4.6 Lemme : Engendrement des polynômes symétriques

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Alors

$$A[X_1, \dots, X_n]^{\text{Sym}(n)} = \bigoplus_{\lambda \in \mathcal{P}_n} AM_\lambda \ . \quad (3.4.6.1)$$

Autrement dit, les monômes symétriques complets forment une  $A$ -base<sup>22</sup> du  $A$ -module  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ .

**Preuve :** C'est évident que la somme à droite de (3.4.6.1) est directe. On a vu déjà que tout polynôme  $P = \sum_{s \in \mathbb{N}_0^n} p_s X^s \in A[X_1, \dots, X_n]$  est symétrique ssi tous ses coefficients  $p_s$  sont égaux sur les orbites de  $\text{Sym}(n)$ . Donc, si  $P$  est symétrique il s'écrit comme

$$P = \sum_{\lambda \in \mathcal{P}_n} p_\lambda \cdot \underbrace{\sum_{s \in \text{Orb}(\lambda)} X^s}_{M_\lambda} \ .$$

Inversement, comme tout monôme symétrique  $M_\lambda$  est symétrique, on sait que

$$\bigoplus_{\lambda \in \mathcal{P}_n} AM_\lambda \subseteq A[X_1, \dots, X_n]^{\text{Sym}(n)} \ .$$

Cela complète la preuve. □

22. Voir 2.2.4 pour la caractérisation d'une base.

### 3.4.7 Lemme : Représentation des polynômes symétriques

Pour toute partition  $\lambda \in \mathcal{P}_n$  de poids  $m := |\lambda|$ , le polynôme  $\sigma_{\lambda^*}$  en les  $\sigma_1, \dots, \sigma_n \in A[X_1, \dots, X_n]$  est de la forme

$$\sigma_{\lambda^*} = M_{\lambda} + \sum_{\substack{\mu \in \mathcal{P}_n(|\lambda|) \\ \mu < \lambda}} a_{\lambda, \mu} M_{\mu} \quad (3.4.7.1)$$

où  $a_{\lambda, \mu} \in \mathbb{N}_0$  sont des coefficients entiers et “<” est l’ordre monomial<sup>23</sup>

**Preuve :** Noter que  $\sigma_{\lambda^*}$  est en fait un polynôme dans  $A[X_1, \dots, X_n]^{\text{Sym}}$ . Par 3.4.6 il peut être écrit comme combinaison linéaire de monômes symétriques complets  $(M_{\mu})_{\mu \in \mathcal{P}_n}$ . Par la représentation

$$\sigma_{\lambda^*} = \sigma_{\lambda_1^*} * \sigma_{\lambda_2^*} * \dots = \text{Sym}(X_1 \dots X_{\lambda_1^*}) * \text{Sym}(X_1 \dots X_{\lambda_2^*}) * \dots \quad (3.4.7.2)$$

c’est évident que les coefficients des  $M_{\lambda}$  sont en principe nombres entiers. Le degré de  $\sigma_{\lambda^*}$  est exactement  $|\lambda|$ , donc la combinaison linéaire consiste seulement de monômes symétriques complets  $M_{\mu}$  où  $|\mu| = |\lambda|$ . Le terme dominant dans (3.4.7.2) par rapport à l’ordre monomial est

$$(X_1 \dots X_{\lambda_1^*}) * (X_1 \dots X_{\lambda_2^*}) * \dots \quad (3.4.7.3)$$

ce qui se trouve dans (3.4.7.2) avec le coefficient 1. De plus, par la définition de  $\lambda^*$ , l’expression (3.4.7.3) est égale à  $X^{\lambda^{**}} = X^{\lambda}$ , donc  $\sigma_{\lambda^*}$  inclut seulement des  $M_{\mu}$  où  $\mu \leq \lambda$ . Cela finit la preuve.  $\square$

**Exemple :** Soit  $m \in \mathbb{N}_0$  quelconque. Par remarque 3.4.4(ii) on sait que le plus petit élément  $\lambda_0 \in \mathcal{P}_n(m)$  est donné par

$$\lambda_0 = \underbrace{(k+1, \dots, k+1)}_{\times r}, \underbrace{(k, \dots, k)}_{\times (n-r)},$$

où  $m = k \cdot n + r$  avec  $k, r \in \mathbb{N}_0$  et  $0 \leq r < n$ . Par la même remarque on sait que

$$\lambda_0^* = \underbrace{(n, \dots, n)}_{\times k}, r.$$

Par (3.4.7.1) on conclut que

$$M_{\lambda_0} = \sigma_{\lambda_0^*} = \underbrace{\sigma_n * \dots * \sigma_n}_{\times k} * \sigma_r = (X_1 \dots X_n)^k * \text{Sym}(X_1 \dots X_r).$$

### 3.4.8 Théorème des polynômes symétriques

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Alors, l’algèbre des polynômes symétriques  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$  est une  $A$ -algèbre de polynômes en  $n$  variables  $\sigma_1(X), \dots, \sigma_n(X)$ .

**Remarque :** Le théorème est équivalent aux suivantes :

- Pour tout polynôme symétrique  $P \in A[X_1, \dots, X_n]^{\text{Sym}(n)}$  il existe un unique  $Q \in A[\sigma_1, \dots, \sigma_n]$  tel que  $P = Q(\sigma_1, \dots, \sigma_n)$ .
- Les monômes en  $\sigma_1, \dots, \sigma_n$  forment une base du  $A$ -module  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ .
- Le morphisme de  $A$ -algèbres  $A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]^{\text{Sym}(n)}$  caractérisé par  $X_k \mapsto \sigma_k(X)$  est un isomorphisme<sup>24</sup>.

23. Voir 3.1.9.

24. Voir 2.2.8 sur l’existence d’isomorphismes.

**Preuve :** Par la remarque ci-dessus, il suffit à montrer que les monômes en les  $\sigma_1, \dots, \sigma_n$  forment une  $A$ -base de  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ . Par 3.4.6 on sait que les monômes symétriques complets  $(M_\mu)_{\mu \in \mathcal{P}_n}$  forment une  $A$ -base de  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ . Donc, par remarque 2.2.1(vii) il suffit à montrer que tout  $M_\mu$  peut être écrit comme combinaison linéaire des polynômes  $\sigma_{\lambda^*}$  en les  $\sigma_1, \dots, \sigma_m$  en unique façon.

Lemme 3.4.7 et en particulier relation (3.4.7.1) donnent une représentation des  $\sigma_{\lambda^*}$  et les  $M_\mu$ . Comme la relation est triangulaire avec des 1 sur la diagonale, elle est inversible. Cela complète la preuve.  $\square$

### 3.4.9 Algorithme sur la représentation des polynômes symétriques

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . On a vu dans théorème 3.4.8, que tout  $P \in A[X_1, \dots, X_n]^{\text{Sym}(n)}$  peut être représenté comme  $P = Q(\sigma_1, \dots, \sigma_n)$  pour un unique polynôme  $Q \in A[X_1, \dots, X_n]$ . On cherche un algorithme pour déterminer ce  $Q$ , donné le polynôme symétrique  $P$ . Autrement dit, donné  $P$  on cherche des coefficients  $(Q_s)_{s \in \mathbb{N}_0^n} \in A^{(\mathbb{N}_0^n)}$  tels que

$$P = \sum_{s \in \mathbb{N}_0^n} Q_s \cdot \sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n} \quad .$$

Notons que le terme dominant d'un monôme  $\sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n}$  en les  $\sigma_i$  est donné par

$$X_1^{s_1 + \dots + s_n} \cdot X_2^{s_2 + \dots + s_n} \cdot \dots \cdot X_n^{s_n} \quad .$$

L'idée est or, d'éliminer un par un les termes dominants de  $P$  par des monômes en des  $\sigma_i$ . On trouve l'algorithme suivant :

1. Déterminer le terme dominant  $pX_1^{\nu_1} \cdot \dots \cdot X_n^{\nu_n}$  de  $P$ .
2. Résoudre le système d'équations

$$\begin{aligned} \nu_1 &= s_1 + s_2 + \dots + s_n \\ \nu_2 &= s_2 + \dots + s_n \\ &\vdots \\ \nu_n &= s_n \end{aligned}$$

en les indéterminées  $s_1, \dots, s_n$ .

3. Soustraire le monôme  $p\sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n}$  de  $P$  pour recevoir le polynôme

$$\tilde{P} := P - p\sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n} \quad ,$$

qui possède un terme dominant plus petit que  $P$ .

4. Répéter les étapes (1),(2) et (3) pour  $\tilde{P}$  et ainsi de suite jusqu'à il reste le polynôme nul.

On arrive donc finalement à une représentation

$$P - p\sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n} - \tilde{p}\sigma_1^{\tilde{s}_1} \cdot \dots \cdot \sigma_n^{\tilde{s}_n} - \dots = 0 \quad ,$$

d'où on trouve

$$P = p\sigma_1^{s_1} \cdot \dots \cdot \sigma_n^{s_n} + \tilde{p}\sigma_1^{\tilde{s}_1} \cdot \dots \cdot \sigma_n^{\tilde{s}_n} + \dots \quad .$$

### Exemples

- Le polynôme symétrique  $X_1^3 + \dots + X_n^3$  possède la représentation

$$X_1^3 + \dots + X_n^3 = \sigma_1^3(X) - 3\sigma_1(X)\sigma_2(X) + 3\sigma_3(X) \quad .$$

- Le polynôme symétrique  $X^2(Y + Z) + Y^2(Z + X) + Z^2(X + Y)$  possède la représentation

$$X^2(Y + Z) + Y^2(Z + X) + Z^2(X + Y) = \sigma_1\sigma_2 - 3\sigma_3 \quad .$$

- Le polynôme symétrique  $X^3(Y + Z) + Y^3(Z + X) + Z^3(X + Y)$  possède la représentation

$$X^3(Y + Z) + Y^3(Z + X) + Z^3(X + Y) = \sigma_1^2\sigma_2 - 2\sigma_2^2 - 3\sigma_1\sigma_3 \quad .$$

**3.4.10 Exemple : Les sommes de Newton**

Soit  $A$  un anneau commutatif tel que  $\mathbb{Q} \subseteq A$  et  $n \in \mathbb{N}$ . On définit la **somme de Newton** dans  $A[X_1, \dots, X_n]$  de degré  $k$  comme le polynôme

$$S_k := \sum_{i=1}^n X_i^k .$$

Alors, les monômes en les  $S_1, \dots, S_n$  engendrent  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ , c'est-à-dire

$$\boxed{A[X_1, \dots, X_n]^{\text{Sym}(n)} = \text{span}_A \{S_1^{s_1} * \dots * S_n^{s_n} : s \in \mathbb{N}_0^n\} .} \quad (3.4.10.1)$$

**Preuve :** Considérons le polynôme

$$P(T) := \prod_{i=1}^n (T - X_i) \in A[X_1, \dots, X_n][T] .$$

Il est égal à

$$P(T) = \sum_{l=0}^n (-1)^l \cdot \sigma_l \cdot T^{n-l} , \quad (3.4.10.2)$$

d'où on déduit l'identité

$$\sum_{l=0}^n (-1)^l \cdot \sigma_l \cdot X_i^{k-l} = 0 \quad \forall k \geq n, i \in \{1, \dots, n\}$$

et par conséquence

$$\sum_{l=0}^n (-1)^l \cdot \sigma_l \cdot S_{k-l} = 0 \quad \forall k \geq n . \quad (3.4.10.3)$$

On considérons la dérivée

$$\frac{dP}{dT} = \sum_{i=1}^n \prod_{j \neq i} (T - X_j) = \sum_{i=1}^n \frac{P - P(X_i)}{T - X_i} . \quad (3.4.10.4)$$

Comme

$$P - P(X_i) \stackrel{(3.4.10.2)}{=} \sum_{j=1}^n (-1)^{n-j} \sigma_{n-j} \cdot (T^j - X_i^j)$$

et

$$\frac{T^j - X_i^j}{T - X_i} = \sum_{l=1}^j T^{l-1} X_i^{j-l} ,$$

la dérivée (3.4.10.4) prend la forme

$$\frac{dP}{dT} = \sum_{j=1}^n (-1)^{n-j} \sigma_{n-j} \sum_{l=1}^j T^{l-1} S_{j-l} = \sum_{l=1}^n T^{l-1} \sum_{j=l}^n (-1)^{n-j} \sigma_{n-j} S_{j-l} . \quad (3.4.10.5)$$

D'autre part, par (3.4.10.2) on sait que

$$\frac{dP}{dT} = \sum_{l=1}^n (-1)^{n-l} \sigma_{n-l} \cdot l \cdot T^{l-1} , \quad (3.4.10.6)$$

En comparaisant (3.4.10.5) et (3.4.10.6) on reçoit

$$\sum_{j=l}^n (-1)^{n-j} \sigma_{n-j} S_{j-l} = l \cdot (-1)^{n-l} \sigma_{n-l} \quad \forall l \in \{1, \dots, n\} ,$$

d'où

$$\sigma_{n-l} \cdot (-1)^{n-l} \underbrace{[l - S_0]}_{n-l} = \sum_{j=l+1}^n (-1)^{n-j} \sigma_{n-j} S_{j-l} \quad \forall l \in \{1, \dots, n\} . \quad (3.4.10.7)$$

Comme  $\mathbb{Q} \subseteq A$ , (3.4.10.7) donne  $\sigma_{n-l}$  pour chaque  $l \in \{1, \dots, n\}$  comme polynôme des  $\sigma_0, \dots, \sigma_{n-l-1}$  et les  $S_1, \dots, S_{n-l}$ . De même, (3.4.10.3) donne  $\sigma_n$  comme polynôme en les  $\sigma_0, \dots, \sigma_{n-1}$  et les  $S_1, \dots, S_n$  (pose  $k = n$ ). Noter que  $\sigma_0 = 1$ . Donc, par récurrence sur  $j = 1, \dots, n$ , on trouve les  $\sigma_j$  comme polynômes en les  $S_1, \dots, S_n$ . Par théorème 3.4.8, les polynômes en les  $S_1, \dots, S_n$  engendrent  $A[X_1, \dots, X_n]^{\text{Sym}(n)}$ .  $\square$

### Remarques

(i) La preuve ci-dessus montre que si  $\mathbb{Q} \subseteq A$ , alors  $\sigma_k$  est une combinaison linéaire des  $S_1, \dots, S_k$  pour tout  $k \in \{1, \dots, n\}$ .

(ii) On a vu dans la preuve les **relations coefficients-racines**

$$\prod_{i=1}^n (T - X_i) = \sum_{i=0}^n (-1)^i \cdot \sigma_i(X_1, \dots, X_n) \cdot T^{n-i} . \quad (3.4.10.8)$$

### 3.4.11 Corollaire sur polynômes symétriques et sous-anneaux

Soit  $A$  un sous-anneau de l'anneau commutatif  $B$ . Soient  $a_1, \dots, a_n \in B$  tels que le polynôme  $\prod_{k=1}^n (X - a_k) \in B[X]$  est en fait dans  $A[X]$ . Alors, pour tout  $Q \in A[X_1, \dots, X_n]^{\text{Sym}(n)}$  on a  $Q(a_1, \dots, a_n) \in A$ .

**Preuve :** Par les relations coefficients-racines (3.4.10.8) on sait que

$$\prod_{k=1}^n (X - a_k) = \sum_{k=0}^n X^k (-1)^{n-k} \sigma_{n-k}(a_1, \dots, a_n) ,$$

d'où on voit que  $\sigma_{n-k}(a_1, \dots, a_n) \in A$  pour tout  $k \in \{1, \dots, n\}$ . Si  $Q \in A[X_1, \dots, X_n]^{\text{Sym}(n)}$  est un polynôme symétrique, alors par théorème 3.4.8 il est combinaison  $A$ -linéaire de monômes en les  $\sigma_1, \dots, \sigma_n$ . Donc  $Q(a_1, \dots, a_n) \in A$ .  $\square$

**Exemple :** Soient  $z_1, \dots, z_n \in \mathbb{C}$  quelconques. Alors, le polynôme

$$\prod_{k=1}^n (X - z_k)(X - \bar{z}_k)$$

est réel. Donc, pour tout polynôme symétrique  $Q \in \mathbb{R}[X_1, \dots, X_{2n}]^{\text{Sym}(n)}$  on a  $Q(z_1, \bar{z}_1, \dots, z_n, \bar{z}_n) \in \mathbb{R}$ .

### 3.4.12 Exemple : Polygones réguliers dans $\mathbb{C}$

Soient  $\xi_0, \dots, \xi_n \in \mathbb{C}$  deux à deux inégales. Alors, les suivantes sont équivalents :

1. Les  $\xi_1, \dots, \xi_n$  sont les sommets d'un polygone régulier de  $n$  côtés centré en  $\xi_0$ .
2. Les valeurs  $(\xi_k - \xi_0)$ ,  $k \in \{1, \dots, n\}$  sont les  $n$   $n$ -ièmes racines d'un nombre complexe  $R \in \mathbb{C} \setminus \{0\}$ .
3. Il existe un  $R \in \mathbb{C} \setminus \{0\}$  tel que

$$\prod_{k=1}^n (X - \xi_k) = (X - \xi_0)^n - R . \quad (3.4.12.1)$$

4. Pour tout polynôme  $P \in \mathbb{C}[X]$  de degré plus petit que  $n$ , on a

$$P(\xi_0) = \frac{1}{n} \prod_{k=1}^n P(\xi_k) . \quad (3.4.12.2)$$

**Preuve :** Noter que les  $\xi_1, \dots, \xi_n$  sont les  $n$  sommets d'un polygone régulier centré à  $\xi_0$  ssi  $(\xi_1 - \xi_0), \dots, (\xi_n - \xi_0)$  sont les  $n$  sommets d'un polygone régulier centré à 0.

**1  $\Rightarrow$  2 :** Par la remarque ci-dessus on peut supposer que  $\xi_0 = 0$ . Il faut donc montrer que les  $\xi_1, \dots, \xi_n$  forment les  $n$   $n$ -ièmes racines d'un  $R \neq 0$ . Noter que  $\xi_1, \dots, \xi_n \neq 0$ . Posons  $R := \xi_1^n$ . Par supposition  $|\xi_k| = |\xi_1|$  et  $\arg(\xi_k) = \arg(\xi_1) + \frac{2\pi}{n} \cdot (k-1)$ . Donc

$$\xi_k^n = |\xi_k|^n \cdot e^{in \arg(\xi_k)} = |\xi_1|^n \cdot \exp \left[ in \cdot \left( \arg(\xi_1) + (k-1) \frac{2\pi}{n} \right) \right] = |\xi_1|^n \exp [in \cdot \arg(\xi_1)] = \xi_1^n = R .$$

**2  $\Rightarrow$  1 :** Les  $n$  racines de  $R \neq 0$  sont données par

$$\sqrt[n]{R} \in \left\{ \underbrace{\sqrt[n]{|R|} \cdot \exp \left[ \frac{i}{n} \arg(R) + \frac{k}{n} 2\pi i \right]}_{(\xi_k - \xi_0)} : k = 1, \dots, n \right\} .$$

Evidement les  $\xi_1, \dots, \xi_n$  forment un polygone régulier centré en  $\xi_0$ , car  $\arg(\xi_k - \xi_0) = \text{const} + \frac{2\pi}{n} \cdot k$  et  $|\xi_k - \xi_0| = \sqrt[n]{|R|}$  pur tout  $k$ .

**3  $\Rightarrow$  2 :** Supposons l'équation (3.4.12.1) pour un certain  $R \in \mathbb{C} \setminus \{0\}$ . Alors, pour tout  $j \in \{1, \dots, n\}$  il faut

$$0 = \prod_{k=1}^n (\xi_j - \xi_k) = (\xi_j - \xi_0)^n - R ,$$

c'est-à-dire les valeurs  $(\xi_1 - \xi_0), \dots, (\xi_n - \xi_0)$  sont les  $n$   $n$ -ièmes racines de  $R$ .

**2  $\Rightarrow$  3 :** Considérons le polynôme unitaire

$$P(X) = (X - \xi_0)^n - R .$$

Alors, ses racines sont exactement  $\xi_1, \dots, \xi_n$ , donc il possède la forme

$$P(X) = \prod_{k=1}^n (X - \xi_k) .$$

**2  $\Rightarrow$  4 :** Montrons d'abord l'affirmation pour le cas  $\xi_0 = 0$ . Il suffit de montrer l'affirmation (3.4.12.2) pour les monômes  $X^1, \dots, X^{n-1}$ , c'est-à-dire que

$$0 = \frac{1}{n} \sum_{k=1}^n \xi_k^j \quad \forall j \in \{1, \dots, n-1\} .$$

Vraiment, comme  $\xi_k = r \cdot \exp \left[ i \frac{2\pi}{n} k \right]$  pour une constante  $r \in \mathbb{C}$ , on trouve

$$\frac{1}{n} \sum_{k=1}^n \xi_k^j = r^j \cdot \sum_{k=1}^n \left( e^{i \frac{2\pi}{n} j} \right)^k = e^{i \frac{2\pi}{n} j} \cdot \frac{1 - \left( e^{i \frac{2\pi}{n} j} \right)^n}{1 - e^{i \frac{2\pi}{n} j}} = 0$$

pour tout  $j \in \{1, \dots, n-1\}$ , comme affirmé. Noter que dans le cas  $j = n$  l'affirmation est vraiment fausse. Soit or  $\xi_0 \neq 0$ , alors on sait déjà que pour tout  $P \in \mathbb{C}[X]$  de degré plus petit que  $n$  :

$$P(0) = \frac{1}{n} \sum_{k=1}^n P(\xi_k - \xi_0) .$$

Soit  $Q \in \mathbb{C}[X]$  avec  $\text{dg}(Q) \leq n-1$  quelconque. Pose  $P(X) := Q(X + \xi_0)$ , alors  $\text{dg}(P) \leq n-1$  et donc

$$Q(\xi_0) = P(0) = \frac{1}{n} \sum_{k=1}^n P(\xi_k - \xi_0) = \frac{1}{n} \sum_{k=1}^n Q(\xi_k) .$$



4  $\Rightarrow$  1 : Par la remarque au début de la preuve et la même argumentation comme dans la preuve de (2  $\Rightarrow$  4), on peut supposer que  $\xi_0 = 0$ . Par les relations coefficients-racines (3.4.10.8) on sait que

$$P(X) := \prod_{k=1}^n (X - \xi_k) = \sum_{k=0}^n X^k \cdot (-1)^{n-k} \sigma_{n-k}(\xi_1, \dots, \xi_n) \quad ,$$

où  $\sigma_0, \dots, \sigma_n$  sont les polynômes symétriques élémentaires dans  $\mathbb{C}[X_1, \dots, X_n]$ . Pour prouver la forme (3.4.12.1) dans le cas  $\xi_0 = 0$ , il suffit de montrer que

$$\sigma_k(\xi_1, \dots, \xi_n) = 0 \quad \forall k \in \{1, \dots, n-1\} \quad .$$

Noter que comme les  $\xi_1, \dots, \xi_n$  sont deux à deux inégales, le terme constant  $R$  du polynôme  $P$  doit être non-nul. Par remarque 3.4.10(i), les  $\sigma_1, \dots, \sigma_{n-1}$  sont polynômes en les sommes de Newton  $S_1, \dots, S_{n-1}$ . Il suffit donc de montrer que  $S_j(\xi_1, \dots, \xi_n) = 0$  pour tout  $j \in \{1, \dots, n-1\}$ . Par supposition

$$0 = 0^j \stackrel{\text{sup.}}{=} \frac{1}{n} \sum_{k=1}^n \xi_k^j = \frac{1}{n} S_j(\xi_1, \dots, \xi_n) \quad \forall j \in \{1, \dots, n-1\} \quad ,$$

ce qui complète la preuve. □

### 3.4.13 Exemple : Caractérisation des polynômes caractéristiques

Soit  $\mathbb{K}$  un corps contenant  $\mathbb{Q}$  et  $n \in \mathbb{N}$ . Soient  $A, B \in \mathbb{K}^{n \times n}$  deux matrices tels que  $\text{tr}(A^k) = \text{tr}(B^k)$  pour tout  $k \in \{1, \dots, n\}$ . Alors leur polynômes caractéristiques  $\chi_A, \chi_B \in \mathbb{K}[X]$  sont égales.

**Preuve :** Il suffit de montrer, que le polynôme caractéristique de toute matrice  $A \in \mathbb{K}^{n \times n}$  est caractérisé par ses traces  $\text{tr}(A^1), \dots, \text{tr}(A^n)$ . On sait que  $A$  est semblable à un  $\tilde{A} \in \mathbb{K}^{n \times n}$  de la forme

$$\tilde{A} = \begin{pmatrix} a_1 & \dots & * \\ & \ddots & \vdots \\ 0 & & a_n \end{pmatrix}$$

pour quelques  $a_1, \dots, a_n \in \mathbb{K}$ . Comme  $\text{tr}(A^k) = \text{tr}(\tilde{A}^k)$  et  $\chi_A = \chi_{\tilde{A}}$ , il suffit de montrer l'affirmation pour  $\tilde{A}$ . On sait d'une partie que

$$\chi_{\tilde{A}}(X) = \prod_{k=1}^n (X - a_k) \quad .$$

D'autre part, par les relations coefficients-racines (3.4.10.8) on sait que

$$\prod_{k=1}^n (X - a_k) = \sum_{k=0}^n X^k (-1)^{n-k} \sigma_{n-k}(a_1, \dots, a_n) \quad ,$$

où  $\sigma_0, \dots, \sigma_n \in \mathbb{K}[X_1, \dots, X_n]$  sont les polynômes symétriques élémentaires. Par 3.4.10, les  $\sigma_1, \dots, \sigma_n$  sont polynômes en les sommes de Newton  $S_1, \dots, S_n$ . Comme

$$S_j(a_1, \dots, a_n) = \sum_{k=1}^n a_k^j = \text{tr}(A^k) \quad \forall j \in \{1, \dots, n\}$$

on déduit que le valeurs  $\sigma_k(a_1, \dots, a_n)$ ,  $1 \in \{0, \dots, n\}$  dépendent seulement des traces  $\text{tr}(A^1), \dots, \text{tr}(A^n)$ . Cela finit la preuve. □

### 3.4.14 Définition: Polynôme antisymétrique

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Un polynôme  $P \in A[X_1, \dots, X_n]$  est dit **antisymétrique** ssi

$$\sigma \cdot P = \text{sgn}(\sigma) \cdot P \quad \forall \sigma \in \text{Sym}(n) \quad .$$

Notons  $A[X_1, \dots, X_n]^{\text{ant}}$  le sous- $A$ -module de  $A[X_1, \dots, X_n]$  des polynômes antisymétriques.

#### Remarques

(i) Le produit de deux polynômes antisymétriques donne un polynôme symétrique, c'est-à-dire

$$A[X_1, \dots, X_n]^{\text{ant}} * A[X_1, \dots, X_n]^{\text{ant}} \subseteq A[X_1, \dots, X_n]^{\text{Sym}(n)} \quad .$$

(ii) Le produit d'un polynôme antisymétrique et un polynôme symétrique est antisymétrique, c'est-à-dire

$$A[X_1, \dots, X_n]^{\text{ant}} * A[X_1, \dots, X_n]^{\text{Sym}(n)} \subseteq A[X_1, \dots, X_n]^{\text{ant}} \quad .$$

### 3.4.15 Lemme : Représentation des polynômes antisymétriques

Soit  $A$  un anneau commutatif et  $n \in \mathbb{N}$ . Alors, tout polynôme antisymétrique  $P \in A[X_1, \dots, X_n]^{\text{ant}}$  est de la forme  $P = Q * V$  où  $Q \in A[X_1, \dots, X_n]^{\text{Sym}(n)}$  et  $V \in A[X_1, \dots, X_n]^{\text{ant}}$  est le *polynôme de Vandermonde*

$$V = \det \left( X_i^{j-1} \right)_{i,j=1}^n = \prod_{i < j} (X_i - X_j) \quad .$$

## 3.5 Séries formelles

### 3.5.1 Définition: Algèbre des séries formelles

Soit  $A$  un anneau commutatif et  $S$  un sous-monoïde de  $\mathbb{N}_0^n$ . On munit le  $A$ -module

$$A[[S]] := \prod_{s \in S} A$$

d'un loi de multiplication

$$(a_s)_{s \in S} * (b_s)_{s \in S} := \left( \sum_{s+t=u} a_s \cdot b_t \right)_{u \in S} \quad , \quad (3.5.1.1)$$

qui fait de  $A[[S]]$  une  $A$ -algèbre, dit l'**algèbre des séries formelles**. Noter que les sommes dans (3.5.1.1) sont finies. On note la suite  $f := (f_s)_{s \in S} \in A[[S]]$  sous la forme

$$f = f(X) = \sum_{s \in S} f_s \cdot X^s \quad .$$

On a donc les lois

$$\sum_{s \in S} a_s \cdot X^s + \sum_{s \in S} b_s \cdot X^s = \sum_{s \in S} (a_s + b_s) \cdot X^s$$

$$\left( \sum_{s \in S} a_s \cdot X^s \right) * \left( \sum_{t \in S} b_t \cdot X^t \right) = \sum_{u \in S} \sum_{s+t=u} (a_s \cdot b_t) \cdot X^u \quad .$$

On dit  $f(X) = \sum_{s \in S} f_s X^s$  une série formelle **finie** ssi  $f_s = 0$  pour qu'un nombre fini des  $s$ . Les polynômes  $P \in A[S]$  sont donc rien autre que les séries formelles finies dans  $A[[S]]$  et forment une sous-algèbre de  $A[[S]]$ . Pour  $n \in \mathbb{N}$  on note  $A[[\mathbb{N}_0]] =: A[[X]]$  et  $A[[\mathbb{N}_0^n]] =: A[[X_1, \dots, X_n]]$ . En ce cas on écrit souvent  $X^s = X_1^{s_1} \dots X_n^{s_n}$  pour  $s = (s_1, \dots, s_n) \in \mathbb{N}_0^n$ .

### 3.5.2 Définition: Valuation d'une série formelle

Soit  $A$  un anneau commutatif. On appelle **valuation** d'une série formelle  $f := \sum_{s \in \mathbb{N}_0} f_s X^s \in A[[X]]$  le plus petit  $s \in \mathbb{N}_0$  tel que  $f_s \neq 0$ ; on le note  $\text{val}(f)$ . Par convention on pose  $\text{val}(0) = \infty$ . On note  $f \in \mathcal{O}(X^n)$  ssi  $\text{val}(f) \geq n$ .

On dit qu'une suite de séries formelles  $(f_n(X))_{n \in \mathbb{N}} \subseteq A[[X]]$  **converge vers zéro**, ssi  $\text{val}(f_n) \xrightarrow{n \rightarrow \infty} 0$ . On dit que  $(f_n)_n$  **converge** vers  $f \in A[[X]]$  ssi la suite  $(f - f_n)_n$  converge vers zéro.

#### Remarques

(i) Pour  $f, g \in A[[X]]$  on a

$$\text{val}(f + g) \geq \min \{ \text{val}(f), \text{val}(g) \} \quad (3.5.2.1)$$

et

$$\text{val}(f * g) \geq \text{val}(f) + \text{val}(g) \quad . \quad (3.5.2.2)$$

(ii) Tout  $\mathcal{O}(X^n)$  est un idéal, plus précisément

$$\mathcal{O}(X^n) = X^n * A[[X]] \quad . \quad (3.5.2.3)$$

Plus généralement, on a

$$\mathcal{O}(X^n) + \mathcal{O}(X^m) \subseteq \mathcal{O}(X^{\min\{n,m\}}) \quad ,$$

$$\mathcal{O}(X^n) * \mathcal{O}(X^m) \subseteq \mathcal{O}(X^{n+m}) \quad .$$

### 3.5.3 Lemme : La valuation comme morphisme de monoides

Soit  $A$  un anneau intègre et  $S$  un sous-monoïde de  $\mathbb{N}_0^n$ . Alors  $(A[[S]], +, *)$  est un anneau intègre. De plus, la valuation

$$\text{val} : (A[[X]] \setminus \{0\}, *) \rightarrow (\mathbb{N}_0, +) \quad , \quad \text{val} : f \mapsto \text{val}(f)$$

est un morphisme de monoides.

**Preuve :** Soient  $f, g \in A[[S]]$  avec les représentations

$$f = \sum_{s \in S} f_s X^s \quad , \quad g = \sum_{t \in S} g_t X^t \quad ,$$

tels que  $s_0, t_0 \in S$  sont (par rapport à l'ordre monômial) les plus petits possibles tels que  $f_{s_0} \neq 0 \neq g_{t_0}$ . Alors

$$(f * g)_{s_0+t_0} = f_{s_0} \cdot g_{t_0} \neq 0$$

car  $A$  est intègre. Donc  $f * g \neq 0$ , c'est-à-dire  $A[[S]]$  est intègre. De plus, on déduit que si  $f, g \in A[[X]] \setminus \{0\}$ , alors

$$\text{val}(f * g) = \text{val}(f) + \text{val}(g)$$

car  $u_0 := (s_0 + t_0)$  est le plus petit possible tel que  $(f * g)_{u_0} \neq 0$ . Finalement,  $\text{val}(1) = 0$ . □

### 3.5.4 Définition: Famille de séries sommable

Soit  $A$  un anneau commutatif et  $S$  un sous-monoïde de  $\mathbb{N}_0^n$ . On dit une famille  $(f_i)_{i \in I} \subseteq A[[S]]$  de séries formelles **sommable** ssi pour tout  $s \in S$  on a  $f_{i,s} = 0$  sauf un nombre fini d'indices  $i \in I$ . On définit alors la **somme** de la famille par

$$\sum_{i \in I} f_i(X) := \sum_{s \in S} \sum_{\substack{i \in I \\ f_{i,s} \neq 0}} f_{i,s} \cdot X^s \quad .$$

**Remarque :** Une suite de séries formelles  $(f_n)_{n \in \mathbb{N}} \subseteq A[[X]]$  est sommable ssi  $f_n \xrightarrow{n \rightarrow \infty} 0$ .

### 3.5.5 Définition: Composition des séries formelles

Soient  $A$  un anneau commutatif,  $f(X) = \sum_{n \in \mathbb{N}_0} f_n X^n \in A[[X]]$  et  $g \in A[[X]] \cap \mathcal{O}(X^1)$ . Alors, par (3.5.2.2) la famille  $(f_n g^n(X))_{n \in \mathbb{N}_0}$  est sommable et on note

$$(f \circ g)(X) := \sum_{n \in \mathbb{N}_0} f_n \cdot g^n(X) .$$

#### Remarques

(i) Par (3.5.2.2) on trouve que

$$\text{val}(f \circ g) \geq \text{val}(f) \cdot \text{val}(g) .$$

### 3.5.6 Lemme : Inversibilité des séries formelles

Soit  $A$  un anneau commutatif. Une série formelle  $f(X) = \sum_{s \in \mathbb{N}_0} f_s X^s$  est inversible par rapport à la multiplication ssi  $f_0$  est inversible dans  $A$ . En ce cas on note  $1/f(X)$  l'inverse unique de  $f$ . Elle prend la forme

$$\boxed{\frac{1}{f(X)} = f_0^{-1} \cdot \sum_{s \in \mathbb{N}_0} [1 - f_0^{-1} \cdot f(X)]^s} . \quad (3.5.6.1)$$

#### Preuve :

**Direction “ $\Rightarrow$ ” :** Soit  $g = \sum_{s \in \mathbb{N}_0} g_s X^s \in A[[X]]$  telle que  $f * g = 1$ . Alors  $f_0 \cdot g_0 = 1$  et  $f_0$  est inversible.

**Direction “ $\Leftarrow$ ” :** Supposons  $f_0$  est inversible, alors  $f$  est de la forme  $f(X) = a_0 \cdot (1 + g(X))$  où  $g(X) \in A[[X]]$  avec  $\text{val}(g) > 0$ . Donc, tout revient à prouver que  $(1 + g)$  est inversible avec inverse  $\sum_{s \in \mathbb{N}_0} (-1)^s g(X)^s$ . Note que  $g^n \in \mathcal{O}(X^n)$  pour tout  $n \in \mathbb{N}$  car  $g \in \mathcal{O}(X^1)$ .

Soit  $n \in \mathbb{N}$  quelconque, alors

$$(1 + g) * (1 - g + g^2 - \cdots + (-1)^n g^n) = 1 + (-1)^n g^{n+1}(X) \in 1 + \mathcal{O}(X^{n+1}) ,$$

et donc par remarques 3.5.2(i) et 3.5.5(i)

$$(1 + g) \sum_{n \in \mathbb{N}_0} (-1)^n g^n \in 1 + \mathcal{O}(X^{n+1}) .$$

Cela étant vrai pour tout  $n \in \mathbb{N}_0$ , on conclut

$$(1 + g) \sum_{n \in \mathbb{N}_0} (-1)^n g^n = 1 .$$

□

#### Remarques & Exemples :

(i) Les inverses des séries  $1 \pm X$  sont données par

$$\frac{1}{1 \pm X} = \sum_{n \in \mathbb{N}_0} (\mp X)^n . \quad (3.5.6.2)$$

(ii) Si  $f, g \in A[[X]]^\times$  et  $h \in \mathcal{O}(X)$  tels que  $1/f = g$ , alors  $1/(f \circ h) = g \circ h$ . Donc, pour  $f \in A[[X]]$  avec  $f(0) =: f_0 \in A^\times$  on trouve

$$\frac{1}{f(X)} = \frac{f_0^{-1}}{f_0^{-1} \cdot f(X)} = \frac{f_0^{-1}}{(1 - X) \circ (1 - f_0^{-1} \cdot f(X))} \stackrel{(3.5.6.2)}{=} f_0^{-1} \sum_{n \in \mathbb{N}_0} [1 - f_0^{-1} \cdot f(X)]^n ,$$

comme déjà vu dans (3.5.6.1). Noter que  $(1 - f_0^{-1} \cdot f(X)) \in \mathcal{O}(X)$ .

### 3.5.7 Corollaire sur séries formelles inversibles par rapport à la multiplication

Soit  $A$  un anneau commutatif. Alors la sous-partie

$$A[[X]]^\times := (A[[X]], *)^\times = \left\{ f = \sum_{n=0}^{\infty} f_n X^n \in A[[X]] : f_0 \in A^\times \right\} \quad (3.5.7.1)$$

forme un groupe abélien par rapport à la multiplication  $*$  avec élément neutre 1.

**Preuve :** L'égalité des deux côtés de (3.5.7.1) suit de 3.5.6. Par 1.1.7 on sait que  $A[[X]]^\times$  est un groupe.  $\square$

### 3.5.8 Lemme : Caractérisation des idéaux dans $\mathbb{K}[[X]]$

Soit  $\mathbb{K}$  un corps,  $I \subseteq \mathbb{K}[[X]]$  un idéal et  $n_0 \in \mathbb{N}_0$ . Alors, il y a équivalence entre :

1.  $I$  est engendré par  $X^{n_0}$ , c'est-à-dire  $I = X^{n_0} * \mathbb{K}[[X]]$ .
2.  $n_0 = \min \{ \text{val}(f) : f \in I \}$ .

En particulier, les idéaux non-triviaux de  $\mathbb{K}[[X]]$  sont exactement ceux engendrés par les  $X^n$ ,  $n \in \mathbb{N}_0$ , c'est-à-dire les classes  $\mathcal{O}(X^n)$ .

**Preuve :**

$1 \Rightarrow 2$  : Soit  $m_0 := \min \{ \text{val}(f) : f \in I \}$ . Comme  $X^{n_0} \in I$  on sait que  $m_0 \leq n_0$ . D'autre part, si  $g \in \mathbb{K}[[X]] \setminus \{0\}$ , alors par 3.5.3

$$\text{val}(X^{n_0} * g) = \text{val}(X^{n_0}) + \text{val}(g) \geq n_0 \quad ,$$

c'est-à-dire  $m_0 \geq n_0$ .

$2 \Rightarrow 1$  : Soit  $g \in I$  quelconque, alors  $\text{val}(g) \geq n_0$ . Donc  $g$  est de la forme

$$g = X^{n_0} * \underbrace{\left[ g_{n_0} + \sum_{k=0}^{\infty} g_{n_0+k} X^k \right]}_{\bar{g}} \quad ,$$

c'est-à-dire  $g \in X^{n_0} * \mathbb{K}[[X]]$ . Choisissons maintenant  $g$  tel que  $\text{val}(g) = n_0$ . Alors,  $g_{n_0} \neq 0$  et  $\bar{g}$  est par 3.5.6 inversible. Donc  $X^{n_0} = g * \bar{g}^{-1} \in I$ , c'est-à-dire  $X^{n_0} * \mathbb{K}[[X]] \subseteq I$ .  $\square$

### 3.5.9 Lemme : Idéaux engendrés dans $\mathbb{K}[[X]]$

Soit  $\mathbb{K}$  un corps et  $g \in \mathbb{K}[[X]] \setminus \{0\}$  quelconque. Alors, l'idéal engendré par  $g$  est donné par

$$\boxed{g * \mathbb{K}[[X]] = X^{\text{val}(g)} * \mathbb{K}[[X]] = \mathcal{O}(X^{\text{val}(g)})} \quad . \quad (3.5.9.1)$$

**Preuve :** Par définition de la valuation sur  $\mathbb{K}[[X]]$ , on peut écrire

$$g = X^{\text{val}(g)} * \underbrace{\sum_{n=\text{val}(g)}^{\infty} g_n X^{n-\text{val}(g)}}_{\bar{g}} \quad ,$$

avec  $g_{\text{val}(g)} \neq 0$ . Donc par 3.5.6  $\bar{g}$  est inversible. Donc, par remarque 1.1.6(ii)  $g$  et  $X^{\text{val}(g)}$  engendrent le même idéal. La deuxième partie est rien autre que (3.5.2.3).  $\square$

### 3.5.10 Lemme sur la valuation

Soit  $\mathbb{K}$  un corps. Alors,  $\mathbb{K}[[X]]$  est un anneau euclidien<sup>25</sup> avec division euclidienne unique par rapport à la valuation  $\text{val} : \mathbb{K}[[X]] \rightarrow \mathbb{N}_0$ .

**Preuve :** Noter que par 3.5.3  $\mathbb{K}[[X]]$  est intègre. Il faut montrer les axiomes 1.1.14(1) et 1.1.14(2). Comme  $\text{val} : (\mathbb{K}[[X]], *) \rightarrow (\mathbb{N}_0, +)$  est un morphisme de monoides, l'axiome (1) est trivial. En fait,  $\text{val}()$  satisfait aussi l'inverse : Si  $\text{val}(g) \leq \text{val}(f)$ , alors  $g \mid f$ . Vraiment, par 3.5.9 on peut décomposer  $f = \bar{f} * X^{\text{val}(f)}$  et  $g = \bar{g} * X^{\text{val}(g)}$ , avec  $\bar{f}, \bar{g} \in \mathbb{K}[[X]]^\times$  inversibles. Donc

$$f = g * X^{\text{val}(f) - \text{val}(g)} * \bar{g}^{-1} * \bar{f} .$$

On montre l'axiome (2). Soient  $f \in \mathbb{K}[[X]]$  et  $g \in \mathbb{K}[[X]] \setminus \{0\}$ . Alors, en cas  $\text{val}(g) > \text{val}(f)$  on a  $f = gq + r$  avec  $q := 0$  et  $r := f \neq 0$ , où  $\text{val}(r) < \text{val}(f)$  si  $r \neq 0$ . Dans l'autre cas que  $\text{val}(g) \leq \text{val}(f)$ , on a déjà vu que  $f = g \cdot q + 0$  pour un  $q \in \mathbb{K}[[X]]$  convenable.

L'unicité suit du fait que, si  $A, B, Q, R \in \mathbb{K}[[X]]$  sont tels que  $B \neq 0$ ,  $A = BQ + R$  et soit  $R = 0$  soit  $\text{val}(R) < \text{val}(B)$ , alors  $Q = 0 = R$ . Vraiment, si  $Q \neq 0$  alors  $QB \neq 0$  et  $\text{val}(QB) \geq \text{val}(B)$ , donc nécessairement  $QB + R \neq 0$ . □

### Remarques

- (i) La preuve du théorème ci-dessus a montré que, pour  $f, g \in \mathbb{K}[[X]] \setminus \{0\}$  on a  $\text{val}(g) \leq \text{val}(f)$  ssi  $g$  divise  $f$ .

### 3.5.11 Définition: Séries formelles inversibles par rapport à la composition

Soit  $A$  un anneau commutatif. On dit une série formelle  $f \in A[[X]]$  **inversible par rapport à la composition** “o” ssi il existe une série formelle  $g \in \mathcal{O}(X^1)$  telle que  $f \circ g = g \circ f = X$ . Noter que en ce cas, cette  $g$  est unique.

**Remarque :** Comme on va voir dans la preuve de 3.5.12, si  $g \in \mathcal{O}(X^1)$  satisfait  $f \circ g = X$ , alors  $f \in \mathcal{O}(X^1)$  et  $g \circ f = X$ .

### 3.5.12 Théorème de la fonction inverse

Soit  $A$  un anneau commutatif et  $f = \sum_{n=0}^{\infty} f_n X^n \in A[[X]]$ . Alors,  $f$  est inversible par rapport à “o” ssi  $f_0 = 0$  et  $f_1$  est inversible dans  $A$ .

**Preuve :** Supposons que  $g \in \mathcal{O}(X^1)$  est telle que  $f \circ g = X$ . Si  $f = \sum_{n=0}^{\infty} f_n X^n$  et  $g = \sum_{n=1}^{\infty} g_n X^n$  cela implique

$$X = \sum_{n=0}^{\infty} f_n g^n = f_0 + \underbrace{\sum_{n=1}^{\infty} f_n g^n}_{\in \mathcal{O}(X^1)} \tag{3.5.12.1}$$

et donc  $f_0 = 0$ . De plus (3.5.12.1) implique  $f_1 g_1 = 1$ , c'est-à-dire  $f_1$  est inversible.

Supposons inversement que  $f_0 = 0$  et  $f_1$  est inversible. Au moyen de la relation  $f(g(X)) = X$  on peut par récurrence déterminer en manière unique les coefficients  $g_n$  de  $g = \sum_{n \in \mathbb{N}} g_n X^n$ . Expression

$$f(g(X)) = \sum_{n=1}^{\infty} f_n \cdot \left[ \sum_{k=1}^{\infty} g_k \cdot X^k \right]^n \stackrel{!}{=} X \tag{3.5.12.2}$$

25. Voir définition 1.1.14.

est équivalente à  $f_1 g_1 = 1$  et

$$a_1 b_n + (\star) = 0 \quad \forall n \geq 2, \quad (3.5.12.3)$$

où  $(\star)$  sont des expressions polynomiales en  $f_1, \dots, f_n, g_1, \dots, g_{n-1}$ . Donc  $g_1 = f_1^{-1}$  et par induction les expressions (3.5.12.3) se résolvent aux  $g_2, g_3, \dots$  et on trouve donc une unique  $g$  telle que  $f \circ g = X$ . Note que car  $g_1$  est inversible, il existe de même un  $h \in \mathcal{O}(X^1)$  tel que  $g \circ h = X$ . Donc

$$h = X \circ h = f \circ g \circ h = f \circ X = f, \quad ,$$

c'est-à-dire  $g \circ f = X$ . □

### 3.5.13 Corollaire sur séries formelles inversibles par rapport à la composition

Soit  $A$  un anneau commutatif. Alors, la sous-partie

$$A[[X]]^\circ := \left\{ f = \sum_{n=1}^{\infty} f_n X^n \in A[[X]] : f_1 \in A^\times \right\} = \{ f \in A[[X]] \text{ inversible par rapport à } \circ \} \quad (3.5.13.1)$$

forme par rapport à la composition  $\circ$  un groupe avec élément neutre  $X$ .

**Preuve :** L'égalité des deux côtés de (3.5.13.1) suit de théorème 3.5.12. Évidemment ssi  $f, g \in A[[X]]^\circ$ , alors  $f \circ g \in A[[X]]^\circ$ . C'est aussi claire que  $f \circ X = X \circ f = f$  pour toute  $f \in A[[X]]^\circ$ . De plus, par définition et théorème 3.5.12 l'inverse de toute série formelle inversible est aussi inversible. □

**Exemples :** Supposons  $\mathbb{Q} \subseteq A$ .

(i) Pour  $\alpha \in A$  on note

$$(1 + X)^\alpha := \sum_{n=0}^{\infty} \binom{\alpha}{n} \cdot X^n .$$

Note que si  $\alpha \in \mathbb{N}_0$  alors

$$(1 + X)^\alpha = \underbrace{(1 + X) * \dots * (1 + X)}_{\times \alpha} .$$

(ii) Pour  $\alpha \in A$  on appelle

$$\exp(aX) := \sum_{n=0}^{\infty} \frac{a^n}{n!} \cdot X^n .$$

la **série exponentielle** dans  $A[[X]]$ . De plus, on note

$$\log(1 + X) := \sum_{n=1}^{\infty} (-1)^{n-1} \cdot \frac{X^n}{n} . \quad (3.5.13.2)$$

Par 3.5.17, on a

$$[\exp(X) - 1] \circ \log(1 + X) = \log(1 + X) \circ [\exp(X) - 1] = X .$$

(iii) Les dérivées de  $\exp(aX)$  et  $\log(1 + X)$  sont données par

$$\frac{d}{dX} \exp(aX) = a \cdot \exp(aX)$$

et

$$\frac{d}{dX} \log(1 + X) \stackrel{(3.5.13.2)}{=} \sum_{n=0}^{\infty} (-X)^n \stackrel{(3.5.6.2)}{=} \frac{1}{1 + X} . \quad (3.5.13.3)$$

**3.5.14 Définition: Dérivée d'une série formelle**

Soit  $A$  un anneau commutatif. Pour  $f \in A[[X_1, \dots, X_n]]$  de la forme  $f = \sum_{s \in \mathbb{N}_0^n} f_s X^s$  et  $i \in \{1, \dots, n\}$  on appelle la série formelle  $\partial_i f \in A[[X_1, \dots, X_n]]$  donnée par

$$\partial_i f = \sum_{s \in \mathbb{N}_0^n} f_i \cdot s_i \cdot X_1^{s_1} \cdots X_i^{s_i-1} \cdots X_n^{s_n}$$

la **dérivée de  $f$  par rapport à  $X_i$** . Pour  $f \in A[[X]]$  on note  $\frac{df}{dX} := \partial_1 f$ .

**3.5.15 Propriétés élémentaires de la dérivée**

Soit  $A$  un anneau commutatif,  $n \in \mathbb{N}$ ,  $i \in \{1, \dots, n\}$ . Alors :

1. L'opérateur  $\partial_i : A[[X_1, \dots, X_n]] \rightarrow A[[X_1, \dots, X_n]]$  est un morphisme de  $A$ -modules.
2. Pour  $f, g \in A[[X_1, \dots, X_n]]$  on a  $\partial_i(f * g) = (\partial_i f) * g + f * (\partial_i g)$ .
3. Pour  $f \in A[[X_1, \dots, X_n]]$  et  $m \in \mathbb{N}$  on a  $\partial_i(f^m) = m f^{m-1} \cdot \partial_i f$ .
4. Si  $f \in A[[X]] \cap \mathcal{O}(X^n)$ , alors  $\frac{df}{dX} \in \mathcal{O}(X^{n-1})$ .
5. Si  $f, g \in A[[X]]$  sont tels que  $f = g + \mathcal{O}(X^n)$ , alors  $\frac{df}{dX} = \frac{dg}{dX} + \mathcal{O}(X^{n-1})$ .
6. Si  $(f_j)_{j \in J} \subseteq A[[X_1, \dots, X_n]]$  est une famille de séries formelles sommable, alors  $(\partial_i f_j)_{j \in J}$  est également et on a

$$\partial_i \sum_{j \in J} f_j = \sum_{j \in J} \partial_i f_j \quad .$$

7. Pour  $f \in A[[X]]$  et  $g \in \mathcal{O}(X)$ , on a

$$\frac{d}{dX}(f \circ g) = \left( \frac{df}{dX} \circ g \right) * \frac{dg}{dX} \quad .$$

**3.5.16 Lemme ; Caractérisation des séries formelles constantes**

Soit  $A$  un anneau commutatif, satisfaisant au moins une des conditions :

- $A$  est intègre et de caractéristique 0.
- $A$  contient  $\mathbb{Q}$ .

Alors, une série formelle  $f \in A[[X]]$  est constante ssi sa dérivée  $\frac{df}{dX}$  est nulle.

**Preuve :** De même façon comme dans 3.3.5.

□

**3.5.17 Exemple : Inverse de la série exponentielle**

Soit  $A$  un anneau commutatif et  $\exp(X)$  la série exponentielle dans  $A[[X]]$ . Alors :

$$\exp[\log(1 + X)] = 1 + X \quad .$$

**Preuve :** On va déduire et résoudre une *équation différentielle* pour la série  $f(X) := \exp[\log(1 + X)]$ . On a

$$\frac{df}{dX} = \left[ \frac{d}{dX} \exp(X) \right] (\log(1 + X)) * \frac{d}{dX} \log(1 + X) \stackrel{(3.5.13.3)}{=} \exp[\log(1 + X)] * \frac{1}{1 + X} = \frac{f}{1 + X} \quad .$$

**Proposition :** Une série formelle  $g \in A[[X]]$  satisfait l'équation différentielle  $\frac{dg}{dX} = \frac{g}{1+X}$  ssi elle est de la forme  $g(X) = g_0 + g_0 X$  pour un  $g_0 \in A$ .



**Preuve :** Soit  $g = \sum_{n=0}^{\infty} g_n X^n$ . Alors, d'une part  $\frac{dg}{dX} = \sum_{n=0}^{\infty} (n+1)g_{n+1}X^n$  et d'autre part

$$\frac{g}{1+X} \stackrel{(3.5.6.2)}{=} \sum_{n=0}^{\infty} g_n X^n * \sum_{k=0}^{\infty} (-X)^k = \sum_{n=0}^{\infty} X^n \sum_{k=0}^n g_k (-1)^{n-k} .$$

Donc, on a la chaîne d'équivalences

$$\begin{aligned} \frac{dg}{dX} = \frac{g}{1+X} &\Leftrightarrow (n+1)p_{n+1} = \sum_{k=0}^n p_k (-1)^{n-k} \quad \forall n \in \mathbb{N}_0 \\ &\Leftrightarrow 1 \cdot p_1 = p_0, \quad 2 \cdot p_2 = p_1 - p_0, \quad 3 \cdot p_3 = p_2 - p_1 + p_0, \quad \dots \\ &\Leftrightarrow p_1 = p_0 \wedge p_n = 0 \quad \forall n \geq 2 \\ &\Leftrightarrow g = p_0 + p_0 X . \end{aligned}$$

Donc,  $f$  est de la forme  $f = f_0 + f_0 X$  pour un  $f_0 \in A$ . Mais, d'autre part  $f(0) = \exp[\log(1)] = 1$ , donc  $f_0 = 1$ , c'est-à-dire

$$\exp[\log(1+X)] = 1+X .$$

□

### 3.5.18 Lemme sur puissances de polynômes

Soit  $A$  un anneau commutatif contenant  $\mathbb{Q}$ . On considère l'algèbre  $A[X]$ . Alors, pour  $\alpha, \beta \in A$  on a

$$(1+X)^\alpha * (1+X)^\beta = (1+X)^{\alpha+\beta} .$$

**Preuve :** Comme

$$(1+X)^\alpha * (1+X)^\beta = \sum_{n \in \mathbb{N}_0} \sum_{p+q=n} \binom{\alpha}{p} \binom{\beta}{q} X^n , \quad (1+X)^{\alpha+\beta} = \sum_{n \in \mathbb{N}_0} \binom{\alpha+\beta}{n} X^n ,$$

il suffit à montrer que

$$\sum_{p+q=n} \binom{\alpha}{p} \binom{\beta}{q} = \binom{\alpha+\beta}{n} .$$

pour tout  $n \in \mathbb{N}_0$ . Pour cela, il suffit de montrer que le polynôme

$$Q_{\beta,n}(X) := \binom{X+\beta}{n} - \sum_{p+q=n} \binom{X}{p} \binom{\beta}{q}$$

est nul dans  $A[X]$ . On va le montrer par récurrence. Le cas  $n=0$  est claire. On suppose  $Q_{\beta,n-1} = 0$  et note que  $Q_{\beta,n}(0) = 0$ . Donc, par 3.3.2 il suffit à montrer que  $\Delta Q_{\beta,n} = 0$ , où  $\Delta : A[X] \rightarrow A[X]$  est l'opérateur de différences défini dans 3.3.1. On trouve en fait

$$\Delta Q_{\beta,n}(X) \stackrel{3.3.3(ii)}{=} \binom{X+\beta}{n-1} - \sum_{p+q=n} \underbrace{\binom{X}{p-1}}_{\substack{=0 \\ \text{si } p=0}} \binom{\beta}{q} = \binom{X+\beta}{n-1} - \sum_{k+l=n-1} \binom{X}{k} \binom{\beta}{l} \stackrel{Q_{\beta,n-1}=0}{=} 0 ,$$

ce qui complet la preuve.

□

**Conséquences :**

(i) Pour  $\alpha \in A$  on a

$$\frac{1}{(1+X)^\alpha} = (1+X)^{-\alpha} = \sum_{n=0}^{\infty} \binom{-\alpha}{n} \cdot X^n .$$

### 3.5.19 Développement en séries formelles d'une fraction rationnelle

Soit  $\mathbb{K}$  un corps. Alors, par 3.5.3 l'anneau  $\mathbb{K}[[X]]$  et donc  $\mathbb{K}[X]$  sont intègres. Soient  $\mathbb{K}(X)$  et  $\mathbb{K}((X))$  leurs corps quotients respectivement (vois 2.1.20). Noter que  $\mathbb{K}[X]$  et  $\mathbb{K}[[X]]$  s'injectent dans  $\mathbb{K}(X)$  et  $\mathbb{K}((X))$  respectivement. Comme  $\mathbb{K}[X]$  s'injecte naturellement dans  $\mathbb{K}[[X]]$ , le corps  $\mathbb{K}(X)$  s'injecte aussi naturellement dans  $\mathbb{K}((X))$ . On peut montrer (voir 3.5.20 ci-dessous), que  $\mathbb{K}((X))$  est effectivement le corps des **séries de Laurent**

$$\left\{ \sum_{n \geq n_0} a_n X^n : n_0 \in \mathbb{Z}, a_n \in \mathbb{K} \right\} ,$$

muni de la même loi de multiplication comme  $\mathbb{K}[[X]]$ . Le monomorphisme DSF :  $\mathbb{K}(X) \hookrightarrow \mathbb{K}((X))$  qui envoie toute **fraction rationnelle** de polynômes à sa série de Laurent, est dit **développement en série formelle**.

Considérons par exemple la fraction  $\frac{P(X)}{Q(X)} \in \mathbb{K}(X)$  avec  $P, Q \in \mathbb{K}[X]$  et  $Q(0) \neq 0$ . Alors  $Q$  est de la forme

$$Q = Q_0 + \sum_{n=1}^{\infty} Q_n X^n .$$

avec  $Q_0 \neq 0$ . Comme  $Q_0$  est inversible, par 3.5.6  $Q(X)$  possède une série formelle inverse  $Q^{-1} \in \mathbb{K}[[X]]$  par rapport à la multiplication. Donc

$$\underbrace{\frac{P(X)}{Q(X)}}_{\in \mathbb{K}(X)} = \underbrace{\frac{P(X) * Q^{-1}(X)}{Q(X) * Q^{-1}(X)}}_{\in \mathbb{K}((X))} = \underbrace{P(X) * Q^{-1}(X)}_{\in \mathbb{K}[[X]] \subseteq \mathbb{K}((X))} .$$

Dans le cas que  $Q(0) = 0$ , on peut extraire le terme  $X^n$  de  $Q$ , où  $n$  soit la multiplicité de la racine 0 dans  $Q$ . On dit que la fraction  $P/Q$  possède dans  $X = 0$  un **pôle d'ordre  $n$** . Donc  $Q = X^n * \tilde{Q}$  pour un  $\tilde{Q} \in \mathbb{K}[X]$  avec  $\tilde{Q}(0) \neq 0$ . Donc, en appliquant le dessus on peut écrire

$$\frac{P(X)}{Q(X)} = X^{-n} * \underbrace{\frac{P(X)}{\tilde{Q}(X)}}_{\in \mathbb{K}((X))} = X^{-n} * \underbrace{P(X) * \tilde{Q}^{-1}(X)}_{\in \mathbb{K}[[X]]} ,$$

l'inverse  $\tilde{Q}^{-1}(X) \in \mathbb{K}[[X]]$  (par rapport à la multiplication) étant donnée par la formule (3.5.6.1). On a donc trouvé le plongement  $\mathbb{K}(X) \hookrightarrow \mathbb{K}((X))$ , du moins formellement. En particulier, fractions sans pôles s'injectent dans  $\mathbb{K}[[X]]$ .

**Exemple :** La fraction  $1 / [(1 - X^3)(1 - X^5)] \in \mathbb{C}(X)$  s'injecte dans  $\mathbb{C}[[X]]$  par la formule (3.5.6.1) comme

$$\begin{aligned} \frac{1}{(1 - X^3)(1 - X^5)} &\mapsto (1 - X^3)^{-1} * (1 - X^5)^{-1} = \sum_{n=0}^{\infty} X^{3n} * \sum_{n=0}^{\infty} X^{5n} \\ &= \sum_{k=0}^{\infty} X^k \cdot |\{(n, m) \in \mathbb{N}_0^2 : 3n + 5m = k\}| = 1 + X^3 + X^5 + X^6 + \mathcal{O}(X^8) . \end{aligned}$$

### 3.5.20 Lemme : Le corps des fractions de $\mathbb{K}[[X]]$

Si  $\mathbb{K}$  est un corps, alors le corps des fractions de l'anneau  $\mathbb{K}[[X]]$  est donné par l'ensemble

$$\mathbb{L}(X) := \left\{ \sum_{n \geq n_0} a_n X^n : n_0 \in \mathbb{Z}, a_n \in \mathbb{K} \right\} \subseteq A^{\mathbb{Z}} ,$$

muni de la loi d'addition

$$\sum_{n \geq n_0} a_n X^n + \sum_{n \geq m_0} b_n X^n = \sum_{n \geq n_0} (a_n + b_n) X^n \quad (3.5.20.1)$$

(où sans perdu de généralité  $m_0 = n_0$ ) et de la multiplication

$$\left[ \sum_{n \geq n_0} a_n X^n \right] * \left[ \sum_{m \geq m_0} b_m X^m \right] = \sum_{k \geq n_0 + m_0} \left[ \sum_{n+m=k} a_n b_m \right] X^k . \quad (3.5.20.2)$$

**Preuve :** On montre tout d'abord que  $\mathbb{L}(X)$  est un corps. C'est facile à voir que  $(\mathbb{L}(X), +, *)$  est bien un anneau commutatif. Si  $0 \neq g \in \mathbb{L}(X)$ , alors  $g = X^{n_0} * \tilde{g}$  pour un  $0 \neq \tilde{g} \in \mathbb{K}[[X]]$  avec valuation 0. Il existe donc dans  $\mathbb{K}[[X]]$  l'inverse  $\tilde{g}^{-1}$  et donc dans  $\mathbb{L}(X)$  l'inverse  $X^{-n_0} * \tilde{g}^{-1}$ . Donc,  $\mathbb{L}(X)$  est vraiment un corps, contenant  $\mathbb{K}[[X]]$ .

D'autre part, le corps des fractions  $\mathbb{K}((X))$  est le plus petit corps contenant  $\mathbb{K}[[X]]$ . Comme il doit inclure les inverses des monômes  $X^m$  et donc une copie de  $\mathbb{L}(X)$ , on conclut que  $\mathbb{K}((X)) \cong \mathbb{L}(X)$ . □

## 4 Anneaux factoriels

### 4.1 Préliminaires

#### 4.1.1 Définition: Élément irréductible

Soit  $A$  un anneau intègre. Un élément  $\pi \in A$  est dit **irréductible** si :

- $\pi$  est non-inversible.
- Pour tout  $x, y \in A$  tels que  $\pi = xy$  un des deux  $x$  ou  $y$  est inversible.

#### Remarques

- (i) Tout irréductible est non-nul.
- (ii) Si  $\pi \in A$  est irréductible et  $a \in A^\times$  inversible, alors  $a\pi$  est aussi irréductible. Cela suit de remarque 1.1.7(i) sur éléments inversibles.

#### 4.1.2 Définition: Éléments associés

Soit  $A$  un anneau intègre. Alors, on dit deux éléments  $x, y \in A$  **associés** et note  $x \sim y$  ssi  $Ax = Ay$ .

#### Remarques

- (i) Par remarque 1.1.6(ii),  $x, y \in A$  sont associés ssi  $y \in A^\times x$  et ssi  $A^\times x = A^\times y$ .
- (ii) L'association entre les éléments de  $A$  est une relation d'équivalence. Ses classes sont données par  $[x] = xA^\times$  pour chaque  $x \in A$ .
- (iii) Par remarque 4.1.1(ii),  $x \in A$  est irréductible ssi sa classe d'équivalence  $[x] = xA^\times$  ne contient que irréductibles.
- (iv) Pour deux  $x, y \in A$  on a  $x \mid y$  ssi  $Ay \subseteq Ax$ .
- (v) Donc, deux  $0 \neq x, y \in A$  sont associés ssi  $x \mid y$  et  $y \mid x$ .
- (vi) Si  $0 \neq x, y \in A$  sont associés et  $a \mid x$ , alors  $a \mid y$ . On peut donc écrire  $a \mid [x]$ .
- (vii) Si  $0 \neq x, y \in A$  sont associés et  $x \mid a$ , alors  $y \mid a$ . On peut donc écrire  $[x] \mid a$ .
- (viii) Le produit de deux non-inversibles  $x, y \in A$  est non-inversible et non-irréductible.
- (ix) Tout  $\pi \in A$  est irréductible ssi  $\pi$  n'est pas associé à 1 et pour tout  $xy = \pi$  il est associé à  $x$  ou  $y$ .

#### Exemples

- (i) Soit  $\mathbb{K}$  un corps, et  $\mathbb{K}[[X]]$  l'anneau des séries formelles sur  $\mathbb{K}$ . Alors, par lemme 3.5.9 deux éléments non nulles sont associées ssi ils possèdent la même valuation.

#### 4.1.3 Définition: Élément premier

Soit  $A$  un anneau intègre. Alors, un élément  $0 \neq \pi \in A$  est dit **premier** si  $A\pi$  est un idéal premier.

#### Remarques

- (i) Par définition d'un idéal premier, tout premier est non-inversible.
- (ii) Un élément  $0 \neq \pi \in A$  est premier ssi il est non-inversible et satisfait la **propriété de Gauss**, c'est-à-dire pour tout  $x, y \in A$  tels que  $\pi \mid xy$ , il faut  $\pi \mid x$  ou  $\pi \mid y$ .
- (iii) Tout premier  $0 \neq \pi \in A$  est irréductible.

**Preuve :** Suppose  $\pi = xy$  pour quelques  $x, y \in A$ . Alors  $xy \in A\pi$  et donc  $x \in A\pi$  ou  $y \in A\pi$ . Supposons sans perdu de généralité  $x \in A\pi$ , c'est-à-dire  $x = a\pi$  pour un  $a \in A$ . Donc  $\pi = xy = ya\pi$ . Comme  $A$  est intègre et  $\pi \neq 0$ , on en déduit que  $ya = 1$ .

- (iv) Si  $A = \mathbb{Z}$ , alors  $p \in \mathbb{Z}$  est premier (dans le sens ci-dessus) ssi  $|p|$  est un nombre premier (dans le sens *traditionnel*). On note  $\mathbb{P} \subseteq \mathbb{N}$  les (positives) premiers de  $\mathbb{Z}$ .

#### 4.1.4 Définition: Anneau factoriel

Un anneau intègre  $A$  est dit **factoriel** si :

- (F1) Tout élément  $0 \neq \pi \in A$  non inversible est produit d'un nombre fini d'éléments irréductibles.  
 (F2) Tout élément  $0 \neq \pi \in A$  est irréductible ssi il est premier.

#### Remarques

- (i) Propriété 4.1.4(2) est équivalente à : Tout élément  $0 \neq \pi \in A$  est irréductible ssi il est non-inversible et satisfait la propriété de Gauss.  
 (ii) Si  $A$  est un anneau intègre, noethérien, alors propriété 4.1.4(1) est satisfait.

**Preuve :** Supposons le contraire, c'est-à-dire il existe un non-inversible  $0 \neq a \in A$  qui n'est pas un produit fini d'irréductibles. En particulier  $a$  n'est pas irréductible, c'est-à-dire il existe  $0 \neq a_1, a_2 \in A \setminus A^\times$  tels que  $a = a_1 a_2$ . Donc  $Aa \subseteq Aa_1$ . Car  $a_2$  est non-inversible et  $a_1 \neq 0$ , par remarque 1.1.6(ii) on a en fait  $Aa \subsetneq Aa_1$ . De plus,  $a_1$  ou  $a_2$  n'est pas produit fini d'irréductibles, supposons  $a_1$ . Donc, il existe deux  $0 \neq a_3, a_4 \in A \setminus A^\times$  tels que  $a_1 = a_3 a_4$ . Donc, de même comme devant,  $Aa_1 \subsetneq Aa_3$  et en façon similaire on peut supposer que  $a_3$  n'est pas produit fini d'irréductibles. Par induction on trouve une suite croissante des idéaux  $Aa \subsetneq Aa_1 \subsetneq Aa_3 \subsetneq \dots$  qui n'est pas stationnaire. Par 1.3.2 cela est une contradiction.

#### 4.1.5 Lemme de Gauss sur anneaux intègres, principaux

Un anneau intègre, principal  $A$  est factoriel.

**Preuve :** Comme tout anneau principal est noethérien, par remarque 4.1.4(ii) il suffit à montrer propriété 4.1.4(2). Par remarque 4.1.3(iii) il faut montrer que tout irréductible est premier.

Soit  $\pi \in A$  irréductible. Comme  $\pi$  est non-inversible, par remarque 4.1.3(ii) il suffit de montrer la propriété de Gauss. Soit  $\pi \mid xy$  pour quelques  $x, y \in A$ . Alors, comme  $A$  est principal, l'idéal  $A\pi + Ax$  est principal et donc  $A\pi + Ax = Az$  pour un  $z \in A$ . En particulier  $\pi = az$  pour un  $a \in A$ . En cas  $a \in A^\times$  on a  $x = bz$  pour un  $b \in A$  et donc  $x = bz = ba^{-1}\pi$ , c'est-à-dire  $\pi \mid x$ . En cas  $a \notin A^\times$  il faut  $z \in A^\times$  et on peut supposer  $z = 1$ . Donc  $1 = a\pi + bx$  pour quelques  $a, b \in A$ , donc  $y = a\pi y + bxy$ . Comme  $\pi \mid a\pi y$  et  $\pi \mid bxy$ , il faut  $\pi \mid y$ . □

#### Remarques & Exemples

- (i) Tout corps  $\mathbb{K}$  est factoriel. En fait, comme  $\mathbb{K}[X]$  est par 3.1.11 intègre et par 3.2.5 principal,  $\mathbb{K}[X]$  est factoriel.  
 (ii)  $(\mathbb{Z}, +, \cdot)$  est factoriel.  
 (iii) Soit  $A$  intègre, principal. Alors, tout idéal  $I \subseteq A$  est maximal ssi il est premier.

**Preuve :** Par 1.2.20 on sait que tout idéal maximal est premier. Soit inversement  $I \subsetneq A$  premier et  $J \subseteq A$  un idéal tel que  $I \subseteq J \subseteq A$ . Alors  $I, J$  sont principaux, c'est-à-dire  $I = Aa$  et  $J = Ab$  pour quelques  $a, b \in A$ , avec  $a$  premier. Alors, comme  $Aa \subseteq Ab$  il faut  $b \mid a$ . Comme  $a$  est irréductible, il faut soit  $b \sim A^\times$  soit  $b \sim a$ , c'est-à-dire soit  $J = A$  soit  $J = I$ .

#### 4.1.6 Lemme : Chaîne des inclusions de classes des anneaux intègres

Dans la famille des anneaux intègres, on a la chaîne d'inclusions suivante :

$$\{\text{euclidiens}\} \subseteq \{\text{principaux}\} \subseteq \{\text{factoriels}\} \quad .$$

### 4.1.7 Caractérisation des anneaux factoriels

Soit  $A$  un anneau intègre. Alors,  $A$  est factoriel ssi tout  $0 \neq x \in A$  non-inversible possède une factorisation en un nombre fini d'éléments irréductibles et cette factorisation est unique dans le sens suivant : Si

$$\pi_1 \dots \pi_r = \xi_1 \dots \xi_s$$

pour quelques irréductibles  $\pi_1, \dots, \pi_r, \xi_1, \dots, \xi_s \in A$ , alors  $r = s$  et il existe une permutation  $\sigma$  de  $\{1, \dots, r\}$  telle que  $\pi_i \sim \xi_{\sigma(i)}$  pour tout  $i \in \{1, \dots, r\}$ .

Autrement dit, on a sur  $A$  l'unicité de la composition en irréductibles modulo la relation d'association et l'ordre près.

**Preuve :**

**Direction “ $\Rightarrow$ ” :** Par remarque 4.1.4(i) tout irréductible satisfait la propriété de Gauss. Soient  $\pi_1, \dots, \pi_r, \xi_1, \dots, \xi_s \in A$  irréductibles tels que  $\pi_1 \dots \pi_r = \xi_1 \dots \xi_s$ . Alors,  $\pi_1$  divise l'un des  $\xi_i$ , supposons  $\pi_1 \mid \xi_1$ . Donc  $\xi_1 = a_1 \pi_1$  pour un  $a_1 \in A$ . Comme  $\xi_1$  est irréductible et  $\pi_1$  non-inversible, il faut  $a_1 \in A^\times$ . Donc, par remarque 1.1.6(ii)  $A\xi_1 = A\pi_1$ , c'est-à-dire  $\xi_1 \sim \pi_1$ . De plus, comme  $A$  est intègre et  $\pi_1 \neq 0$ , on trouve

$$\pi_2 \dots \pi_r = a_1 \xi_2 \xi_3 \dots \xi_s = \tilde{\xi}_2 \xi_3 \dots \xi_s \quad ,$$

où  $\tilde{\xi}_2 := a_1 \xi_2$  est par remarque 4.1.1(ii) aussi irréductible. Par récurrence suit l'affirmation.

**Direction “ $\Leftarrow$ ” :** Soit  $a \in A$  irréductible et  $x, y \in A$  tels que  $a \mid xy$ , c'est-à-dire  $xy = ab$  pour un  $b \in A$ . Noter que  $a, b, x, y \neq 0$ . Alors :

- Si  $x \in A^\times$ , alors  $y = abx^{-1}$  et donc  $a \mid y$ . De même pour le cas  $y \in A^\times$ .
- Si  $b \in A^\times$ , alors  $ab$  est irréductible et donc soit  $x \in A^\times$  soit  $y \in A^\times$ . Par le précédent soit  $a \mid y$  soit  $a \mid x$ .
- Si  $x, y, b \notin A^\times$ , alors par supposition il existe irréductibles  $\pi_1, \dots, \pi_n, \xi_1, \dots, \xi_m, \rho_1, \dots, \rho_l$  tels que

$$\underbrace{\pi_1 \dots \pi_n}_x \cdot \underbrace{\xi_1 \dots \xi_m}_y = a \cdot \underbrace{\rho_1 \dots \rho_l}_b \quad .$$

Par unicité de factorisation il faut que  $a \sim \pi_i$  ou  $a \sim \xi_i$  pour un certain  $i$ . Donc  $a \mid x$  ou  $a \mid y$ , c'est-à-dire  $a$  satisfait la propriété de Gauss. D'après remarque 4.1.3(ii) cela et le fait que  $a$  est non-inversible impliquent que  $a$  est premier, donc  $A$  factoriel. □

### 4.1.8 Corollaire : Factorisation de produits

Soit  $A$  un anneau factoriel,  $\pi_1, \dots, \pi_n \in A$  irréductibles et  $0 \neq a_1, \dots, a_m \in A$  quelconques tels que  $a_1 \dots a_m \sim \pi_1 \dots \pi_n$ . Alors il existe une partition  $\{1, \dots, n\} = \bigsqcup_{i=1}^m I_i$  telle que  $a_i \sim \prod_{j \in I_i} \pi_j$ .

**Preuve :** Suit de caractérisation 4.1.7. □

### 4.1.9 Définition: pgcd et ppcm

Soit  $A$  un anneau factoriel. Par théorème 4.1.7, tout élément  $0 \neq x \in A$  peut être écrit sous la forme  $x = a \cdot \pi_1 \dots \pi_n$  ( $n \in \mathbb{N}_0$ ), où  $a \in A^\times$  est inversible et  $\pi_1, \dots, \pi_n \in A$  sont des irréductibles, uniques modulo la relation d'association et l'ordre près. Inversement, si  $\xi_1, \dots, \xi_n \in A$  sont irréductibles deux à deux associées aux  $\pi_1, \dots, \pi_n$ ,  $x$  possède aussi la représentation  $b \cdot \xi_1 \dots \xi_n$  pour un certain inversible  $b \in A^\times$ .

Il est donc convient de travailler avec un système représentatif d'irréductibles  $\mathcal{J}_A$ . On fait le choix d'un élément dans chaque classe d'équivalence d'irréductibles. Alors, il existe pour  $0 \neq x \in A$  une unique décomposition  $x = a \cdot \pi_1^{p_1} \dots \pi_n^{p_n}$  avec  $a \in A^\times$ ,  $\pi_i \in \mathcal{J}_A$ ,  $p_i \in \mathbb{N}_0$  et  $\pi_i \neq \pi_j \forall i \neq j$ , modulo l'ordre et facteurs triviales de type

$\pi_i^0$ . Soient  $0 \neq x, y \in A$  avec les décompositions uniques  $x = a \cdot \pi_1^{p_1} \dots \pi_n^{p_n}$  et  $y = b \cdot \xi_1^{q_1} \dots \xi_m^{q_m}$  de tel type. Alors, en supposant sans perdu de généralité que  $n = m$  et  $\pi_i = \xi_i \forall i$  on pose

$$\text{ppcm}(x, y) := ab \cdot \prod_{i=1}^n \pi_i^{\max(p_i, q_i)} ,$$

$$\text{pgcd}(x, y) := ab \cdot \prod_{i=1}^n \pi_i^{\min(p_i, q_i)} .$$

Par convention, on pose  $\text{ppcm}(x, 0) := 0$  et  $\text{pgcd}(x, 0) := x$ .

**Remarques :** Soient  $0 \neq a, b, c \in A$ . Alors :

- (i) Les valeurs  $\text{ppcm}(a, b)$  et  $\text{pgcd}(a, b)$  ne sont pas uniques ; ils dépendent du choix de  $\mathcal{J}_A$ . Néanmoins, ils sont uniques à association près. Il faudrait donc parler des  $\text{pgcd}(a, b)$  et  $\text{ppcm}(a, b)$  comme classes d'équivalence. On note pourtant souvent  $\text{pgcd}(a, b)$  et  $\text{ppcm}(a, b)$  par un de leurs représentants.
- (ii) Inversement,  $\text{ppcm}(a, b)$  et  $\text{pgcd}(a, b)$  sont constantes dans les classes d'équivalence des  $a, b$ .
- (iii) Les opérations  $\text{ppcm}, \text{pgcd} : (A/\sim) \times (A/\sim) \rightarrow (A/\sim)$  sont symétriques et associatives. On peut donc parler des  $\text{ppcm}$  et  $\text{pgcd}$  de plusieurs éléments.
- (iv) On a toujours  $a \mid \text{ppcm}(a, b)$  et  $\text{pgcd}(a, b) \mid a$ .
- (v) Le diviseur  $\text{pgcd}(a, b)$  en commun des  $a, b$ , est le *plus grand* : Si  $c \mid a$  et  $c \mid b$ , alors  $c \mid \text{pgcd}(a, b)$ .
- (vi) Le multiple  $\text{ppcm}(a, b)$  en commun des  $a, b$ , est le *plus petit* : Si  $a \mid c$  et  $b \mid c$ , alors  $\text{ppcm}(a, b) \mid c$ . Autrement dit

$$Aa \cap Ab = A \text{ppcm}(a, b) .$$

(vii) Pour  $a_1, \dots, a_n \in A$  on a

$$\text{pgcd}(a_1, \dots, a_n) = 1 \Leftrightarrow \text{ppcm}(a_1, \dots, a_n) = \prod_{i=1}^n a_i .$$

(viii) Si  $A$  est principal et  $a_1, \dots, a_n \in A$ , alors  $Aa_1 + \dots + Aa_n = A \text{pgcd}(a_1, \dots, a_n)$  [Bézout]. En particulier,

$$Aa_1 + \dots + Aa_n = A \Leftrightarrow \text{pgcd}(a_1, \dots, a_n) = 1 .$$

- (ix) Si  $a_1, \dots, a_n \in A$  sont tels que  $\text{pgcd}(a_1, \dots, a_n) = 1$  on les dit **premiers entre eux dans leur ensemble**.
- (x) Si  $a_1, \dots, a_n \in A$  possèdent  $\text{pgcd}(a_i)_{i=1}^n = a$ , alors il existe  $\alpha_1, \dots, \alpha_n \in A$  (uniques d'association près) tels que

$$a_i = \alpha_i \cdot a \wedge \text{pgcd}(\alpha_i)_{i=1}^n = 1 .$$

- (xi) Pour  $a, a_1, \dots, a_n \in A$  on a  $\text{pgcd}(a \cdot a_i)_{i=1}^n = a \cdot \text{pgcd}(a_i)_{i=1}^n$  et  $\text{ppcm}(a \cdot a_i)_{i=1}^n = a \cdot \text{ppcm}(a_i)_{i=1}^n$ .
- (xii) Si  $b \mid a_1, \dots, a_n \in A$ , alors  $b = \text{pgcd}(b, a_1, \dots, a_n)$ .

**Preuve :** Suit de remarque 4.1.2(v) et remarques (iv), (v).

- (xiii) Pour  $a_1, \dots, a_n \in A \setminus \{0\}$  on a  $\text{pgcd}(a_1, \dots, a_n) = 1$  ssi il n'existe aucun irréductible divisant tous  $a_1, \dots, a_n$  et ssi il n'existe aucun non-inversible divisant tous  $a_1, \dots, a_n$ .
- (xiv) Si  $\mathbb{K}$  est un corps, alors tous non-nulles sont associés à 1 et donc pour tous  $0 \neq a, b \in \mathbb{K}$  on a

$$\text{pgcd}(a, b) = 1 = \text{ppcm}(a, b) .$$

Les notions de la multiplication, de l'irréductibilité, de la premierité, de la divisibilité et les opérations  $\text{pgcd}$ ,  $\text{ppcm}$  sont invariants par rapports à l'association  $\sim$  sur  $A$ . Ils passent donc tous au quotient  $A/\sim$ .

#### 4.1.10 Théorème de Bachet-Bézout

On reformule l'affirmation de Bézout déjà vu dans remarque 4.1.9(viii) pour  $\mathbb{Z}$  : Soient  $x, y \in \mathbb{Z} \setminus \{0\}$  avec plus grand commun diviseur  $x \wedge y$ . Alors, il existe  $n, m \in \mathbb{Z}$  tels que

$$n \cdot x + m \cdot y = x \wedge y$$

En particulier,  $x, y$  sont premiers entre eux ssi il existe  $a, b \in \mathbb{Z}$  tels que  $n \cdot x + m \cdot y = 1$ .

## 4.2 Factorialité d'algèbres des polynômes

### 4.2.1 Définition: Polynôme primitif

Soit  $A$  un anneau factoriel et  $P \in A[X_1, \dots, X_n]$  de la forme

$$P = \sum_{s \in S} P_s \cdot X^s$$

avec  $S \subseteq \mathbb{N}_0^n$  fini. Alors, on appelle **contenu** de  $P$  la classe<sup>26</sup>  $\text{pgcd}(a_s)_{s \in S}$ . On la note  $\mathcal{C}(P)$ . Si  $\mathcal{C}(P) = 1$ , c'est-à-dire les coefficients de  $P$  sont premiers entre eux, alors  $P$  est dit **primitif**.

#### Remarques

(i) Si  $\mathbb{K}$  est un corps, alors par remarque 4.1.9(xiv) pour tout  $0 \neq P \in \mathbb{K}[X]$  on a  $\mathcal{C}(P) = 1$ .

(ii) Pour  $P \in A[X]$ , il existe un primitif  $P^* \in A[X]$  tel que  $P = \mathcal{C}(P) \cdot P^*$ .

**Preuve :** Soit  $P = \sum_{i=0}^n a_i \cdot X^i$ , alors il existe  $\alpha_0, \dots, \alpha_n \in A$  tels que  $\text{pgcd}(\alpha_i)_{i=0}^n = 1$  et  $a_i = \mathcal{C}(P) \cdot \alpha_i \forall i$ .  
Donc

$$P = \mathcal{C}(P) \cdot \underbrace{\sum_{i=0}^n \alpha_i \cdot X^i}_{P^*},$$

avec  $\mathcal{C}(P^*) = 1$ .

(iii) Soit  $\mathbb{K}$  le corps quotient de  $A$ . Alors, pour  $P \in \mathbb{K}[X]$ , il existe  $a, b \in A$  premiers entre eux tels que  $P = (a/b)P^*$  pour un primitif  $P^* \in A[X]$ .

**Preuve :** Soit  $P$  de la forme  $P = \sum_{i=0}^n c_i \cdot X^i$ . Alors, on peut supposer<sup>27</sup> que  $c_i = a_i/b$  avec  $a_i, b \in A$  et  $\text{pgcd}(b, a_1, \dots, a_n) = 1$ . Pose  $a := \text{pgcd}(a_i)_{i=1}^n$ , alors par remarque 4.1.9(x) il existe  $\alpha_1, \dots, \alpha_n \in A$  tels que  $a_i = a \cdot \alpha_i$  et  $\text{pgcd}(\alpha_i)_{i=1}^n = 1$ . Donc  $c_i = \alpha_i \cdot (a/b)$  et  $P = (a/b)P^*$  pour un primitif  $P^* \in A[X]$ . Comme  $1 = \text{pgcd}(b, a_1, \dots, a_n) = \text{pgcd}(b, a)$  les  $b, a$  sont premiers entre eux.

### 4.2.2 Définition: Réduction d'un polynôme

Soit  $A$  un anneau commutatif et  $I \subseteq A$  un idéal de  $A$ . Alors, le morphisme d'anneaux

$$A[X] \rightarrow (A/I)[X], \quad \sum_i a_i \cdot X^i \mapsto \sum_i [a_i] \cdot X^i$$

est dit **réduction modulo  $I$** . Si  $I = A\pi$  pour un  $\pi \in A$ , on parle du morphisme

$$A[X] \rightarrow (A/\pi A)[X] \stackrel{3.2.11}{\cong} A[X]/(\pi A)[X], \quad \underbrace{P}_{\in A[X]} \mapsto \underbrace{P + (\pi A)[X]}_{\in A[X]/\pi A[X]}$$

comme **réduction des polynômes modulo  $\pi$** .

#### Remarques

(i) Soit  $A$  un anneau intègre. Alors  $0 \neq \pi \in A$  est premier dans  $A$  ssi  $\pi A$  est premier, ssi  $A/\pi A$  intègre, ssi  $(A/\pi A)[X] \cong A[X]/\pi A[X]$  intègre, ssi  $\pi A[X]$  premier et donc ssi  $\pi$  premier dans  $A[X]$ .

### 4.2.3 Lemme : Caractérisation des polynômes primitifs

Soit  $A$  un anneau factoriel et  $P \in A[X]$ . Alors,  $P$  est primitif ssi pour tout  $\pi \in A$  irréductible la réduction  $\overline{P}$  de  $P$  modulo  $\pi$  est non-nul.

<sup>26</sup>. Par rapport à la relation d'équivalence d'association (voir 4.1.9).

<sup>27</sup>. On peut supposer  $c_i = \frac{p_i}{q}$  pour quelques  $p_i \in A$ ,  $q \in A \setminus \{0\}$ . Par remarque 4.1.9(x) on peut trouver des  $a_i, a, b \in A$  tels que  $p_i = a \cdot a_i$ ,  $q = a \cdot b$  et  $\text{pgcd}(b, a_1, \dots, a_n) = 1$ . Donc  $c_i = \frac{p_i}{q} = \frac{a_i a}{ab} = \frac{a_i}{b}$ .



**Preuve :** Si  $P$  n'était pas primitif, alors par remarque 4.1.9(xiii) il existerait un irréductible  $\pi$  qui divise tous coefficients de  $P$ , donc la réduction de  $P$  modulo  $\pi$  serait nulle. Inversement, si la réduction de  $P$  modulo un irréductible  $\pi \in A$  était nulle, alors  $\pi$  diviserait tous coefficients de  $P$ , donc  $\pi \mid \mathcal{C}(P)$  et par conséquence  $\mathcal{C}(P) \neq 1$ . □

#### 4.2.4 Lemme de Gauss sur le contenu de polynômes

Soit  $A$  un anneau factoriel. Alors, le contenu  $\mathcal{C} : (A[X], *) \rightarrow (A, \cdot)$  est un morphisme de monoides. En particulier, si  $P, Q \in A[X]$  sont primitifs, alors  $P * Q$  est également.

**Preuve :** Soient  $P, Q \in A[X]$ . Par remarque 4.2.1(ii) on peut trouver des primitifs  $P^*, Q^* \in A[X]$  tels que  $P = \mathcal{C}(P) \cdot P^*$  et  $Q = \mathcal{C}(Q) \cdot Q^*$ . En particulier

$$P * Q = \mathcal{C}(P) \cdot \mathcal{C}(Q) \cdot P^* * Q^*$$

et donc par remarque 4.1.9(xi)

$$\mathcal{C}(P * Q) = \mathcal{C}(P) \cdot \mathcal{C}(Q) \cdot \mathcal{C}(P^* * Q^*) .$$

Il reste donc à montrer que  $P^* * Q^*$  est primitif. On va utiliser la caractérisation 4.2.3. Soit  $\pi \in A$  irréductible et  $\overline{P^*}, \overline{Q^*}$  et  $\overline{P^* * Q^*} \in A[X]$  les réductions des  $P^*, Q^*$  et  $P^* * Q^*$  modulo  $\pi$ . Comme  $P^*, Q^*$  sont primitifs, on sait que  $\overline{P}, \overline{Q} \neq 0$ . Par remarque 4.2.2(i)  $\pi A[X]$  est premier et donc  $A[X]/\pi A[X]$  intègre, d'où on déduit

$$\overline{P^* * Q^*} \stackrel{4.2.2}{=} \overline{P^*} * \overline{Q^*} \neq 0 .$$

Par conséquence,  $P^* * Q^*$  est primitif. □

#### 4.2.5 Lemme : Division dans $R[X]$ et $\mathbb{K}[X]$

Soit  $R$  un anneau factoriel et  $\mathbb{K}$  son corps quotient. Soient  $A, B \in \mathbb{K}[X]$  polynômes tels que  $C := A * B \in R[X]$ . Supposons que deux des trois  $\{A, B, C\}$  sont unitaires. Alors, tous  $\{A, B, C\}$  sont unitaires et  $A, B$  appartiennent à  $R[X]$ .

**Preuve :** Comme le coefficient dominant de  $C$  est le produit des termes dominants des  $A, B$ , tous les trois  $\{A, B, C\}$  sont unitaires. En particulier  $\mathcal{C}(C) = 1$ . Soient  $a, b \in R$  tels que  $aA, bB \in R[X]$ . Alors

$$\mathcal{C}(aA) \cdot \mathcal{C}(bB) = \mathcal{C}(aA * bB) = ab\mathcal{C}(A * B) = ab\mathcal{C}(C) = ab .$$

On a donc

$$C = \frac{aA * bB}{ab} = \underbrace{\frac{aA}{\mathcal{C}(aA)}}_{=: \tilde{A}} \cdot \underbrace{\frac{bB}{\mathcal{C}(bB)}}_{=: \tilde{B}} ,$$

avec  $\tilde{A}, \tilde{B} \in R[X]$ . Comme le coefficient dominant de  $C$ , égal à 1, est produit des coefficients dominants des  $\tilde{A}, \tilde{B}$ , il faut que les derniers sont inversibles dans  $A$ . Donc,  $A$  et  $\tilde{A}$  sont deux polynômes proportionnels avec coefficient de proportionnalité dans  $\mathbb{K}$ , dont les coefficients sont inversibles dans  $A$ . Donc, ce coefficient de proportionnalité est aussi inversible dans  $A$  et par conséquence  $A \in R[X]$ . De même façon on déduit que  $B \in R[X]$ . □

**Cas typique :**  $R = \mathbb{Z}$  et  $\mathbb{K} = \mathbb{Q}$ .

### 4.2.6 Lemme : Polynômes comme diviseurs

Soit  $A$  un anneau factoriel et  $\mathbb{K}$  son corps des quotients. Alors :

1. Soit  $P \in A[X]$  primitif et  $F \in A[X]$  tel que  $P \mid F$  dans  $\mathbb{K}[X]$ , alors  $P \mid F$  dans  $A[X]$ .
2. Si  $P \in A[X]$  est irréductible dans  $A[X]$  et non-constant, alors il est primitif dans  $A[X]$  et irréductible dans  $\mathbb{K}[X]$ .
3. Si  $P \in A[X]$  est primitif dans  $A[X]$  et irréductible dans  $\mathbb{K}[X]$ , alors  $P$  est irréductible dans  $A[X]$  et non-constant.

**Preuve :**

1. Soit  $Q \in \mathbb{K}[X]$  de la forme  $Q = \sum_{i=0}^n c_i X^i$  où  $c_i \in \mathbb{K}$ , tel que  $F = P * Q$ . Alors, par remarque 4.2.1(iii) il existe  $a, b \in A$  premiers entre eux et  $Q^* \in A[X]$  primitif tel que  $Q = (a/b) \cdot Q^*$ . Donc  $F = (a/b)P * Q^*$ , c'est-à-dire  $bF = aP * Q^*$  (noter : dans  $A[X]$ ). Par conséquence

$$b \cdot \mathcal{C}(F) = \mathcal{C}(bF) = \mathcal{C}(aP * Q^*) = a \cdot \underbrace{\mathcal{C}(P)}_{\sim 1} \cdot \underbrace{\mathcal{C}(Q^*)}_{\sim 1} = a \pmod{\sim} ,$$

d'où on déduit  $b \mid a$ . Donc, comme  $\text{pgcd}(b, a) = 1$ , d'après remarque 4.1.9(xii)  $b \sim 1$ , c'est-à-dire  $b$  est inversible. Donc  $F = ab^{-1}P * Q^*$ .

2. Montrons d'abord que  $P$  est primitif. Sinon, par remarque 4.2.1(ii) on peut écrire  $P = a \cdot P^*$ , où  $a \in A$  est non-inversible et  $P^* \in A[X]$  primitif. Si  $P^*$  était inversible, alors par 3.1.12 il serait constant et dans  $A^\times$ , donc  $P$  serait en fait une constante, une contradiction. Donc  $P^*$  n'est pas inversible, c'est-à-dire  $P$  est produit de deux non-inversibles, une contradiction comme  $P$  est irréductible. Donc,  $P$  est primitif dans  $A[X]$ . Supposons  $P = F * G$  pour quelques  $F, G \in \mathbb{K}[X]$ . Alors, par remarque 4.2.1(iii) il existe primitifs  $F^*, G^* \in A[X]$  et  $a, b, c, d \in A$  tels que  $\text{pgcd}(a, b) = 1 = \text{pgcd}(c, d)$  et

$$F = \frac{a}{b} \cdot F^* \quad , \quad G = \frac{c}{d} \cdot G^* \quad .$$

Donc  $bdP = acF^* * G^*$  et par conséquence

$$bd = bd \cdot \underbrace{\mathcal{C}(P)}_1 = \mathcal{C}(bdP) = \mathcal{C}(acF^* * G^*) = ac \cdot \underbrace{\mathcal{C}(F^* * G^*)}_1 = ac \pmod{\sim} ,$$

c'est-à-dire  $bd \sim ac$ . Donc  $ac = \varepsilon \cdot bd$  pour un  $\varepsilon \in A^\times$ , donc  $P = \varepsilon \cdot F^* * G^*$  (on peut supposer que  $\varepsilon = 1$ ). Comme  $P$  est irréductible dans  $A[X]$ , alors  $F^*$  ou  $G^*$  est inversible dans  $A[X]$ . Par 3.1.12 cela implique que  $F^*$  ou  $G^*$  est constant, supposons  $F^* = \alpha \in A \setminus \{0\}$ . Alors,  $F = (a/b)\alpha$  est inversible dans  $\mathbb{K}[X]$ . Comme  $P$  n'est pas inversible dans  $\mathbb{K}[X]$  (sinon il serait constant et par primitivité inversible dans  $A[X]$ ), on déduit que  $P$  est irréductible dans  $\mathbb{K}[X]$ .

3. Soit  $P \in A[X]$  primitif et irréductible dans  $\mathbb{K}[X]$ . Par irréductibilité,  $P$  n'est pas inversible dans  $\mathbb{K}[X]$  (et donc pas constant) et donc non plus dans  $A[X]$ . Supposons  $P = G * H$  pour deux  $G, H \in A[X]$ , alors  $G$  ou  $H$  est inversible dans  $\mathbb{K}[X]$ , supposons par exemple  $G$ . Alors, par 3.1.12  $G$  est une constante. Comme

$$1 = \mathcal{C}(P) = \mathcal{C}(G) \cdot \mathcal{C}(H) \quad ,$$

on trouve que  $\mathcal{C}(G)$  et  $\mathcal{C}(H)$  contient des inversibles, donc  $G$  est en fait une constante inversible dans  $A$ , c'est-à-dire  $P$  est irréductible. □

### 4.2.7 Théorème : Factorialité de $A[X_1, \dots, X_n]$

Si  $A$  est un anneau factoriel, alors  $A[X_1, \dots, X_n]$  est également pour tout  $n \in \mathbb{N}$ .

**Preuve :** Il suffit par récurrence et théorème 3.1.8 de montrer que  $A[X]$  est factoriel si  $A$  est factoriel. Soit  $\mathbb{K}$  le corps quotient de  $A$ .

**Proposition :** Les irréductibles constants de  $A[X]$  sont premiers.

Soit  $\pi \in A[X]$  un polynôme constant irréductible. Alors, par remarque 4.2.2(i) il suffit de montrer que  $\pi$  est aussi irréductible dans  $A$ . Evidemment  $\pi$  n'est pas dans  $A^\times$ . Si  $\pi = ab$  avec  $a, b \in A$ , alors un des deux  $a, b$  est inversible comme polynôme, donc par 3.1.12 aussi dans  $A$ , c'est-à-dire  $\pi$  est vraiment irréductible.

**Proposition :** Les irréductibles non-constants de  $A[X]$  sont premiers.

Par 4.2.6(2), ces sont exactement les irréductibles, primitifs dans  $\mathbb{K}[X]$ . Soit  $P \in A[X]$  un tel polynôme. Par remarque 4.1.3(ii) il suffit de montrer que  $P$  satisfait la propriété de Gauss. Supposons  $P \mid F * G$  pour deux  $F, G \in A[X]$ . Par exemple 4.1.5(i) on sait que  $\mathbb{K}[X]$  est factoriel, donc  $P$  divise  $F$  ou  $G$  dans  $\mathbb{K}[X]$ , supposons  $P \mid F$ . Il faut montrer que cette division est en fait dans  $A[X]$ . Mais cela est déjà montré dans théorème 4.2.6(1).

Il reste à voir, que tout  $0 \neq F \in A[X]$  est un produit fini d'irréductibles. Par 4.2.1(ii) il existe un  $F^* \in A[X]$  primitif et  $0 \neq a \in A$  tel que  $F = aF^*$ . Comme  $A$  est factoriel, il existe irréductibles  $\pi_1, \dots, \pi_n \in A$  tels que  $a = \pi_1 \dots \pi_n \pmod{A^\times}$ . Noter que par remarque 4.2.2(i) les  $\pi_1, \dots, \pi_n$  sont premiers dans  $A[X]$ . Si  $F^*$  était irréductible dans  $A[X]$ , on aurait fini. Autrement, si  $F^*$  n'est pas irréductible dans  $A[X]$ , alors  $F^* = G * H$  avec  $G, H \in A[X]$  non-inversibles (dans  $A[X]$ ). Comme

$$1 = \mathcal{C}(F^*) = \mathcal{C}(G) \cdot \mathcal{C}(H) \quad ,$$

on trouve que  $\mathcal{C}(G), \mathcal{C}(H)$  sont inversibles, c'est-à-dire  $G, H$  sont primitives. Donc,  $\text{dg}(G) \geq 1$  (car sinon  $G = \text{const} \in A^\times$ ). De même  $\text{dg}(H) \geq 1$  et par conséquent  $\text{dg} G < \text{dg} F^*$ ,  $\text{dg} H < \text{dg} F^*$ . La décomposition du primitif  $F^*$  en deux primitifs de degré plus petit stoppe après un nombre fini d'étapes, arrivant à une décomposition par irréductibles. □

### Remarques & Exemples

- (i) Par 4.1.5, tout corps  $\mathbb{K}$  est factoriel. Donc,  $\mathbb{K}[X_1, \dots, X_n]$  est factoriel.
- (ii) Par 4.1.5,  $\mathbb{Z}$  est factoriel. Donc  $\mathbb{Z}[X_1, \dots, X_n]$  est factoriel.
- (iii) Soit  $p \in \mathbb{Z}$  premier et  $P \in \mathbb{Z}[X]$  tel que sa réduction  $\bar{P}$  modulo  $p$  est irréductible. Alors l'idéal

$$\mathfrak{M} := \langle p, P \rangle := p \cdot \mathbb{Z}[X] + P \cdot \mathbb{Z}[X]$$

est maximal dans  $\mathbb{Z}[X]$ . Vraiment,

$$\mathbb{Z}[X]/\mathfrak{M} \stackrel{\substack{1.2.14 \& \\ 1.2.5(1)}}{\cong} \underbrace{\mathbb{Z}[X]/p\mathbb{Z}[X]}_{\substack{\cong (\mathbb{Z}/p\mathbb{Z})[X] \\ \text{par 3.2.11}}} \Big/ \langle \bar{P} \rangle \cong \underbrace{\mathbb{F}_p[X]/\langle \bar{P} \rangle}_{\substack{\text{corps} \\ \text{par lemme 5.1.7}}}$$

où on a utilisé le fait que  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  est un corps. Donc, par 1.2.18  $\mathfrak{M}$  est maximal dans  $\mathbb{Z}[X]$ .

- (iv) Soit  $A$  un anneau intègre et  $P \in A[X]$  irréductible. Alors,  $P$  est soit de degré  $\leq 1$  soit de degré plus grand que 1 et sans racines.

**Preuve :** Supposer  $\text{dg}(P) \geq 2$  et  $P$  irréductible. Si  $P$  avait la racine  $x \in A$ , alors par 3.1.14 il se décomposerait comme  $P = Q * (X - x)$ , où  $\text{dg}(Q) \geq 1$ . Par 3.1.12  $Q$  et  $(X - x)$  ne sont pas inversibles, une contradiction à l'irréductibilité de  $P$ .

- (v) L'inverse de (iv) n'est pas forcément vrai : Le polynôme  $(X^2 + 1) * (X^2 + 2) \in \mathbb{R}[X]$  ne possède pas de racines dans  $\mathbb{R}$  mais est réductible.

Similairement, le polynôme  $4X \in \mathbb{Z}[X]$  de degré 1 est réductible, car 2 et  $2X$  sont polynômes dans  $\mathbb{Z}[X]$  non-inversibles.

Le polynôme 6 n'est pas irréductible, le polynôme 3 est irréductible.

- (vi) Si  $\mathbb{K}$  est un corps, alors tout polynôme  $P \in \mathbb{K}[X]$  de degré 1 est irréductible et tout polynôme de degré 0 inversible. En particulier, la factorisation d'un polynôme scindé en facteurs de degré 1, est une factorisation en irréductibles.

(vii) Soit  $A$  un anneau factoriel,  $P_1, \dots, P_n \in A[X]$  irréductibles et  $Q_1, \dots, Q_m \in A[X]$  quelconques tels que  $Q_1 \dots Q_m = P_1 \dots P_n$ . Alors, il existe une partition  $\{1, \dots, n\} = \bigsqcup_{i=1}^m I_i$  telle que  $Q_i = \prod_{j \in I_i} P_j$  de multiplication par inversibles près. Cela est simplement un cas spécial de 4.1.8, appliqué à l'anneau factoriel  $A[X]$ .

#### 4.2.8 Lemme : Division euclidienne dans $\mathbb{K}[X]$

Soit  $\mathbb{K}$  un sous-corps du corps  $\mathbb{L}$ . Alors, si  $A, B \in \mathbb{K}[X]$  et  $Q, R \in \mathbb{L}[X]$  sont tels que  $A = QB + R$  et  $\text{dg}(R) < \text{dg}(B)$  ou  $R = 0$ , alors  $Q, R \in \mathbb{K}[X]$ .

**Preuve :** Noter que par 3.2.12  $\mathbb{K}[X]$  et  $\mathbb{L}[X]$  sont anneaux euclidiens avec division euclidienne unique et  $\mathbb{K}[X] \subseteq \mathbb{L}[X]$ , avec la même valuation  $\text{val}() := \text{dg}()$ . Donc, l'affirmation est juste un cas spécial de lemme 1.1.15 sur anneaux euclidiens. □

#### 4.2.9 Lemme : Changement de variables dans polynômes

Soit  $A$  un anneau commutatif et  $P, Q \in A[X]$ . Supposer que  $Q$  est inversible dans  $A[X]$  par rapport à la composition, c'est-à-dire il existe un  $Q^{-1} \in A[X]$  tel que  $Q(Q^{-1}(X)) = Q^{-1}(Q(X)) = X$ . Alors :

1.  $P(X)$  est inversible par rapport à la multiplication ssi  $P(Q(X))$  est également.
2.  $P(X)$  est irréductible ssi  $P(Q(X))$  est irréductible.

**Preuve :**

1. Supposer que  $P(X) * R(X) = 1$  pour un  $R \in A[X]$ . Alors  $P(Q(X)) * R(Q(X)) = (P * R)(Q(X)) = 1$ . Inversement, si  $P(Q(X)) * R(X) = 1$ , alors  $P(X) * R(Q^{-1}(X)) = (P(Q) * R)(Q^{-1}(X)) = 1$ .
2. Supposons que  $P$  est irréductible et  $P(Q) = P_1 * P_2$  pour deux  $P_1, P_2 \in A[X]$ . Alors,  $P = P_1(Q^{-1}) * P_2(Q^{-1})$  et donc  $P_i(Q^{-1})$  est inversible pour exactement un  $i \in \{1, 2\}$ . Par (1) on sait que  $P_i$  est inversible pour exactement un  $i \in \{1, 2\}$ . De même façon pour l'autre direction. □

#### Exemples

- (i) Un polynôme  $P(X) \in A[X]$  est inversible (irréductible) ssi  $P(X+a)$  est inversible (irréductible), où  $a \in A$  est quelconque.
- (ii) Si  $\mathbb{K}$  est un corps et  $\lambda \in \mathbb{K} \setminus \{0\}$ , alors  $P(X) \in \mathbb{K}[X]$  est inversible (irréductible) ssi  $P(\lambda X)$  est inversible (irréductible).

#### 4.2.10 Le critère d'Eisenstein pour l'irréductibilité dans $\mathbb{Q}[X]$

1. Si  $P \in \mathbb{Z}[X]$  est de degré  $\geq 1$  et réductible dans  $\mathbb{Q}[X]$ , alors il existe des éléments  $Q, R \in \mathbb{Z}[X]$  de degrés strictement positifs tels que  $P = Q * R$ . En particulier,  $P$  est réductible dans  $\mathbb{Z}[X]$ .
2. Soit  $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$  de degré  $n \geq 1$  et  $p \in \mathbb{P}$  premier. On suppose que :
  - (i)  $p$  ne divise pas  $a_n$ .
  - (ii)  $p$  divise  $a_0, \dots, a_{n-1}$ .
  - (iii)  $p^2$  ne divise pas  $a_0$ .

Alors,  $P$  est irréductible dans  $\mathbb{Q}[X]$ . On appelle ce critère d'irréductibilité **critère d'Eisenstein**.

3. Si  $p \in \mathbb{P}$  est premier, alors le polynôme  $P(X) := X^{p-1} + \dots + X^1 + X^0$  est irréductible dans  $\mathbb{Q}[X]$ .

**Preuve :**

1. Supposons que  $P \in \mathbb{Z}[X]$  est réductible dans  $\mathbb{Q}[X]$ . Quitter à remplacer  $P$  par  $P/\mathcal{C}(P) \in \mathbb{Z}[X]$ , on peut supposer que  $P$  est primitif, c'est-à-dire  $\mathcal{C}(P) = 1$ . Il existe deux  $U, V \in \mathbb{Q}[X]$  de degré  $\geq 1$  tels que  $P = U * V$ . Soient  $a, b \in \mathbb{Z}$  tels que  $aU, bV \in \mathbb{Z}[X]$ . Alors

$$\mathcal{C}(aU)\mathcal{C}(bV) = \mathcal{C}(abU * V) = \mathcal{C}(abP) = ab\mathcal{C}(P) = ab \quad . \quad (4.2.10.1)$$

Par conséquence

$$P = \frac{1}{ab}(aU) * (bV) \stackrel{(4.2.10.1)}{=} \underbrace{\frac{aU}{\mathcal{C}(aU)}}_{\in \mathbb{Z}[X]} * \underbrace{\frac{bV}{\mathcal{C}(bV)}}_{\in \mathbb{Z}[X]} \quad .$$

2. Supposons que  $P$  est réductible dans  $\mathbb{Q}[X]$ , alors par (1) il existe polynômes  $Q, R \in \mathbb{Z}[X]$  de degrés strictement positifs tels que  $P = Q * R$ . Considérons la réduction des polynômes par  $p$ , c'est-à-dire le morphisme d'anneaux

$$\pi : \mathbb{Z}[X] \rightarrow \underbrace{(\mathbb{Z}/p\mathbb{Z})}_{\mathbb{F}_p}[X] \quad , \quad \sum_i b_i X^i \mapsto \bar{b}_i X^i \quad .$$

On a

$$\pi(P) = \sum_{i=1}^n \bar{a}_i X^i \stackrel{(ii)}{=} \bar{a}_n X^n \quad ,$$

avec  $\bar{a}_n \neq 0$  par hypothèse (i). En particulier  $\text{dg}(\pi(P)) = \text{dg}(P)$  et donc

$$\text{dg}(Q) + \text{dg}(R) = \text{dg}(Q * R) = \text{dg}(P) = \text{dg}(\pi(P)) = \text{dg}(\pi(Q) * \pi(R)) = \text{dg}(\pi(Q)) + \text{dg}(\pi(R)) \quad , \quad (4.2.10.2)$$

où on a utilisé le fait que  $\mathbb{Z}$  et  $\mathbb{F}_p$  sont intègres. Comme  $\text{dg}(\pi(Q)) \leq \text{dg}(Q)$  et  $\text{dg}(\pi(R)) \leq \text{dg}(R)$ , on conclut de (4.2.10.2) que

$$\text{dg}(\pi(Q)) = \text{dg}(Q) \quad \wedge \quad \text{dg}(\pi(R)) = \text{dg}(R) \quad . \quad (4.2.10.3)$$

Noter que  $\bar{a}_n X^n = \bar{a}_n X * \dots * X$  donne une décomposition de  $\pi(P)$  en irréductibles dans  $\mathbb{F}_p$ . Par 4.1.5(i) et 4.2.7 on sait que  $\mathbb{F}_p[X]$  est factoriel. Par l'unicité de la décomposition en produit d'irréductibles dans  $\mathbb{F}_p[X]$ , on a  $\pi(Q) = \bar{q} X^\varkappa$  et  $\pi(R) = \bar{r} X^\rho$  pour quelques  $\bar{q}, \bar{r} \in \mathbb{F}_p$  et  $\varkappa := \text{dg}(Q) \geq 1$ ,  $\rho := \text{dg}(R) \geq 1$ . Donc, si  $Q = \sum_{i=0}^{\varkappa} q_i X^i$  et  $R = \sum_{i=0}^{\rho} r_i X^i$ , il faut que  $p$  divise  $q_0, \dots, q_{\varkappa-1}$  et  $r_0, \dots, r_{\rho-1}$ . Comme  $a_0 = q_0 r_0$ , on conclut que  $p^2$  divise  $a_0$ , une contradiction à l'hypothèse (iii).

3. L'irréductibilité de  $P(X)$  est par lemme 4.2.9 équivalente à l'irréductibilité de  $A(X) := P(X + 1)$ . On considère  $\mathbb{Q}[X]$  plongé dans  $\mathbb{Q}[[X]]$ . Alors

$$P(X) = \sum_{i=0}^{p-1} X^i = \frac{X^p - 1}{X - 1}$$

et donc

$$A(X) = \frac{(X + 1)^p - 1}{X} = \sum_{k=1}^p \binom{p}{k} X^{k-1} \in \mathbb{Z}[X] \quad .$$

On voit que  $p$  divise  $\binom{p}{k}$  pour tout  $k \in \{1, \dots, p-1\}$ , ne divise pas  $\binom{p}{p}$  et que  $p^2$  ne divise pas  $\binom{p}{1}$ . Donc,  $A \in \mathbb{Z}[X]$  satisfait les hypothèses de (2), d'où  $P$  est irréductible dans  $\mathbb{Q}[X]$ . □

**Exemples**

- (i) Le polynôme  $P(X) := 3X^{100} + 2X + 2 \in \mathbb{Z}[X]$  est irréductible dans  $\mathbb{Q}[X]$ , comme le premier  $p := 2$  satisfait les hypothèses de 4.2.10(2). De plus,  $P$  est primitif dans  $\mathbb{Z}[X]$  et donc par 4.2.6(3) aussi irréductible dans  $\mathbb{Z}[X]$ .

**4.2.11 Le critère d'Eisenstein pour le cas général**

Soit  $A$  un anneau factoriel et  $P(X) = a_0 + \dots + a_{n-1}X^{n-1} + X^n \in A[X]$ . Supposer que  $\pi \in A$  est irréductible tel que :

- $\pi$  divise les  $a_0, \dots, a_{n-1}$ .
- $\pi^2$  ne divise pas  $a_0$ .

Alors,  $P(X)$  est irréductible.

**4.2.12 Exemple : Irréductibilité de  $X^2 - a$** 

Soit  $A$  un anneau intègre et  $a \in A$ . Alors,  $X^2 - a \in A[X]$  est irréductible ssi  $a$  n'est pas un carré dans  $A$ .

**Preuve :**

**Direction "⇒" :** Supposer  $a = b^2$  pour un  $b \in A$ . Alors  $X^2 - a = (X - b) * (X + b)$ , avec  $X - b$  et  $X + b$  non-inversibles. Donc,  $X^2 - a$  n'est pas irréductible.

**Direction "⇐" :** Soit  $X^2 - a = QP$  pour quelques  $Q, P \in A[X]$ . Notons  $Q = \sum_i Q_i X^i$  et  $P = \sum_i P_i X^i$ . Alors, dans le cas  $Q = \text{const}$  on a fini, car cela implique  $Q_0 P_2 = 1$  et donc  $Q \in A[X]^\times$ . Le cas  $P = \text{const}$  est similaire. Dans le cas  $\text{dg}(Q) = q = \text{dg}(P)$ , c'est-à-dire

$$X^2 - a = (Q_0 + Q_1 X) * (P_0 + P_1 X) = Q_1 P_1 X^2 + (Q_1 P_0 + Q_0 P_1) X + Q_0 P_0 \quad ,$$

on trouve  $Q_1 \in A^\times$  et donc

$$P_0 = -Q_0 \frac{P_1}{Q_1} = -Q_0 P_1^2 \quad .$$

Donc  $a = -Q_0 P_0 = -Q_0^2 P_1^2$ , une contradiction.

□

## 5 Extensions de corps

### 5.1 Préliminaires

#### 5.1.1 Définition: Extension d'un corps

Soient  $\mathbb{K}, \mathbb{L}$  corps. Si  $K \hookrightarrow \mathbb{L}$ , on identifie souvent  $\mathbb{K}$  à son image dans  $\mathbb{L}$ . On appelle donc  $\mathbb{K}$  un **sous-corps** de  $\mathbb{L}$  et  $\mathbb{L}$  une **extension** de  $\mathbb{K}$ . On note souvent  $\mathbb{L}/\mathbb{K}$  pour  $\mathbb{L}$  comme extension de  $\mathbb{K}$ . Le corps  $\mathbb{L}$  peut être considéré comme  $\mathbb{K}$ -espace vectoriel. On note  $[\mathbb{L} : \mathbb{K}]$  sa dimension et on l'appelle le **degré** de l'extension  $\mathbb{L}/\mathbb{K}$ .

On dit que  $\mathbb{L}/\mathbb{K}$  est de **degré fini**  $n$  si  $n := [\mathbb{L} : \mathbb{K}] < \infty$ . Si  $\mathbb{L}$  est lui-même un sous-corps du corps  $\mathbb{E}$ , alors  $\mathbb{E}/\mathbb{K}$  est de degré fini ssi  $\mathbb{L}/\mathbb{K}$  et  $\mathbb{E}/\mathbb{L}$  sont de degré fini. Dans ce cas on a

$$[\mathbb{E} : \mathbb{K}] = [\mathbb{E} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}] .$$

#### Exemples & Remarques

- (i)  $\mathbb{C}$  est une extension de  $\mathbb{R}$  de degré 2.
- (ii) Pour deux corps  $\mathbb{K} \subseteq \mathbb{L}$  on a  $[\mathbb{L} : \mathbb{K}] = 1$  ssi  $\mathbb{K} = \mathbb{L}$ .
- (iii) Si  $A, B \in \mathbb{K}[X]$  et  $Q \in \mathbb{L}[X]$  sont polynômes tels que  $A = Q * B$ , alors  $Q \in \mathbb{K}[X]$  (voir 4.2.8).

#### 5.1.2 Lemme : Polynômes premiers entre eux

Soit  $\mathbb{K}$  un sous-corps du corps  $\mathbb{L}$ . Alors, deux polynômes  $P, Q \in \mathbb{K}[X]$  sont premiers entre eux dans  $\mathbb{K}[X]$  ssi ils sont premiers entre eux dans  $\mathbb{L}[X]$ .

**Preuve :** Se rappeler que  $\mathbb{K}[X]$  est factoriel et principal. Par Bézout (remarque 4.1.9(viii)) on a  $\text{pgcd}(P, Q) = 1$  dans  $\mathbb{K}[X]$  ssi  $\langle P, Q \rangle = \mathbb{K}[X]$ , c'est-à-dire  $A * P + B * Q = 1$  pour quelques  $A, B \in \mathbb{K}[X]$ . Donc, si  $\text{pgcd}(P, Q) = 1$  dans  $\mathbb{K}$ , l'identité  $A * P + B * Q = 1$  reste valable dans  $\mathbb{L}[X]$ , donc  $P, Q$  sont premiers entre eux aussi dans  $\mathbb{L}[X]$ .

D'autre part, l'identité  $A * P + B * Q = 1$  se traduit en : La classe  $\bar{P}$  de  $P$  dans  $V := \mathbb{K}[X]/\langle Q \rangle$  est inversible. Noter que par 3.2.13,  $V$  est un  $\mathbb{K}$ -espace vectoriel munit de la base  $\bar{X}^0, \dots, \bar{X}^{m-1}$ , où  $m := \text{dg}(Q)$ . Donc,  $\bar{P}$  est inversible ssi l'opérateur  $\mathbb{K}$ -linéaire  $V \rightarrow V$  donné par  $\bar{R} \mapsto \bar{P} * \bar{R}$ , est inversible, c'est-à-dire sa matrice  $(p_{ij})_{i,j=0}^{m-1}$  par rapport à la base  $\bar{X}^0, \dots, \bar{X}^{m-1}$  possède déterminante non-nulle. Noter qu'elle est donnée par

$$\bar{P} * \bar{X}^j = \sum_{i=0}^{m-1} p_{ji} \cdot \bar{X}^i, \quad j \in \{0, \dots, m-1\} .$$

Si on passe à l'espace  $V' := \mathbb{L}[X]/\langle Q \rangle$ , la matrice de  $(\bar{R} \mapsto \bar{P} * \bar{R})$  reste la même. Donc, si  $P, Q$  sont premiers entre eux dans  $\mathbb{L}[X]$ , alors  $\det(p_{ij})_{i,j} \neq 0$  et donc inversement  $P, Q$  sont premiers entre eux dans  $\mathbb{K}$ . □

#### 5.1.3 Lemme : Caractéristique d'un anneau intègre

Soit  $A$  un anneau non-trivial intègre et  $\chi : \mathbb{Z} \rightarrow A$  le (seule) morphisme d'anneaux (uniquement défini par  $1_{\mathbb{Z}} \mapsto 1_A$ ). Alors,  $\ker \chi = p\mathbb{Z}$  pour un  $p \in \{0\} \cup \mathbb{P}$ .

**Preuve :** C'est facile à voir que  $\chi$  est vraiment un morphisme d'anneaux. Donc  $\ker(\chi)$  est un sous-groupe de  $\mathbb{Z}$  et donc de la forme  $\ker(\chi) = p\mathbb{Z}$  pour un  $p \in \mathbb{N}_0$ . Par définition d'un anneau non-trivial  $0_A \neq 1_A$ , donc  $\ker(\chi) \neq \mathbb{Z}$ . Par le théorème d'isomorphismes pour anneaux, on sait que  $\mathbb{Z}/\ker(\chi)$  se injecte dans  $A$ , et est donc lui-même intègre. Par remarque 1.2.15(ii)  $\ker(\chi)$  est premier dans  $\mathbb{Z}$ . Donc,  $p = 0$  ou  $p$  est premier. □

**Remarques**

- (i) On appelle  $p$  la **caractéristique** de  $A$ . Si  $p > 0$ , il est l'ordre de l'unité  $1_A$  dans le groupe additive  $(A, +)$ . Si  $p = 0$ , l'ordre de  $1_A$  est infinie.
- (ii) Si  $\mathbb{K}$  est un corps, alors son caractéristique est 0 ou premier.
- (iii) La caractéristique des  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  est 0.
- (iv) La caractéristique du corps  $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$  est 2.
- (v) Par 5.5.1 l'anneau  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  est un corps ssi  $p$  est premier. En ce cas, il est de caractéristique  $p$ .
- (vi) Si  $A$  n'était pas intègre, alors sa caractéristique n'est pas forcément première ou zéro. Par exemple, tout anneau de la forme  $\mathbb{Z}/n\mathbb{Z}$ , où  $n \in \mathbb{N}$ , est de caractéristique  $n$ .

**5.1.4 Définition: Corps engendré**

Soit  $B$  un anneau et  $A$  un sous-anneau de  $B$ . Pour éléments  $x_1, \dots, x_n \in B$  on pose

$$A[x_1, \dots, x_n] := \{P(x_1, \dots, x_n) : P \in A[X_1, \dots, X_n]\} .$$

Alors,  $A[x_1, \dots, x_n]$  est le plus petit sous-anneau de  $B$  contenant  $A$  et les éléments  $x_1, \dots, x_n$ . Si  $\mathbb{K}$  est un sous-corps du corps  $\mathbb{L}$  et  $x_1, \dots, x_n \in \mathbb{L}$ , on note  $\mathbb{K}(x_1, \dots, x_n)$  le plus petit corps contenant l'anneau  $\mathbb{K}[x_1, \dots, x_n]$ . Il est exactement le corps des fractions de  $\mathbb{K}[x_1, \dots, x_n]$  (voir 2.1.20) et on a

$$\mathbb{K} \hookrightarrow \mathbb{K}[x_1, \dots, x_n] \hookrightarrow \mathbb{K}(x_1, \dots, x_n) \hookrightarrow \mathbb{L} .$$

où le diagramme ci-dessous commute :

$$\begin{array}{ccc}
 \mathbb{K} & \xleftrightarrow{\quad} & \mathbb{K}[x_1, \dots, x_n] \\
 \uparrow & \nearrow & \downarrow \\
 \mathbb{L} & \xleftarrow{\quad} & \mathbb{K}(x_1, \dots, x_n)
 \end{array}$$

**5.1.5 Éléments algébriques**

Soit  $\mathbb{K}$  un sous-corps du corps  $\mathbb{L}$ . Pour un  $x \in \mathbb{L}$  fixe, on considère le morphisme de  $\mathbb{K}$ -algèbres

$$\varkappa : (\mathbb{K}[X], +, *) \rightarrow (\mathbb{L}, +, \cdot) , \quad P(X) \mapsto P(x) .$$

Alors, il y a équivalence entre

1. L'image

$$\mathbb{K}[x] := \text{image}(\varkappa) = \left\{ \sum_{i=0}^n p_i \cdot x^i : p_i \in \mathbb{K}, n \in \mathbb{N}_0 \right\}$$

est un corps, c'est-à-dire  $\mathbb{K}[x] = \mathbb{K}(x)$ .

2.  $\dim_{\mathbb{K}} \mathbb{K}[x] < \infty$ .
3. Il existe un  $P \in \mathbb{K}[X]$  non-constant tel que  $P(x) = 0$ .
4.  $\ker \varkappa \neq \{0\}$ .

En tout cas, on dit que  $x$  est **algébrique** sur  $\mathbb{K}$ . On appelle

$$\text{dg}_{\mathbb{K}}(x) := \dim_{\mathbb{K}} \mathbb{K}[x]$$

le **degré** de  $x$  sur  $\mathbb{K}$ . Noter que  $\mathbb{K}[X]$  est par 3.2.5 principal, donc  $\ker(\varkappa) = \langle P \rangle = \mathbb{K}[X] * P$  pour un certain  $0 \neq P \in \mathbb{K}[X]$ . Comme  $\mathbb{K}[x]$  est un corps et  $\mathbb{K}[X]/\ker(\varkappa) \cong \mathbb{K}[x]$ , on sait par 1.2.18 que  $\ker(\varkappa)$  est un idéal



maximal dans  $\mathbb{K}[X]$ . En particulier, par 1.2.20  $\ker(\varkappa)$  est premier et donc  $P$  premier dans  $\mathbb{K}[X]$ . En particulier,  $P$  est irréductible dans  $\mathbb{K}[X]$ . Si on suppose  $P$  unitaire, alors  $P$  est l'unique polynôme<sup>28</sup> de plus petit degré, nul en  $x$ , appelé le **polynôme minimal** de  $x$  sur  $\mathbb{K}$  et noté  $P_x$ . Il est aussi caractérisé comme étant le seul polynôme irréductible dans  $\mathbb{K}[X]$ , unitaire et nul en  $x$ .

Par 3.2.13,  $\mathbb{K}[X]/\langle P_x \rangle$  est un  $\mathbb{K}$ -espace vectoriel de dimension égale à  $\text{dg}(P_x)$ , donc

$$\text{dg}(P_x) = \text{dg}_{\mathbb{K}}(x) \quad .$$

On dit une extension  $\mathbb{L}$  de  $\mathbb{K}$  **algébrique** si tout élément  $x \in \mathbb{L}$  est algébrique sur  $\mathbb{K}$ .

### Remarques & Exemples :

- (i) Soit  $\mathbb{K} := \mathbb{Q}$  et  $\mathbb{L} := \mathbb{C}$ . Alors, toute  $n$ -ième racine  $x$  de l'unité dans  $\mathbb{C}$  est algébrique sur  $\mathbb{Q}$ , comme elle annule le polynôme  $X^n - 1$ . En particulier, l'élément  $x := e^{2\pi i/n}$ , avec  $n \in \mathbb{N}$ , est algébrique sur  $\mathbb{Q}$ . Mais pour  $n \geq 2$ , le polynôme  $X^n - 1$  n'est pas son polynôme minimal, car  $X^n - 1 = (X - 1)(X^{n-1} + \dots + X + 1)$  est produit de deux non-inversibles, donc réductible. En fait, comme on verra dans 5.5.6, son polynôme minimal est donné par le  $n$ -ième polynôme cyclotomique et

$$\text{dg}_{\mathbb{Q}}(e^{2\pi i/n}) = \varphi(n) \quad ,$$

où  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  est l'indicatrice d'Euler, donnée par

$$\varphi(n) := |\{m \in \{1, \dots, n\} : \text{pgcd}(m, n) = 1\}| \quad . \quad (5.1.5.1)$$

- (ii) Si  $\mathbb{L}$  est une extension de  $\mathbb{K}$  de degré fini  $n = [\mathbb{L} : \mathbb{K}]$ , alors elle est algébrique et tout  $x \in \mathbb{L}$  est algébrique sur  $\mathbb{K}$  avec degré  $\text{dg}_{\mathbb{K}}(x) \leq n$ .
- (iii) Soient  $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{E}$  trois corps. Alors, l'extension  $\mathbb{E}/\mathbb{K}$  est algébrique ssi les extensions  $\mathbb{L}/\mathbb{K}$  et  $\mathbb{E}/\mathbb{L}$  sont algébriques.
- (iv) Soient  $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{E}$  trois corps. Alors, si  $x \in \mathbb{E}$  est algébrique sur  $\mathbb{K}$ , il est aussi algébrique sur  $\mathbb{L}$ .
- (v) Soient  $\mathbb{K} \subseteq \mathbb{L}$  deux corps et  $x_1, \dots, x_n \in \mathbb{L}$  algébriques sur  $\mathbb{K}$ . Alors  $\mathbb{K}[x_1, \dots, x_n]$  est aussi un corps, en fait une extension de  $\mathbb{K}$  de degré fini. Cela suit de la décomposition

$$\mathbb{K} \subseteq \mathbb{K}[x_1] \subseteq \mathbb{K}[x_1, x_2] \subseteq \dots \subseteq \mathbb{K}[x_1, \dots, x_n] \subseteq \mathbb{L}$$

et une argumentation de récurrence.

- (vi) Soient  $\mathbb{K} \subseteq \mathbb{L}$  deux corps. Alors, l'ensemble des éléments algébriques de  $\mathbb{L}$  sur  $\mathbb{K}$  est un sous-corps de  $\mathbb{L}$ , appelé la **clôture algébrique de  $\mathbb{K}$  dans  $\mathbb{L}$** .

#### 5.1.6 Lemme sur la dérivée du polynôme minimal

Soit  $\mathbb{K}$  un sous-corps du corps  $\mathbb{L}$  et  $x \in \mathbb{L}$  algébrique sur  $\mathbb{K}$ , avec polynôme minimal  $P_x \in \mathbb{K}[X]$ . Soit  $P'_x := \frac{dP_x}{dX}$  la dérivée de  $P_x$ . Alors, il y a équivalence entre :

1.  $x$  n'est pas racine simple de  $P_x$  dans  $\mathbb{L}[X]$ .
2.  $P'_x(x) = 0$ .
3.  $P'_x \equiv 0$ .
4.  $P_x(X) = Q(X^p)$  pour un  $Q \in \mathbb{K}[X]$ , où  $p \in \mathbb{N}$  est la caractéristique non-nulle de  $\mathbb{K}$ .
5.  $\text{pgcd}(P_x, P'_x) \neq 1$  (se rappeler à 5.1.2).

#### Preuve :

1  $\Leftrightarrow$  2 : Cas spécial de remarque 3.1.15(ii).

2  $\Leftrightarrow$  3 : Supposons  $P'_x(x) = 0$ , alors par définition de  $P_x$ ,  $P_x$  divise  $P'_x$ . Cela est possible si et seulement si  $P'_x \equiv 0$ , car sinon,  $\text{dg}(P'_x) \geq \text{dg}(P_x)$ , une contradiction!

---

28. Voir aussi 3.1.12(2).

3  $\Rightarrow$  4 : Noter que comme  $x$  est algébrique,  $P_x \neq 0$  et donc  $P_x \neq \text{const.}$  Supposons  $P'_x \equiv 0$ . Cela est possible seulement si la caractéristique  $p$  de  $\mathbb{K}$  est inégale à zéro (c'est-à-dire  $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{K}$ ). Si  $P_x$  est de la forme

$$P_x = X^n + p_1 \cdot X^{n-1} + \cdots + p_n \cdot X^0 \quad ,$$

alors  $P'_x$  possède la forme

$$P'_x = n \cdot X^{n-1} + (n-1) \cdot p_1 \cdot X^{n-2} + \cdots + 1 \cdot p_{n-1} \cdot X^0 \quad .$$

Donc, il faut que  $p \mid n$  et  $p \mid j$  pour chaque  $j \in \{1, \dots, n-1\}$  tel que  $p_j \neq 0$ . Donc,  $n = s_n \cdot p$  et quand  $p_j \neq 0$ ,  $j = s_j \cdot p$  avec  $s_n, s_j \in \mathbb{N}$ . Donc

$$P_x = (X^p)^{s_n} + \sum_{\substack{1 \leq j \leq n-1 \\ p_j \neq 0}} p_j \cdot (X^p)^{s_n - s_j} + p_n \quad ,$$

c'est-à-dire  $P_x(X) = Q(X^p)$  pour un polynôme  $Q \in \mathbb{K}[X]$ .

4  $\Rightarrow$  3 : Supposons  $P(X) = Q(X^p)$ , où  $p \in \mathbb{N}$  est la caractéristique de  $\mathbb{K}$ . Alors

$$\frac{dP}{dX} = \frac{d}{dX} Q(X^p) = \underbrace{p}_0 \cdot X^{p-1} \cdot Q'(X^p) \equiv 0 \quad .$$

4  $\Rightarrow$  5 : Si  $P'_x \equiv 0$  alors par convention  $\text{pgcd}(P_x, P'_x) = P_x$ . Mais  $P_x$  est irréductible, donc pas associé à 1.

5  $\Rightarrow$  2 : Supposer que  $Q \in \mathbb{K}[X]$  est irréductible dans  $\mathbb{K}[X]$  tel que  $Q \mid P_x$  et  $Q \mid P'_x$ . Comme  $P_x$  est irréductible dans  $\mathbb{K}[X]$ , il faut que  $Q = P_x$  (modulo  $\mathbb{K}[X]^\times$ ) et donc  $P_x \mid P'_x$ . Cela implique  $P'_x(x) = 0$ . □

### 5.1.7 Lemme : Anneaux quotients sur polynômes irréductibles

Soit  $\mathbb{K}$  un corps et  $P \in \mathbb{K}[X]$  irréductible dans  $\mathbb{K}[X]$ . Alors, l'anneau quotient  $\mathbb{K}[X]/\langle P \rangle$  est un corps, extension de  $\mathbb{K}$  de degré  $\text{dg}(P)$ .

**Preuve :** Par 3.2.13 on sait que  $\mathbb{K}[X]/\langle P \rangle$  est un  $\mathbb{K}$ -espace vectoriel de dimension  $m := \text{dg}(P) < \infty$ . Noter que

$$\mathbb{K}[X]/\langle P \rangle = \mathbb{K}[\overline{X}] := \{Q(\overline{X}) : Q \in \mathbb{K}[X]\} \quad .$$

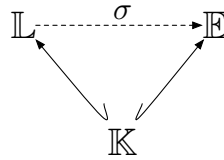
Par 4.2.7 on sait que  $\mathbb{K}[X]$  est factoriel, donc  $P$  est premier. Autrement dit,  $\langle P \rangle$  est un idéal premier dans  $\mathbb{K}[X]$ . Par remarque 1.2.15(ii),  $\mathbb{K}[X]/\langle P \rangle$  est intègre. Par 2.1.20, on peut donc supposer  $\mathbb{K}[X]/\langle P \rangle$  plongé dans son corps quotient  $\mathbb{L}$ . Alors,  $\overline{X} \in \mathbb{L}$  est un élément algébrique sur  $\mathbb{K}$  comme  $\mathbb{K}[\overline{X}]$  est de  $\mathbb{K}$ -dimension finie. Par 5.1.5  $\mathbb{K}[\overline{X}]$  est un corps. □

**Remarque :** Par la preuve on a vu que, l'élément  $\overline{X} \in \mathbb{K}[X]/\langle P \rangle$  est algébrique sur  $\mathbb{K}$  de degré  $\text{dg}(P)$  et en fait  $\mathbb{K}[X]/\langle P \rangle = \mathbb{K}[\overline{X}]$ . Supposer que  $P$  est unitaire. Alors, comme il est irréductible et satisfait  $P(\overline{X}) = \overline{0}$ , il est le polynôme minimal de  $\overline{X}$  sur  $\mathbb{K}$ .

## 5.2 Morphismes et Automorphismes

### 5.2.1 Définition: $\mathbb{K}$ -morphisme

Soit  $\mathbb{K}$  un corps et  $\mathbb{L}, \mathbb{E}$  deux corps-extensions de  $\mathbb{K}$ . Un  **$\mathbb{K}$ -morphisme de corps**  $\sigma : \mathbb{L} \rightarrow \mathbb{E}$  est un morphisme de corps qui rend commutatif le triangle :



Dans un certain façon,  $\sigma$  est l'identité sur  $\mathbb{K}$ . En cas que  $\mathbb{L} = \mathbb{E}$  et  $\sigma : \mathbb{L} \rightarrow \mathbb{L}$  est bijective, on appelle  $\sigma$  un  **$\mathbb{K}$ -automorphisme de corps** de  $\mathbb{L}$ .

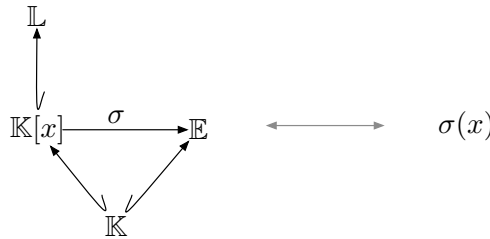
### 5.2.2 Lemme sur $\mathbb{K}$ -automorphismes de corps

Soit  $\mathbb{K}$  un corps et  $\mathbb{L}$  une extension de  $\mathbb{K}$  de degré fini. Alors, tout  $\mathbb{K}$ -morphisme de corps  $\mathbb{L} \rightarrow \mathbb{L}$  est bijective, c'est-à-dire un  $\mathbb{K}$ -automorphisme de corps.

**Preuve :** Par hypothèse  $\mathbb{L}$  est un  $\mathbb{K}$ -espace vectoriel de dimension finie. Tout  $\mathbb{K}$ -morphisme de corps est un opérateur  $\mathbb{K}$ -linéaire de  $\mathbb{L}$  dans lui même. Comme morphisme de corps, il est injective et donc bijective.  $\square$

### 5.2.3 Théorème : Éléments algébriques et $\mathbb{K}$ -morphisms $\mathbb{K}[x] \rightarrow \mathbb{E}$

Soient  $\mathbb{L}, \mathbb{E}$  deux extensions du corps  $\mathbb{K}$ . Si  $x \in \mathbb{L}$  est algébrique sur  $\mathbb{K}$ , alors  $\mathbb{K}[x]$  est aussi une extension de  $\mathbb{K}$ . Si  $P_x \in \mathbb{K}[X]$  est le polynôme minimal de  $x$ , alors les  $\mathbb{K}$ -morphisms de corps  $\sigma : \mathbb{K}[x] \rightarrow \mathbb{E}$  sont en bijection avec les racines (distinctes) de  $P_x$  dans  $\mathbb{E}$ , via l'association  $\sigma \mapsto \sigma(x)$ .



**FIGURE 15:** Sur théorème 5.2.3 : Les  $\mathbb{K}$ -morphisms de corps  $\sigma : \mathbb{K}[x] \rightarrow \mathbb{E}$  sont en bijection avec les racines de  $P_x$  dans  $\mathbb{E}$ .

**Preuve :** Se rappeler que  $\mathbb{K}[X]/\langle P_x \rangle \cong \mathbb{K}[x]$ , via l'isomorphisme  $\bar{Q} \mapsto Q(x)$ . Soit  $P_x$  de la forme  $P_x = \sum_i p_i \cdot X^i$ , avec  $p_i \in \mathbb{K}$ . Soit  $\mathcal{R}_{\mathbb{E}}(P_x)$  l'ensemble des racines de  $P_x$  dans  $\mathbb{E}$ . Tout  $\mathbb{K}$ -morphisme de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$  est déterminé par son image  $\sigma(x)$ . Noter que

$$P_x(\sigma(x)) = \sum_i p_i \cdot [\sigma(x)]^i = \sum_i \underbrace{p_i}_{\sigma(p_i)} \cdot \sigma(x^i) = \sigma \left[ \sum_i p_i \cdot x^i \right] = \sigma(P_x(x)) = 0 \quad ,$$

c'est-à-dire  $\sigma(x)$  est impérativement une racine de  $P_x$  dans  $\mathbb{E}$ . L'association injective  $\sigma \mapsto \sigma(x)$  est en fait surjective dans  $\mathcal{R}_{\mathbb{E}}(P_x)$  : Pour tout  $y \in \mathbb{E}$  on peut choisir le morphisme d'anneaux  $\sigma_0 : \mathbb{K}[X] \rightarrow \mathbb{E}$  comme la *spécification*  $Q(X) \xrightarrow{\sigma_0} Q(y)$ . Si  $y \in \mathcal{R}_{\mathbb{E}}(P_x)$ , alors

$$\sigma_0(P_x) \stackrel{\text{def}}{=} P_x(y) = 0 \quad ,$$

c'est-à-dire  $\sigma_0$  passe au quotient  $\mathbb{K}[X]/\langle P_x \rangle \cong \mathbb{K}[x]$  comme le  $\mathbb{K}$ -morphisme de corps  $\sigma : \mathbb{K}[x] \rightarrow \mathbb{E}$ , donné par  $\sigma : Q(x) \mapsto Q(y)$ . En particulier  $\sigma(x) = y$ .  $\square$

### 5.2.4 Corollaire sur le nombre de $\mathbb{K}$ -morphisms de corps $\mathbb{K}[x] \rightarrow \mathbb{E}$

Soit  $\mathbb{K}$  un sous-corps du corps  $\mathbb{L}$ ,  $x \in \mathbb{L}$  algébrique sur  $\mathbb{K}$  avec polynôme minimal  $P_x \in \mathbb{K}[X]$ . Soit  $\mathbb{E}$  une deuxième extension de  $\mathbb{K}$ . Alors, le nombre des  $\mathbb{K}$ -morphisms de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$  est plus petit ou égal à  $\text{dg}_{\mathbb{K}}(x) = \text{dg}(P_x)$ , avec égalité ssi  $P_x$  est scindé dans  $\mathbb{E}[X]$  avec racines (dans  $\mathbb{E}$ ) simples.

**Preuve :** Suit de 5.2.3.

### 5.2.5 Théorème : Existence du corps de décomposition

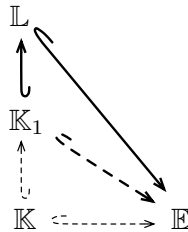
Soit  $\mathbb{K}$  un corps et  $P \in \mathbb{K}[X]$ . Alors, il existe un corps  $\mathbb{L}$  extension de  $\mathbb{K}$  de degré fini tel que :

1.  $P$  est scindé dans  $\mathbb{L}[X]$ .
2.  $\mathbb{L}$  est **minimal**, c'est-à-dire : Si  $\mathbb{E}$  est une extension de  $\mathbb{K}$  telle que  $P$  est scindé dans  $\mathbb{E}[X]$ , alors il existe un  $\mathbb{K}$ -morphisme de corps  $\mathbb{L} \rightarrow \mathbb{E}$  (pas unique). Autrement dit,  $\mathbb{L}$  se plonge<sup>29</sup> par un  $\mathbb{K}$ -morphisme dans tout corps dans lequel  $P$  est scindé.

**Preuve :** Si  $\text{dg}(P) = 0$  il n'y a rien à faire, supposons donc  $\text{dg}(P) \geq 1$ . On écrit  $P = \prod_{i=1}^r P_i$  pour irréductibles  $P_1, \dots, P_r \in \mathbb{K}[X]$ . Alors  $\text{dg}(P) = \sum_{i=1}^r \text{dg}(P_i)$ . La preuve consiste d'une récurrence décroissante en  $r \leq \text{dg}(P)$ .

Dans le cas  $r = \text{dg}(P)$ , il faut  $\text{dg}(P_i) = 1$  pour tout  $i$ , donc  $P$  est déjà scindé dans  $\mathbb{K}[X]$ , posons donc  $\mathbb{L} := \mathbb{K}$ . Dans le cas contraire, il existe un  $i$  tel que  $\text{dg}(P_i) \geq 2$ , supposons  $i = 1$ . Comme  $P_1$  est irréductible,  $\mathbb{K}_1 := \mathbb{K}[X]/\langle P_1 \rangle$  est par 5.1.7 un corps extension de  $\mathbb{K}$ , de la forme  $\mathbb{K}_1 = \mathbb{K}[x]$  avec  $x := \bar{X}$  et  $P_1$  polynôme minimal de  $x$  sur  $\mathbb{K}$  (modulo multiplication par  $\mathbb{K}^\times$ ). Si  $\mathbb{E}$  est une extension du corps  $\mathbb{K}$  telle que  $P$  est scindé dans  $\mathbb{E}$ , alors par remarque 4.2.7(vii)  $P_1$  est aussi scindé dans  $\mathbb{E}$ , donc possède dans  $\mathbb{E}$  une racine. Par théorème 5.2.3, il existe donc un  $\mathbb{K}$ -morphisme de corps  $\mathbb{K}_1 \rightarrow \mathbb{E}$ .

Noter que  $P$  se plonge dans  $\mathbb{K}_1$ , éventuellement avec une nouvelle décomposition en irréductibles, dont le nombre est en tout cas plus grand que  $r$ . Par hypothèse de récurrence,  $\mathbb{K}_1$  se plonge dans un corps  $\mathbb{L}$  extension de  $\mathbb{K}_1$ , satisfaisant propriété (2) par rapport à  $\mathbb{K}_1$ . Si  $\mathbb{E}$  est une extension du corps  $\mathbb{K}$  telle que  $P$  est scindé dans  $\mathbb{E}$ , alors on a vu l'existence d'un  $\mathbb{K}$ -morphisme de corps  $\mathbb{K}_1 \hookrightarrow \mathbb{E}$ , se traduisant en  $\mathbb{K} \subseteq \mathbb{K}_1 \subseteq \mathbb{E}$ . Donc, par hypothèse de récurrence il existe un  $\mathbb{K}_1$ -morphisme de corps  $\mathbb{L} \hookrightarrow \mathbb{E}$ , ce qui induit le  $\mathbb{K}$ -morphisme de corps  $\mathbb{L} \rightarrow \mathbb{E}$ .



**FIGURE 16:** Sur la preuve de théorème 5.2.5. Le sous-diagramme indiqué fortement commute, de même pour le diagramme *coupé*. Par conséquence, tout le diagramme commute.

Noter que  $\mathbb{L}/\mathbb{K}_1$  est par l'hypothèse de la récurrence de degré fini. Comme  $\mathbb{K}_1/\mathbb{K}$  est par construction une extension de degré fini, par 5.1.1 l'extension  $\mathbb{L}/\mathbb{K}$  est aussi une extension de degré fini. □

### Remarques

- (i) Le corps  $\mathbb{L}$  est unique de  $\mathbb{K}$ -isomorphisme de corps près.

29. Noter que tout morphisme de corps est injectif.

**Preuve :** En fait, si  $\mathbb{L}, \tilde{\mathbb{L}}$  satisfont tous les deux les affirmations ci-dessus, alors il existe  $\mathbb{K}$ -morphisme de corps  $f : \mathbb{L} \rightarrow \tilde{\mathbb{L}}$  et  $\tilde{f} : \tilde{\mathbb{L}} \rightarrow \mathbb{L}$ . Par conséquence,  $\tilde{f} \circ f : \mathbb{L} \rightarrow \mathbb{L}$  est un  $\mathbb{K}$ -morphisme de corps et par 5.2.2 un  $\mathbb{K}$ -automorphisme de corps. Par la surjectivité de  $\tilde{f} \circ f$  et l'injectivité de  $\tilde{f}$  on conclut que  $f$  est surjective, donc un  $\mathbb{K}$ -isomorphisme de corps entre  $\mathbb{L}$  et  $\tilde{\mathbb{L}}$ .

On appelle  $\mathbb{L}$  le **corps de décomposition** de  $P$  sur  $\mathbb{K}$ .

- (ii) Si  $x_1, \dots, x_n \in \mathbb{L}$  sont les racines de  $P$  dans  $\mathbb{L}$ , alors la *minimalité* de  $\mathbb{L}$  implique  $\mathbb{L} = \mathbb{K}[x_1, \dots, x_n]$ .
- (iii) La preuve ci-dessus a montré que si  $P \in \mathbb{K}[X]$  est irréductible, alors son corps de décomposition  $\mathbb{L}$  (sur  $\mathbb{K}$ ) inclut une *copie* du corps  $\mathbb{K}[X]/\langle P \rangle$ . De plus,  $P$  est polynôme minimal (de multiplication par  $\mathbb{K}^\times$  près) sur  $\mathbb{K}$  de tous ses racines dans  $\mathbb{L}$ .

### 5.2.6 Définition: Corps algébriquement clos

Un corps  $\mathbb{K}$  est dit **algébriquement clos** si tout polynôme  $P \in \mathbb{K}[X]$  est scindé dans  $\mathbb{K}[X]$ .

#### Remarques

- (i) Pour tout  $P \in \mathbb{K}[X]$ ,  $\mathbb{K}$  est le corps de décomposition de  $P$  sur  $\mathbb{K}$ .

### 5.2.7 Théorème : Existence d'une clôture algébrique

Soit  $\mathbb{K}$  un corps quelconque. Alors, il existe un corps  $\mathbb{L}$  extension de  $\mathbb{K}$  tel que  $\mathbb{L}$  est algébriquement clos. De plus, toute extension de  $\mathbb{K}$  algébriquement close est isomorphe à  $\mathbb{L}$  via un  $\mathbb{K}$ -isomorphisme de corps. On appelle ce corps  $\mathbb{L}$  la **clôture algébrique** de  $\mathbb{K}$ .

#### Exemples

- (i) La clôture algébrique de  $\mathbb{R}$  est  $\mathbb{C}$ .
- (ii) La clôture algébrique de  $\mathbb{F}_p$  est un corps infini dénombrable, contenant une *copie* du corps  $\mathbb{F}_{p^n}$  pour chaque  $n \in \mathbb{N}$ .

### 5.2.8 Définition: Polynôme séparable

Soit  $\mathbb{K}$  un corps et  $0 \neq P \in \mathbb{K}[X]$ . Alors,  $P$  est dit **séparable** si  $\text{pgcd}(P, P') = 1$ . Noter que si  $\mathbb{E}$  est une extension de  $\mathbb{K}$ , alors par 5.1.2  $\text{pgcd}(P, P') = 1$  dans  $\mathbb{K}[X]$  ssi  $\text{pgcd}(P, P') = 1$  dans  $\mathbb{E}[X]$ . Par 5.2.5 et remarque 4.2.7(vi),  $P$  est séparable ssi tous ses racines sont simples dans son corps de décomposition.

### 5.2.9 Lemme : Separabilité de polynômes irréductibles

Soit  $\mathbb{K}$  un corps et  $P \in \mathbb{K}[X]$  irréductible. Alors  $P$  est séparable ssi  $P' \neq 0$ . En particulier, si  $\mathbb{K}$  est de caractéristique 0, tout irréductible dans  $\mathbb{K}[X]$  est séparable.

**Preuve :** Supposons sans perdu de généralité que  $P$  est unitaire. Alors,  $P$  est polynôme minimal de ses racines sur  $\mathbb{K}$  dans son corps de décomposition. Par lemme 5.1.6 on a donc une équivalence entre  $P' \neq 0$  et  $\text{pgcd}(P, P') = 1$ . Evidemment, comme  $P$  est non-constant, si  $\mathbb{K}$  est de caractéristique 0 alors toujours  $P' \neq 0$ .  $\square$

### 5.2.10 Théorème d'Artin sur l'indépendance des $\mathbb{K}$ -morphisms de corps

Soit  $\mathbb{K}$  un corps avec extensions  $\mathbb{L}, \mathbb{E}$ . Notons  $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$  le  $\mathbb{E}$ -espace vectoriel des applications  $\mathbb{K}$ -linéaires de  $\mathbb{L}$  dans  $\mathbb{E}$ . Alors, les  $\mathbb{K}$ -morphisms de corps  $\mathbb{L} \rightarrow \mathbb{E}$  sont  $\mathbb{E}$ -linéairement indépendants dans  $\mathcal{L}_{\mathbb{K}}(\mathbb{E}, \mathbb{L})$ .

**Preuve :** Soient  $\sigma_1, \dots, \sigma_r : \mathbb{L} \rightarrow \mathbb{E}$   $\mathbb{K}$ -morphisms de corps distinctes et supposer qu'il existe  $a_1, \dots, a_r \in \mathbb{E} \setminus \{0\}$  tels que

$$0 = \sum_{i=1}^r a_i \cdot \sigma_i \quad . \quad (5.2.10.1)$$

On peut supposer  $r \in \mathbb{N}$  minimal (et donc  $r > 1$ ). Pour tout  $x, y \in \mathbb{L}$  on a

$$0 = \sum_{i=1}^r a_i \sigma_i(xy) = \sum_{i=1}^r a_i \sigma_i(x) \sigma_i(y) \quad .$$

En fixant  $x$ , on obtient un morphisme trivial

$$\sum_{i=1}^r a_i \sigma_i(x) \cdot \sigma_i = 0 \quad . \quad (5.2.10.2)$$

En combinant (5.2.10.1) et (5.2.10.2) on obtient

$$0 = \sigma_1(x) \cdot \sum_{i=1}^r a_i \cdot \sigma_i - \sum_{i=1}^r a_i \sigma_i(x) \sigma_i(y) = \sum_{i=2}^r [\sigma_1(x) - \sigma_i(x)] \cdot a_i \cdot \sigma_i \quad . \quad (5.2.10.3)$$

Comme les  $\sigma_1, \dots, \sigma_r$  sont distinctes, on peut choisir  $x \in \mathbb{L}$  tel que  $\sigma_1(x) \neq \sigma_2(x)$ . En ce cas, dans (5.2.10.3) on trouve une relation de dépendance  $\mathbb{E}$ -linéaire plus courte que (5.2.10.1), une contradiction à la minimalité de  $r$ .  $\square$

### 5.2.11 Corollaire sur le nombre des $\mathbb{K}$ -morphisms de corps

Soit  $\mathbb{K}$  un corps,  $\mathbb{L}, \mathbb{E}$  deux extensions de  $\mathbb{K}$ . On suppose que  $[\mathbb{L} : \mathbb{K}] < \infty$ . Alors, on a

$$\dim_{\mathbb{E}} \mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E}) = [\mathbb{L} : \mathbb{K}] \quad .$$

En particulier, il existe au maximum  $[\mathbb{L} : \mathbb{K}]$   $\mathbb{K}$ -morphisms de corps de  $\mathbb{L}$  dans  $\mathbb{E}$ .

**Preuve :** Soit  $\dim_{\mathbb{K}} \mathbb{L} =: n$  et  $l_1, \dots, l_n \in \mathbb{L}$  une  $\mathbb{K}$ -base. Toute  $f \in \mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$  est caractérisée par ses valeurs  $f(l_i) \in \mathbb{E}$ , c'est-à-dire  $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E}) \cong_{\mathbb{E}} \mathbb{E}^n$ . Une  $\mathbb{E}$ -base de  $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$  est donnée par exemple par les  $f_1, \dots, f_n \in \mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$  satisfaisant  $f_i(l_j) = \delta_{ij}$ . Par 5.2.10, les  $\mathbb{K}$ -morphisms de corps de  $\mathbb{L}$  dans  $\mathbb{E}$  forment un système  $\mathbb{E}$ -linéairement indépendant dans  $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$ .  $\square$

### 5.2.12 Lemme : Restrictions de morphismes de corps

Soient  $\mathbb{K} \hookrightarrow \mathbb{L}$  et  $\mathbb{E}$  trois corps. Supposons que  $\mathbb{L}/\mathbb{K}$  est de degré fini. Alors, l'ensemble des morphismes de corps  $\mathbb{L} \rightarrow \mathbb{E}$  égaux sur  $\mathbb{K}$ , est plus petit ou égal à  $[\mathbb{L} : \mathbb{K}]$ .

**Preuve :** Soit  $\{\sigma_i\}_{i=1}^r$  une telle famille. Alors, tout  $\sigma_i$  fait de  $\mathbb{K}$  un sous-corps de  $\mathbb{E}$  par l'injection  $\sigma_i|_{\mathbb{K}} : \mathbb{K} \hookrightarrow \mathbb{E}$ . Comme tous  $\sigma_1, \dots, \sigma_r$  sont égaux sur  $\mathbb{K}$ , cette injection est *globale* dans le contexte actuel. Par rapport à elle, tout  $\sigma_i$  est un  $\mathbb{K}$ -morphisme de corps  $\mathbb{L} \rightarrow \mathbb{E}$ . Par 5.2.11, il existe au maximum  $[\mathbb{L} : \mathbb{K}]$   $\mathbb{K}$ -morphisms de corps  $\mathbb{L} \rightarrow \mathbb{E}$ .  $\square$

### 5.3 Extensions de corps séparables

#### 5.3.1 Définition: Extension séparable

Une extension  $\mathbb{L}$  d'un corps  $\mathbb{K}$  de degré fini  $n := [\mathbb{L} : \mathbb{K}]$  est dit **séparable** s'il existe une extension  $\mathbb{E}$  de  $\mathbb{K}$  telle que le nombre des  $\mathbb{K}$ -morphisms de corps  $\mathbb{L} \rightarrow \mathbb{E}$  est égal à  $n$ .

#### 5.3.2 Lemme : Transitivité de la séparabilité d'extensions

Soient  $\mathbb{K} \hookrightarrow \mathbb{L} \hookrightarrow \mathbb{E}$  trois corps. Alors l'extension  $\mathbb{E}/\mathbb{K}$  est séparable ssi  $\mathbb{E}/\mathbb{L}$  et  $\mathbb{L}/\mathbb{K}$  sont séparables.

#### 5.3.3 Théorème : Caractérisation de la séparabilité de $\mathbb{K}[x]/\mathbb{K}$

Soit  $\mathbb{L}/\mathbb{K}$  une extension de corps et  $x \in \mathbb{L}$  algébrique sur  $\mathbb{K}$ . Alors, l'extension  $\mathbb{K}[x]/\mathbb{K}$  est séparable ssi  $x$  est racine simple de son polynôme minimal  $P_x \in \mathbb{K}[X]$ , ce qui est par 5.1.6 équivalent à la séparabilité de  $P_x$ .

#### 5.3.4 Théorème : Caractérisation de séparabilité par simplicité de racines

Soit  $\mathbb{K}$  un corps et  $\mathbb{L}$  une extension de  $\mathbb{K}$  de degré fini. Alors,  $\mathbb{L}/\mathbb{K}$  est séparable ssi tout  $x \in \mathbb{L}$  est racine simple de son polynôme minimal<sup>30</sup>  $P_x \in \mathbb{K}[X]$ , c'est-à-dire ssi tout  $\mathbb{K}[x]/\mathbb{K}$  (avec  $x \in \mathbb{L}$ ) est séparable.

**Preuve :**

**Direction “ $\Rightarrow$ ” :** Soit  $\mathbb{E}$  une extension de  $\mathbb{K}$  quelconque et  $\sigma : \mathbb{L} \rightarrow \mathbb{E}$  un  $\mathbb{K}$ -morphisme de corps. De même façon comme dans la preuve de 5.2.3, on montre que  $\sigma(x)$  est une racine de  $P_x$  dans  $\mathbb{E}$ . Par 3.1.15(ii),  $x$  est une racine simple de  $P_x$  dans  $\mathbb{L}$  ssi  $P'_x(x) \neq 0$  et par injectivité de  $\sigma$  ssi  $\sigma(P'_x(x)) \neq 0$ . Comme  $P'_x \in \mathbb{K}[X]$  et  $\sigma$  est un  $\mathbb{K}$ -morphisme de corps, on sait que  $\sigma(P'_x(x)) = P'_x(\sigma(x))$ . Donc  $x$  est simple dans  $\mathbb{L}$ , ssi  $\sigma(x)$  est simple dans  $\mathbb{E}$ .

Par 5.2.3 on sait que les racines de  $P_x$  dans  $\mathbb{E}$  sont en bijection avec les  $\mathbb{K}$ -morphisms de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$ . D'autre part,  $\text{dg}(P_x) = [\mathbb{K}[x] : \mathbb{K}] =: q$ , c'est-à-dire pour montrer que  $\sigma(x)$  est une racine simple de  $P_x$  dans  $\mathbb{E}$ , il suffit de montrer que  $P_x$  possède dans  $\mathbb{E}$  exactement  $q$  racines distinctes. Donc, il suffit à montrer qu'il existe  $q$   $\mathbb{K}$ -morphisms de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$ , pour un  $\mathbb{E}$  convenant, c'est-à-dire  $\mathbb{K}[x]/\mathbb{K}$  est séparable.

Supposons que  $\mathbb{L}/\mathbb{K}$  est séparable de degré  $n := [\mathbb{L} : \mathbb{K}]$ , c'est-à-dire il existe  $\mathbb{K}$ -morphisms de corps  $\sigma_1, \dots, \sigma_n : \mathbb{L} \rightarrow \mathbb{E}$  pour un  $\mathbb{E}$  convenant. Chaque  $\sigma_i$  induit un  $\mathbb{K}$ -morphisme de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$  par restriction  $\sigma_i|_{\mathbb{K}[x]}$ . Par 5.2.12, pour tout  $i \in \{1, \dots, n\}$ , il existe au maximum  $p := [\mathbb{L} : \mathbb{K}[x]]$  indices  $j \in \{1, \dots, n\}$  satisfaisant  $\sigma_j|_{\mathbb{K}[x]} = \sigma_i|_{\mathbb{K}[x]}$ . D'autre part, par 5.2.11 il existe au maximum  $q$  distinctes  $\mathbb{K}$ -morphisms de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$ . Comme

$$n = [\mathbb{L} : \mathbb{K}] = \underbrace{[\mathbb{L} : \mathbb{K}[x]]}_p \cdot \underbrace{[\mathbb{K}[x] : \mathbb{K}]}_q ,$$

on déduit que il existe exactement  $q$  distinctes  $\mathbb{K}$ -morphisms de corps  $\mathbb{K}[x] \rightarrow \mathbb{E}$ , chacun induit par la restriction de  $p$   $\mathbb{K}$ -morphisms de corps  $\sigma_i$ . Donc  $\mathbb{K}[x]/\mathbb{K}$  est séparable. De même façon comme dans la preuve de 5.2.12, on conclut de plus que  $\mathbb{L}/\mathbb{K}[x]$  est aussi séparable.

**Direction “ $\Leftarrow$ ” :** De même façon.

□

**Remarques :**

<sup>30</sup>. Se rappeler que par 5.1.5 tout  $x \in \mathbb{L}$  est algébrique de degré  $\leq [\mathbb{L} : \mathbb{K}]$ .

- (i) Soient  $\mathbb{K} \subseteq \mathbb{L}$  deux corps de caractéristique nulle et  $x \in \mathbb{L}$  algébrique sur  $\mathbb{K}$ . Alors, par 5.1.6 on sait que  $x$  est nécessairement racine simple de son polynôme minimal  $P_x \in \mathbb{K}[X]$ , donc par 5.3.3 l'extension  $\mathbb{K}[x]/\mathbb{K}$  est séparable.
- (ii) Cela se généralise par théorème 5.3.4 à toute extension  $\mathbb{L}/\mathbb{K}$  de degré finie : Si  $\mathbb{K}$  est de caractéristique nulle, alors  $\mathbb{L}/\mathbb{K}$  est séparable.

### 5.3.5 Théorème : Génération des extensions séparables

Soit  $\mathbb{L}/\mathbb{K}$  une extension de corps séparable de degré  $n \in \mathbb{N}$ . Alors, il existe  $x \in \mathbb{L}$  tel que  $\mathbb{L} = \mathbb{K}[x]$ .

## 5.4 Groupes de Galois

### 5.4.1 Définition: Groupe de Galois

Soit  $\mathbb{K}$  un corps et  $\mathbb{L}$  une extension de  $\mathbb{K}$ . Notons  $\text{Aut}(\mathbb{L}/\mathbb{K})$  le groupe des  $\mathbb{K}$ -automorphismes de corps de  $\mathbb{L}$ . Si  $\mathbb{L}/\mathbb{K}$  est de degré fini  $[\mathbb{L} : \mathbb{K}]$ , alors par 5.2.11 on sait que  $|\text{Aut}(\mathbb{L}/\mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]$ . Si  $|\text{Aut}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$ , l'extension  $\mathbb{L}/\mathbb{K}$  est dit **galoisienne** et  $\text{Aut}(\mathbb{L}/\mathbb{K})$  est appelé le **groupe de Galois** de  $\mathbb{L}/\mathbb{K}$ , souvent noté  $\text{Gal}(\mathbb{L}/\mathbb{K})$ .

#### Remarques

- (i) Toute extension  $\mathbb{L}/\mathbb{K}$  galoisienne est séparable.
- (ii) Par lemme 5.2.2, une extension  $\mathbb{L}/\mathbb{K}$  de degré fini est Galoisienne ssi il existe  $[\mathbb{L} : \mathbb{K}]$   $\mathbb{K}$ -morphisms de corps  $\mathbb{L} \rightarrow \mathbb{L}$ .

#### Exemples

- (i) Le corps  $\mathbb{C}$  est une extension de  $\mathbb{R}$  galoisienne de degré 2, avec

$$\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{Id}, (\text{conjugaison complexe})\} \cong \mathbb{Z}/2\mathbb{Z}$$

comme groupe de Galois.

### 5.4.2 Théorème : Correspondance galoisienne

Soit  $\mathbb{K}$  un corps et  $\mathbb{L}$  une extension de  $\mathbb{K}$  galoisienne. Pour tout sous-groupe  $H \leq \text{Gal}(\mathbb{L}/\mathbb{K})$  on note

$$\mathbb{L}^H := \{x \in \mathbb{L} \mid g(x) = x \ \forall g \in H\} \ .$$

Alors :

1. Pour tout  $H \leq \text{Gal}(\mathbb{L}/\mathbb{K})$ , l'ensemble  $\mathbb{L}^H$  est un corps satisfaisant  $\mathbb{K} \subseteq \mathbb{L}^H \subseteq \mathbb{L}$ .
2.  $\mathbb{L}^{\{\text{Id}\}} = \mathbb{L}$  et  $\mathbb{L}^{\text{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$ .
3. Soit  $\mathbb{E}$  un corps tel que  $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ . Alors  $\mathbb{L}/\mathbb{E}$  est galoisienne et on a

$$\text{Aut}(\mathbb{L}/\mathbb{E}) \leq \text{Gal}(\mathbb{L}/\mathbb{K}) \ .$$

4. La correspondance  $H \leq \text{Gal}(\mathbb{L}/\mathbb{K}) \mapsto \mathbb{L}^H$  est une bijection décroissante entre sous-groupes  $H$  de  $\text{Gal}(\mathbb{L}/\mathbb{K})$  et corps  $\mathbb{E}$  entre  $\mathbb{K}$  et  $\mathbb{L}$ . La correspondance inverse est donnée par  $\mathbb{E} \mapsto \text{Aut}(\mathbb{L}/\mathbb{E})$ .
5. Les degrés des extensions sont reliées aux ordres des sous-groups via

$$[\mathbb{L} : \mathbb{L}^H] = |H| \ , \quad [\text{Gal}(\mathbb{L}/\mathbb{K}) : H] = [\mathbb{L}^H : \mathbb{K}] \ .$$



6. Soit  $\mathbb{E}$  un corps entre  $\mathbb{K}$  et  $\mathbb{L}$ . Alors  $\text{Aut}(\mathbb{L}/\mathbb{E}) \trianglelefteq \text{Gal}(\mathbb{L}/\mathbb{K})$  ssi  $\mathbb{E}/\mathbb{K}$  est galoisienne et ssi  $g(\mathbb{E}) = \mathbb{E}$  pour tout  $g \in \text{Gal}(\mathbb{L}/\mathbb{K})$ . En ce cas on a un isomorphisme

$$\text{Aut}(\mathbb{E}/\mathbb{K}) \cong \text{Gal}(\mathbb{L}/\mathbb{K}) / \text{Aut}(\mathbb{L}/\mathbb{E}) \quad ,$$

induit via la restriction des automorphismes de  $\text{Gal}(\mathbb{L}/\mathbb{K})$  sur  $\mathbb{E}$ .

### 5.4.3 Théorème : Génération de sous-corps galoisiens

Soit  $\mathbb{L}$  un corps quelconque et  $G \leq \text{Aut}(\mathbb{L})$  un groupe fini d'automorphismes de corps  $\mathbb{L} \rightarrow \mathbb{L}$ . Alors

$$\mathbb{K} := \mathbb{L}^G := \{x \in \mathbb{L} : g(x) = x \ \forall g \in G\}$$

est un sous-corps de  $\mathbb{L}$  et  $\mathbb{L}/\mathbb{K}$  une extension galoisienne de groupe de Galois  $G$ .

### 5.4.4 Théorème : Groupe de Galois d'un polynôme

Soit  $\mathbb{K}$  un corps et  $P \in \mathbb{K}[X]$  un polynôme irréductible, séparable. Alors son corps de décomposition  $\mathbb{L}$  est une extension galoisienne. Mieux, il est la plus petite extension galoisienne de  $\mathbb{K}$  contenant le corps<sup>31</sup>  $\mathbb{K}[X]/\langle P \rangle$ . Le groupe de Galois  $\text{Gal}(\mathbb{L}/\mathbb{K})$  est dit **groupe de Galois de  $P$** .

### 5.4.5 Théorème : Action de l'extension galoisienne sur racines

Soit  $\mathbb{K}$  un corps,  $P \in \mathbb{K}[X]$  irréductible, séparable et  $\mathbb{L}$  son corps de décomposition avec groupe de Galois  $\text{Gal}(\mathbb{L}/\mathbb{K})$ . Alors,  $\text{Gal}(\mathbb{L}/\mathbb{K})$  agit fidèlement, transitivement sur les racines  $x_1, \dots, x_n$  de  $P$  dans  $\mathbb{L}$ .

**Preuve :** Soit  $n := \text{dg}(P)$  et  $x_1, \dots, x_n \in \mathbb{L}$  les racines de  $P$  dans  $\mathbb{L}$ . Noter que par 5.2.8 ils sont deux à deux inégales. Soit  $g \in \text{Gal}(\mathbb{L}/\mathbb{K})$ , alors

$$0 = g(P(x_i)) = P(g(x_i)) \quad \forall i \in \{1, \dots, n\} \quad ,$$

c'est-à-dire  $g(x_i)$  est une racine de  $P$ . Donc,  $g$  agit vraiment sur  $\{x_1, \dots, x_n\}$  comme permutation et on a un morphisme de groupes  $\text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow \text{Sym}(n)$ . Ce morphisme est injectif, car si  $g \in \text{Gal}(\mathbb{L}/\mathbb{K})$  fixe tous les racines  $x_i$ , alors il fixe tout  $\mathbb{L} = \mathbb{K}[x_1, \dots, x_n]$ , c'est-à-dire  $g = \text{Id}$ . Soit  $\text{Orb}(x_1)$  l'orbite de la racine  $x_1$  sous  $\text{Gal}(\mathbb{L}/\mathbb{K})$  et poser

$$Q(X) := \prod_{y \in \text{Orb}(x_1)} (X - y) \in \mathbb{L}[X] \quad .$$

Alors pour tout  $g \in \text{Gal}(\mathbb{L}/\mathbb{K})$  on a

$$g(Q(X)) = \prod_{y \in \text{Orb}(x_1)} (X - g(y)) = Q(X) \quad ,$$

c'est-à-dire  $Q$  a des coefficients  $\text{Gal}(\mathbb{L}/\mathbb{K})$ -invariants. Par 5.4.2 cela implique  $Q \in \mathbb{K}[X]$ . Comme  $Q \in \mathbb{K}[X]$  divise  $P \in \mathbb{K}[X]$  dans  $\mathbb{L}[X]$ , par remarque 5.1.1(iii) il divise  $P$  en fait dans  $\mathbb{K}[X]$ . Comme  $Q$  est non-inversible et  $P$  irréductible dans  $\mathbb{K}[X]$ , il faut que  $P = Q$  (modulo  $\mathbb{K}^\times$ ). En particulier,  $\text{Orb}(x_1) = \{x_1, \dots, x_n\}$ . □

**Interprétation :** Via restriction des  $\mathbb{K}$ -automorphismes de corps  $\mathbb{L} \rightarrow \mathbb{L}$  sur les racines  $x_1, \dots, x_n \in \mathbb{L}$  de  $P$ , on obtient une représentation fidèle de  $\text{Gal}(\mathbb{L}/\mathbb{K})$  comme sous-groupe transitive de  $\text{Sym}(x_1, \dots, x_n)$ .

31. Se rappeler que par remarque 5.2.5(iii) le corps de décomposition de  $P$  sur  $\mathbb{K}$  contient toujours une copie du corps  $\mathbb{K}[X]/\langle P \rangle$ .

## 5.5 Corps finis

### 5.5.1 Théorème : $\mathbb{Z}/p\mathbb{Z}$ comme corps

Soit  $n \in \mathbb{N}$ . Alors, l'anneau  $\mathbb{Z}/n\mathbb{Z}$  est un corps ssi  $n$  est un nombre premier. Le cas échéant, on note  $\mathbb{F}_n := \mathbb{Z}/n\mathbb{Z}$ .

**Preuve :** La caractéristique de l'anneau  $\mathbb{Z}/n\mathbb{Z}$  est  $n$ . Donc, si  $n$  n'était pas premier, par 5.1.3 l'anneau  $\mathbb{Z}/n\mathbb{Z}$  ne serait pas intègre, donc pas un corps. Soit inversement  $n$  premier. Alors, par la caractérisation 1.2.18, il faut montrer que l'idéal  $n\mathbb{Z}$  est maximal dans  $\mathbb{Z}$ . Supposons  $I \subseteq \mathbb{Z}$  est un idéal tel que  $n\mathbb{Z} \subsetneq I \subseteq \mathbb{Z}$ . Alors, comme sous-groupe de  $\mathbb{Z}$  il possède la forme  $m\mathbb{Z}$  pour un  $m \in \mathbb{N}$ . Comme  $n \in m\mathbb{Z}$ , il faut que  $m \mid n$ . Comme  $n$  est premier et  $m \neq n$ , il faut que  $m = 1$ , c'est-à-dire  $I = \mathbb{Z}$ . Donc,  $n\mathbb{Z}$  est maximal.  $\square$

### 5.5.2 Théorème : Caractérisation des corps finis

Soit  $p \in \mathbb{P}$  premier et  $\mathbb{K}$  un corps. Alors, les suivantes sont équivalents :

1.  $\mathbb{K}$  est fini de caractéristique  $p$ .
2.  $\mathbb{K}$  est de cardinal  $p^n$  pour un  $n \in \mathbb{N}$ .

Le cas échéant, on a :

1.  $\mathbb{K}$  est la seule extension de  $\mathbb{F}_p$  de degré  $n := [\mathbb{K} : \mathbb{F}_p]$ .
2.  $\mathbb{K}$  est le corps de décomposition de  $P(X) := X^{p^n} - X \in \mathbb{F}_p[X]$  sur  $\mathbb{F}_p$ .
3.  $\mathbb{K}/\mathbb{F}_p$  est une extension galoisienne de groupe de Galois  $\mathbb{Z}/n\mathbb{Z}$ , engendrée par le morphisme de Frobenius.

On note  $\mathbb{K} =: \mathbb{F}_{p^n}$ . Par 5.1.3, tout corps fini est donc de la forme  $\mathbb{F}_{p^n}$ , avec  $p \in \mathbb{P}$  sa caractéristique et  $n \in \mathbb{N}$ .

**Noter :** Ne pas confondre  $\mathbb{F}_q$  et  $\mathbb{Z}/q\mathbb{Z}$ , qui par 5.5.1 est seulement un corps si  $q$  est premier.

**Preuve :** Soit  $\mathbb{K}$  de cardinal  $p^n$ , alors par Fermat-Euler  $p^n \times 1 = 0$ . Par 5.1.3 la caractéristique de  $\mathbb{K}$  est un nombre premier  $q \in \mathbb{P}$ , c'est-à-dire 1 possède dans  $(\mathbb{K}, +)$  l'ordre  $q$ . Donc,  $q \mid p^n$ , ce qui implique  $p = q$ .

Inversement, soit  $\mathbb{K}$  fini de caractéristique  $p$ . Alors par définition, le morphisme d'anneaux  $\mathbb{Z} \rightarrow \mathbb{K}$ ,  $n \mapsto n_{\mathbb{K}}$  est un morphisme de noyau  $p\mathbb{Z}$ . Donc, le corps  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  s'injecte dans  $\mathbb{K}$ , c'est-à-dire  $\mathbb{K}$  est une extension de  $\mathbb{F}_p$ . Comme  $\mathbb{F}_p$ -espace vectoriel, il possède la dimension finie  $n := [\mathbb{K} : \mathbb{F}_p]$ . Donc, sa cardinalité est donnée par  $|\mathbb{K}| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p} \mathbb{K}} = p^n$ .

Sa groupe multiplicatif  $\mathbb{K}^\times$  est d'ordre  $p^n - 1$ , donc par Fermat-Euler  $x^{p^n - 1} = 1$  pour  $x \in \mathbb{K}^\times$ , c'est-à-dire

$$x^{p^n} = x \quad \forall x \in \mathbb{K} . \quad (5.5.2.1)$$

Considérons le polynôme  $P(X) := X^{p^n} - X \in \mathbb{F}_p[X]$ . Alors, sa dérivée

$$\frac{dP}{dX} = \underbrace{p^n}_{=0} X^{p^n - 1} - 1 = -1$$

est première à  $P$ , c'est-à-dire  $P$  est séparable. Donc, le corps de décomposition de  $P(X)$  doit être de cardinalité au moins  $\text{dg}(P) = p^n$ . D'autre part,  $P(X)$  est scindé dans  $\mathbb{K}$  car par (5.5.2.1) tous  $p^n$  éléments de  $\mathbb{K}$  sont racines de  $P(X)$ . Donc par 5.2.5, le corps de décomposition se plonge dans  $\mathbb{K}$  via un  $\mathbb{F}_p$ -morphisme de corps, d'où il est en fait  $\mathbb{F}_p$ -isomorphe à  $\mathbb{K}$ .

Donc,  $\mathbb{K}$  est exactement le corps de décomposition de  $P(X)$  sur  $\mathbb{F}_p$ , noté  $\mathbb{F}_{p^n}$ . L'automorphisme de Frobenius

$$F := \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n} , \quad x \mapsto x^p ,$$

(voir 1.1.16) est un élément de  $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$  d'ordre  $n$ , donc  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ .

**Preuve :** Par Fermat-Euler on a  $x^p = x$  pour tout  $x \in \mathbb{F}_p$ . Évidemment  $(xy)^p = x^p y^p$  pour tout  $x, y \in \mathbb{F}_{p^n}$ . De plus

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^k x^{p-k} = x^p + y^p$$

car  $p$  divise tout  $\binom{p}{k}$  avec  $k \in \{1, \dots, p-1\}$ . Donc  $F : x \mapsto x^p$  est un  $\mathbb{F}_p$ -morphisme de corps  $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ , donc par 5.2.2 dans  $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ . Soit  $s \in \{1, \dots, n\}$  son ordre<sup>32</sup>. Comme

$$F^n(x) = x^{p^n} \stackrel{(5.5.2.1)}{=} x \quad \forall x \in \mathbb{F}_{p^n} ,$$

il faut que  $s \mid n$ . D'autre part, par définition

$$x = \text{Id}(x) = F^s(x) = x^{p^s} \quad \forall x \in \mathbb{F}_{p^n} ,$$

c'est-à-dire le polynôme  $X^{p^s} - X$  possède au moins  $|\mathbb{F}_{p^n}| = p^n$  racines, ce qu'est seulement possible si  $s \geq n$ . Donc  $s = n$ .

Donc  $\mathbb{F}_{p^n}$  est une extension de  $\mathbb{F}_p$  galoisienne, avec groupe de Galois engendré par le morphisme de Frobenius.  $\square$

### 5.5.3 Théorème : Sous-corps de corps finis

Soient  $p, q \in \mathbb{P}$  premiers. Alors, pour  $n, m \in \mathbb{N}$  le corps  $\mathbb{F}_{q^m}$  est un sous-corps de  $\mathbb{F}_{p^n}$  ssi  $q = p$  et  $m \mid n$ .

**Preuve :**

**Direction “ $\Rightarrow$ ” :** Par théorème 5.5.2 la caractéristique des  $\mathbb{F}_{q^m}$  et  $\mathbb{F}_{p^n}$  sont  $q$  et  $p$  respectivement, donc  $q = p$ .

Par le même théorème,  $\mathbb{F}_{p^m}$  et  $\mathbb{F}_{p^n}$  sont extensions du même corps  $\mathbb{F}_p$  de degré  $m$  et  $n$  respectivement, donc par 5.1.1  $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$  divise  $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ .

**Direction “ $\Leftarrow$ ” :** Noter que par théorème 5.5.2,  $\mathbb{F}_{p^n}/\mathbb{F}_p$  est galoisienne avec groupe de Galois cyclique  $\mathbb{Z}/n\mathbb{Z}$ . Pour  $m \mid n$  il existe donc par Lagrange un (unique) sous-groupe  $H \leq \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$  d'ordre  $n/m$ . Par la correspondance galoisienne 5.4.2, il existe donc un sous-corps  $\mathbb{K}$  entre  $\mathbb{F}_p$  et  $\mathbb{F}_{p^n}$ , tel que

$$[\mathbb{K} : \mathbb{F}_p] = |\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : H| = m .$$

Par 5.5.2,  $\mathbb{K}$  est exactement  $\mathbb{F}_{p^m}$ .  $\square$

### 5.5.4 Lemme sur polynômes dans $\mathbb{F}_p[X]$

Soit  $\mathbb{F}_p$  le corps de cardinalité  $p$ . Alors, pour tout polynôme  $Q \in \mathbb{F}_p[X]$  on a

$$(Q(X))^p = Q(X^p) .$$

**Preuve :** Comme le groupe multiplicatif  $\mathbb{F}_p^\times$  est d'ordre  $p-1$ , on sait par Fermat-Euler que  $x^p = x$  pour tout  $x \in \mathbb{F}_p$ . Pour polynômes  $P_1, P_2 \in \mathbb{F}_p[X]$  on a

$$(P_1 + P_2)^p = \sum_{k=0}^p \binom{p}{k} (P_1)^k (P_2)^{p-k} = (P_1)^p + (P_2)^p ,$$

car  $p$  divise tout  $\binom{p}{k}$  avec  $k \in \{1, \dots, p-1\}$ . Donc, pour  $Q = \sum_i q_i X^i \in \mathbb{F}_p[X]$  on a

$$(Q(X))^p = \sum_i (q_i X^i)^p = \sum_i q_i^p (X^i)^p = \sum_i q_i (X^p)^i = Q(X^p) .$$

$\square$

32. Noter que  $|\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ .

### 5.5.5 Exemple : Racines de l'unité et polynômes cyclotomiques

Pour un anneau intègre  $A$  notons  $\mathbb{U}_n(A)$  le groupe multiplicatif des racines  $n$ -ièmes de l'unité  $1_A$ . On appelle une racine  $r \in \mathbb{U}_n(A)$  **primitive** si elle engendre tout  $\mathbb{U}_n(A)$ , c'est-à-dire est d'ordre  $|\mathbb{U}_n(A)|$ . On note  $\mathcal{P}_n(A)$  l'ensemble des racines primitives  $n$ -ièmes de l'unité. Pour  $n \in \mathbb{N}$  on appelle

$$\Phi_{n,A} := \prod_{r \in \mathcal{P}_n(A)} (X - r) \in A[X]$$

le  $n$ -ième **polynôme cyclotomique sur  $A$** . Alors :

1. Pour tout  $n \in \mathbb{N}$  on a  $|\mathbb{U}_n(A)| \leq n$ .
2. Pour tout  $n \in \mathbb{N}$ ,  $\mathbb{U}_n = \bigcup_{m|n} \mathcal{P}_m(A)$ .
3. Si  $|\mathbb{U}_m| = m$  pour tout  $m | n$ , alors  $(\mathcal{P}_m(A))_{m|n}$  est une partition de  $\mathbb{U}_n(A)$ .
4. Si  $|\mathbb{U}_m| = m$  pour tout  $m | n$ , alors  $X^n - 1 = \prod_{r \in \mathbb{U}_n(A)} (X - r) = \prod_{m|n} \Phi_{m,A}$ .
5. Supposons que  $A = \mathbb{K}$  est un corps de caractéristique  $p \in \mathbb{P} \cup \{0\}$ , telle que  $n \notin p\mathbb{Z}$ . Alors,  $X^n - 1$  est séparable. De plus,  $|\mathbb{U}_n(\mathbb{K})| = n$  ssi  $X^n - 1$  est scindé dans  $\mathbb{K}[X]$ .
6. Pour tout  $n \in \mathbb{N}$  on a  $\mathbb{U}_n(\mathbb{C}) = \{e^{2\pi i \frac{m}{n}}\}_{m=1}^n$  et en particulier  $|\mathbb{U}_n(\mathbb{C})| = n$ .
7. Pour n'importe quel  $r \in \mathcal{P}_n(\mathbb{C})$ , on a  $\mathcal{P}_n(\mathbb{C}) = \{r^m \mid m \in \{1, \dots, n\}, \text{pgcd}(m, n) = 1\}$ . En particulier

$$|\mathcal{P}_n(\mathbb{C})| = \varphi(n) \quad ,$$

où  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  est l'indicatrice d'Euler.

8. Pour  $n$  soit

$$\Phi_{n,\mathbb{C}} := \prod_{r \in \mathcal{P}_n(\mathbb{C})} (X - r) \in \mathbb{C}[X]$$

le  $n$ -ième polynôme cyclotomique sur  $\mathbb{C}$ . Alors  $\Phi_{n,\mathbb{C}} \in \mathbb{Z}[X]$ .

9. Pour tout  $r \in \mathcal{P}_n(\mathbb{C})$  on a  $\mathbb{Q}(\mathbb{U}_n(\mathbb{C})) = \mathbb{Q}(r) = \mathbb{Q}[r]$ . On appelle  $\mathbb{Q}(r)$  le  **$n$ -ième corps cyclotomique**.
10. L'extension  $\mathbb{Q}(\mathbb{U}_n(\mathbb{C}))$  de  $\mathbb{Q}$  est de degré  $\varphi(n)$  et Galoisienne, de groupe de Galois  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

#### Preuve :

1. Les  $r \in \mathbb{U}_n$  sont exactement les racines du polynôme  $X^n - 1 \in A[X]$ . Par 3.1.15,  $X^n - 1$  possède au maximum  $n$  racines, donc  $|\mathbb{U}_n| \leq n$ .
2. Si  $m | n$  et  $x \in \mathcal{P}_m$ , on a évidemment  $x^n = 1$  car  $x^m = 1$ . Inversement, soit  $x \in \mathbb{U}_n$ . Soit  $m$  l'ordre de  $x$  dans  $(\mathbb{U}_n, \cdot)$ , alors  $x \in \mathbb{U}_m$ . En fait,  $\mathbb{U}_m$  est engendré par  $x$  car  $|\mathbb{U}_m| \leq m$ , donc  $x \in \mathcal{P}_m$ . Comme  $x^n = 1$ , il faut que  $m | n$ . Donc

$$\mathbb{U}_n = \bigcup_{\substack{m \in \mathbb{N} \\ m|n}} \mathcal{P}_m \quad . \quad (5.5.5.1)$$

3. Par hypothèse,  $\mathcal{P}_m \neq \mathcal{P}_{m'}$  pour tout  $m \neq m'$ . Donc, l'union dans (5.5.5.1) est une union de parties disjointes.
4. Par (2) on sait que le groupe  $\mathbb{U}_n$  est fini. Tout  $r \in \mathbb{U}_n$  est donc racine du polynôme  $X^{|\mathbb{U}_n|} - 1$ . Donc, par 3.1.15,  $\prod_{r \in \mathbb{U}_n} (X - r)$  divise  $X^{|\mathbb{U}_n|} - 1$ . Comme ils sont unitaires et de même degré, il faut que

$$\prod_{r \in \mathbb{U}_n} (X - r) = X^{|\mathbb{U}_n|} - 1 \quad .$$

Par conséquence

$$X^{|\mathbb{U}_n|} - 1 = \prod_{r \in \mathbb{U}_n} (X - r) \stackrel{(3)}{=} \prod_{m|n} \prod_{r \in \mathcal{P}_m} (X - r) = \prod_{m|n} \Phi_m$$

5. Supposons que  $\text{pgcd}(P, P') \neq 1$ , alors il existerait un irréductible  $\alpha \in \mathbb{K}[X]$  tel que  $\alpha | P$  et  $\alpha | P' = nX^{n-1}$ . Comme  $n \neq 0$  dans  $\mathbb{K}$  il est inversible, donc  $X^{n-1}$  est une décomposition de  $P'$  en irréductibles  $X, \dots, X$ . Par unicité d'une cette décomposition (modulo multiplication par inversibles), il faudrait que  $\alpha = X$ , donc  $X | P$ , une contradiction! Se rappeler que par 5.2.8 tous racines de  $X^n - 1$  dans son corps de décomposition sont simples.

Si  $|\mathbb{U}_n| = n$ , alors  $X^n - 1$  possède  $n$  racines distinctes, donc est scindé. Si inversement  $X^n - 1$  est scindé, alors par sa séparabilité tous ses  $n$  racines sont distinctes. Donc  $|\mathbb{U}_n| = n$ .

6. Trivial.

7. Soit  $r \in \mathcal{P}_n(\mathbb{C})$ , alors  $r$  est d'ordre  $n$ . Donc, ses puissances  $r^m$  recouvrent tout  $\mathbb{U}_n(\mathbb{C})$ . Comme on sait, pour tout  $m \in \mathbb{N}$ ,  $r^m$  est d'ordre  $\frac{n}{\text{pgcd}(m,n)}$ . Donc,  $r^m \in \mathcal{P}_n(\mathbb{C})$  ssi  $\text{pgcd}(m,n) = 1$ . Donc

$$|\mathcal{P}_n(\mathbb{C})| = |\{1 \leq m \leq n : \text{pgcd}(m,n) = 1\}| = \varphi(n) \quad .$$

8. Se rappeler que par (4) le polynôme  $X^n - 1 \in \mathbb{Z}[X]$  est un produit fini des polynômes cyclotomiques  $\Phi_{m,\mathbb{C}}$ . Comme tout produit des  $\Phi_{m,\mathbb{C}}$  est unitaire, par lemme 4.2.5 sur divisions dans  $\mathbb{Z}[X]$  il suffit donc de montrer que tout  $\Phi_{m,\mathbb{C}}$  appartient à  $\mathbb{Q}[X]$ . Mais cela est implique par lemme 4.2.8 sur divisions dans  $\mathbb{Q}[X]$  et  $\mathbb{C}[X]$ .

9. Comme  $r \in \mathcal{P}_n(\mathbb{C})$  est d'ordre  $n = |\mathbb{U}_n(\mathbb{C})|$ , ses puissances engendrent tout  $\mathbb{U}_n(\mathbb{C})$ . Donc,  $\mathbb{Q}(\mathbb{U}_n(\mathbb{C})) = \mathbb{Q}(r)$ . Comme  $r$  est algébrique sur  $\mathbb{Q}$ , on a  $\mathbb{Q}(r) = \mathbb{Q}[r]$ .

10. Par 5.5.6(i), l'extension  $\mathbb{Q}(\mathbb{U}_n(\mathbb{C}))/\mathbb{Q}$  est de degré  $\varphi(n)$ . Par 5.5.6(ii) elle est Galoisienne. La dernière affirmation ne sera pas prouvée. □

**Exemple :** Considérons les racines 12-ièmes de l'unité dans  $\mathbb{C}$ . Alors

$$\mathbb{U}_{12}(\mathbb{C}) = \{e^{i2\pi \frac{m}{12}} : m \in \{1, \dots, 12\}\} \quad .$$

Une racine primitive est donnée par  $r := e^{i2\pi \frac{1}{12}}$ . Donc, par 5.5.5(7) on obtient tous les autres racines primitives comme

$$\mathcal{P}_{12}(\mathbb{C}) = \{r^m : m \in \{1, \dots, 12\}, \text{pgcd}(12, m) = 1\} = \{r^1, r^5, r^7, r^{11}\} \quad .$$

Le 12-ième polynôme cyclotomique sur  $\mathbb{C}$  est donc donné par

$$\Phi_{12,\mathbb{C}}(X) = \prod_{x \in \mathcal{P}_{12}(\mathbb{C})} (X - x) = (X - r^1)(X - r^5)(X - r^7)(X - r^{11}) = X^4 - X^2 + 1 \quad .$$

Comme affirmé dans 5.5.5(8), il se trouve dans  $\mathbb{Z}[X]$ .

### 5.5.6 Théorème : Irréductibilité des polynômes cyclotomiques

Pour tout  $n \in \mathbb{N}$ , le polynôme cyclotomique

$$\Phi_{n,\mathbb{C}} := \prod_{r \in \mathcal{P}_n(\mathbb{C})} (X - r)$$

est irréductible dans  $\mathbb{Q}[X]$ .

**Conséquences :** Soit  $r \in \mathcal{P}_n(\mathbb{C})$  une  $n$ -ième racine primitive de l'unité dans  $\mathbb{C}$ . Alors :

- (i) Le nombre complexe  $r$  est racine du polynôme cyclotomique  $\Phi_{n,\mathbb{C}} \in \mathbb{Z}[X]$ . Comme  $\Phi_{n,\mathbb{C}}$  est unitaire et irréductible dans  $\mathbb{Q}[X]$ , il est le polynôme minimal de  $r \in \mathbb{C}$  sur  $\mathbb{Q}$ . En particulier, le degré de  $r$  sur  $\mathbb{Q}$  est donné par  $[\mathbb{Q}(r) : \mathbb{Q}] = \text{dg}(\Phi_n) = \varphi(n)$  (voir 5.5.5).
- (ii) Par 5.2.3, les  $\mathbb{Q}$ -morphisms de corps  $\mathbb{Q}(r) \rightarrow \mathbb{Q}(r)$  sont en bijection avec les racines du polynôme minimal  $\Phi_{n,\mathbb{C}}$  de  $r$  dans  $\mathbb{Q}(r)$ . Par construction, les éléments de  $\mathcal{P}_n(\mathbb{C})$  sont exactement les racines de  $\Phi_{n,\mathbb{C}}$  dans  $\mathbb{C}$ , qui se trouvent par 5.5.5(9) en fait dans  $\mathbb{Q}(r)$ . Donc, il y a  $|\mathcal{P}_n(\mathbb{C})| = \varphi(n)$   $\mathbb{Q}$ -morphisms de corps  $\mathbb{Q}(r) \rightarrow \mathbb{Q}(r)$ . Par remarque 5.4.1(ii), cela implique que  $\mathbb{Q}(r)/\mathbb{Q}$  est Galoisienne.

**Idée de preuve :** Soit  $n \in \mathbb{N}$  fixé. Choisissons une racine  $n$ -ième  $r \in \mathcal{P}_n(\mathbb{C})$  de l'unité dans  $\mathbb{C}$  n'importe laquelle et notons  $f \in \mathbb{Q}[X]$  le polynôme minimal de  $r$  sur  $\mathbb{Q}$ . Alors :

- On montre que  $f$  divise  $X^n - 1$  dans  $\mathbb{Q}[X]$ .
- On en déduit par 4.2.5 que  $f \in \mathbb{Z}[X]$  et qu'il existe un  $h \in \mathbb{Z}[X]$  unitaire tel que  $X^n - 1 = f * h$ .

On montre de plus que pour toute racine  $u \in \mathbb{C}$  de  $f$  et  $p \in \mathbb{P}$  premier ne divisant pas  $n$ , on a aussi  $f(u^p) = 0$ .

On raisonne par l'absurde en supposant que  $f(u^p) \neq 0$ . Alors :

- On montre que  $f$  est le polynôme minimal de  $u$  sur  $\mathbb{Q}$ .
- En montrant d'abord que  $h(X^p)$  s'annule à  $u$ , on montre que  $f$  divise  $h(X^p)$  dans  $\mathbb{Q}[X]$ .
- Comme  $f$  et  $h(X^p)$  sont unitaires, on en déduit par 4.2.5 qu'il existe un  $g \in \mathbb{Z}[X]$  unitaire tel que  $h(X^p) = f * g$ .
- Pour  $P \in \mathbb{Z}[X]$ , on note  $\bar{P}$  le polynôme à coefficients dans  $\mathbb{F}_p$  obtenu en réduisant les coefficients de  $P$  modulo  $p$ . En utilisant lemme 5.5.4, on montre que  $\bar{h}(X^p) = \bar{f} * \bar{g}$ .
- Soit  $\tilde{\mathbb{F}}_p$  une clôture algébrique de  $\mathbb{F}_p$ . On montre qu'il existe  $z \in \tilde{\mathbb{F}}_p$  tel que  $\bar{f}(z) = 0 = \bar{h}(z)$ ,
- On en déduit que  $X^n - 1 = \bar{f} * \bar{h} \in \mathbb{F}_p[X]$  a une racine  $z \in \tilde{\mathbb{F}}_p$  au moins double.
- On en déduit que  $\frac{d}{dX}(X^n - 1)|_z = 0$  dans  $\mathbb{F}_p$ . Mais cela est faux, car à cause de  $\frac{d}{dX}(X^n - 1) = nX^{n-1}$  et  $n \neq 0$  dans  $\mathbb{F}_p$  par hypothèse, il faudrait que  $z^{n-1} = 0$ , donc  $z = 0$ . Mais  $z = 0$  n'est pas une racine de  $X^n - 1$ . Donc, pour toute racine  $u \in \mathbb{C}$  de  $f$  et tout  $k \in \mathbb{N}$  tel que  $\text{pgcd}(k, n) = 1$ , la puissance  $u^k$  est aussi une racine de  $f$ . En particulier,  $\{u^k : k \in \mathbb{N}, \text{pgcd}(k, n) = 1\} \stackrel{5.5.5(7)}{=} \mathcal{P}_n$  sont tous racines de  $f$ . Donc, par 3.1.15 on conclut que le produit

$$\prod_{\rho \in \mathcal{P}_n(\mathbb{C})} (X - \rho) = \Phi_{n, \mathbb{C}} \stackrel{5.5.5(8)}{\in} \mathbb{Q}[X]$$

divise  $f \in \mathbb{Q}[X]$  dans  $\mathbb{C}[X]$  et par 4.2.8 aussi dans  $\mathbb{Q}[X]$ . Comme  $f$  est irréductible dans  $\mathbb{Q}[X]$ , on en déduit que  $\Phi_{n, \mathbb{C}} = f$  de multiplication par inversibles près, c'est-à-dire  $\Phi_{n, \mathbb{C}}$  est aussi irréductible dans  $\mathbb{Q}[X]$ .  $\square$

## 6 Modules sur anneaux principaux, intègres

On étudie les modules  $M$  de type fini sur un anneau intègre, principal  $A$ . Noter que par définition,  $M$  est de type fini s'il existe  $m_1, \dots, m_n \in M$  tels que

$$M = \text{span}_A\{m_1, \dots, m_n\} = \sum_{i=1}^n Am_i \quad ,$$

c'est-à-dire le morphisme

$$\varphi : A^n \rightarrow M \quad , \quad (a_i)_{i=1}^n \mapsto \sum_{i=1}^n a_i m_i$$

et surjectif. En général,  $M$  n'est pas nécessairement libre, c'est-à-dire les  $(m_i)_i$  ne forment pas une base.

### 6.0.7 Théorème sur sous-modules libres

Soit  $A$  un anneau intègre, principal et  $n \in \mathbb{N}$ . Alors, tout sous- $A$ -module de  $A^n$  est libre de rang  $\leq n$ .

**Preuve :** (Par récurrence sur  $n$ ). En cas  $n = 1$ , les sous- $A$ -modules de  $A$  sont exactement les idéaux  $J \subseteq A$ . Comme  $A$  est principal,  $J$  est de la forme  $J = Aa$  pour un  $a \in A$ . Le morphisme de  $A$ -modules  $A \rightarrow J$ ,  $\alpha \mapsto \alpha a$  est donc surjective. Comme  $A$  est intègre, il est aussi injectif. Donc  $J$  est libre avec base  $\{a\}$ .

Supposons l'affirmation valide pour  $A^1, \dots, A^n$ . Soit  $M \subseteq A^n$  un sous- $A$ -module de  $A^n$ . Considérons la projection

$$\Pi : A^n \rightarrow A \quad , \quad (a_1, \dots, a_n) \mapsto a_1 \quad ,$$

qui est un morphisme de  $A$ -modules. Si  $M \subseteq \ker(\Pi) = \{0\} \times A^{n-1}$  on a fini par récurrence. Supposons que  $\Pi(M) \neq \{0\}$ , alors l'idéal  $\Pi(M)$  est de la forme  $\Pi(M) = Aa$  pour un  $0 \neq a \in A$ . Soit  $m \in M$  tel que  $\Pi(m) = a$ .

**Proposition :**  $M = Am \oplus (M \cap \ker(\Pi))$ .

**Preuve :** Soit  $x \in M$  quelconque, alors  $\Pi(x) = \alpha a$  pour un  $\alpha \in A$ , donc  $\Pi(x - \alpha m) = 0$ . Donc

$$x = \underbrace{\alpha m}_{\in Am} + \underbrace{(x - \alpha m)}_{\in M \cap \ker(\Pi)} \quad ,$$

d'où  $M = Am + (M \cap \ker(\Pi))$ . De plus, si  $0 = \alpha m + y$  pour  $\alpha \in A$  et  $y \in M \cap \ker(\Pi)$ , alors

$$0 = \Pi(0) = \Pi(\alpha m + y) = \alpha \Pi(m) + 0 = \alpha a \quad .$$

Comme  $a \neq 0$  et  $A$  est intègre, on conclut que  $\alpha = 0$  et donc  $y = 0$ . Par remarque 2.1.22(iv), cela implique que la somme est directe.

Par récurrence,  $M \cap \ker(\Pi) \subseteq A^{n-1}$  possède une base de  $m_2, \dots, m_k \in M \cap \ker(\Pi)$ , avec  $k \leq n$ . Comme  $Am$  possède la base  $\{m\}$ , leur somme directe possède la base  $\{m, m_2, \dots, m_k\}$ . □

**Conséquence :** Soit  $M$  un  $A$ -module de type fini, engendré par les  $m_1, \dots, m_n \in M$ . Alors, comme on sait, il existe un morphisme de  $A$ -modules surjectif  $\varphi : A^n \rightarrow M$ . Par conséquence,  $M \cong_A A^n / \ker(\varphi)$  est un quotient d'un  $A$ -module libre de rang  $n$  sur un  $A$ -module libre de rang  $\leq n$ .

### 6.0.8 Définition: Le groupe linéaire, générale

Soit  $A$  un anneau commutatif. Pour  $n, m \in \mathbb{N}$  on définit  $M_{n,m}(A)$  le  $A$ -module des matrices  $n \times m$  à coefficients dans  $A$ . Le  $A$ -module  $M_n(A) := M_{n,n}(A)$  est munit de la structure de multiplication de matrices, et devient donc une  $A$ -algèbre. On définit sur  $M_n(A)$  la déterminant  $\det : M_n(A) \rightarrow A$  comme

$$\det((B)_{i,j}) := \sum_{\sigma \in \text{Sym}(n)} \text{sgn}(\sigma) \prod_{i=1}^n B_{i,\sigma(i)} \quad , \quad B = (B_{i,j})_{i,j=1}^n$$

On note  $\text{GL}_n(A) := M_n(A)^\times$  le groupe multiplicatif des matrices  $n \times n$  inversibles par rapport à la multiplication.

**Remarques**

(i) On peut montrer que, pour  $B \in M_n(A)$  on a  $\det(B) \in A^\times$  ssi  $B \in \text{GL}_n(A)$ . Le cas échéant, on a

$$B^{-1} = \frac{\text{com}(B)}{\det(B)} ,$$

où  $\text{com}(B)$  est la comatrice de  $B$ .

(ii) Toute matrice  $B \in M_{n,m}(A)$  peut être vue comme application  $A$ -linéaire  $A^m \rightarrow A^n$ , via

$$(a_j)_{j=1}^m \mapsto \left( \sum_{j=1}^m B_{i,j} a_j \right)_{i=1}^n .$$

Inversement, toute application  $A$ -linéaire  $\Phi : A^m \rightarrow A^n$  est induit une telle matrice. Comme  $\Phi$  est déterminé par les images de la base canonique  $e_1, \dots, e_m \in A^m$ , représentés par la base canonique  $e_1, \dots, e_n \in A^n$ , il existe une unique matrice  $B \in M_{n,m}(A)$  associée, donnée par

$$B_{i,j} := (\Phi e_j)_i .$$

L'association induit

$$(M_{n,m}(M), +, \cdot) \rightarrow (\text{Hom}_A(A^m, A^n), +, \circ) := \{A^m \rightarrow A^n \text{ } A\text{-linéaires}\}$$

est un isomorphisme de  $A$ -algèbres.

(iii) Le groupe  $\text{GL}_n(A) \times \text{GL}_m(A)$  opère sur  $M_{n,m}(A)$  par

$$(P, Q) \cdot B := PBQ^{-1} , \quad B \in M_{n,m}(A), (P, Q) \in \text{GL}_n(A) \times \text{GL}_m(A) .$$

(iv) Si  $A = \mathbb{K}$  est un corps, alors on sait que  $B, B' \in M_{n,m}(\mathbb{K})$  sont dans le même orbite de l'action de  $\text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K})$ , ssi ils possèdent le même *rang*. Autrement dit,  $B \in M_{n,m}(\mathbb{K})$  possède le rang  $r \in \{0, \dots, \min\{n, m\}\}$  ssi elle est dans l'orbite de

$$\begin{pmatrix} 1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} 1_{r \times r} & 0_{r, m-r} \\ 0_{n-r, r} & 0_{n-r, m-r} \end{pmatrix} .$$

Cela donne une indication pour une généralisation de la théorie du rang au delà les corps (voir 6.0.10).

**6.0.9 Lemme : Extensions à bases**

Soit  $A$  un anneau intègre, principal et  $x_1, \dots, x_n \in A$ . Alors, les suivants sont équivalents :

1. Il existe une matrice dans  $\text{GL}_n(A)$  dont la première ligne est  $(x_1, \dots, x_n)$ .
2.  $\text{pgcd}(x_1, \dots, x_n) \sim 1$ . Noter que par 4.1.5,  $A$  est factoriel.
3.  $(x_1, \dots, x_n)$  appartient à une  $A$ -base du  $A$ -module  $A^n$ .

**6.0.10 Théorème de Gauss : Réduction de matrices**

Soit  $A$  un anneau intègre, principal et  $B \in M_{n,m}(A)$  une  $n \times m$  matrice à coefficients dans  $A$ . On considère l'action de  $\text{GL}_n(A) \times \text{GL}_m(A)$  sur  $M_{n,m}(A)$  introduit dans remarque 6.0.8(iii). Alors, il existe dans l'orbite de



$B$  une matrice **réduite** de la forme

$$\begin{pmatrix} a_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & & \vdots & \ddots & \vdots \\ 0 & & a_r & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

avec  $0 \neq a_1 \mid a_2 \mid \dots \mid a_r$ . Les  $a_i \in A$  sont uniques à multiplication par inversibles près, c'est-à-dire les idéaux principaux  $Aa_1, \dots, Aa_r$  sont uniques. On dit  $r$  le **rang** de la matrice  $B$ .

### 6.0.11 Théorème : Structure des modules de type fini

Soit  $A$  un anneau intègre, principal et  $M$  un  $A$ -module de type fini. Alors,  $M$  est une somme directe de  $A$ -modules cycliques<sup>33</sup>

$$M \cong_A A/(Aa_1) \oplus \dots \oplus A/(Aa_n) \oplus A \oplus \dots \oplus A$$

avec  $0 \neq a_1 \mid a_2 \mid \dots \mid a_n \in A \setminus A^\times$ . De plus, les idéaux  $(Aa_i)$  sont déterminés de manière unique pour  $M$ .

<sup>33</sup>. Se rappeler que par remarque 2.1.9(vi) tout  $A$ -module cyclique est isomorphe à  $A/J$  pour un idéal  $J \subseteq A$ . Comme  $A$  est principal,  $J$  est principal.

## A Annexe

### A.0.12 Lemme : Factorisation des applications linéaires

Soient  $U, V, W$   $\mathbb{K}$ -espaces vectoriels,  $U$  de dimension fini, et  $f : U \rightarrow W$  une application linéaire.

1. Si  $F : U \rightarrow V$  est une application linéaire telle que  $\ker(F) \subseteq \ker(f)$ , alors il existe une application linéaire  $g : V \rightarrow W$  telle que  $f = g \circ F$ .
2. Si  $F : V \rightarrow W$  est une application linéaire telle que  $f(U) \subseteq F(V)$ , alors il existe une application linéaire  $g : U \rightarrow V$  telle que  $f = F \circ g$ .

**Preuve :**

1. Soit  $e_1, \dots, e_n$  une base de  $U$  telle que  $e_1, \dots, e_l$  est une base de  $\ker(f)$  et  $e_1, \dots, e_k$  une base de  $\ker(F)$ ,  $k \leq l \leq n$ . Alors  $F(e_{k+1}), \dots, F(e_n) \in V$  sont linéairement indépendants. Définissons

$$g(F(e_i)) := \begin{cases} f(e_i) & : l+1 \leq i \leq n \\ 0 & : k+1 \leq i \leq l \end{cases}$$

(et étendre au reste de  $V$  si nécessaire), donc  $g$  satisfait l'affirmation.

2. Soit  $e_1, \dots, e_k$  une base de  $f(U)$  et  $b_1, \dots, b_k \in V$  tels que  $F(b_i) = e_i$ . Soient  $U_i \in f^{-1}(\{e_i\})$ , alors

$$U = \text{span} \bigcup_{i=1}^k U_i .$$

Définissons l'application linéaire  $g : U \rightarrow V$  comme  $g(a_i) := b_i$  pour  $a_i \in U_i$  (et étendons au reste de  $U$  linéairement). Noter que  $g$  est bien défini, car si  $\sum_{i=1}^k \lambda_{ij} a_{ij} = \sum_{i=1}^k \mu_{ij} a'_{ij}$  pour  $a_{ij}, a'_{ij} \in U_i$  on a

$$\sum_j \lambda_{ij} = \sum_j \mu_{ij} \quad \forall i = 1, \dots, k$$

et donc

$$\sum_i \sum_j \lambda_{ij} \underbrace{g(a_{ij})}_{b_i} = \sum_i \sum_j \mu_{ij} \underbrace{g(a'_{ij})}_{b_i} .$$

L'application  $g$  satisfait  $F(g(a_{ij})) = F(b_i) = e_i = f(a_{ij})$ , donc  $f = F \circ g$ .

□

### A.0.13 Lemme : Représentation des endomorphismes sur espaces vectoriels

Soit  $V$  un  $\mathbb{K}$ -espace vectoriel de dimension fini.

1. Soient  $f, f_1, \dots, f_m \in \text{End}_{\mathbb{K}}(V)$  endomorphismes tels que

$$\bigcap_{i=1}^m \ker(f_i) \subseteq \ker(f) .$$

Alors il y a  $g_1, \dots, g_m \in \text{End}_{\mathbb{K}}(V)$  tels que  $f = \sum_{i=1}^m g_i \circ f_i$ .

2. Soient  $f, f_1, \dots, f_m \in \text{End}_{\mathbb{K}}(V)$  endomorphismes tels que

$$f(V) \subseteq \sum_{i=1}^m f_i(V) .$$

Alors il y a  $g_1, \dots, g_m \in \text{End}_{\mathbb{K}}(V)$  tels que  $f = \sum_{i=1}^m f_i \circ g_i$ .

**Preuve :**

1. Considérons l'application linéaire  $F : V \rightarrow \bigoplus_{i=1}^m V$  défini par  $F(x) := (f_1(x), \dots, f_m(x))$ . Alors

$$\ker(F) = \bigcap_{i=1}^m \ker(f_i) \subseteq \ker(f) ,$$

donc selon lemme A.0.12(1) il y a une application linéaire  $g : \bigoplus_{i=1}^m V \rightarrow V$  telle que  $g \circ F = f$ . Définissons  $g_i(x) := g(0, \dots, x_i, \dots, 0)$ ,  $x_i \in V$ , alors  $g_i \in \text{End}_{\mathbb{K}}(V)$  et on a

$$f = g \circ F = \sum_{i=1}^m g_i \circ f_i ,$$

comme affirmé.

2. Considérons l'application linéaire  $F : \bigoplus_{i=1}^m V \rightarrow V$  défini par  $F(x_1, \dots, x_m) := \sum_{i=1}^m f_i(x_i)$ . Alors

$$F(V) = \sum_{i=1}^m f_i(V) \supseteq f(V) ,$$

donc selon lemme A.0.12(2) il y a une application linéaire  $g = (g_1, \dots, g_m) : V \rightarrow \bigoplus_{i=1}^m V$  telle que  $F \circ g = f$ .  
Donc

$$f = F \circ g = \sum_{i=1}^m f_i \circ g_i .$$

□

**A.0.14 Lemme de Zorn**

Soit  $\mathcal{F} \neq \emptyset$  un ensemble ordonné dans lequel toute partie totalement ordonnée admet un majorant<sup>34</sup> dans  $\mathcal{F}$ . Alors  $\mathcal{F}$  a un élément maximal<sup>35</sup>.

34. Un élément  $x \in \mathcal{F}$  est un majorant de  $F \subseteq \mathcal{F}$  si  $y \leq x \ \forall y \in F$ .

35. Un élément  $x \in \mathcal{F}$  est dit maximal si pour  $y \in \mathcal{F}$  tel que  $x \leq y$  on a  $x = y$ .

## B Symboles

$\mathbb{R}_+$  :  $= [0, \infty)$ .

$\mathbb{C}_+$  :  $\mathbb{R}_+ + i\mathbb{R}_+$ .

$\mathbb{N}_{\geq k}$  : Entiers plus grands ou égales à  $k \in \mathbb{R}$ .

$\mathbb{K}$  : Corps général.

$\mathbb{P}$  : Les nombres premiers. Voir 4.1.3.

$\mathbb{F}_{p^n}$  : Le corps de cardinalité  $p^n$  et caractéristique  $p$ . Voir 5.5.2.

$Z(G)$  : Centre du groupe  $G$ .

$Z(A)$  : Centre de l'anneau  $A$ . Voir 1.1.10.

$\mathcal{Z}(I)$  : Les idéaux premiers contenant l'idéal bilatère  $I$ . Voir la topologie Zariski 1.2.16.

$e_i$  : Base canonique dans le module libre  $A^{(I)}$ . Voir 2.2.1.

$\text{End}_{\mathbb{K}}(V)$  : Anneau des  $\mathbb{K}$ -endomorphismes sur un  $\mathbb{K}$ -espace vectoriel  $V$ .

$\ker(f)$  : Noyau du homomorphisme  $f$ .

$\delta_{ij}$  : Symbole de Kronecker :  $\delta_{ij} = 1$  si  $i = j$  et  $\delta_{ij} = 0$  si  $i \neq j$ .

$A^\times$  : Le sous-ensemble des éléments inversibles d'un ring  $(A, +, \cdot)$ . Voir 1.1.7.

$\prod_{i \in I} A_i$  : L'anneau produit d'une famille  $(A_i)_{i \in I}$  d'anneaux. Voir 1.1.4.

$\prod_{i \in I} G_i$  : Le module produit directe d'une famille  $(G_i)_{i \in I}$  de modules. Voir 2.1.21.

$\bigoplus_{i \in I} G_i$  : La somme directe des modules  $(G_i)_{i \in I}$ . Voir 2.1.21.

$\text{Spec}(A)$  : Famille des idéaux premiers dans l'anneau  $A$ . Voir 1.2.15.

$\text{Specmax}(A)$  : Famille des idéaux maximaux dans l'anneau  $A$ . Voir 1.2.17.

$\text{span}_A(X)$  : Sous- $A$ -module engendré par  $X$ . Voir 2.1.9.

$\cong$  : Isomorphisme de groupes ou anneaux. Voir 1.1.12.

$\cong_A$  : Isomorphisme de  $A$ -modules. Voir 2.1.3.

$A^{(I)}$  : Module libre engendré par l'anneau  $A$  sur l'ensemble  $I$ . Voir 2.2.1.

$\text{Ann}_A(g)$  : Annulateur de l'élément  $g \in G$  du  $A$ -module  $G$ . Voir 2.1.19.

$A[S]$  : L'algèbre des polynômes sur l'anneau commutatif  $A$ , où  $S$  est un monoïde commutatif. Voir 3.1.4.

$A[X]$  :  $A[\mathbb{N}]$ . Voir exemple 3.1.4(i).

$A[X^{\pm 1}]$  :  $A[\mathbb{Z}]$ . Voir exemple 3.1.4(ii).

$A[[S]]$  : L'algèbre des séries formelles sur l'anneau commutatif  $A$ , où  $S$  est un monoïde commutatif. Voir 3.5.1.

$A[[X]]^\times$  : Le sous-groupe des séries formelles inversibles sur l'anneau  $A$  par rapport à “\*”. Voir 3.5.7.

$A[[X]]^\circ$  : Le sous-groupe des séries formelles inversibles sur l'anneau  $A$  par rapport à “o”. Voir 3.5.13.

$\mathcal{F}(B^n, B)$  : Algèbre des fonctions polynomiales  $B^n \rightarrow B$  sur la  $A$ -algèbre  $B$ . Voir 3.2.7.

$\mathbb{K}(X)$  : Corps quotient de  $\mathbb{K}[X]$ . Voir 3.5.19.

$\mathbb{K}((X))$  : Corps quotient de  $\mathbb{K}[[X]]$ . Voir 3.5.19.

$\leq_l$  : Ordre lexicographique sur  $\mathbb{R}^n$ . Voir 3.1.9.

$\leq$  : Ordre monomial sur  $\mathbb{R}^n$ . Voir 3.1.9.

$\mathcal{P}_n$  : Ensemble des partitions dans  $\mathbb{N}_0^n$ . Voir 3.4.4.

$\lambda^*$  : Partition duale de la partition  $\lambda$ . Voir 3.4.4.

$M_\lambda(X)$  : Monôme symétrique complet associé à la partition  $\lambda \in \mathbb{N}_0^n$ . Voir 3.4.5.

$\sigma_k(X)$  : Polynôme symétrique élémentaire de degré  $k$ . Voir 3.4.5.

$\mathcal{C}(P)$  : Contenu d'un polynôme  $P$ . Voir 4.2.1.

$[\mathbb{L} : \mathbb{K}]$  : Dimension de l'extension  $\mathbb{L}$  d'un corps  $\mathbb{K}$  comme  $\mathbb{K}$ -espace vectoriel. Voir 5.1.1.

$\text{Aut}(\mathbb{L}/\mathbb{K})$  : Groupe des  $\mathbb{K}$ -automorphismes de corps de  $\mathbb{L}$ . Voir 5.4.1.

$\mathbb{L}^H$  : Le sous corps entre  $\mathbb{K}$  et  $\mathbb{L}$  point par point stable sous  $H \leq \text{Gal}(\mathbb{L}/\mathbb{K})$ . Voir 5.4.2.

$M_{n,m}(A)$  :  $A$ -module des matrices  $n \times m$  à coefficients dans l'anneau  $A$ . Voir 6.0.8.

$M_{n,n}(A)$  : La  $A$ -algèbre des matrices  $n \times n$  à coefficients dans l'anneau  $A$ . Voir 6.0.8.

$\text{GL}_n(A)$  : Le groupe multiplicatif des matrices inversibles dans  $M_n(A)$ . Voir 6.0.8.

# Index

- $A$ -module, [23](#)
- $R$ -algèbre, [21](#)
- $\mathbb{K}$ -automorphisme, [91](#)
- $\mathbb{K}$ -morphisme de corps, [90](#)
- élément
  - inversible, [8](#)
  - irréductible, [8](#)
  - nilpotent, [8](#)
  - unité, [8](#)
- élément algébrique, [88](#)
- éléments premiers entre eux, [79](#)
- addition, [6](#)
- algèbre, [40](#)
  - commutative, [40](#)
- algèbre des séries formelles, [66](#)
- algèbres
  - isomorphes, [40](#)
- anneau, [6](#)
  - à division, [8](#)
  - base, [40](#), [40](#)
  - commutatif, [6](#)
  - de base, [21](#)
  - euclidien, [9](#)
  - factoriel, [77](#)
  - intègre, [7](#)
  - local, [18](#)
  - noetherien, [21](#)
  - principal, [11](#)
  - produit, [7](#)
  - quotient, [13](#)
  - simple, [11](#)
- annulateur, [31](#)
- associés, [76](#)
- base
  - canonique, [33](#)
  - de module, [33](#)
- bilatère, [10](#)
- central, [8](#)
- centre, [8](#)
- clôture algébrique, [93](#)
- coefficient binomial, [55](#)
- coefficient dominant, [45](#)
- contenu, [80](#)
- convergence de séries formelles, [67](#)
- corps
  - algébriquement clos, [93](#)
  - cyclotomique, [100](#)
  - fini, [98](#)
  - quotient, [31](#)
- corps de décomposition, [93](#)
- critère d'Eisenstein, [84](#)
- dérivée
  - d'une série formelle, [72](#)
  - dérivée d'un polynôme, [55](#)
  - développement en série formelle, [74](#)
- degré
  - d'un polynôme, [45](#)
- degré d'une extension, [87](#)
- diagramme de Young, [57](#)
- diviseur, [7](#)
- diviseur de zéro, [7](#)
- entiers de Gauss, [10](#)
- extension d'un corps, [87](#)
- extension de corps
  - algébrique, [89](#)
  - galoisienne, [96](#)
- extension séparable, [95](#)
- factorisation
  - de morphisme, [13](#)
- fermé principal, [16](#)
- Field., [8](#)
- forme initiale, [45](#)
- générateur
  - d'un module, [27](#)
- génératrice minimale, [33](#)
- groupe de Galois, [96](#)
  - d'un polynôme, [97](#)
- homothétie, [23](#)
- idéal
  - à droite, [10](#)
  - à gauche, [10](#)
  - de type fini, [12](#)
  - engendré, [11](#)
  - maximal, [16](#)
  - premier, [15](#)
  - principal, [11](#)
  - produit, [12](#)
- idéaux
  - étrangers, [19](#)
- indépendance linéaire, [33](#)
- indicatrice d'Euler, [89](#), [100](#)
- injection
  - dans un module produit, [32](#)
- irréductibilité, [76](#)
- isomorphe, [9](#)
- isomorphisme
  - canonique, [44](#)
  - d'algèbres, [22](#)
  - d'anneaux, [9](#)
  - de modules, [23](#)
- liée, [33](#)
- longueur d'une partition, [57](#)

- matrice
  - d'un morphisme, [36](#)
- matrice réduite, [105](#)
- module
  - cyclique, [27](#)
  - de type fini, [27](#)
  - libre, [33](#)
  - noetherien, [27](#)
  - produit direct, [32](#)
  - quotient, [24](#)
  - simple, [23](#)
  - somme directe, [32](#)
- monôme, [41](#)
- monôme symétrique complet, [59](#)
- monoïde, [6](#)
  - commutatif, [6](#)
  - produit, [6](#)
- morphisme
  - canonique, [13](#)
  - d'algèbres, [40](#)
  - d'anneaux, [8](#)
  - de  $R$ -algèbres, [22](#)
  - de corps, [9](#)
  - de modules, [23](#)
  - de monoïdes, [6](#)
  - quotient, [24](#)
  - universal, [25](#)
  - universel, [13](#)
- morphisme de Frobenius, [10](#)
- multiplication, [6](#)
- multiplicité, [47](#)
- opération
  - d'anneau sur un groupe, [23](#)
- ordre
  - monômial, [45](#)
- ordre lexicographique, [44](#)
- ouvert principal, [16](#)
- pôle
  - d'une fraction, [74](#)
- partie
  - multiplicatif, [18](#)
- partition, [57](#)
- plongement
  - canonique, [41](#)
- polynôme, [41](#)
  - antisymétrique, [66](#)
  - constant, [41](#)
  - cyclotomique, [100](#)
  - séparable, [93](#)
  - symétrique élémentaire, [59](#)
  - unitaire, [45](#)
- polynôme primitif, [80](#)
- polynôme scindé, [47](#)
- polynôme symétrique, [58](#)
- premier, [76](#)
- produit
  - des idéaux, [12](#)
  - extérieur, [40](#)
- projection
  - de module produit, [32](#)
- propriété de Gauss, [76](#)
- réduction d'un polynôme, [80](#)
- réduction de polynômes, [80](#)
- racine, [47](#), [53](#)
- racine primitive, [100](#)
- racine simple, [47](#)
- rang
  - d'un module, [36](#)
  - d'une matrice, [105](#)
- représentation canonique
  - d'un polynôme, [45](#)
- série
  - exponentielle, [71](#)
- série formelle
  - finie, [66](#)
- séries de Laurent, [74](#)
- séries formelle
  - inversible, [70](#)
- sommabilité, [67](#)
- somme de Newton, [62](#)
- somme de séries formelles, [67](#)
- somme directe, [32](#)
- sous-anneau, [8](#)
- sous-corps, [87](#)
- sous-module, [23](#)
  - engendré, [27](#)
  - supplémentaire, [32](#)
- spectre
  - d'anneau, [15](#)
- stathme, [9](#)
- symétrisation d'un monôme, [59](#)
- terme dominant, [45](#)
- topologie Zariski, [16](#)
- torsion, [30](#)
- valuation, [9](#), [67](#)