Algèbre

UJF Grenoble - Hiver 2010/2011

Manuscrit Personnel

Stilianos Louca

1er janvier 2011

Table des matières

1 Préface

1.1 Qu'est-ce ce ?

Le suivent est un manuscrit personnel du cours d'Algèbre, offert par Prof. Bertin à l'UJF l'année 2010/2011.

2 Anneaux, idéaux, algèbres

2.1 Anneaux

2.1.1 Definition: Monoide

Un **monoide** $(S, \circ)$ et un ensemble S munit d'un loi binaire $\circ : S \times S \to S$ 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 $f : S \to T$ entre deux monoides $(S, \circ)$, $(T, \circ)$ est dit **morphisme de monoides** ssi :
- Elle commute avec l'opération du monoide, 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 monoide et $f : G \to S$ un morphisme de monoides. Alors, $f(G)$ est un groupe et $f : G \to f(G)$ un morphisme de groupes.

Exemples :

(i) Tout groupe est un monoide.

(ii) $(\mathbb{N}_0, +)$ et $(\mathbb{R}_+, +)$ sont monoides mais pas de groupes.

2.1.2 Definition: Monoide produit

Soit $(S_i)_{i \in I}$ une famille de monoides. Alors, le produit $\bigtimes_{i \in I} S_i$ 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 monoide et dit **monoide produit** des $(S_i)_{i \in I}$.

2.1.3 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 monoid avec l'élément unité $1 \in A$, c.a.d. $a \cdot 1 = 1 \cdot a = a \ \ \forall \ a \in A$ et $\cdot : A \times A \to A$ 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) $\mathbb{Z}/n\mathbb{Z} = \{[0], .., [n-1]\}$, où $n \in \mathbb{N}$, est un anneaux par rapport à la multiplication

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

(iii) Souvent on parle de l'anneau d'endomorphismes d'une structure. Si V est un $\mathbb{K}$-espace vectoriel, ses endomorphismes $\mathrm{End}_{\mathbb{K}}(V)$ forment un anneau par rapport à l'addition et à la composition.

(iv) On considère l'anneau des endomorphismes $\mathrm{End}(C_n)$ de la groupe cyclique C_n d'ordre $n \geq 2$, engendré par $c \in C_n$. Tout endomorphisme $f : C_n \to C_n$ est déterminé par $f(c) \in C_n$ et on a $f(kc) = kf(c), \quad k \in \mathbb{N}_0$. Donc on a une correspondance naturelle entre C_n et $\mathrm{End}(C_n)$.

2.1.4 Definition: Anneau produit

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

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

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

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

2.1.5 Definition: 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 $x \mid y$.

2.1.6 Definition: Anneau intègre

Un anneau commutatif $(A, +, \cdot)$ est dit **intègre**[1] (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 $(2 + 6\mathbb{Z}) \cdot (3 + 6\mathbb{Z}) = 0 + 6\mathbb{Z}$.

1. Anglais : Integral domain.

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 2.1.7) $a \in A$ 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 $Ay \subseteq Ax$.

2.1.7 Definition: 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** [2]. Si en plus A est non-trivial, commutatif, $(A, +, \cdot)$ s'appelle un **corps** [3].

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 $\mathrm{End}_{\mathbb{K}}(V)^* = \mathrm{GL}(V)$.

2.1.8 Definition: 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.

2.1.9 Definition: Élément nilpotent

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

2.1.10 Definition: 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.

2.1.11 Definition: 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.

2. Anglais : Division ring.
3. Anglais : Field.

2.1.12 Definition: Morphisme d'anneaux

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

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

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 $f^{-1} : B \to A$ 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 $f : A \to B$, $g : B \to C$ morphismes d'anneaux, alors $g \circ f$ est un morphisme d'anneaux aussi.

(iv) Si A, B sont anneaux, $f : A \to B$ un morphisme d'anneaux et $\widetilde{A} \subseteq A$, $\widetilde{B} \subseteq B$ sous-anneaux, alors $f(\widetilde{A}) \subseteq B$ et $f^{-1}(\widetilde{B}) \subseteq A$ sont sous-anneaux.

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

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

2.1.13 Lemme sur l'anneau des endomorphismes

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

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

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

Preuve : Il suffit de montrer $Z(\mathrm{End}_{\mathbb{K}}(V)) \subseteq \mathbb{K} \cdot \mathbb{1}_V$. Si $f, g \in \mathrm{End}_{\mathbb{K}}(V)$ 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 évidement 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 $\{e_1, .., e_n\}$ est une base de V et $\lambda_i \in \mathbb{K}$, $i = 1, .., n$.

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 $\lambda_i = \lambda \; \forall \; i = 1, ..., n$ et donc $f = \lambda \cdot \mathbb{1}_V$.
□

2.1.14 Definition: Anneau euclidien

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

1. Pour $a, b \in A \setminus \{0\}$ on a toujours $\mathrm{val}(a) \leq \mathrm{val}(ab)$.
2. Pour $(a, b) \in A \times (A \setminus \{0\})$ il existe deux $q, r \in A$ tels que $a = bq + r$ et $\mathrm{val}(r) < \mathrm{val}(b)$ 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 val(1) est la plus petite valeur de val() sur $A \setminus \{0\}$.

(ii) S'il existe une $\varphi : A \setminus \{0\} \to \mathbb{N}_0$ satisfaisante l'axiome (2), alors il existe toujours une valuation sur A, donnée par exemple par

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

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

(iii) Souvent on demande que val() soit définit sur tout l'anneau et satisfaisante $\mathrm{val}(0) = 0$.

(iv) Si $a, b, c \in A \setminus \{0\}$ sont tels que $a = bc$ et $c \notin A^\times$, alors $\mathrm{val}(b) < \mathrm{val}(a)$.

(v) Si $a \in A$ n'est pas inversible, alors $\mathrm{val}(a) > 0$.

Exemples

(i) Tout corps $\mathbb{K}$ est euclidien avec division euclidienne unique, en posant $\mathrm{val}(x) = 1$ pour tout $x \in \mathbb{K}^\times$.

(ii) L'anneau $\mathbb{Z}$ est euclidien avec division euclidienne unique, en posant $\mathrm{val}(n) := |n|$ 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 $\mathrm{val} : z \mapsto |z|^2$.

2.1.15 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 val() de B. Si $a, b \in A$ et $q, r \in B$ sont tels que $a = qb + r$ avec $\mathrm{val}(r) < \mathrm{val}(b)$ ou $r = 0$, alors $q, r \in A$.

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

□

2.1.16 Le morphisme de Frobenius

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

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

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.

2.2 Ideaux

2.2.1 Definition: Ideal

Soit $(A, +, \cdot)$ un anneau. Un **ideal 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 2.1.7.

Exemple : Considérons l'anneau A^{op} (anneau *oppose*) obtenu en modifiant la multiplication par $a \cdot_{\mathrm{op}} b := b \cdot a$. 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 $M_n(\mathbb{K})^{\mathrm{op}}$ avec la correspondance $M \mapsto M^T,\ M \in M_n(\mathbb{K})$.

2.2.2 Definition: Anneau simple

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

2.2.3 Lemme : Stabilité des idéaux sous morphismes

Soient A, B anneaux et $f : A \to B$ 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 $(B^\times, \cdot)$.

2.2.4 Definition: L'idéal engendré

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

$$\langle X \rangle_g := \bigcap_{\substack{X \subseteq I \subseteq A \\ I \text{ idéal à gauche}}} I \tag{2.2.4.1}$$

(resp. $\langle \cdot \rangle_d$ à **d**roite, $\langle \cdot \rangle_b$ **b**ilatère) est le plus petit idéal à gauche (à droite, bilatère) contenant X. On l'appelle l'idéal **engendré** [4] à gauche (à droite, bilatère) par X.

2.2.5 Lemme : Invariance de générateurs sous morphismes

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

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

2.2.6 Proposition : Représentation du $\langle X \rangle$

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

$$\langle X \rangle_g = \left\{ \sum_{i=1}^{n} a_i x_i : a_i \in A,\ x_i \in X \right\} =: \mathrm{span}_A(X) \quad . \tag{2.2.6.1}$$

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 (2.2.6.1) 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.

□

4. Anglais : Generated ideal.

2.2.7 Definition: 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**[5] si tout son idéal est principal.

2.2.8 Definition: 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 $a_1, .., a_n \in I$, c.a.d.

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

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

2.2.9 Idéaux engendré par idéaux

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

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

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

$$\prod_{j=1}^{n} I_j := \left\{ \prod_{j=1}^{n} a_j \ : \ a_j \in I_j \right\} \tag{2.2.9.1}$$

est exactement

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

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 $t \in \{\text{g,d,b}\}$ certain) on a

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

2.2.10 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 $\text{End}_{\mathbb{K}}(V)$.

5. Anglais : Principal ideal ring.

Preuve :

1. C'est évident que I_W est une sous-groupe additive du $\mathrm{End}_{\mathbb{K}}(V)$. En plus, si $f \in I_W$ et $g \in \mathrm{End}_{\mathbb{K}}(V)$ on a $(g \circ f)(W) = g(\{0\}) = \{0\}$, donc I_W est un idéal.
2. Soit $I \subseteq \mathrm{End}_{\mathbb{K}}(V)$ 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 $f_1, .., f_m \in I$ tels que

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

   Chaque $f \in I_W$ satisfait par définition $f(W) = \{0\}$, donc selon A.0.13(1) il y a $g_1, .., g_m \in \mathrm{End}_{\mathbb{K}}(V)$ 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 $J \subseteq \mathrm{End}_{\mathbb{K}}(V)$ 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 $f_1, .., f_m \in J$ tels que

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

   Chaque $f \in J_W$ satisfait $f(V) \leq W$, donc par A.0.13(2) il y a $g_1, .., g_m \in \mathrm{End}_{\mathbb{K}}(V)$ 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 $I := I_W = J_{\widetilde{W}} \subseteq \mathrm{End}_{\mathbb{K}}(V)$ un anneau bilatère définit par eux. Si $\{0\} \neq I \neq \mathrm{End}_{\mathbb{K}}(V)$, 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 $g :\in \mathrm{End}_{\mathbb{K}}(V)$ telle que

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

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

□

2.2.11 Definition: 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 [6]

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

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

2.2.12 Théorème : Factorisation des morphismes

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

1. $\ker \Pi = \{0\}$.
2. Le morphisme Π est *universel* : Soit $f : A \to B$ un morphisme d'anneaux avec $f(I) = \{0\}$, alors f *factorise* par A/I, c.a.d. il existe un unique morphisme $\overline{f} : A/I \to B$ d'anneaux tel que $f = \overline{f} \circ \Pi$.

6. Cette opération est bien définit, 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 $a'b' + I = ab + a\beta + \alpha b + \alpha\beta + I = ab + I$.

3. L'anneau A/I et le morphisme canonique $\Pi : A \to A/I$ est le *seul*[7] paire d'anneau et morphisme qui satisfont $\Pi(I) = \{0\}$ et (2). Autrement dit, si A_1 est un anneau et $\Pi_1 : A \to A_1$ un morphisme tel que $\Pi_1(I) = \{0\}$ et pour tout morphisme $f : A \to B, f(I) = \{0\}$ on a $f = \overline{f} \circ \Pi_1$ pour un unique morphisme $\overline{f} : A_1 \to B$, il faut $A/I \cong A_1$. En plus, Π_1 est simplement le transport du Π par un isomorphisme certain entre A/I et A_1.

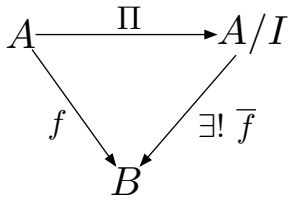


Figure 1: Sur la factorisation des morphismes.

Preuve :

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

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

et par l'unicité de factorisation Π_1 par Π_1 lui même, il faut $\overline{\Pi}_1 \circ \overline{\Pi}_2 = \mathrm{Id}$. De même on trouve que $\overline{\Pi}_2 \circ \overline{\Pi}_1 = \mathrm{Id}$, donc $\overline{\Pi}_1 : A_2 \to A_1$ est un isomorphisme avec l'inverse $\overline{\Pi}_2$.

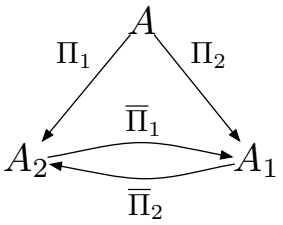


Figure 2: Sur la preuve du 2.2.12(3). Les factors $\overline{\Pi}_1, \overline{\Pi}_2$ sont des isomorphismes entre A_1 et A_2.

□

2.2.13 Théorème d'isomorphismes d'anneaux

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

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

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

Preuve : L'application $\overline{f}$ 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 $\overline{f}(a + \ker(f)) = 0_B$ il faut $a \in \ker(f)$ et donc $a + \ker(f) = 0_{A/\ker f}$, donc $\overline{f}$ est injective. Donc, $\overline{f}$ est un isomorphisme d'anneaux.

□

7. À isomorphismes.

Remarques :

(i) Se rappelle que $\ker(f)$ est un idéal bilatère dans A. Le morphisme $\overline{f} : A/\ker(f) \to f(A)$ est simplement un des deux factors de la factorisation comme décrit à 2.2.12(2). En particulier $f = \overline{f} \circ \Pi$ où $\Pi : A \to A/\ker(f)$ est le morphisme canonique de $A/\ker(f)$.

(ii) Soit $f : A \to B$ 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 quelqu'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 subjectivité de f satisfait $f(f^{-1}(V)) = V$.
Si en plus $f : A \to B$ est un morphisme d'anneaux, alors par 2.2.3 il envoie idéaux au idéaux du même type et vice versa.

2.2.14 Lemme : Transitivité des quotients

Soit $(A, +, \cdot)$ un anneau et $I \subseteq J \subseteq A$ deux idéaux bilatères. Soit $\Pi_I : A \to A/I$ 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 $\Pi_I : A \to A/I$ est un homomorphisme surjectif, par 2.2.3(2) $\Pi_I(J)$ est un idéal bilatère de $f(A) = A/I$. Soit $\Pi_J : A/I \to (A/I)/\Pi_I(J)$ le morphisme d'anneau quotient $(A/I)/\Pi_I(J)$ et $\Pi := \Pi_J \circ \Pi_I$. Par 2.2.13 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

$$\ker\Pi = \Pi_I^{-1}(\ker\Pi_J) = \Pi_I^{-1}\left(\Pi_I(J)\right) = \left\{a \in A \;\middle|\; \exists\, j \in J : a \in \underbrace{j + I}_{\subseteq J}\right\} \subseteq J$$

et donc finalement

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

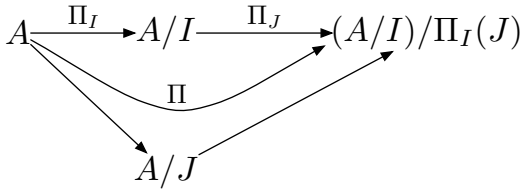


Figure 3: Sur la transitivité des anneaux quotients.

□

2.2.15 Definition: Idéal premier

Un idéal $I \subsetneq A$ d'anneau $(A, +, \cdot)$ est dit **premier**[8] 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 idéals 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 $u : A \to B$ 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 $\overline{u} : A/u^{-1}(I_B) \to B/I_B$ est injectif. Donc $A/u^{-1}(I_B)$ est intègre comme sous-anneau d'un anneau intègre.

2.2.16 Definition: Topologie de Zariski

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

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

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

Ainsi $\{\mathcal{Z}(I) \mid I \subseteq A \text{ idéal bilatère}\}$ est l'ensemble des fermés d'une topologie sur $\mathrm{Spec}(A)$ appelée **topologie Zariski**. Si $I \subseteq A$ est un idéal bilatère principal, la fermé $\mathcal{Z}(I)$ est appelé **fermé principal** et l'ouvert $\mathcal{Z}(I)^c := \mathrm{Spec}(A) \setminus \mathcal{Z}(I)$ **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

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

2.2.17 Definition: Idéal maximal

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

2.2.18 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 2.2.1(iv), A/I est un corps ssi il n'a que les deux idéaux $\{0\}$ et A. Par remarque 2.2.13(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.

□

2.2.19 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'une ordre. Soit $\mathcal{J} \subseteq \mathcal{F}$ un ensemble totalement ordonnée. 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 2.2.1(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.

□

2.2.20 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, $\mathrm{Specmax}(A) \subseteq \mathrm{Spec}(A)$.

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 2.2.18, l'anneau A/I est un corps et donc intègre. Donc I est premier et on retrouve lemme 2.2.20.

□

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 :

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

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 $\mathcal{Z}(0\mathbb{Z}) = \mathrm{Spec}(\mathbb{Z})$. Donc, le singleton $\{0\mathbb{Z}\} \in \mathrm{Spec}(\mathbb{Z})$ 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 $\mathrm{Spec}(\mathbb{Z})$, car $\mathcal{Z}(p\mathbb{Z}) = \{p\mathbb{Z}\}$.
Les idéaux maximaux sont

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

inclus dans $\mathrm{Spec}(\mathbb{Z})$ comme prévu par 2.2.20.

(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 engendré par les polynômes de degré 1 (*premiers*) :

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

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 $\mathcal{Z}(0 \cdot \mathbb{C}[X]) = \mathrm{Spec}(\mathbb{C}[X])$. 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 $\mathrm{Spec}(\mathbb{C}[X])$, car $\mathcal{Z}(P \cdot \mathbb{C}[X]) = \{P \cdot \mathbb{C}[X]\}$.

2.2.21 Théorème : Idéaux maximaux et anneaux locals

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) idéals maximaux à gauche, droite et bilatères sont égaux et on dit A un anneau **local**[10]. Si en plus A est commutatif, son idéal maximal (unique) est $A \setminus A^\times$.

2.2.22 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-enseble totalement ordonnée 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 du 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 !

□

2.2.23 Corollaire

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

Démonstration : Sens "⇒". 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 "⇐". Soit $a \in A$ un élément pas nilpotent, c.a.d. $a^n \neq 0 \ \ \forall\ n \in \mathbb{N}$. Considérons l'ensemble multiplicatif $S := \{a^n : n \in \mathbb{N}\}$, alors $\emptyset \neq S \subseteq A \setminus \{0\}$. Donc, par lemme 2.2.22 il y a un idéal premier $I \subseteq A$ disjoint de S. En particulier $a \notin I$.

□

2.2.24 Exemple : Les fonctions continues

Soit X un espace topologique compacte, de cardinal ≥ 2, connexe, fonctionnellement Hausdorff[11] et $A := \mathcal{C}(X, \mathbb{R})$ l'anneau des fonctions continues, réelles sur X. Pour $x \in X$ on pose $\mathfrak{M}_x := \{f \in A : f(x) = 0\}$. 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 Specmax(A) est une bijection.
3. Tout $\mathfrak{M}_x$ n'est pas un idéal de type fini.

Preuve :

1. La projection $\delta_x : A \to \mathbb{R}$ définie par $\delta_x : f \mapsto f(x)$ est un homomorphisme surjective d'anneaux, avec noyau $\ker \delta_x = \mathfrak{M}_x$. Donc par 2.2.13, $A/\mathfrak{M}_x \cong \mathbb{R}$ pour chaque $x \in X$. Car $\mathbb{R}$ est un corps, $A/\mathfrak{M}_x$ est un corps et donc par 2.2.18 $\mathfrak{M}_x$ 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 $f_1, .., f_n \in \mathfrak{M}$ 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 2.2.1(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 $f_1, .., f_n \in \mathfrak{M}_x$ tels que $\mathfrak{M}_x = \langle f_1, .., f_n\rangle$. 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 $\alpha_1, .., \alpha_n \in A$ 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 [12] $0 \not\equiv f \in \mathfrak{M}_x$ 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 $f : X \to \mathbb{R}$ est une fonction continue dont l'image n'est pas connexe. Ça, c'est une contradiction car X est connexe.

□

2.2.25 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 2.2.9) est donné par
$$\left\langle \prod_{i=1}^n I_i \right\rangle = \bigcap_{i=1}^n I_i \quad . \tag{2.2.25.1}$$
Son anneau quotient est isomorphe à l'anneau produit des anneaux quotients individuels :
$$A \Big/ \bigcap_{i=1}^n I_i \cong \bigtimes_{i=1}^n A/I_i$$
avec l'isomorphisme
$$\Phi : \left[a + \bigcap_{i=1}^n I_i\right] \mapsto (a + I_i)_{i=1}^n \quad , \quad a \in A \quad . \tag{2.2.25.2}$$

12. Note que par les propriétés de X il faut $\mathfrak{M}_x \neq \{0\}$ et donc $f \not\equiv 0$.

Preuve : On note $I := \bigcap_{i=1}^n I_i$. C'est évident que l'application $\Phi : A/I \to \overset{n}{\underset{i=1}{\times}} A/I_i$ de (2.2.25.2) est bien définie et un morphisme d'anneaux. Si $\Phi(a+I) = (0,..,0)$ il faut $a \in I_i \ \forall\ i$ et donc $a \in I$, donc Φ est injective. On va montrer par induction que Φ 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 subjectivité du Φ 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

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

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 $\Phi : A/I_1 \cap I_2 \to (A/I_1) \times (A/I_2)$ est surjectif.

Cas $n \geq 3$ **:** On suppose l'affirmation reste vrai pour $n-1$. Soit $I_1 + I_i = A$ pour $i \in \{2,..,n\}$, 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

$$I_1 + \left\langle \prod_{i=2}^n I_i \right\rangle = A \quad . \tag{2.2.25.3}$$

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

$$\left\langle \prod_{i=2}^n I_i \right\rangle = \bigcap_{i=2}^n I_i \tag{2.2.25.4}$$

et donc par le cas $n = 2$:

$$I_1 \cap \bigcap_{i=2}^n I_i \overset{(2.2.25.4)}{=} I_1 \cap \left\langle \prod_{i=2}^n I_i \right\rangle \overset{\substack{(2.2.25.3) \\ \text{cas } n=2}}{=} \left\langle I_1 \cdot \left\langle \prod_{i=2}^n I_i \right\rangle \right\rangle = \left\langle \prod_{i=1}^n I_i \right\rangle \quad .$$

De plus, on a le chaîne des isomorphismes

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

Ça finit la preuve.

□

Remarques

(i) L'isomorphie du morphisme (2.2.25.2) est équivalent à la déclaration suivante :

$$\forall\ b_1,..,b_n \in A \ :\ \exists\ a \in A \ :\ a \in b_i + I_i \ \ \forall\ i \tag{2.2.25.5}$$

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 $n_1,..,n_k \in \mathbb{N}$ deux à deux premiers entre eux [13] et $a_1,..,a_k \in \mathbb{Z}$ n'importante quels. Alors, il existe un entier $x \in \mathbb{Z}$, unique modulo [14] $n := \prod_{i=1}^k n_i$, tel que $x = a_i \pmod{n_i}$ $\ \forall i \in \{1,..,k\}$.

13. Noter que par Bézout 5.1.10, 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 5.1.9(vi) on a $\bigcap_{i=1}^k \mathbb{Z}n_i = \mathbb{Z}\,\mathrm{ppcm}(n_1,..,n_k) = \mathbb{Z}\prod_{i=1}^k n_i$.

2.3 Anneaux Noetheriens

2.3.1 Definition: 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.

2.3.2 Théorème : Caractérisation des anneaux noetheriens

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

1. A est noetherien.
2. Toute suite croisante $I_1 \subseteq I_2 \subseteq .. \subseteq A$ 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-vide d'idéaux à gauche admet un élément maximal.

Preuve :

1 ⇒ 2 **:** L'ensemble $I := \bigcup_{i=1}^{\infty} I_i$ est un idéal dans A, donc avec un nombre fini de générateurs $a_1, .., a_n$. Il existe donc un $N \in \mathbb{N}$ assez grand tel que $a_1, .., a_n \in I_N$. Donc $I = I_N$.

2 ⇒ 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 croisante des idéaux. Ça, c'est une contradiction !

3 ⇒ 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 !

□

2.3.3 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 $\Pi : A \to A/I$, 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 $a_1, .., a_n \in A$. Après 2.2.5(1) on a

$$J = \Pi(\Pi^{-1}(J)) = \Pi\big(\langle a_1, .., a_n \rangle_g\big) \overset{2.2.5(1)}{=} \langle \Pi(a_1), .., \Pi(a_n) \rangle_g$$

et J est donc de type fini.

□

2.4 Algèbres

2.4.1 Definition: R-Algèbre

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

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

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

2.4.2 Definition: Morphisme de R-algèbres

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

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

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

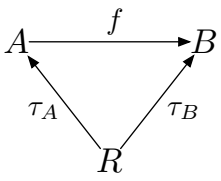


Figure 4: Illustration d'un morphisme de R-algèbres. Le diagramme commute.

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

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

Le morphisme d'anneaux

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

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 $\mathbb{K} \hookrightarrow \mathbb{L}$.

3 Modules

3.1 Modules

3.1.1 Definition: Opération d'un anneau sur un groupe, module

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

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

Autrement dit, ρ 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. $\rho(1_A) = \mathrm{Id}_G$.

On appelle $\rho(a) \in \mathrm{End}(G)$ l'**homothetie** 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. $ax \in G_0 \ \ \forall\ x \in G_0,\ a \in A$.

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.

3.1.2 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.

3.1.3 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 $f : G \to H$ qui commute avec l'opération de A, ça veut dire $f(ax) = a(f(x))$ pour $a \in A,\ x \in G$.

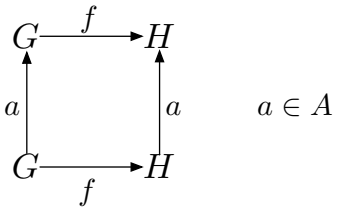


Figure 5: Illustration d'une application A-linéaire entre deux A-modules. Le diagramme commute.

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

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

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

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

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

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

munit $\mathrm{Hom}_A(G, H)$ 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 $f : G \to H$ A-linéaire. Alors $f(G_0)$ et $f^{-1}(H_0)$ sont sous-A-modules de H et G respectivement.

(iii) Si $f : G \to H$ est un isomorphisme de A-modules, alors l'inverse f^{-1} est également. De plus, l'isomorphie entre A-modules est une relation d'équivalence.

3.1.4 Definition: 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 $\Pi : N \to G/N$ 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

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

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 $\Phi : A \to B$ un morphisme d'anneaux. Si $(G, +)$ est un B-module à gauche, alors l'application $A \times G \to G$ 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 $u \in \mathrm{Hom}_B(G, H)$ est une application B-linéaire entre deux B-modules G, H, alors $u \in \mathrm{Hom}_A(\Phi_* G, \Phi_* H)$. La réciproque n'est pas forcement vrais.

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 $G \to H$ 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 et 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 2.2.11. Alors, il existe une *correspondance bijective* entre (A/I)-modules et A-modules annulés 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.

3.1.5 Théorème : Universalité d'un module quotient

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

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

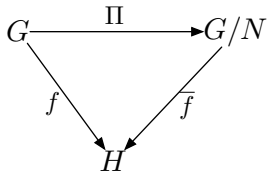


Figure 6: Sur la universalité du groupe quotient G/N : Factorisation d'un morphisme f. Le diagramme commute.

Preuve :

1. Trivial.
2. Le preuve serait être proche à la preuve de 2.2.12. Pose $\overline{f}(g+N) := f(g)$ pour $g \in G$, alors $\overline{f} : G/N \to H$ est bien défini, A-linéaire et satisfait $f = \overline{f} \circ \Pi$. Unicité suit de la surjectivité de Π.
3. Par supposition on sait déjà que $N \subseteq \ker(f)$. Si $\overline{f}$ 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 $\overline{f}(x+N) = 0$ implique $f(x) = 0$ et donc $x \in N$, c'est-à-dire $\ker(\overline{f}) = \{0_{G/N}\}$.
4. Soient G_1, G_2 deux A-modules et $\Pi_1 : G \to G_1,\ \Pi_2 : G \to G_2$ morphismes universels satisfaisant $\Pi_1(N) = \Pi_2(N) = \{0\}$. Alors il existe morphismes A-linéaires $\overline{\Pi}_1 : G_2 \to G_1,\ \overline{\Pi}_2 : G_1 \to G_2$ tels que $\Pi_1 = \overline{\Pi}_1 \circ \Pi_2$ et $\Pi_2 = \overline{\Pi}_2 \circ \Pi_1$. Donc
$$\overline{\Pi}_1 \circ \overline{\Pi}_2 \circ \Pi_1 = \overline{\Pi}_1 \circ \Pi_2 = \Pi_1$$
et par l'unicité de la factorisation de Π_1 par Π_1 lui même il faut $\overline{\Pi}_1 \circ \overline{\Pi}_2 = \mathrm{Id}$. De même on trouve que $\overline{\Pi}_2 \circ \overline{\Pi}_1 = \mathrm{Id}$, donc $\overline{\Pi}_1 : G_2 \to G_1$ est un isomorphisme de A-modules avec l'inverse $\overline{\Pi}_2$.

□

3.1.6 Lemme : Sous-modules de modules quotients

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

$$(G/N)/Q \cong_A G/\Pi^{-1}(Q) \tag{3.1.6.1}$$

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

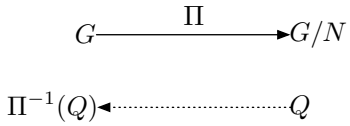


Figure 7: Sur la correspondance entre sous modules de G et du module quotient G/N.

Preuve : Soit $Q \leq G/N$ un sous-A-module de G/N. Alors, par remarque 3.1.3(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 contentant 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 $Q \to \Pi^{-1}(Q)$ 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 Π est surjective.

Soit $Q \leq G/N$ un sous-A-module de G/N et $\Pi_1 : (G/N) \to (G/N)/Q$ le morphisme quotient de $(G/N)/Q$. Soit $\Pi_0 : G \to G/\Pi^{-1}(Q)$ le morphisme quotient de $G/\Pi^{-1}(Q)$. Pour prouver l'isomorphisme (3.1.6.1) on va montrer que $\Pi_1 \circ \Pi : G \to (G/N)/Q$ satisfait la propriété universelle 3.1.5(2) de $\Pi_0 : G \to G/\Pi^{-1}(Q)$ et utilise l'unicité d'universalité 3.1.5(4). Évidement $\Pi_1 \circ \Pi(N) = \{0\}$ et $\Pi_1 \circ \Pi$ est surjective.

Soit or $f : G \to H$ A-linéaire telle que $f(\Pi^{-1}(Q)) = \{0\}$. Alors $f(N) = 0$ et on peut trouver une A-linéaire $\overline{f} : (G/N) \to H$ telle que $f = \overline{f} \circ \Pi$. Car $f(\Pi^{-1}(Q)) = \{0\}$ il faut $\overline{f}(Q) = 0$. Donc, on peut trouver une A-linéaire $\overline{f}' : (G/N)/Q \to H$ telle que $\overline{f} = \overline{f}' \circ \Pi_1$, c'est-à-dire $f = \overline{f}' \circ \Pi_1 \circ \Pi$. Car $\Pi_1 \circ \Pi$ est surjective, $\overline{f}'$ est unique. Par 3.1.5(4) on a trouvé $(G/N)/Q \cong_A G/\Pi^{-1}(Q)$.

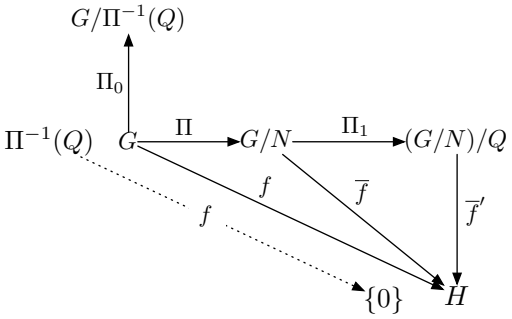


Figure 8: Sur la preuve de l'isomorphie $(G/N)/Q \cong_A G/\Pi^{-1}(Q)$, par factorisation des fonctions $f : G \to H$ satisfaisant $f(\Pi^{-1}(Q)) = \{0\}$.

□

3.1.7 Le théorème d'isomorphismes pour modules

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

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

□

3.1.8 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 $f := \Pi \circ i : M \to (M + N)/N$ où $\Pi : (M + N) \to (M + N)/N$ est le morphisme quotient de $(M + N)/N$ et $i : M \to (M + N)$ 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

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

□

3.1.9 Definition: Sous-module engendré

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

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

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

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

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

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

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'importante quel et $f : G \to H$ A-linéaire, alors

$$\mathrm{span}_A f(X) = f\left[\mathrm{span}_A(X)\right] \quad . \tag{3.1.9.1}$$

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'importante quel, alors il existe un nombre fini d'éléments $x_1, .., x_n \in X$ tel que $G = \mathrm{span}_A(x_1, .., x_n)$. 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 $\bigcup_{y \in Y} \{x_{y1}, .., x_{yn_y}\}$.

(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 $\overline{1}$ et est donc cyclique.

(vi) Inversement, tout A-module cyclique $G = \mathrm{span}_A\{g\}$ est isomorphe à un quotient A/J pour un idéal $J \subseteq A$. Pour le voir, considérer le morphisme de A-modules surjectif

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

et appliquer le théorème d'isomorphismes 3.1.7.

(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 rappeller qu'il existe une association bijective, croisante entre les idéaux de A/J et les idéaux entre J et A.

3.1.10 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 3.1.16 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 $\mathbb{Z}^n = \text{span}_{\mathbb{Z}}\{(1,0,..,0),..,(0,..,0,1)\}$.

(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 $\text{span}_{\mathbb{Z}}\left\{\frac{p_1}{q_1},..,\frac{p_n}{q_n}\right\}$ 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 $q_1,..,q_n$.

(vi) Le $\mathbb{Z}$-module $\mathbb{R}$ n'est pas de type fini. S'il était, il faudrait existe $r_1,..,r_n \in \mathbb{R}$ tels que l'application $\mathbb{Z}^n \to \mathbb{R},\ (k_1,..,k_n) \mapsto k_1r_1 + \cdots + k_nr_n$ est surjective. Mais cela est impossible, car $\mathbb{R}$ est de cardinal plus grand que $\mathbb{Z}^n$.

3.1.11 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 croisante $G_1 \leq G_2 \leq .. \leq G$ 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 : Analogue à la preuve de théorème 2.3.2 sur anneaux noetheriens.

3.1.12 Definition: 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 $f_n : G_n \to G_{n+1}$ qui satisfait $\text{image}(f_n) = \ker(f_{n+1})$. Souvent tous sauf un nombre fini de modules $G_1,..,G_n$ 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 $\text{image}(f_k) = \ker(f_{k+1})\ \forall k \in \{1,..,n-2\}$.

3.1.13 Lemme sur modules de type fini et suites exactes

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

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

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

□

3.1.14 Corollaire sur modules de type fini

Soit $(A, +, \cdot)$ un anneau, G, H A-modules et $f : G \to H$ 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 appliquer lemme 3.1.13 sur la suite exacte

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

on déduit l'affirmation.

□

3.1.15 Lemme sur modules noetheriens et suites exactes

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

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

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

Preuve :

Direction "⇐" : Supposons que G_2 est noetherien. Soit $N_1 \leq N_2 \leq \cdots \leq G_3$ une suite croissante de sous-modules de G_3, alors $g^{-1}(N_1) \leq g^{-1}(N_2) \leq \cdots \leq G_2$ est une suite croissante de sous-modules de G_2. Par 3.1.11 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

$$N_n \overset{g}{\underset{\text{surj.}}{=}} g(g^{-1}(N_n)) = g(g^{-1}(N_{n_0})) \overset{g}{\underset{\text{surj.}}{=}} N_{n_0} \quad \forall n \geq n_0 \quad ,$$

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

Direction "⇒" : Supposons que G_1, G_2 sont noetheriens. Soit $N_1 \leq N_2 \leq \cdots \leq G_2$ une suite croissante de sous-modules de G_2, alors $f^{-1}(N_1) \leq f^{-1}(N_2) \leq \cdots \leq G_1$ et $g(N_1) \leq g(N_2) \leq \cdots \leq G_3$ sont suites croissantes de sous-modules de G_1 et G_3 respectivement. Par supposition et théorème 3.1.11, 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

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

Note qu'on à 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 $f : G \to H$ un morphisme de A-modules, alors $f(G)$ est un sous-module noetherien. Pour le voir considère la suite exacte

$$0 \longrightarrow \ker(f) \overset{\text{inclusion}}{\longrightarrow} G \xrightarrow{f} f(G) \longrightarrow 0 \quad .$$

3.1.16 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 "⇒" : Démonstration par récurrence : Considérons l'inclusion $i : A \hookrightarrow A^n,\ a \mapsto (a, 0, .., 0)$ et la projection $p : A^n \to A^{n-1},\ (a_1, .., a_n) \mapsto (a_2, .., a_n)$. Alors la suite

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

est exacte. Par lemme 3.1.15, si A et A^{n-1} sont A-modules noetheriens, alors A^n est également.

Direction "⇐" : Considérons le sous-A-module $A \times \{0\} \times \cdots \times \{0\} \leq A^n$ qui est isomorphe à A. Comme tout sous-module d'un module noetherien est lui même noetherien, on conclut l'affirmation.

□

Remarque : Voir 7.0.7 pour une affirmation plus forte sur anneaux intègres, principaux.

3.1.17 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

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

est surjective. Par 3.1.16 A^n est noetherien. Par conséquence 3.1.15(i) G est noetherien.

□

3.1.18 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_{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_{tor} est un sous-module de G.

(ii) G/G_{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

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

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

3.1.20 Exemple : Le corps quotient

Soit $(A, +, \cdot)$ un anneau commutatif et $S \subseteq A$ un sous ensemble multiplicatif [15] 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

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

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

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 $\sigma : A \to S^{-1}A,\ a \overset{\sigma}{\mapsto} \frac{a}{1}$ est un morphisme d'anneaux, qui est injectif si A est intègre et $0 \notin S$. En particulier, par exemple 3.1.4(iii) tout $S^{-1}A$-module peut être regardé comme A-module via le transport de σ.

Note :

> En cas que A est intègre, $S := A\setminus\{0\}$ est une partie multiplicatif de A contenant 1 et $S^{-1}A =: \mathrm{Quot}(A)$ est un corps, le **corps quotient** [16] 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 $\sigma : A \hookrightarrow \mathrm{Quot}(A)$ est un plongement de A dans son corps quotient.
>
> En fait, $\mathrm{Quot}(A)$ 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 $\Phi : \mathrm{Quot}(A) \hookrightarrow \mathbb{K}$ 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 $A \cong \mathrm{Quot}(A)$.
>
> Un exemple typique est $\mathrm{Quot}(\mathbb{Z}) \cong \mathbb{Q}$.

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

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

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

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

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 $i : M \to S^{-1}M,\ m \overset{i}{\mapsto} \frac{m}{1}$ 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.

15. C'est-à-dire $S \cdot S \subseteq S$.
16. Anglais : Field of Fractions ou Field of Quotients.

3.1.21 Definition: 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 $\bigtimes_{i\in I} G_i$ possède une structure *naturelle* d'un A-module avec les lois coordonnées par coordonnées :

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

Avec ce lui, on dit $\bigtimes_{i\in I} G_i$ 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 $\bigtimes_{i\in I} G_i$ des uplets à support fini :

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

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

3.1.22 Definition: 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

$$\bigoplus_{i\in I} G_i \to \sum_{i\in I} G_i \quad , \quad (g_i)_{i\in I} \mapsto \sum_{\substack{i\in I \\ g_i \neq 0}} g_i \quad . \tag{3.1.22.1}$$

La somme $\sum_{i\in I} G_i$ (vois 3.1.9) est dit **directe** ssi (3.1.22.1) 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 $0 \neq (g_i)_{i\in I_0} \in \bigtimes_{i\in I_0} G_i$ 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 $f : G \to G$ défini comme $f(\varkappa + \lambda) := \varkappa$ pour $\varkappa \in K$, $\lambda \in L$ et applique le théorème d'isomorphismes 3.1.7.

3.2 Modules libres

3.2.1 Definition: 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 $a_1, .., a_n \in A$ et $i_1, .., i_n \in I$ tels que $a_1 b_{i_1} + \cdots + a_n b_{i_n} = 0$, 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 $G = \operatorname{span}_A(b_i : i \in I)$ et $(b_i)_{i\in I}$ est A-linéairement indépendant. On dit G **libre** s'il possède une base.

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

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

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 $e_i = (0,..,0,\underset{\substack{\uparrow\\ i}}{1},0,..)$. 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 $\Phi : G \to H$ 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 $\mathrm{Ann}_A(b_{i_1} + \cdots + b_{i_n}) = \{0\}$ pour tout $i_1,..,i_n \in I$ 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 $f : G \to H$ 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 3.2.11(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 indépendant, alors B est A-linéairement indépendant.

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 ≥ 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 3.2.1(iv), ça implique que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module libre.

3.2.2 Definition: 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 $\mathrm{span}_A(B) = G$ et si pour toute $B_0 \subsetneq B$ on a $\mathrm{span}_A(B_0) \subsetneq G$.
- **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 $\mathrm{span}_A(B)$ minimale.

(ii) Soit $B \subseteq G$ linéairement indépendant. Alors, B est linéairement indépendant maximal dans $\mathrm{span}_A(B)$.

(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 3.2.16 pour quelques exemples.

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

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

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

□

3.2.4 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'importante quelle. Alors, le 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 $\Phi : A^{(I)} \to G$ 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 $\Phi : A^{(I)} \to G$ comme

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

Alors, Φ est surjective et injective d'après remarque 3.2.1(v).

2 $\Rightarrow$ 1 **:** Par remarque 3.2.1(iii) les $(b_i)_{i \in I}$ forment une base de G.

3 $\Leftrightarrow$ 1 **:** Par définition 3.1.22 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 3.2.1(v) ça c'est vrai ssi $(b_i)_{i \in I}$ forme une base de G.

□

3.2.5 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 $\overline{g} := g + M$ la classe correspondant à g. Soit $B \subseteq G$ tel que $\overline{B} := \{\overline{b}\}_{b\in B}$ est une base de G/M. Pose $N := \mathrm{span}_A(B)$. Note que par remarque 3.2.1(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 un classe $\overline{g}$ de G/M, où

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

pour quelques $\overline{b}_i \in \overline{B},\ a_i \in A$, c'est-à-dire $x \in \mathrm{span}_A(B) + M$. 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 $\overline{n} = \overline{0}$. 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 $\overline{n} = \sum_i a_i\overline{b_i}$. Par supposition les $\overline{b}_i$ sont linéairement indépendants, donc $a_i = 0$ et $n = 0$. Par conséquence ainsi $m = 0$.

□

3.2.6 Corollaire sur morphismes surjectifs

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

$$\boxed{G \cong \ker(\varphi) \oplus L}$$

Preuve : Par le théorème d'isomorphismes on sait que $G/\ker(\varphi) \cong_A L$. Comme L est libre, par 3.2.5 on sait que $\ker(\varphi)$ possède un supplément $\widetilde{L}$ dans G, isomorphe à L. Donc $G = \ker(\varphi) \oplus \widetilde{L} \cong_A \ker(\varphi) \oplus L$.

□

3.2.7 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 3.2.5, G est la somme directe de deux sous-A-modules libres et par 3.2.12 libre lui même.

□

3.2.8 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 $f : G \to H$ tel que $f(g_i) = h_i \ \ \forall\ i \in I$. Si de plus $(h_i)_{i\in I}$ est une base de H, ce morphisme est en fait un isomorphisme.

Preuve : Soit $\Phi_G : A^{(I)} \to G$ l'isomorphisme satisfaisant $\Phi_G(e_i) = g_i$ (vois 3.2.4). 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 $f : G \to H$ est un morphisme de A-modules satisfaisant $f(g_i) = h_i\ \forall i$. L'unicité de f suit de remarque 3.2.1(viii). Si de plus $(h_i)_{i\in I}$ est une base de H, soit $\Phi_H : A^{(I)} \to H$ l'isomorphisme satisfaisant $\Phi_H(e_i) = h_i$. Alors, l'isomorphisme $f := \Phi_H \circ \Phi_G^{-1}$ satisfait les conditions.

□

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

3.2.9 Definition: 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 $\Phi_G : A^{(I)} \to G$ et $\Phi_H : A^{(J)} \to H$ les isomorphismes satisfaisant $\Phi_G(e_i) = g_i$ et $\Phi_H(e_i) = h_i$ respectivement (voir 3.2.4(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 $\widetilde{f} : H \to C$ A-linéaire avec matrice $\Lambda(\widetilde{f}) := (\Lambda_{kj}(\widetilde{f}))_{j\in J, k\in K}$, alors $\widetilde{f}\circ f : G \to C$ a la matrice

$$\Lambda_{ki}(\widetilde{f}\circ f) = \sum_{\substack{j\in J \\ \Lambda_{ji}(f)\neq 0 \\ \Lambda_{kj}(\widetilde{f})\neq 0}} \Lambda_{ji}(f)\cdot\Lambda_{kj}(\widetilde{f}) \quad . \tag{3.2.9.1}$$

Remarques :

(i) Fait attention à l'ordre des matrices dans (3.2.9.1) en cas que A est non-commutatif !

(ii) Si $f : G \to H$ est l'isomorphisme donné par lemme 3.2.8, il possède la matrice $\Lambda_{ji}(f) = \delta_{ij}$.

3.2.10 Lemme : Bases de corps quotients

Soit $(A,+,\cdot)$ un anneau intègre et $n \in \mathbb{N}$. On considère A plongé dans son corps quotient $\mathbb{K} := \mathrm{Quot}(A)$ par l'identification $a \mapsto \frac{a}{1}$, $a \in A$ (vois 3.1.20). 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 $\frac{a_1}{s_1}, .., \frac{a_m}{s_m} \in \mathbb{K}$ on peut suppose $s_1 = .. = s_m$. Les $(c_j)_{j\in J}$ sont $\mathbb{K}$-linéairement indépendants :

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

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

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

□

3.2.11 Théorème : Cardinalité des bases finies

Soit $(A,+,\cdot)$ un anneau commutatif 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 pour anneaux intègres : D'après lemme 3.2.4 G est isomorphe à $A^n := \overset{n}{\underset{i=1}{\times}} A$, qui possède la A-base canonique $(e_i)_{i=1}^n$. Donc par remarque 3.2.1(iii) il suffit de montrer l'affirmation pour le A-module A^n. On considère A plongé dans son corps quotient $\mathbb{K} := \mathrm{Quot}(A)$ et donc $A^n \hookrightarrow \mathbb{K}^n$. D'après lemme 3.2.10 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 $sx = (\frac{s}{1}\frac{a_i}{s})_{i=1}^n = (a_i)_{i=1}^n \in A^n$.

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, alors A^n est un A-module de rang n.

(iii) Considère l'anneau $A := \mathcal{C}(X)$ d'exemple 2.2.24 et l'idéal $\mathfrak{M}_x := \{f \in A : f(x) = 0\}$. Alors, par 2.2.24 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 3.2.1(iii) $\mathfrak{M}_x$ n'est pas libre, car sinon il serait de type fini.

3.2.12 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'importante quels. 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, $I = \{1, .., N\}$ 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). □

3.2.13 Lemme : Condition suffisante pour modules libres

Soit $(A, +, \cdot)$ un anneau commutatif, G, H A-modules et $f : G \to H$ 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 3.1.7, $G/\ker(f) \cong_A f(G)$ et donc $G/\ker(f)$ est libre de rang n. Par 3.2.5, $\ker(f)$ possède un sous-A-module $N \leq G$ supplémentaire de rang n, c'est-à-dire $G = \ker(f) \oplus N$. Par 3.2.12(4) G est libre de rang $m + n$.

□

3.2.14 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 $f \in \mathrm{End}_{\mathbb{K}}(V)$. Alors le loi de composition

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

munit le groupe sous-adjent 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 $f : V \to V$ 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 $e_0 := (1, 0, ..)$, c'est-à-dire V est de type fini. De plus, V n'a pas de torsion.

3.2.15 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

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

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
$$\frac{1}{p^n}\mathbb{Z} \subsetneq \frac{1}{p^m}\mathbb{Z} \quad .$$
3. Si $(n_k)_{k=1}^{\infty} \subseteq \mathbb{N}_0$ sont tels que $\sup\limits_{k\in\mathbb{N}} n_k = \infty$, on a
$$\mathbb{Z}[p^{-1}] = \bigcup_{k=1}^{\infty} \frac{1}{p^{n_k}}\mathbb{Z} \quad .$$
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 $b_1, .., b_m \in B$ tels que $\mathbb{Z} \subseteq \operatorname{span}\{b_k\}_{k=1}^m$ 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
$$\mathbb{Z}[p^{-1}] = \operatorname{span}_{\mathbb{Z}} \left\{ \tfrac{q_1}{p^{n_1}}, .., \tfrac{q_m}{q^{n_m}} \right\} \subseteq \operatorname{span}_{\mathbb{Z}} \left\{ \tfrac{1}{p^{n_1}}, .., \tfrac{1}{p^{n_m}} \right\} \quad .$$
Alors, par (2) il faudrait $\mathbb{Z}[p^{-1}] \subseteq \frac{1}{q^n}\mathbb{Z}$ où $n := \max\limits_{1\le k\le m} n_k$. Mais ça n'est pas possible.
5. **Direction "⇒" :** Soit $B \subseteq \mathbb{Z}[p^{-1}]$ génératrice. Alors $1 \in \operatorname{span}_{\mathbb{Z}}(B)$, c'est-à-dire il existe $b_1, .., b_m \in B$ tels que $1 \in \operatorname{span}_{\mathbb{Z}}\{b_i\}_{i=1}^m$ et donc $\mathbb{Z} \subseteq \operatorname{span}_{\mathbb{Z}}\{b_i\}_{i=1}^m$.
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 $\operatorname{span}_{\mathbb{Z}}(B) \subseteq p^{-N}\mathbb{Z}$ 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 $n_k \overset{k\to\infty}{\longrightarrow} \infty$.
Direction "⇐" : Soient $B \subseteq \mathbb{Z}[p^{-1}]$ quelconque et $b_1, .., b_m \in B,\ (c_k)_{k=1}^n \subseteq B$ comme décrit. Alors, pour tout $c_k = \frac{a_k}{p^{n_k}}$ on a

$$\operatorname{span}\{c_k, b_1, .., b_n\} = c_k\mathbb{Z} + \operatorname{span}_{\mathbb{Z}}\{b_k\}_{k=1}^m \supseteq c_k\mathbb{Z} + \mathbb{Z} = \frac{1}{p^{n_k}} \underbrace{[a_k\mathbb{Z} + p^{n_k}\mathbb{Z}]}_{\mathbb{Z} \text{ par Bézout 5.1.10}} = \frac{1}{p^{n_k}}\mathbb{Z} \quad . \tag{3.2.15.1}$$

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

$$\operatorname{span}_{\mathbb{Z}}\left[\{c_k\}_{k=1}^{\infty} \cup \{b_k\}_{k=1}^m\right] \overset{(3.2.15.1)}{\supseteq} \bigcup_{k=1}^{\infty} \frac{1}{p^{n_k}} \overset{(3)}{=} \mathbb{Z}[p^{-1}] \quad .$$

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 $\mathbb{Z} \subseteq \mathrm{span}_{\mathbb{Z}}(B_0)$ 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 inégales. 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 3.2.2(iii) ça implique que B n'est pas une base.

□

3.2.16 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 $\mathfrak{M}_x$ pour un $x \in [0, 1]$. Vois exemple 3.2.11(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 $M := \{\overline{0}, \overline{2}\}$ 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.

3.2.17 Théorème : Modules de type fini sur un anneau noetherien

Soit $(A, +, \cdot)$ un anneau noetherien à gauche (vois 2.3.1). Alors, tout sous-A-module d'un A-module $(M, +)$ de type fini est de type fini.

Preuve : Soit M engendré par la famille $(\xi_i)_{i=1}^n$. Alors, le morphisme de A-modules $\Phi : A^n := \overset{n}{\underset{i=1}{\times}} A \to M$ défini par $\Phi : (a_i)_{i=1}^n \mapsto \sum_{i=1}^n a_i \xi_i$ est surjectif. Alors, par remarques 3.1.3(ii) et 3.1.9(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 3.1.9(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 $\Pi : A^n \to A,\ \Pi : ((a_i)_{i=1}^n) \mapsto a_1$ sur N. Alors $\Pi\big|_N(N) =: J$ est un idéal à gauche et car A est noetherien, de type fini. D'autre part, $\ker \Pi\big|_N \subseteq \ker(\Pi) \hookrightarrow A^{n-1}$, donc $\ker \Pi\big|_N$ est par supposition de type fini. Par 3.1.14 ça implique que N est de type fini.

□

3.2.18 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 $I = \{1, .., n\}$. 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.

□

4 Polynômes et séries formelles

4.1 Polynômes

4.1.1 Definition: 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** $*: A\times A\to A$ 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 $f: A\to B$ 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 2.4.1. Puisque, tout homomorphisme $\tau: R\to Z(A)$ 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 4.1.1, alors $\tau: R\to Z(A)$ donnée par $\tau(\rho):=\rho\cdot 1_A$, $\rho\in R$ fait de A une R-algèbre de type 2.4.1.
La même équivalence existe entre les définitions 2.4.2 et 4.1.1 des morphismes de R-algèbres.

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

4.1.2 Definition: 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 monoide, tels que :
- A est la somme directe des A_n,
- Pour $n,m\in S$ on a $A_n*A_m\subseteq A_{n+m}\ \ \forall\, n,m\in S$.

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

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

4.1.3 Definition: 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

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

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

4.1.4 Definition: L'anneau des polynômes

Soit $(S,+)$ un monoide commutatif et $(A,+,\cdot)$ un anneau commutatif (vois 2.1.1), dit l'**anneau base**. On forme le A-module libre $A^{(S)}$ sur S (vois 3.2.1) 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

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

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 $A[S] := \left[A^{(S)}, +, *\right]$ la A-algébre 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 $A[\mathbb{N}_0^n] =: A[X_1, .., X_n]$. Pour $s = (s_1, .., s_n) \in \mathbb{N}_0^n$ on note

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

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

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

En particulier, on note

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

(ii) Pour $S := (\mathbb{Z}^n, +)$, $A[\mathbb{Z}^n] =: A[X_1^{\pm 1}, .., X_n^{\pm 1}]$ 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

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

4.1.5 Théorème : La propriété universelle

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

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

   Soit $f : (A, +, \cdot) \to (B, +, \cdot)$ 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 [18]) [19] $\overline{f} : (A[S], +, *) \to (B, +, \cdot)$ tel que $f = \overline{f} \circ i$. En fait, les prolongements $\overline{f}$ de f par i sont en bijection avec les morphismes de monoides $(S, +) \to (B, \cdot)$ via l'attribution $\overline{f} \mapsto \overline{f} \circ \sigma$.

2. Soit $(C, +, *)$ une A-algèbre commutative, $j : A \to C$ un morphisme de A-algèbres et $\tau : (S, +) \to (C, *)$ un morphisme de monoides. Si le triplet (j, τ, 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 $f : A \to B$ 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.

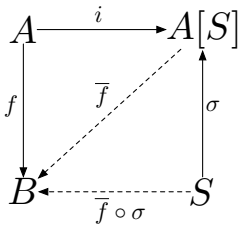


Figure 9: Sur la propriété universelle de $A[S]$: Les prolongements d'un morphisme d'anneaux fixé $f : A \to B$ sont en bijection avec les morphismes des monoides $S \to B$. Le diagramme ci-dessus commute.

Preuve :

(i) Évidement, si $\overline{f} : (A[S], +, *) \to (B, +, \cdot)$ est un morphisme d'anneaux, la composition $\overline{f} \circ \sigma : (S, +) \to (B, \cdot)$ est un morphisme de monoides. Soit $\mu : (S, +) \to (B, \cdot)$ un morphisme de monoides quelconque. Pose

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

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

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

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

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

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

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

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

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

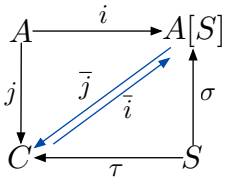


Figure 10: Sur l'unicité du $A[S]$ par rapport à son universalité : Si (j, τ, C) satisfait la même propriété, alors $A[S]$ et C sont A-algèbres isomorphes.

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

□

4.1.6 Corollaire : Morphismes de A-algèbres de $A[S]$

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

Preuve : Toute d'abord, notons que tout morphisme de A-algèbres $\overline{f} : A[S] \to B$ est prolongement du morphisme de A-algèbres $\overline{f} \circ i : A \to B$, où $i : A \hookrightarrow A[S]$ est l'inclusion. Mais $\overline{f} \circ i$ est unique, donné par $(\overline{f} \circ i)(a) = a \circ 1_B \ \forall a \in A$ et noté $f := \overline{f} \circ i$. Par théorème 4.1.5, les morphismes de monoides $(S,+) \to (B,\cdot)$ 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 monoides $\mu : (\mathbb{N}_0^n,+) \to (B,\cdot)$ et déterminé par les images $\mu(e_i),\ i = 1,..,n$ 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 $\mu : S \to B$ tel que $\mu(e_i) = b_i$, c'est-à-dire les morphismes de monoides $(\mathbb{N}_0^n,+) \to (B,\cdot)$ sont en bijection avec B^n via l'attribution $\mu \mapsto (\mu(e_i))_{i=1}^n$.

D'autre part, par 4.1.6 les morphismes de A-algèbres $\overline{f} : A[X_1,..,X_n] \to (B,+,\cdot)$ sont en bijection avec les morphismes de monoides $(\mathbb{N}_0^n,+) \to (B,\cdot)$ via l'attribution $\overline{f} \mapsto \overline{f} \circ \sigma$, donc en bijection avec B^n. En fait, cette bijection est donnée par l'attribution $\overline{f} \mapsto (\overline{f}(X_i))_{i=1}^n \in B^n$. Autrement dit, les morphismes de A-algèbres $A[X_1,..,X_n] \to B$ sont caractérisés par leurs images des monômes $X_1,..,X_n$.

4.1.7 Théorème : Produits des algèbres des polynômes

Soient $(A,+,\cdot)$ un anneau commutatif, $(S_1,+),(S_2,+)$ monoides commutatifs et $S_1 \times S_2$ leur monoide 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

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

les morphismes de monoides 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 4.1.5(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 $f : (A,+,\cdot) \to (B,+,\cdot)$ un morphisme de A-algèbres, alors ses prolongements $\overline{f} : (A[S_1])[S_2] \to B$ (morphismes de A-algèbres) via j sont en bijection avec les uplets $(\overline{f}_1,\overline{f}_2)$ où $\overline{f}_1 : A[S_1] \to B$ est son prolongement par i_1 et $\overline{f}_2 : (A[S_1])[S_2] \to B$ est le prolongement de $\overline{f}_1$ par i_2 : Pour un tel uplet pose $\overline{f} := \overline{f}_2$. D'autre part, les prolongements $\overline{f}_1$ et $\overline{f}_2$ sont à chaque fois en bijection avec les morphismes de monoides $\mu_1 : S_1 \to B$ et $\mu_2 : S_2 \to B$ via $\overline{f}_1 \mapsto \overline{f}_1 \circ \sigma_1$ et $\overline{f}_2 \mapsto \overline{f}_2 \circ \sigma_2$. Eux, ils sont en bijection avec les morphismes de monoides $\mu : S_1 \times S_2 \to B$ via

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

Donc, les prolongements $\overline{f} : (A[S_1])[S_2] \to B$ sont en bijection avec les morphismes de monoides $\mu : S_1 \to S_2$ via

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

Cela complète la preuve.

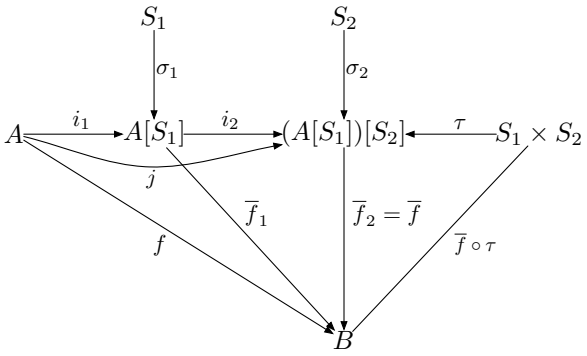


Figure 11: Sur la preuve de théorème 4.1.7. Le diagramme ci-dessus commute. Les prolongements $\overline{f}$ d'un morphisme $f : A \to B$ par j sont en bijection avec les morphismes de monoides $S_1 \times S_2 \to B$ via $\overline{f} \mapsto \overline{f} \circ \tau$.

□

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

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

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.

4.1.8 Corollaire : Produits d'algèbres des polynômes

Soient $(A, +, \cdot)$ un anneau commutatif, $(S_1, +), .., (S_n, +)$ monoides commutatifs et $\overset{n}{\underset{i=1}{\times}} S_i$ leur monoide produite. Alors

$$A\left[\overset{n}{\underset{i=1}{\times}} S_i\right] \cong_A A\left[\overset{k}{\underset{i=1}{\times}} S_i\right]\left[\overset{n}{\underset{i=k+1}{\times}} S_i\right] \cong_A ((((A[S_1])\,[S_2])\,[S_3])\ldots)\,[S_n] \quad .$$

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

Preuve : Suit par induction de théorème 4.1.7.

□

4.1.9 Definition: L'ordre lexicographique & monômial

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

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

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 monômial** 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 $\mathbf{x} = (x_1, .., x_n) \in \mathbb{R}^n$. On écrire $\mathbf{x} < \mathbf{y}$ 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 une ordre totale, c'est-à-dire, elle est :
- Réflexive : $\mathbf{x} \leq_l \mathbf{x}$ pour tout $\mathbf{x} \in \mathbb{R}$.
- 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 une 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 $\leq$.

4.1.10 Definition: Degré des polynômes dans $A[S]$

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

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

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

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

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 écrire tout polynôme $P \in A[S]$ non-nul comme

$$P = P_{s_1} e^{s_1} + \cdots + P_{s_n} e^{s_n} \quad , \tag{4.1.10.1}$$

où $P_{s_1}, .., P_{s_n} \neq 0$ et $s_1 > s_2 > \cdots > s_n$ et appelle la forme (4.1.10.1) la **représentation canonique** de P. En cette représentation, on a $\mathrm{dg}(P) = |s_1|$. On dit $P_{s_1} e^{s_1} =: \mathrm{ini}(P)$ 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 $\mathrm{dg}(P)$ et $\mathrm{dg}(Q)$, alors $P * Q$ est soit nul soit homogène de degré $\mathrm{dg}(P) + \mathrm{dg}(Q)$.

(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 3.2.4(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. 4.1.2).

(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 $\mathrm{dg}(P_n) < \mathrm{dg}(P_{n+1})$ $\forall n$. Car pour tout $0 \neq P, Q \in A[S]$ et $a, b \in A$ on a toujours $aP + bQ = 0$ ou $\mathrm{dg}(aP + bQ) \leq \max\{\mathrm{dg}(P), \mathrm{dg}(Q)\}$ (vois 4.1.11), le A-module $A[S]$ n'est pas de type fini.

4.1.11 Lemme : Le degré comme morphisme de monoides

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

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

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

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

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

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

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

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

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

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

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

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

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

□

4.1.12 Corollaire sur les polynômes inversibles

Soit A un anneau intègre. Alors :

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

Preuve :

1. Supposons $Q \in A[X_1, .., X_n]$ tel que $P * Q = 1$. Évidement $Q, P \neq 0$. Alors par 4.1.11

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

   donc $\deg(P) = 0 = \deg(Q)$. 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 évidement $P * (p_0^{-1} \cdot X^0) = 1$.
2. Par 4.1.11 on sait que $A[X_1, .., X_n]$ est intègre. Par remarque 2.1.6(ii) on sait que $A[X_1, .., X_n] * P = A[X_1, .., X_n] * Q$ ssi $P \in A[X_1, .., X_n]^\times * Q$. Par affirmation (1) on sait que $A[X_1, .., X_n]^\times = A^\times$.

□

4.1.13 Definition: Racines et polynôme scindés

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

4.1.14 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

$$P = (X - x)^\varepsilon * Q \tag{4.1.14.1}$$

pour un $\varepsilon \in \mathbb{N}$ et un polynôme $Q \in A[X]$ ne possédant pas x comme racine. Sous cette condition, Q et ε sont uniques et Q est de degré $\deg(Q) = \deg(P) - \varepsilon$. On appelle ε 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

$$p_0 + p_1 \cdot x^1 + \cdots + p_n \cdot x^n = 0 \ . \tag{4.1.14.2}$$

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

$$-xq_0 + \sum_{i=1}^{n-1} (q_{i-1} - q_i \cdot x) \cdot X^i + q_{n-1} \cdot X^i + \sum_{i=n+1}^{m} b_{i-1} X^i \overset{!}{=} \sum_{i=0}^{n} p_i \cdot X^i \ . \tag{4.1.14.3}$$

Noter que comme A est intègre, par 4.1.11 il faut que $\deg(Q) = n - 1$. La condition (4.1.14.3) est équivalente aux conditions

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

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

$$q_0 = p_1 + q_1 x = (..) = p_1 + p_2 x + \cdots + p_n x^{n-1} \ . \tag{4.1.14.4}$$

Mais avec (4.1.14.2), cela est compatible à la troisième condition

$$x \cdot q_0 \overset{(4.1.14.4)}{=} p_1 x^1 + \cdots + p_n x^n \overset{(4.1.14.2)}{=} -p_0 \ .$$

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 (4.1.14.1). Noter que par 4.1.11 il faut que $\deg(Q) = \deg(P) - \varepsilon$.

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

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

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

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

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

□

4.1.15 Corollaire : Factorisation de polynômes

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

$$P(X) = Q(X) * \prod_{i=1}^{k} (X-x_i)^{\varepsilon_i} \quad , \tag{4.1.15.1}$$

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

Preuve d'existence : Par théorème 4.1.14 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 $i \in \{2, .., n\}$ 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 $x_2, .., x_n$ sont les seules racines de Q_1. On peut donc répéter la même procédure et obtenir par récurrence la forme (4.1.15.1), où Q ne possède pas de racines dans A.

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

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

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

$$Q * \prod_{i=1}^{k-1} (X-x_i)^{\varepsilon_i} \quad , \quad \widetilde{Q} * \prod_{i=1}^{k-1} (X-x_i)^{\widetilde{\varepsilon}_i} \tag{4.1.15.2}$$

ne possèdent que les racines $x_1, .., x_{k-1}$. Par théorème 4.1.14, il faut que $\varepsilon_k = \widetilde{\varepsilon}_k$ et les polynômes (4.1.15.2) sont égales. Par récurrence, on montre que $\varepsilon_i = \widetilde{\varepsilon}_i$ pour tout i et $Q = \widetilde{Q}$. Noter que pour tout $l \in \{1, .., n\}$, le polynôme $Q * \prod_{i \neq l} (X-x_i)$ ne possède pas x_l comme racine et par la même argumentation ε_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 $Q = \mathrm{const}$ dans la factorisation (4.1.15.1) 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

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

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

4.1.16 Lemme sur polynômes linéairement indépendants

Soit A un anneau commutatif, $n \in \mathbb{N}$ et $(P_i)_{i\in I} \subseteq A[X_1, .., X_n]$ 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.

4.1.17 Lemme sur bases de polynômes

Soit A un anneau commutatif, $n \in \mathbb{N}$ et $(P_s)_{s\in\mathbb{N}_0^n} \subseteq A[X_1, .., X_n]$ une famille de polynômes. On suppose que tout $P_s \in A[X_1, .., X_n]$ 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 $A[X_1, .., X_n]$.

Preuve : Comme tout inversible de A et non-diviseur de zéro, par 4.1.16 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

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

ce qui évidement contient tout polynôme de $A[X_1, .., X_n]$.

□

4.2 Idéaux dans $A[S]$

4.2.1 Definition: Idéal monômial dans $A[S]$

Soit $(A, +, \cdot)$ un anneau commutatif et $(S, +)$ un monoide 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'importante 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 $\Delta(I) = \{n, n+1, ..\}$. 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).

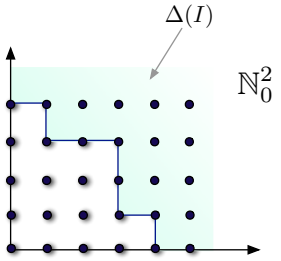


Figure 12: Exemple de la famille $\Delta(I) := \left\{s \in \mathbb{N}_0^2 : X^s \in I\right\}$ pour un idéal $I \subseteq A[X_1, X_2]$. On a $\Delta(I) + \mathbb{N}_0^2 = \Delta(I)$, c'est-à-dire $s + \mathbb{N}_0^2 \subseteq \Delta(I)$ pour tout $s \in \Delta(I)$.

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

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

4.2.2 Lemme sur idéaux monômiaux

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

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

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

□

4.2.3 Théorème sur anneaux noetheriens

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

Preuve : Par 4.1.8, 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

$$P = a_0X^0 + a_1X^1 + \cdots + a_nX^n \quad , \quad a_n \neq 0$$

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

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

l'idéal dans A engendré par les coefficients dominants $\mathrm{ini}(P),\ P \in J$. Car A est noetherien, $\mathcal{J}$ est de type fini, c'est-à-dire engendré par des éléments $\lambda_1,..,\lambda_d \in \mathcal{J}$. 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

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

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 $\mathrm{ini}(P_{k,i}) =: \lambda_{k,i}$ engendrent $\mathcal{J}_k$.

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

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

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

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

D'autre part, le polynôme

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

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

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

D'autre part, le polynôme

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

est dans $J/\widetilde{J}$ et de degré $< \mathrm{dg}(P)$, encore une contradiction.

□

4.2.4 Exemple : $\mathbb{Z}[X]$

Par théorème 4.2.3 on sait que $\mathbb{Z}[X]$ est noetherien. On va montrer que $\mathbb{Z}[X]$ n'est pas principal. On considère l'idéal

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

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 $\mathrm{dg}\, P = 0$, c'est-à-dire $P = p_0$: 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 !

4.2.5 Corollaire : Théorème de la base de Hilbert

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

Preuve : Suit de théorème 4.2.3 et du fait que tout corps $\mathbb{K}$ est noetherien.

□

4.2.6 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 ⇒ 2 **:** Soit $\{0\} \neq J \subseteq A[X]$ un idéal et $0 \neq P \in J$ de degré minimal. Si $\mathrm{dg}(P) = 0$, 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 2.2.1(ii) $J = A[X]$ et J est engendré par X^0. On suppose donc que $\mathrm{dg}(P) > 0$ et va montrer que P engendre J. Soit

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

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

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

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

$$Q - \frac{Q_{t_1}}{P_{s_1}} \cdot X^{t_1 - s_1} * P \quad \in J \tag{4.2.6.1}$$

possède degré plus petit que $t_1 = \mathrm{dg}(Q)$. Supposant que $A[X] * P \subsetneq J$, on pourrait choisir un $Q \notin A[X] * P$ de degré minimal. Par (4.2.6.1) on trouverait une contradiction.

2 ⇒ 1 **:** Par le théorème d'isomorphismes d'anneaux 2.2.13, les anneaux A et $A[X]/\langle X \rangle$ sont isomorphes. Donc, par 2.2.18 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

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

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 ⇒ 3 **:** Voir lemme 4.2.12.

3 ⇒ 2 **:** Par 5.1.6, tout anneau euclidien est principal.

4.2.7 Fonctions polynomiales

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

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

Il est donné par

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

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

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

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

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

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

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

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

$$[A[X_1, .., X_n], +, *] \to [\mathcal{F}(B^n, B), +, \cdot] \quad , \quad P \mapsto \widetilde{P}$$

est un morphisme de A-algèbres. Le cas plus important est $B = A$. On dit un $a \in A$ **racine** d'un polynôme $P \in A[X_1, .., X_n]$ ssi $\widetilde{P}(a) = 0$ (voir aussi 4.2.7).

Remarque :

(i) En général, le morphisme $P \mapsto \widetilde{P}$ 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 $1 \leq n < p$.

4.2.8 Théorème : Fonctions polynomiales sur corps infinies

Si $\mathbb{K}$ est un corps infini et $n \in \mathbb{N}$, alors le morphisme $\mathbb{K}[X_1, .., X_n] \to \mathcal{F}(\mathbb{K}^n, \mathbb{K}),\ P \mapsto \widetilde{P}$ 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 $\widetilde{P}(x) = 0\ \forall x \in \mathbb{K}$. Alors, P possède par 4.1.15 au plus $\mathrm{dg}(P)$ racines dans $\mathbb{K}$, une contradiction à l'infinitude de $\mathbb{K}$.

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

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

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

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

Alors, car $\widetilde{P} = 0$ il faut $\widetilde{P}(a, \cdot) = 0$ qui par suppositions de la récurrence implique $\widetilde{P}_s(a) = 0$ pour tout $s \in \mathbb{N}_0$. Cela étant vrai pour tout $a \in \mathbb{K}^{n-1}$, c'est-à-dire $\widetilde{P}_s \equiv 0\ \forall s$, 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 in l'existe pas d'équations algébriques non-triviales sur $\mathbb{K}$, résolues par tout $\mathbb{K}$.

4.2.9 Application : Principe de prolongement des identités algébriques

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

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

Alors, $G = 0$.

Preuve : On a $\widetilde{P * G} = 0$ et donc par théorème 4.2.8 $P * G = 0$. Par 4.1.11 on sait que $\mathbb{K}[X_1, .., X_n]$ est intègre. Donc, $P \neq 0$ implique impérativement $G = 0$.

□

4.2.10 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 $\mathbb{F}_p[X_1, .., X_n] \to \mathcal{F}\left(\mathbb{F}_p^n, \mathbb{F}_p\right),\ P \mapsto \widetilde{P}$ est l'idéal engendré par les polynômes $X_1^p - X_1, .., X_n^p - X_n$. De plus, la $\mathbb{F}_p$-algèbre $\mathcal{F}(\mathbb{F}_p^n, \mathbb{F}_p)$ est libre de rang p^n.

4.2.11 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

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

4.2.12 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 val : $P \mapsto \deg(P),\ P \in \mathbb{K}[X]$.

4.2.13 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 $\overline{X}^0, \overline{X}^1, .., \overline{X}^{m-1}$, où $m := \deg(Q)$ si $Q \neq 0$ et $m = \infty$ si $Q = 0$.

Preuve : Se rappeler que par 4.2.12 $\mathbb{K}[X]$ est euclidien avec stathme val := 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 $\deg(R) < \deg(Q)$ si $R \neq 0$. En particulier, $P \in \langle Q\rangle + \mathrm{span}_{\mathbb{K}}\left\{X^0, .., X^{m-1}\right\}$, d'où on déduit que les $\overline{X}^0, .., \overline{X}^{m-1}$ engendrent $\mathbb{K}[X]/\langle Q\rangle$. D'autre part, soient $\varkappa_0, .., \varkappa_{m-1}$ 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 $\deg(B * Q) = \deg(B) + \deg(Q) \geq m$, ce qui est impossible. Donc $\varkappa_0, .., \varkappa_{m-1} = 0$, ça veut dire les $\overline{X}^0, .., \overline{X}^{m-1}$ sont linéairement indépendants.

□

4.3 Dérivation de polynômes

4.3.1 Definition: Opérateur de différences

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

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

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

4.3.2 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 et de la forme

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

alors

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

Note que $n \in A$ n'est pas diviseur de zéro. Or, si $\Delta P = 0$, alors par lemme 4.1.16 on conclut que $P_n = 0$ pour tout $n \in \{1, .., N\}$. Par conséquence $P = P_0$.

□

4.3.3 Definition: 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 4.1.17 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

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

4.3.4 Definition: Dérivée d'un polynôme

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

$$\partial_i : A[X_1, .., X_n] \to A[X_1, .., X_n]$$

satisfaisant :

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

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

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

4.3.5 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 $P \in A[X_1, .., X_n]$ est constant ssi toute dérivée $\partial_i P$ est nulle.

Preuve : Direction "⇒" et triviale. Supposons donc $\partial_i P = 0$ pour un polynôme P et tout $i \in \{1, .., n\}$. En considérons $P(X_1, .., X_n)$ comme polynôme dans $A[X_1, .., X_{n-1}][X_n]$, 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

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

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

□

4.4 Polynômes invariants sous un groupe fini

4.4.1 Definition: 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 agissante sur $A[X_1, .., X_n]$ via automorphismes de A-algèbres, qui sont eux mêmes donnés par leur valeurs des $X_1, .., X_n$:

$$M \cdot X_i := \sum_{j=1}^{n} (M^{-1})_{ij} \cdot X_j \quad , \quad M \in \mathrm{GL}_n(A) \quad . \tag{4.4.1.1}$$

Note que l'action (4.4.1.1) est vraiment un action à gauche sur $A[X_1, .., X_n]$.

4.4.2 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 $A[X_1, .., X_n]^G$.

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

□

4.4.3 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

$$\sigma \mapsto M_\sigma \quad , \quad (M_\sigma)_{ij} := \delta_{i,\sigma(j)} \quad . \tag{4.4.3.1}$$

Alors, (4.4.3.1) est un monomorphisme de groupes $\mathrm{Sym}(n) \hookrightarrow \mathrm{GL}_n(A)$, c'est-à-dire $M_{\sigma \circ \tau} = M_\sigma \cdot M_\tau$ pour $\sigma, \tau \in \mathrm{Sym}(n)$. On considère le groupe $\mathrm{Sym}(n)$ agissante sur $A[X_1, .., X_n]$ via son plongement dans $\mathrm{GL}_n(A)$, c'est-à-dire

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

et plus généralement

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

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

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

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

$$\sigma \cdot \sum_{s\in\mathbb{N}_0^n} p_s \cdot X^s = \sum_{s\in\mathbb{N}_0^n} p_s \cdot X^{\sigma(s)} = \sum_{s\in\mathbb{N}_0^n} p_{\sigma^{-1}(s)} \cdot X^s \quad . \tag{4.4.3.2}$$

4.4.4 Partitions et diagrammes de Young

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

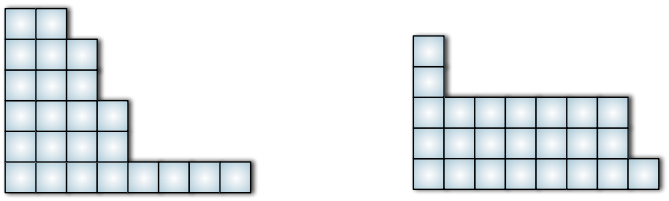
$$\sigma \cdot (s_1, .., s_n) := \big(s_{\sigma^{-1}(1)}, .., s_{\sigma^{-1}(n)}\big) \quad , \quad s \in \mathbb{N}_0,\ \sigma \in \mathrm{Sym}(n) \quad .$$

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

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

On dit λ une **partition du poids** $m := |\lambda|$ et écrit souvent $\lambda = (\lambda_1 \geq .. \geq \lambda_n)$. 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 λ_i non-nules.

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 λ. Vois figure 13 ci-dessous pour un exemple.



$(8, 4, 4, 3, 3, 2)$ $(8, 7, 7, 1, 1, 0)$

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 λ^* de m dans $\mathbb{N}_0^{\lambda_1}$, appelée la **partition duale** de λ. Note que $|\lambda^*| = |\lambda|$ et $\lambda^{**} = \lambda$.

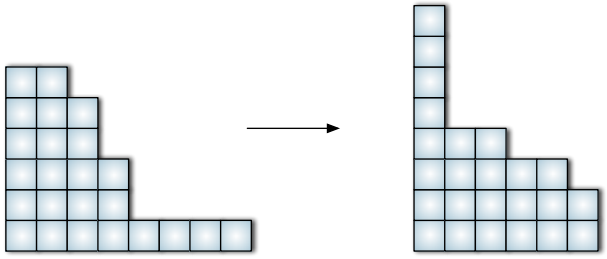


Figure 14: Sur la partition duale : Montré est la partition de 24 dans $\mathbb{N}_0^6$ et sa duale dans $\mathbb{N}_0^8$.

En fait, le composant λ_i^* de λ^* correspond au nombre des composants de λ plus grands ou égales à i. En particulier, λ_1^* est la longueur de λ. On note

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

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

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

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

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

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

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

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

4.4.5 Definition: Monômes symétriques

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

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

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

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

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

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

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

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

la **symétrisation** de X^s.

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

$$\sigma_k(X) = \sum_{1 \le i_1 < .. < i_k \le n} X_{i_1} \cdot .. \cdot X_{i_k} = \mathrm{Sym}(X_1 \cdot .. \cdot X_k) \quad .$$

En particulier

$$\sigma_0(X) = 1 \quad , \quad \sigma_1(X) = X_1 + \cdots + X_n \quad , \quad \sigma_n(X) = X_1 \cdot .. \cdot X_n \quad .$$

Pour partition $\lambda = (\lambda_1 \ge \lambda_2 \ge ..) \in \mathcal{P}_n^*$ (c'est-à-dire $\lambda_1 \le n$) on note

$$\sigma_\lambda := \sigma_{\lambda_1} \cdot .. \cdot \sigma_{\lambda_n} \quad .$$

Noter que les σ_λ sont exactement les monômes en les *variables* $\sigma_1,..,\sigma_n$. En fait, tout monôme $\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n}$ en $\sigma_1,..,\sigma_n$, avec $s \in \mathbb{N}_0^n$, s'écrit dans la forme

$$\underbrace{(\sigma_n * .. * \sigma_n)}_{\times s_n} * \underbrace{(\sigma_{n-1} * .. * \sigma_{n-1})}_{\times s_{n-1}} * \cdots * \underbrace{(\sigma_1 * .. * \sigma_1)}_{\times s_1} = \sigma_\lambda$$

où

$$\lambda = (\underbrace{n,..,n}_{\times s_n}, \underbrace{n-1,..,n-1}_{\times s_{n-1}}, .., \underbrace{1,..,1}_{\times s_1}) \in \mathcal{P}_n^* \quad .$$

Noter que le degré de $\sigma_\lambda(X)$ (comme polynôme dans $A[X_1,..,X_n]$) est exactement le poids $|\lambda|$.

4.4.6 Lemme : Engendrement des polynômes symétriques

Soit A un anneau commutatif et $n \in \mathbb{N}$. Alors

$$A[X_1,..,X_n]^{\mathrm{Sym}(n)} = \bigoplus_{\lambda \in \mathcal{P}_n} AM_\lambda \quad . \tag{4.4.6.1}$$

Autrement dit, les monômes symétriques complets forment une A-base [22] du A-module $A[X_1,..,X_n]^{\mathrm{Sym}(n)}$.

Preuve : C'est évident que la somme à droite de (4.4.6.1) est directe. On a vu déjà que tout polynôme $P = \sum_{s \in \mathbb{N}_0^n} p_s X^s \in A[X_1,..,X_n]$ est symétrique ssi tous ses coefficients p_s sont égales sur les orbites de $\mathrm{Sym}(n)$. Donc, si P est symétrique il s'écrit comme

$$P = \sum_{\lambda \in \mathcal{P}_n} p_\lambda \cdot \underbrace{\sum_{s \in \mathrm{Orb}(\lambda)} X^s}_{M_\lambda} \quad .$$

Inversement, comme tout monôme symétrique M_λ est symétrique, on sait que

$$\bigoplus_{\lambda \in \mathcal{P}_n} AM_\lambda \subseteq A[X_1,..,X_n]^{\mathrm{Sym}(n)} \quad .$$

Cela complète la preuve.

□

22. Voir 3.2.4 pour la caractérisation d'une base.

4.4.7 Lemme : Représentation des polynômes symétriques

Pour toute partition $\lambda \in \mathcal{P}_n$ de poids $m := |\lambda|$, le polynôme σ_{λ^*} en les $\sigma_1, .., \sigma_n \in A[X_1, .., X_n]$ est de la forme

$$\sigma_{\lambda^*} = M_\lambda + \sum_{\substack{\mu \in \mathcal{P}_n(|\lambda|) \\ \mu < \lambda}} a_{\lambda,\mu} M_\mu \tag{4.4.7.1}$$

où $a_{\lambda,\mu} \in \mathbb{N}_0$ sont des coefficients entiers et "$<$" est l'ordre monômial [23]

Preuve : Noter que σ_{λ^*} est en fait un polynôme dans $A[X_1, .., X_n]^{\mathrm{Sym}}$. Par 4.4.6 il peut être écrit comme combinaison linéaire de monômes symétriques complets $(M_\mu)_{\mu \in \mathcal{P}_n}$. Par la représentation

$$\sigma_{\lambda^*} = \sigma_{\lambda_1^*} * \sigma_{\lambda_2^*} * \cdots = \mathrm{Sym}(X_1 \cdot .. \cdot X_{\lambda_1^*}) * \mathrm{Sym}(X_1 \cdot .. \cdot X_{\lambda_2^*}) * \ldots \tag{4.4.7.2}$$

c'est évident que les coefficients des M_λ sont en principe nombres entiers. Le degré de σ_{λ^*} est exactement $|\lambda|$, donc la combinaison linéaire consiste seulement de monômes symétriques complets M_μ où $|\mu| = |\lambda|$. Le terme dominant dans (4.4.7.2) par rapport à l'ordre monômial est

$$(X_1 \cdot .. \cdot X_{\lambda_1^*}) * (X_1 \cdot .. \cdot X_{\lambda_2^*}) * \ldots \quad . \tag{4.4.7.3}$$

ce qui se trouve dans (4.4.7.2) avec le coefficient 1. De plus, par la définition de λ^*, l'expression (4.4.7.3) est égale à $X^{\lambda^{**}} = X^\lambda$, donc σ_{λ^*} inclut seulement des M_μ où $\mu \leq \lambda$. Cela finit la preuve.

□

Exemple : Soit $m \in \mathbb{N}_0$ quelconque. Par remarque 4.4.4(ii) on sait que le plus petit élément $\lambda_0 \in \mathcal{P}_n(m)$ est donné par

$$\lambda_0 = (\underbrace{k+1, .., k+1}_{\times r}, \underbrace{k, .., k}_{\times(n-r)}) \quad ,$$

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

$$\lambda_0^* = (\underbrace{n, .., n}_{\times k}, r) \quad .$$

Par (4.4.7.1) on conclut que

$$M_{\lambda_0} = \sigma_{\lambda_0^*} = \underbrace{\sigma_n * \cdots * \sigma_n}_{\times k} * \sigma_r = (X_1 \cdot .. \cdot X_n)^k * \mathrm{Sym}(X_1 \cdot .. \cdot X_r) \quad .$$

4.4.8 Théorème des polynômes symétriques

Soit A un anneau commutatif et $n \in \mathbb{N}$. Alors, l'algèbre des polynômes symétriques $A[X_1, .., X_n]^{\mathrm{Sym}(n)}$ est une A-algèbre de polynômes en n variables $\sigma_1(X), .., \sigma_n(X)$.

Remarque : Le théorème est équivalent aux suivantes :
- Pour tout polynôme symétrique $P \in A[X_1, .., X_n]^{\mathrm{Sym}(n)}$ il existe un unique $Q \in A[X_1, .., X_n]$ tel que $P = Q(\sigma_1, .., \sigma_n)$.
- Les monômes en $\sigma_1, .., \sigma_n$ forment une base du A-module $A[X_1, .., X_n]^{\mathrm{Sym}(n)}$.
- Le morphisme de A-algèbres $A[X_1, .., X_n] \to A[X_1, .., X_n]^{\mathrm{Sym}(n)}$ caractérisé par $X_k \mapsto \sigma_k(X)$ est un isomorphisme [24].

23. Voir 4.1.9.
24. Voir 3.2.8 sur l'existence d'isomorphismes.

Preuve : Par la remarque ci-dessus, il suffit à montrer que les monômes en les $\sigma_1, .., \sigma_n$ forment une A-base de $A[X_1, .., X_n]^{\mathrm{Sym}(n)}$. Par 4.4.6 on sait que les monômes symétriques complets $(M_\mu)_{\mu\in\mathcal{P}_n}$ forment une A-base de $A[X_1, .., X_n]^{\mathrm{Sym}(n)}$. Donc, par remarque 3.2.1(vii) il suffit à montrer que tout M_μ peut être écrit comme combinaison linéaire des polynômes σ_{λ^*} en les $\sigma_1, .., \sigma_m$ en unique façon.

Lemme 4.4.7 et en particulier relation (4.4.7.1) donnent une représentation des σ_{λ^*} et les M_μ. Comme la relation est triangulaire avec des 1 sur la diagonale, elle est inversible. Cela complète la preuve.

□

4.4.9 Algorithme sur la représentation des polynômes symétriques

Soit A un anneau commutatif et $n \in \mathbb{N}$. On a vu dans théorème 4.4.8, que tout $P \in A[X_1, .., X_n]^{\mathrm{Sym}(n)}$ peut être représenté comme $P = Q(\sigma_1, .., \sigma_n)$ pour un unique polynôme $Q \in A[X_1, .., X_n]$. 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

$$P = \sum_{s\in\mathbb{N}_0^n} Q_s \cdot \sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n} \quad .$$

Notons que le terme dominant d'un monôme $\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n}$ en les σ_i est donné par

$$X_1^{s_1+..+s_n} \cdot X_2^{s_2+..+s_n} \cdot .. \cdot X_n^{s_n} \quad .$$

L'idée est or, d'*éliminer* un par un les termes dominants de P par des monômes en des σ_i. On trouve l'algorithme suivant :

1. Déterminer le terme dominant $pX_1^{\nu_1} \cdot .. \cdot X_n^{\nu_n}$ de P.
2. Résoudre le système d'équations

$$\begin{aligned} \nu_1 &= s_1 + s_2 + \cdots + s_n \\ \nu_2 &= s_2 + \cdots + s_n \\ &\vdots \\ \nu_n &= s_n \end{aligned}$$

   en les indéterminées $s_1, .., s_n$.
3. Soustraire le monôme $p\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n}$ de P pour recevoir le polynôme

$$\widetilde{P} := P - p\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n} \quad ,$$

   qui possède un terme dominant plus petit que P.
4. Répéter les étapes (1),(2) et (3) pour $\widetilde{P}$ et ainsi de suite jusqu'à il reste le polynôme nul.

On arrive donc finalement à une représentation

$$P - p\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n} - \widetilde{p}\sigma_1^{\widetilde{s}_1} \cdot .. \cdot \sigma_n^{\widetilde{s}_n} - \cdots = 0 \quad ,$$

d'où on trouve

$$P = p\sigma_1^{s_1} \cdot .. \cdot \sigma_n^{s_n} + \widetilde{p}\sigma_1^{\widetilde{s}_1} \cdot .. \cdot \sigma_n^{\widetilde{s}_n} + \ldots \quad .$$

Exemples

- Le polynôme symétrique $X_1^3 + \cdots + X_n^3$ possède la représentation

$$X_1^3 + \cdots + X_n^3 = \sigma_1^3(X) - 3\sigma_1(X)\sigma_2(X) + 3\sigma_3(X) \quad .$$

- 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

$$X^3(Y+Z) + Y^3(Z+X) + Z^3(X+Y) = \sigma_1^2\sigma_2 - 2\sigma_2^2 - 3\sigma_1\sigma_3 \quad .$$

4.4.10 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 $A[X_1, .., X_n]$ de degré k comme le polynôme

$$S_k := \sum_{i=1}^{n} X_i^k \quad .$$

Alors, les monômes en les $S_1, .., S_n$ engendrent $A[X_1, .., X_n]^{\mathrm{Sym}(n)}$, c'est-à-dire

$$\boxed{A[X_1, .., X_n]^{\mathrm{Sym}(n)} = \mathrm{span}_A \left\{ S_1^{s_1} * .. * S_n^{s_n} : s \in \mathbb{N}_0^n \right\} \quad .} \tag{4.4.10.1}$$

Preuve : Considérons le polynôme

$$P(T) := \prod_{i=1}^{n} (T - X_i) \in A[X_1, .., X_n][T] \quad .$$

Il est égal à

$$P(T) = \sum_{l=0}^{n} (-1)^l \cdot \sigma_l \cdot T^{n-l} \quad , \tag{4.4.10.2}$$

d'où on déduit l'identité

$$\sum_{l=0}^{n} (-1)^l \cdot \sigma_l \cdot X_i^{k-l} = 0 \quad \forall k \geq n, \ i \in \{1, .., n\}$$

et par conséquence

$$\sum_{l=0}^{n} (-1)^l \cdot \sigma_l \cdot S_{k-l} = 0 \quad \forall \ k \geq n \quad . \tag{4.4.10.3}$$

On considérons la dérivée

$$\frac{dP}{dT} = \sum_{i=1}^{n} \prod_{j \neq i} (T - X_j) = \sum_{i=1}^{n} \frac{P - P(X_i)}{T - X_i} \quad . \tag{4.4.10.4}$$

Comme

$$P - P(X_i) \overset{(4.4.10.2)}{=} \sum_{j=1}^{n} (-1)^{n-j} \sigma_{n-j} \cdot (T^j - X_i^j)$$

et

$$\frac{T^j - X_i^j}{T - X_i} = \sum_{l=1}^{j} T^{l-1} X_i^{j-l} \quad ,$$

la dérivée (4.4.10.4) prend la forme

$$\frac{dP}{dT} = \sum_{j=1}^{n} (-1)^{n-j} \sigma_{n-j} \sum_{l=1}^{j} T^{l-1} S_{j-l} = \sum_{l=1}^{n} T^{l-1} \sum_{j=l}^{n} (-1)^{n-j} \sigma_{n-j} S_{j-l} \quad . \tag{4.4.10.5}$$

D'autre part, par (4.4.10.2) on sait que

$$\frac{dP}{dT} = \sum_{l=1}^{n} (-1)^{n-l} \sigma_{n-l} \cdot l \cdot T^{l-1} \quad , \tag{4.4.10.6}$$

En comparaissant (4.4.10.5) et (4.4.10.6) on reçois

$$\sum_{j=l}^{n} (-1)^{n-j} \sigma_{n-j} S_{j-l} = l \cdot (-1)^{n-l} \sigma_{n-l} \quad \forall l \in \{1, .., n\} \quad ,$$

d'où

$$\sigma_{n-l}\cdot(-1)^{n-l}\underbrace{[l-S_0]}_{n-l}=\sum_{j=l+1}^{n}(-1)^{n-j}\sigma_{n-j}S_{j-l}\quad\forall l\in\{1,..,n\}\quad. \tag{4.4.10.7}$$

Comme $\mathbb{Q}\subseteq A$, (4.4.10.7) donne σ_{n-l} pour chaque $l\in\{1,..,n\}$ comme polynôme des $\sigma_0,..,\sigma_{n-l-1}$ et les $S_1,..,S_{n-l}$. De même, (4.4.10.3) donne σ_n comme polynôme en les $\sigma_0,..,\sigma_{n-l}$ et les $S_1,..,S_n$ (pose $k=n$). Noter que $\sigma_0=1$. Donc, par récurrence sur $j=1,..,n$, on trouve les σ_j comme polynômes en les $S_1,..,S_n$. Par théorème 4.4.8, les polynômes en les $S_1,..,S_n$ engendrent $A[X_1,..,X_n]^{\mathrm{Sym}(n)}$.

□

Remarques

(i) La preuve ci-dessus montre que si $\mathbb{Q}\subseteq A$, alors σ_k est une combinaison linéaire des $S_1,..,S_k$ pour tout $k\in\{1,..,n\}$.

(ii) On a vu dans la preuve les **relations coefficients-racines**

$$\boxed{\prod_{i=1}^{n}(T-X_i)=\sum_{i=0}^{n}(-1)^i\cdot\sigma_i(X_1,..,X_n)\cdot T^{n-i}\quad.} \tag{4.4.10.8}$$

4.4.11 Corollaire sur polynômes symétriques et sous-anneaux

Soit A un sous-anneau de l'anneau commutatif B. Soient $a_1,..,a_n\in B$ tels que le polynôme $\prod_{k=1}^{n}(X-a_k)\in B[X]$ est en fait dans $A[X]$. Alors, pour tout $Q\in A[X_1,..,X_n]^{\mathrm{Sym}(n)}$ on a $Q(a_1,..,a_n)\in A$.

Preuve : Par les relations coefficients-racines (4.4.10.8) on sait que

$$\prod_{k=1}^{n}(X-a_k)=\sum_{k=0}^{n}X^k(-1)^{n-k}\sigma_{n-k}(a_1,..,a_n)\quad,$$

d'où on voit que $\sigma_{n-k}(a_1,..,a_n)\in A$ pour tout $k\in\{1,..,n\}$. Si $Q\in A[X_1,..,X_n]^{\mathrm{Sym}(n)}$ est un polynôme symétrique, alors par théorème 4.4.8 il est combinaison A-linéaire de monômes en les $\sigma_1,..,\sigma_n$. Donc $Q(a_1,..,a_n)\in A$.

□

Exemple : Soient $z_1,..,z_n\in\mathbb{C}$ quelconques. Alors, le polynôme

$$\prod_{k=1}^{n}(X-z_k)(X-\overline{z}_k)$$

est réel. Donc, pour tout polynôme symétrique $Q\in\mathbb{R}[X_1,..,X_{2n}]^{\mathrm{Sym}(n)}$ on a $Q(z_1,\overline{z}_1,..,z_n,\overline{z}_n)\in\mathbb{R}$.

4.4.12 Exemple : Polygones réguliers dans $\mathbb{C}$

Soient $\xi_0,..,\xi_n\in\mathbb{C}$ deux à deux inégales. Alors, les suivantes sont équivalents :

1. Les $\xi_1,..,\xi_n$ sont les sommets d'un polygone régulier de n côtés centré en ξ_0.
2. Les valeurs $(\xi_k-\xi_0),\ k\in\{1,..,n\}$ 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

$$\prod_{k=1}^{n}(X-\xi_k)=(X-\xi_0)^n-R\quad. \tag{4.4.12.1}$$

4. Pour tout polynôme $P\in\mathbb{C}[X]$ de degré plus petit que n, on a

$$P(\xi_0)=\frac{1}{n}\prod_{k=1}^{n}P(\xi_k)\quad. \tag{4.4.12.2}$$

Preuve : Noter que les $\xi_1,..,\xi_n$ sont les n sommets d'un polygone régulier centré à ξ_0 ssi $(\xi_1-\xi_0),..,(\xi_n-\xi_0)$ sont les n sommets d'un polygone régulier centré à 0.

1 ⇒ 2 **:** Par la remarque ci-dessus on peut supposer que ξ_0. Il faut donc montrer que les $\xi_1,..,\xi_n$ forment les n n-ièmes racines d'un $R\neq 0$. Noter que $\xi_1,..,\xi_n\neq 0$. 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

$$\xi_k^n=|\xi_k|^n\cdot e^{in\arg(\xi_k)}=|\xi_1|^n\cdot\exp\left[in\cdot\left(\arg(\xi_1)+(k-1)\frac{2\pi}{n}\right)\right]=|\xi_1|^n\exp\left[in\cdot\arg(\xi_1)\right]=\xi_1^n=R\quad.$$

2 ⇒ 1 **:** Les n racines de $R\neq 0$ sont données par

$$\sqrt[n]{R}\in\left\{\underbrace{\sqrt[n]{|R|}\cdot\exp\left[\frac{i}{n}\arg(R)+\frac{k}{n}2\pi i\right]}_{(\xi_k-\xi_0)}:k=1,..,n\right\}\quad.$$

Evidement les $\xi_1,..,\xi_n$ forment un polygone régulier centré en ξ_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 ⇒ 2 **:** Supposons l'équation (4.4.12.1) pour un certain $R\in\mathbb{C}\setminus\{0\}$. Alors, pour tout $j\in\{1,..,n\}$ il faut

$$0=\prod_{k=1}^n(\xi_j-\xi_k)=(\xi_k-\xi_0)^n-R\quad,$$

c'est-à-dire les valeurs $(\xi_1-\xi_0),..,(\xi_n-\xi_0)$ sont les n n-ièmes racines de R.

2 ⇒ 3 **:** Considérons le polynôme unitaire

$$P(X)=(X-\xi_0)^n-R\quad.$$

Alors, ses racines sont exactement $\xi_1,..,\xi_n$, donc il possède la forme

$$P(X)=\prod_{k=1}^n(X-\xi_k)\quad.$$

2 ⇒ 4 **:** Montrons d'abord l'affirmation pour le cas $\xi_0=0$. Il suffit de montrer l'affirmation (4.4.12.2) pour les monômes $X^1,..,X^{n-1}$, c'est-à-dire que

$$0=\frac{1}{n}\sum_{k=1}^n\xi_k^j\quad\forall j\in\{1,..,n-1\}\quad.$$

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 $j\in\{1,..,n-1\}$, 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 :

$$P(0)=\frac{1}{n}\sum_{k=1}^nP(\xi_k-\xi_0)\quad.$$

Soit $Q\in\mathbb{C}[X]$ avec $\deg(Q)\leq n-1$ quelconque. Pose $P(X):=Q(X+\xi_0)$, alors $\deg(P)\leq n-1$ et donc

$$Q(\xi_0)=P(0)=\frac{1}{n}\sum_{k=1}^nP(\xi_k-\xi_0)=\frac{1}{n}\sum_{k=1}^nQ(\xi_k)\quad.$$

4 ⇒ 1 : Par la remarque au début de la preuve et la même argumentation comme dans la preuve de (2 ⇒ 4), on peut supposer que $\xi_0 = 0$. Par les relations coefficients-racines (4.4.10.8) on sait que

$$P(X) := \prod_{k=1}^{n}(X - \xi_k) = \sum_{k=0}^{n} X^k \cdot (-1)^{n-k}\sigma_{n-k}(\xi_1, .., \xi_n) \quad ,$$

où $\sigma_0, .., \sigma_n$ sont les polynômes symétriques élémentaires dans $\mathbb{C}[X_1, .., X_n]$. Pour prouver la forme (4.4.12.1) dans le cas $\xi_0 = 0$, il suffit de montrer que

$$\sigma_k(\xi_1, .., \xi_n) = 0 \quad \forall k \in \{1, .., n-1\} \quad .$$

Noter que comme les $\xi_1, .., \xi_k$ sont deux à deux inégales, le terme constant R du polynôme P doit être non-nul. Par remarque 4.4.10(i), les $\sigma_1, .., \sigma_{n-1}$ sont polynômes en les sommes de Newton $S_1, .., S_{n-1}$. Il suffit donc de montrer que $S_j(\xi_1, .., \xi_n) = 0$ pour tout $j \in \{1, .., n-1\}$. Par supposition

$$0 = 0^j \overset{\text{sup.}}{=} \frac{1}{n}\sum_{k=1}^{n} \xi_k^j = \frac{1}{n} S_j(\xi_1, .., \xi_n) \quad \forall j \in \{1, .., n-1\} \quad ,$$

ce qui complète la preuve.

□

4.4.13 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 $\mathrm{tr}(A^k) = \mathrm{tr}(B^k)$ pour tout $k \in \{1, .., n\}$. 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 $\mathrm{tr}(A^1), .., \mathrm{tr}(A^n)$. On sait que A est semblable à un $\widetilde{A} \in \mathbb{K}^{n\times n}$ de la forme

$$\widetilde{A} = \begin{pmatrix} a_1 & \dots & * \\ & \ddots & \vdots \\ 0 & & a_n \end{pmatrix}$$

pour quelques $a_1, .., a_n \in \mathbb{K}$. Comme $\mathrm{tr}(A^k) = \mathrm{tr}(\widetilde{A}^k)$ et $\chi_A = \chi_{\widetilde{A}}$, il suffit de montrer l'affirmation pour $\widetilde{A}$. On sait d'une partie que

$$\chi_{\widetilde{A}}(X) = \prod_{k=1}^{n}(X - a_k) \quad .$$

D'autre part, par les relations coefficients-racines (4.4.10.8) on sait que

$$\prod_{k=1}^{n}(X - a_k) = \sum_{k=0}^{n} X^k(-1)^{n-k}\sigma_{n-k}(a_1, .., a_n) \quad ,$$

où $\sigma_0, .., \sigma_n \in \mathbb{K}[X_1, .., X_n]$ sont les polynômes symétriques élémentaires. Par 4.4.10, les $\sigma_1, .., \sigma_n$ sont polynômes en les sommes de Newton $S_1, .., S_n$. Comme

$$S_j(a_1, .., a_n) = \sum_{k=1}^{n} a_k^j = \mathrm{tr}(A^k) \quad \forall j \in \{1, .., n\}$$

on déduit que le valeurs $\sigma_k(a_1, .., a_n),\ 1 \in \{0, .., n\}$ dépendent seulement des traces $\mathrm{tr}(A^1), .., \mathrm{tr}(A^n)$. Cela finit la preuve.

□

4.4.14 Definition: Polynôme antisymétrique

Soit A un anneau commutatif et $n \in \mathbb{N}$. Un polynôme $P \in A[X_1, .., X_n]$ est dit **antisymétrique** ssi

$$\sigma \cdot P = \mathrm{sgn}(\sigma) \cdot P \quad \forall\ \sigma \in \mathrm{Sym}(n) \quad .$$

Notons $A[X_1, .., X_n]^{\mathrm{ant}}$ le sous-A-module de $A[X_1, .., X_n]$ des polynômes antisymétriques.

Remarques

(i) Le produit de deux polynômes antisymétriques donne un polynôme symétrique, c'est-à-dire

$$A[X_1, .., X_n]^{\mathrm{ant}} * A[X_1, .., X_n]^{\mathrm{ant}} \subseteq A[X_1, .., X_n]^{\mathrm{Sym}(n)} \quad .$$

(ii) Le produit d'un polynôme antisymétrique et un polynôme symétrique est antisymétrique, c'est-à-dire

$$A[X_1, .., X_n]^{\mathrm{ant}} * A[X_1, .., X_n]^{\mathrm{Sym}(n)} \subseteq A[X_1, .., X_n]^{\mathrm{ant}} \quad .$$

4.4.15 Lemme : Représentation des polynômes antisymétriques

Soit A un anneau commutatif et $n \in \mathbb{N}$. Alors, tout polynôme antisymétrique $P \in A[X_1, .., X_n]^{\mathrm{ant}}$ est de la forme $P = Q * V$ où $Q \in A[X_1, .., X_n]^{\mathrm{Sym}(n)}$ et $V \in A[X_1, .., X_n]^{\mathrm{ant}}$ est définie comme

$$V = \det\left(X_i^{j-1}\right)_{i,j=1}^{n} = \prod_{i<j}(X_i - X_j) \quad .$$

4.5 Séries formelles

4.5.1 Definition: Algèbre des séries formelles

Soit A un anneau commutatif et S un sous-monoide de $\mathbb{N}_0^n$. On munit le A-module

$$A[[S]] := \bigtimes_{s \in S} A$$

d'un loi de multiplication

$$(a_s)_{s\in S} * (b_s)_{s\in S} := \left(\sum_{s+t=u} a_s \cdot b_t\right)_{u\in S} \quad , \tag{4.5.1.1}$$

qui fait de $A[[S]]$ une A-algèbre, dit l'**algèbre des séries formelles**. Noter que les sommes dans (4.5.1.1) 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 $A[[\mathbb{N}_0^n]] =: A[[X_1, .., X_n]]$. En ce cas on écrit souvent $X^s = X_1^{s_1} \cdot .. \cdot X_n^{s_n}$ pour $s = (s_1, .., s_n) \in \mathbb{N}_0^n$.

4.5.2 Definition: 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 $\mathrm{val}(f)$. Par convention on pose $\mathrm{val}(0) = \infty$. On note $f \in \mathcal{O}(X^n)$ ssi $\mathrm{val}(f) \geq n$.

On dit qu'une suite de séries formelles $(f_n(X))_{n\in\mathbb{N}} \subseteq A[[X]]$ **converge vers zéro**, ssi $\mathrm{val}(f_n) \overset{n\to\infty}{\longrightarrow} 0$. On dit que $(f_n)_n$ **converge** vers $f \in A[[X]]$ ssi la suite $(f - f_n)_n$ converse vers zéro.

Remarques

(i) Pour $f, g \in A[[X]]$ on a

$$\mathrm{val}(f+g) \geq \min\{\mathrm{val}(f), \mathrm{val}(g)\} \tag{4.5.2.1}$$

et

$$\mathrm{val}(f * g) \geq \mathrm{val}(f) + \mathrm{val}(g) \quad . \tag{4.5.2.2}$$

(ii) Tout $\mathcal{O}(X^n)$ est un idéal, plus précisément

$$\mathcal{O}(X^n) = X^n * A[[X]] \quad . \tag{4.5.2.3}$$

Plus généralement, on a

$$\mathcal{O}(X^n) + \mathcal{O}(X^m) \subseteq \mathcal{O}(X^{\min\{n,m\}}) \quad ,$$

$$\mathcal{O}(X^n) * \mathcal{O}(X^m) \subseteq \mathcal{O}(X^{n+m}) \quad .$$

4.5.3 Lemme : La valuation comme morphisme de monoides

Soit A un anneau intègre et S un sous-monoide de $\mathbb{N}_0^n$. Alors $(A[[S]], +, *)$ est un anneau intègre. De plus, la valuation

$$\mathrm{val} : (A[[X]] \setminus \{0\}, *) \to (\mathbb{N}_0, +) \quad , \quad \mathrm{val} : f \mapsto \mathrm{val}(f)$$

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

$$\mathrm{val}(f * g) = \mathrm{val}(f) + \mathrm{val}(g)$$

car $u_0 := (s_0 + t_0)$ est le plus petit possible tel que $(f * g)_{u_0} \neq 0$. Finalement, $\mathrm{val}(1) = 0$.

□

4.5.4 Definition: Famille de séries sommable

Soit A un anneau commutatif et S un sous-monoide 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 $f_n \overset{n\to\infty}{\longrightarrow} 0$.

4.5.5 Definition: 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 (4.5.2.2) la famille $(f_n g^n(X))_{n\in\mathbb{N}_0}$ est sommable et on note

$$(f \circ g)(X) := \sum_{n\in\mathbb{N}_0} f_n \cdot g^n(X) \quad .$$

Remarques

(i) Par (4.5.2.2) on trouve que

$$\mathrm{val}(f \circ g) \geq \mathrm{val}(f) \cdot \mathrm{val}(g) \quad .$$

4.5.6 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

$$\boxed{\frac{1}{f(X)} = f_0^{-1} \cdot \sum_{s\in\mathbb{N}_0} \left[1 - f_0^{-1} \cdot f(X)\right]^n \quad .} \tag{4.5.6.1}$$

Preuve :

Direction "⇒" : 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 "⇐" : 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 $\mathrm{val}(g) > 0$. Donc, tout revient à prouver que $(1 + g)$ est inversible avec inverse $\sum_{s\in\mathbb{N}_0}(-1)^n g(X)^n$. 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

$$(1 + g) * \left(1 - g + g^2 + \cdots + (-1)^n g^n\right) = 1 + (-1)^n g^{n+1}(X) \in 1 + \mathcal{O}(X^{n+1}) \quad ,$$

et donc par remarques 4.5.2(i) et 4.5.5(i)

$$(1 + g) \sum_{n\in\mathbb{N}_0} (-1)^n g^n \in 1 + \mathcal{O}(X^{n+1}) \quad .$$

Cela étant vrai pour tout $n \in \mathbb{N}_0$, on conclut

$$(1 + g) \sum_{n\in\mathbb{N}_0} (-1)^n g^n = 1 \quad .$$

□

Remarques & Exemples :

(i) Les inverses des séries $1 \pm X$ sont données par

$$\frac{1}{1 \pm X} = \sum_{n\in\mathbb{N}_0} (\mp X)^n \quad . \tag{4.5.6.2}$$

(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

$$\frac{1}{f(X)} = \frac{f_0^{-1}}{f_0^{-1} \cdot f(X)} = \frac{f_0^{-1}}{(1 - X) \circ (1 - f_0^{-1} \cdot f(X))} \overset{(4.5.6.2)}{=} f_0^{-1} \sum_{n\in\mathbb{N}_0} \left[1 - f_0^{-1} \cdot f(X)\right]^n \quad ,$$

comme déjà vu dans (4.5.6.1). Noter que $(1 - f_0^{-1} \cdot f(X)) \in \mathcal{O}(X)$.

4.5.7 Corollaire sur séries formelles inversibles par rapport à la multiplication

Soit A un anneau commutatif. Alors la sous-partie

$$A[[X]]^\times := (A[[X]],*)^\times = \left\{ f = \sum_{n=0}^{\infty} f_n X^n \in A[[X]] : f_0 \in A^\times \right\} \tag{4.5.7.1}$$

forme un groupe abélien par rapport à la multiplication $*$ avec élément neutre 1.

Preuve : L'égalité des deux côtés de (4.5.7.1) suit de 4.5.6. Par 2.1.7 on sait que $A[[X]]^\times$ est un groupe. □

4.5.8 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. $n_0 = \min\{\mathrm{val}(f) : f \in I\}$.

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 ⇒ 2 : Soit $m_0 := \min\{\mathrm{val}(f) : f \in I\}$. 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 4.5.3

$$\mathrm{val}(X^{n_0} * g) = \mathrm{val}(X^{n_0}) + \mathrm{val}(g) \geq n_0 \quad ,$$

c'est-à-dire $m_0 \geq n_0$.

2 ⇒ 1 : Soit $g \in I$ quelconque, alors $\mathrm{val}(g) \geq n_0$. Donc g est de la forme

$$g = X^{n_0} * \underbrace{\left[g_{n_0} + \sum_{k=0}^{\infty} g_{n_0+k} X^k \right]}_{\overline{g}} \quad ,$$

c'est-à-dire $g \in X^{n_0} * \mathbb{K}[[X]]$. Choisissons maintenant g tel que $\mathrm{val}(g) = n_0$. Alors, $g_{n_0} \neq 0$ et $\overline{g}$ est par 4.5.6 inversible. Donc $X^{n_0} = g * \overline{g}^{-1} \in I$, c'est-à-dire $X^{n_0} * \mathbb{K}[[X]] \subseteq I$.

□

4.5.9 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

$$\boxed{g * \mathbb{K}[[X]] = X^{\mathrm{val}(g)} * \mathbb{K}[[X]] = \mathcal{O}(X^{\mathrm{val}(g)}) \quad .} \tag{4.5.9.1}$$

Preuve : Par définition de la valuation sur $\mathbb{K}[[X]]$, on peut écrire

$$g = X^{\mathrm{val}(g)} \cdot \underbrace{\sum_{n=\mathrm{val}(g)}^{\infty} g_n X^{n-\mathrm{val}(g)}}_{\overline{g}} \quad ,$$

avec $g_{\mathrm{val}(g)} \neq 0$. Donc par 4.5.6 $\overline{g}$ est inversible. Donc, par remarque 2.1.6(ii) g et $X^{\mathrm{val}(g)}$ engendrent le même idéal. La deuxième partie est rien autre que (4.5.2.3).

□

4.5.10 Lemme sur la valuation

Soit $\mathbb{K}$ un corps. Alors, $\mathbb{K}[[X]]$ est un anneau euclidien[25] avec division euclidienne unique par rapport à la valuation $\mathrm{val} : \mathbb{K}[[X]] \to \mathbb{N}_0$.

Preuve : Noter que par 4.5.3 $\mathbb{K}[[X]]$ est intègre. Il faut montrer les axiomes 2.1.14(1) et 2.1.14(2). Comme $\mathrm{val} : (\mathbb{K}[[X]], *) \to (\mathbb{N}_0, +)$ est un morphisme de monoides, l'axiome (1) est trivial. En fait, val() satisfait aussi l'inverse : Si $\mathrm{val}(g) \leq \mathrm{val}(f)$, alors $g \mid f$. Vraiment, par 4.5.9 on peut décomposer $f = \overline{f} * X^{\mathrm{val}(f)}$ et $g = \overline{g} * X^{\mathrm{val}(g)}$, avec $\overline{f}, \overline{g} \in \mathbb{K}[[X]]^\times$ inversibles. Donc

$$f = g * X^{\mathrm{val}(f)-\mathrm{val}(g)} * \overline{g}^{-1} * \overline{f} \quad .$$

On montre l'axiome (2). Soient $f \in \mathbb{K}[[X]]$ et $g \in \mathbb{K}[[X]] \setminus \{0\}$. Alors, en cas $\mathrm{val}(g) > \mathrm{val}(f)$ on a $f = gq + r$ avec $q := 0$ et $r := f \neq 0$, où $\mathrm{val}(r) < \mathrm{val}(f)$ si $r \neq 0$. Dans l'autre cas que $\mathrm{val}(g) \leq \mathrm{val}(f)$, 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 $\mathrm{val}(R) < \mathrm{val}(B)$, alors $Q = 0 = R$. Vraiment, si $Q \neq 0$ alors $QB \neq 0$ et $\mathrm{val}(QB) \geq \mathrm{val}(B)$, 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 $\mathrm{val}(g) \leq \mathrm{val}(f)$ ssi g divise f.

4.5.11 Definition: Séries formelles inversibles par rapport à la composition

Soit A un anneau commutatif. On dit une séries formelle $f \in A[[X]]$ **inversible par rapport à la composition** "$\circ$" 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 4.5.12, si $g \in \mathcal{O}(X^1)$ satisfait $f \circ g = X$, alors $f \in \mathcal{O}(X^1)$ et $g \circ f = X$.

4.5.12 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 "$\circ$" 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

$$X = \sum_{n=0}^{\infty} f_n g^n = f_0 + \underbrace{\sum_{n=1}^{\infty} f_n g^n}_{\in \mathcal{O}(X^1)} \tag{4.5.12.1}$$

et donc $f_0 = 0$. De plus (4.5.12.1) 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

$$f(g(X)) = \sum_{n=1}^{\infty} f_n \cdot \left[\sum_{k=1}^{\infty} g_k \cdot X^k \right]^n \stackrel{!}{=} X \tag{4.5.12.2}$$

25. Voir définition 2.1.14.

est équivalente à $f_1 g_1 = 1$ et

$$a_1 b_n + (\star) = 0 \quad \forall\ n \geq 2 \quad , \tag{4.5.12.3}$$

où $(\star)$ sont des expressions polynomiales en $f_1, .., f_n, g_1, .., g_{n-1}$. Donc $g_1 = f_1^{-1}$ et par induction les expressions (4.5.12.3) se résolvent aux $g_2, g_3, \ldots$ 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 $g \circ f = X$.

□

4.5.13 Corollaire sur séries formelles inversibles par rapport à la composition

Soit A un anneau commutatif. Alors, la sous-partie

$$A[[X]]^\circ := \left\{ f = \sum_{n=1}^{\infty} f_n X^n \in A[[X]] : f_1 \in A^\times \right\} = \{ f \in A[[X]] \text{ inversible par rapport à } \circ \} \tag{4.5.13.1}$$

forme par rapport à la composition $\circ$ un groupe avec élément neutre X.

Preuve : L'égalité des deux côtés de (4.5.13.1) suit de théorème 4.5.12. Évidement 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 4.5.12 l'inverse de toute série formelle inversible est aussi inversible.

□

Exemples : Supposons $\mathbb{Q} \subseteq A$.

(i) Pour $\alpha \in A$ on note

$$(1+X)^\alpha := \sum_{n=0}^{\infty} \binom{\alpha}{n} \cdot X^n \quad .$$

Note que si $\alpha \in \mathbb{N}_0$ alors

$$(1+X)^\alpha = \underbrace{(1+X) * \cdots * (1+X)}_{\times \alpha} \quad .$$

(ii) Pour $\alpha \in A$ on appelle

$$\exp(aX) := \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \cdot X^n \quad .$$

la **série exponentielle** dans $A[[X]]$. De plus, on note

$$\log(1+X) := \sum_{n=1}^{\infty} (-1)^{n-1} \cdot \frac{X^n}{n} \quad . \tag{4.5.13.2}$$

Par 4.5.17, on a

$$[\exp(X) - 1] \circ \log(1+X) = \log(1+X) \circ [\exp(X) - 1] = X \quad .$$

(iii) Les dérivées de $\exp(aX)$ et $\log(1+X)$ sont données par

$$\frac{d}{dX} \exp(aX) = a \cdot \exp(aX)$$

et

$$\frac{d}{dX} \log(1+X) \overset{(4.5.13.2)}{=} \sum_{n=0}^{\infty} (-X)^n \overset{(4.5.6.2)}{=} \frac{1}{1+X} \quad . \tag{4.5.13.3}$$

4.5.14 Definition: Dérivée d'une série formelle

Soit A un anneau commutatif. Pour $f \in A[[X_1, .., X_n]]$ de la forme $f = \sum_{s\in\mathbb{N}_0^n} f_s X^s$ et $i \in \{1, .., n\}$ on appelle la série formelle $\partial_i f \in A[[X_1, .., X_n]]$ donnée par

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

la **dérivée de f par rapport à X_i**. Pour $f \in A[[X]]$ on note $\frac{df}{dX} := \partial_1 f$.

4.5.15 Propriétés élémentaires de la dérivée

Soit A un anneau commutatif, $n \in \mathbb{N}$, $i \in \{1, .., n\}$. Alors :

1. L'opérateur $\partial_i : A[[X_1, .., X_n]] \to A[[X_1, .., X_n]]$ est un morphisme de A-modules.
2. Pour $f, g \in A[[X_1, .., X_n]]$ on a $\partial_i(f * g) = (\partial_i f) * g + f * (\partial_i g)$.
3. Pour $f \in A[[X_1, .., X_n]]$ 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 $(f_j)_{j\in J} \subseteq A[[X_1, .., X_n]]$ 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
$$\frac{d}{dX}(f \circ g) = \left(\frac{df}{dX} \circ g\right) * \frac{dg}{dX} \quad .$$

4.5.16 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 4.3.5.

□

4.5.17 Exemple : Inverse de la série exponentielle

Soit A un anneau commutatif et $\exp(X)$ la série exponentielle dans $A[[X]]$. Alors :

$$\exp\left[\log(1 + X)\right] = 1 + X \quad .$$

Preuve : On va déduire et resoudre une *équation différentielle* pour la série $f(X) := \exp\left[\log(1 + X)\right]$. On a

$$\frac{df}{dX} = \left[\frac{d}{dX}\exp(X)\right](\log(1 + X)) * \frac{d}{dX}\log(1 + X) \overset{(4.5.13.3)}{=} \exp\left[\log(1 + X)\right] * \frac{1}{1 + X} = \frac{f}{1 + X} \quad .$$

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 partie $\frac{dg}{dX} = \sum_{n=0}^{\infty}(n+1)g_{n+1}X^n$ et d'autre part

$$\frac{g}{1+X} \overset{(4.5.6.2)}{=} \sum_{n=0}^{\infty} g_n X^n * \sum_{k=0}^{\infty}(-X)^k = \sum_{n=0}^{\infty} X^n \sum_{k=0}^{n} g_k(-1)^{n-k} \quad .$$

Donc, on a la chaîne d'équivalences

$$\begin{aligned}\frac{dg}{dX} = \frac{g}{1+X} &\Leftrightarrow (n+1)p_{n+1} = \sum_{k=0}^{n} p_n(-1)^{n-k} \quad \forall n \in \mathbb{N}_0 \\ &\Leftrightarrow 1\cdot p_1 = p_0,\ 2\cdot p_2 = p_1 - p_0,\ 3\cdot p_3 = p_2 - p_1 + p_0,\ \ldots \\ &\Leftrightarrow p_1 = p_0 \ \wedge\ p_n = 0 \ \ \forall n \geq 2 \\ &\Leftrightarrow g = p_0 + p_0 X \quad .\end{aligned}$$

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

$$\exp[\log(1+X)] = 1 + X \quad .$$

□

4.5.18 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

$$(1+X)^{\alpha} * (1+X)^{\beta} = (1+X)^{\alpha+\beta} \quad .$$

Preuve : Comme

$$(1+X)^{\alpha} * (1+X)^{\beta} = \sum_{n\in\mathbb{N}_0} \sum_{p+q=n} \binom{\alpha}{p}\binom{\beta}{q} X^n \quad , \quad (1+X)^{\alpha+\beta} = \sum_{n\in\mathbb{N}_0} \binom{\alpha+\beta}{n} X^n \quad ,$$

il suffit à montrer que

$$\sum_{p+q=n} \binom{\alpha}{p}\binom{\beta}{q} = \binom{\alpha+\beta}{n} \quad .$$

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 4.3.2 il suffit à montrer que $\Delta Q_{\beta,n} = 0$, où $\Delta : A[X] \to A[X]$ est l'opérateur de différences définit dans 4.3.1. On trouve en fait

$$\Delta Q_{\beta,n}(X) \overset{4.3.3(ii)}{=} \binom{X+\beta}{n-1} - \sum_{p+q=n} \underbrace{\binom{X}{p-1}}_{\substack{=:0 \\ \text{si } p=0}} \binom{\beta}{q} = \binom{X+\beta}{n-1} - \sum_{k+l=n-1} \binom{X}{k}\binom{\beta}{l} \overset{Q_{\beta,n-1}=0}{=} 0 \quad ,$$

ce qui complet la preuve.

□

Conséquences :

(i) Pour $\alpha \in A$ on a

$$\frac{1}{(1+X)^{\alpha}} = (1+X)^{-\alpha} = \sum_{n=0}^{\infty} \binom{-\alpha}{n} \cdot X^n \quad .$$

4.5.19 Développement en séries formelles d'une fraction rationnelle

Soit $\mathbb{K}$ un corps. Alors, par 4.5.3 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 3.1.20). 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 4.5.20 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 lui 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 4.5.6 $Q(X)$ 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 $Q = X^n * \widetilde{Q}$ pour un $\widetilde{Q} \in \mathbb{K}[X]$ avec $\widetilde{Q}(0) \neq 0$. Donc, en appliquant le dessus on peut écrire

$$\frac{P(X)}{Q(X)} = X^{-n} * \frac{P(X)}{\widetilde{Q}(X)} = \underbrace{X^{-n} * P(X) * \underbrace{\widetilde{Q}^{-1}(X)}_{\in \mathbb{K}[[X]]}}_{\in \mathbb{K}((X))} \ ,$$

l'inverse $\widetilde{Q}^{-1}(X) \in \mathbb{K}[[X]]$ (par rapport à la multiplication) étant donnée par la formule (4.5.6.1). 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 $1/\left[(1-X^3)(1-X^5)\right] \in \mathbb{C}(X)$ s'injecte dans $\mathbb{C}[[X]]$ par la formule (4.5.6.1) comme

$$\frac{1}{(1-X^3)(1-X^5)} \mapsto (1-X^3)^{-1} * (1-X^5)^{-1} = \sum_{n=0}^{\infty} X^{3n} * \sum_{n=0}^{\infty} X^{5n}$$

$$= \sum_{k=0}^{\infty} X^k \cdot \left|\left\{(n,m) \in \mathbb{N}_0^2 : 3n+5m = k\right\}\right| = 1 + X^3 + X^5 + X^6 + \mathcal{O}(X^8) \ .$$

4.5.20 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 lui d'addition

$$\sum_{n\geq n_0} a_n X^n + \sum_{n\geq m_0} b_n X^n = \sum_{n\geq n_0} (a_n + b_n) X^n \tag{4.5.20.1}$$

(où sans perdu de généralité $m_0 = n_0$) et de la multiplication

$$\left[\sum_{n\geq n_0} a_n X^n\right] * \left[\sum_{m\geq m_0} b_m X^m\right] = \sum_{k\geq n_0+m_0} \left[\sum_{n+m=k} a_n b_m\right] X^k \quad . \tag{4.5.20.2}$$

Preuve : On montre toute 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 $g = X^{n_0} * \widetilde{g}$ pour un $0 \neq \widetilde{g} \in \mathbb{K}[[X]]$ avec valuation 0. il existe donc dans $\mathbb{K}[[X]]$ l'inverse $\widetilde{g}^{-1}$ et donc dans $\mathbb{L}(X)$ l'inverse $X^{-n_0} * \widetilde{g}^{-1}$. 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 $\mathbb{K}((X)) \cong \mathbb{L}(X)$.

□

5 Anneaux factoriels

5.1 Préliminaires

5.1.1 Definition: Elément irréductible

Soit A un anneau intègre. Un élément $\pi \in A$ est dit **irréductible** si :
- π 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 2.1.7(i) sur éléments inversibles.

5.1.2 Definition: 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 2.1.6(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 5.1.1(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 π 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 4.5.9 deux éléments non nulles sont associées ssi ils possèdent la même valuation.

5.1.3 Definition: 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 $\pi = yx = ya\pi$. 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 $|p|$ et un nombre premier (dans le sens *traditionnel*). On note $\mathbb{P} \subseteq \mathbb{N}$ les (positives) premiers de $\mathbb{Z}$.

5.1.4 Definition: 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 5.1.4(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, noetherien, alors propriété 5.1.4(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 2.1.6(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 2.3.2 cela est une contradiction.

5.1.5 Lemme de Gauss sur anneaux intègres, principaux

Un anneau intègre, principal A est factoriel.

Preuve : Comme tout anneau principal est noetherien, par remarque 5.1.4(ii) il suffit à montrer propriété 5.1.4(2). Par remarque 5.1.3(iii) il faut montrer que tout irréductible est premier.

Soit $\pi \in A$ irréductible. Comme π est non-inversible, par remarque 5.1.3(ii) il suffit de montrer la propriété de Gauss. Soit $\pi \mid xy$ pour quelques $x, y \in A$. Alors, comme A et 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 4.1.11 intègre et par 4.2.5 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 2.2.20 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 $J = I$.

5.1.6 Lemme : Chaîne des inclusions de classes des anneaux intègres

Dans la famille des anneaux intègres, on a la chaîne d'inclusions suivante :

$$\{\text{euclidiens}\} \subseteq \{\text{principaux}\} \subseteq \{\text{factoriels}\} \quad .$$

5.1.7 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 $\pi_1, .., \pi_r, \xi_1, .., \xi_s \in A$, alors $r = s$ et il existe une permutation σ de $\{1, .., r\}$ telle que $\pi_1 \sim \xi_{\sigma(i)}$ pour tout $i \in \{1, .., r\}$.

Autrement dit, on a sur A l'unicité de la composition en irréductibles modulo la relation d'association et l'ordre près.

Preuve :

Direction "⇒" : Par remarque 5.1.4(i) tout irréductible satisfait la propriété de Gauss. Soient $\pi_1, .., \pi_r, \xi_1, .., \xi_s \in A$ irréductibles tels que $\pi_1 \dots \pi_r = \xi_1 \dots \xi_s$. Alors, π_1 divise l'un des ξ_1, supposons $\pi_1 \mid \xi_1$. Donc $\xi_1 = a_1\pi_1$ pour un $a_1 \in A$. Comme ξ_1 est irréductible et π_1 non-inversible, il faut $a \in A^\times$. Donc, par remarque 2.1.6(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

$$\pi_2 \dots \pi_r = a_1\xi_2\xi_3 \dots \xi_s = \widetilde{\xi_2}\xi_3 \dots \xi_s \quad ,$$

où $\widetilde{\xi_2} := a_1\xi_2$ est par remarque 5.1.1(ii) aussi irréductible. Par récurrence suit l'affirmation.

Direction "⇐" : 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 précèdent soit $a \mid y$ soit $a \mid x$.
- Si $x, y, b \notin A^\times$, alors par supposition il existe irréductibles $\pi_1, .., \pi_n, \xi_1, .., \xi_m, \rho_1, .., \rho_l$ tels que

$$\underbrace{\pi_1..\pi_n}_{x} \cdot \underbrace{\xi_1..\xi_m}_{y} = a \cdot \underbrace{\rho_1..\rho_k}_{b} \quad .$$

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 5.1.3(ii) cela et le fait que a est non-inversible impliquent que a est premier, donc A factoriel.

□

5.1.8 Corollaire : Factorisation de produits

Soit A un anneau factoriel, $\pi_1, .., \pi_n \in A$ irréductibles et $0 \neq a_1, .., a_m \in A$ quelconques tels que $a_1..a_m \sim \pi_1..\pi_n$. Alors il existe une partition $\{1, .., n\} = \biguplus_{i=1}^{m} I_i$ telle que $a_i \sim \prod_{j \in I_i} \pi_i$.

Preuve : Suit de caractérisation 5.1.7.

□

5.1.9 Definition: pgcd et ppcm

Soit A un anneau factoriel. Par théorème 5.1.7, tout élément $0 \neq x \in A$ peut être écrit sous la forme $x = a \cdot \pi_1..\pi_n$ ($n \in \mathbb{N}_0$), où $a \in A^\times$ est inversible et $\pi_1, .., \pi_n \in A$ sont des irréductibles, uniques modulo la relation d'association et l'ordre près. Inversement, si $\xi_1, .., \xi_n \in A$ sont irréductibles deux à deux associées aux $\pi_1, .., \pi_n$, x possède aussi la représentation $b \cdot \xi_1..\xi_n$ 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 $x = a \cdot \pi_1^{p_1}..\pi_n^{p_n}$ 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

π_i^0. Soient $0 \neq x, y \in A$ avec les décompositions uniques $x = a \cdot \pi_1^{p_1} .. \pi_n^{p_n}$ et $y = b \cdot \xi_1^{q_1} .. \xi_m^{q_m}$ de tel type. Alors, en supposant sans perdu de généralité que $n = m$ et $\pi_i = \xi_i \ \forall i$ on pose

$$\operatorname{ppcm}(x, y) := ab \cdot \prod_{i=1}^{n} \pi_i^{\max(p_i, q_i)} \quad ,$$

$$\operatorname{pgcd}(x, y) := ab \cdot \prod_{i=1}^{n} \pi_i^{\min(p_i, q_i)} \quad .$$

Par convention, on pose $\operatorname{ppcm}(x, 0) := 0$ et $\operatorname{pgcd}(x, 0) := x$.

Remarques : Soient $0 \neq a, b, c \in A$. Alors :

(i) Les valeurs $\operatorname{ppcm}(a, b)$ et $\operatorname{pgcd}(a, b)$ ne sont pas uniques ; ils dépendent du choix de $\mathcal{J}_A$. Neanmois, ils sont uniques à association près. Il faudrait donc parler des $\operatorname{pgcd}(a, b)$ et $\operatorname{ppcm}(a, b)$ comme classes d'équivalence. On note pourtant souvent $\operatorname{pgcd}(a, b)$ et $\operatorname{ppcm}(a, b)$ par un de leurs représentatifs.

(ii) Inversement, $\operatorname{ppcm}(a, b)$ et $\operatorname{pgcd}(a, b)$ sont constantes dans les classes d'équivalence des a, b.

(iii) Les opérations $\operatorname{ppcm}, \operatorname{pgcd} : (A/\sim) \times (A/\sim) \to (A/\sim)$ sont symétriques et associatives. On peut donc parler des ppcm et pgcd de plusieurs éléments.

(iv) On a toujours $a \mid \operatorname{ppcm}(a, b)$ et $\operatorname{pgcd}(a, b) \mid a$.

(v) Le diviseur $\operatorname{pgcd}(a, b)$ en commun des a, b, est le *plus grand* : Si $c \mid a$ et $c \mid b$, alors $c \mid \operatorname{pgcd}(a, b)$.

(vi) Le multiple $\operatorname{ppcm}(a, b)$ en commun des a, b, est le *plus petit* : Si $a \mid c$ et $b \mid c$, alors $\operatorname{ppcm}(a, b) \mid c$. Autrement dit

$$Aa \cap Ab = A \operatorname{ppcm}(a, b) \quad .$$

(vii) Pour $a_1, .., a_n \in A$ on a

$$\operatorname{pgcd}(a_1, .., a_n) = 1 \quad \Leftrightarrow \quad \operatorname{ppcm}(a_1, .., a_n) = \prod_{i=1}^{n} a_i \quad .$$

(viii) Si A est principal et $a_1, .., a_n \in A$, alors $Aa_1 + .. + Aa_n = A \operatorname{pgcd}(a_1, .., a_n)$ [Bézout]. En particulier,

$$Aa_1 + .. + Aa_n = A \ \Leftrightarrow \ \operatorname{pgcd}(a_1, .., a_n) = 1 \quad .$$

(ix) Si $a_1, .., a_n \in A$ sont tels que $\operatorname{pgcd}(a_1, .., a_n) = 1$ on les dit **premiers entre eux dans leur ensemble**.

(x) Si $a_1, .., a_n \in A$ possèdent $\operatorname{pgcd}(a_i)_{i=1}^n = a$, alors il existe $\alpha_1, .., \alpha_n \in A$ (uniques d'association près) tels que

$$a_i = \alpha_i \cdot a \quad \wedge \quad \operatorname{pgcd}(\alpha_i)_{i=1}^n = 1 \quad .$$

(xi) Pour $a, a_1, .., a_n \in A$ on a $\operatorname{pgcd}(a \cdot a_i)_{i=1}^n = a \cdot \operatorname{pgcd}(a_i)_{i=1}^n$ et $\operatorname{ppcm}(a \cdot a_i)_{i=1}^n = a \cdot \operatorname{ppcm}(a_i)_{i=1}^n$.

(xii) Si $b \mid a_1, .., a_n \in A$, alors $b = \operatorname{pgcd}(b, a_1, .., a_n)$.
Preuve : Suit de remarque 5.1.2(v) et remarques (iv), (v).

(xiii) Pour $a_1, .., a_n \in A \setminus \{0\}$ on a $\operatorname{pgcd}(a_1, .., a_n) = 1$ ssi il n'existe aucun irréductible divisant tous $a_1, .., a_n$ et ssi il n'existe aucun non-inversible divisant tous $a_1, .., a_n$.

(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

$$\operatorname{pgcd}(a, b) = 1 = \operatorname{ppcm}(a, b) \quad .$$

Les notions de la multiplication, de l'irréductibilité, de la premierité, de la divisibilité et les opérations pgcd, ppcm sont invariants par rapports à l'association $\sim$ sur A. Ils passent donc tous au quotient $A/\sim$.

5.1.10 Théorème de Bachet-Bézout

On reformule l'affirmation de Bézout déjà vu dans remarque 5.1.9(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 $n \cdot x + m \cdot y = 1$.

5.2 Factorialité d'algèbres des polynômes

5.2.1 Definition: Polynôme primitif

Soit A un anneau factoriel et $P \in A[X_1, .., X_n]$ 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[26] $\operatorname{pgcd}(a_s)_{s\in S}$. On la note $\mathscr{C}(P)$. Si $\mathscr{C}(P) = 1$, 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 5.1.9(xiv) pour tout $0 \neq P \in \mathbb{K}[X]$ on a $\mathscr{C}(P) = 1$.

(ii) Pour $P \in A[X]$, il existe un primitif $P^* \in A[X]$ tel que $P = \mathscr{C}(P) \cdot P^*$.
Preuve : Soit $P = \sum_{i=0}^n a_i \cdot X^i$, alors il existe $\alpha_0, .., \alpha_n \in A$ tels que $\operatorname{pgcd}(\alpha_i)_{i=0}^n = 1$ et $a_i = \mathscr{C}(P) \cdot \alpha_i \ \forall i$. Donc

$$P = \mathscr{C}(P) \cdot \underbrace{\sum_{i=0}^n \alpha_i \cdot X^i}_{P^*} \ ,$$

avec $\mathscr{C}(P^*) = 1$.

(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[27] que $c_i = a_i/b$ avec $a_i, b \in A$ et $\operatorname{pgcd}(b, a_1, .., a_n) = 1$. Pose $a := \operatorname{pgcd}(a_i)_{i=1}^n$, alors par remarque 5.1.9(x) il existe $\alpha_1, .., \alpha_n \in A$ tels que $a_i = a \cdot \alpha_i$ et $\operatorname{pgcd}(\alpha_i)_{i=1}^n = 1$. Donc $c_i = \alpha_i \cdot (a/b)$ et $P = (a/b)P^*$ pour un primitif $P^* \in A[X]$. Comme $1 = \operatorname{pgcd}(b, a_1, .., a_n) = \operatorname{pgcd}(b, a)$ les b, a sont premiers entre eux.

5.2.2 Definition: Réduction d'un polynôme

Soit A un anneau commutatif et $I \subseteq A$ un idéal de A. Alors, le morphisme d'anneaux

$$A[X] \to (A/I)[X] \ \ , \ \ \sum_i a_i \cdot X^i \mapsto \sum_i [a_i] \cdot X^i$$

et dit **réduction modulo** I. Si $I = A\pi$ pour un $\pi \in A$, on parle du morphisme

$$A[X] \to (A/\pi A)[X] \overset{4.2.11}{\cong} A[X]/(\pi A)[X] \ \ , \ \ \underbrace{P}_{\in A[X]} \mapsto \underbrace{P + (\pi A)[X]}_{\in A[X]/\pi A[X]}$$

comme **réduction** des polynômes **modulo** π.

Remarques

(i) Soit A un anneau intègre. Alors $0 \neq \pi \in A$ est premier dans A ssi πA 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 π premier dans $A[X]$.

5.2.3 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 π est non-nul.

26. Par rapport à la relation d'équivalence d'association (voir 5.1.9).
27. On peut supposer $c_i = \frac{p_i}{q}$ pour quelques $p_i \in A, \ q \in A \setminus \{0\}$. Par remarque 5.1.9(x) on peut trouver des $a_i, a, b \in A$ tels que $p_i = a \cdot a_i, \ q = a \cdot b$ et $\operatorname{pgcd}(b, a_1, .., a_n) = 1$. 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 5.1.9(xiii) il existerait un irréductible π qui divise tous coefficients de P, donc la réduction de P modulo π serait nulle. Inversement, si la réduction de P modulo un irréductible $\pi \in A$ était nulle, alors π diviserait tous coefficients de P, donc $\pi \mid \mathscr{C}(P)$ et par conséquence $\mathscr{C}(P) \neq 1$.

□

5.2.4 Lemme de Gauss sur le contenu de polynômes

Soit A un anneau factoriel. Alors, le contenu $\mathscr{C} : (A[X], *) \to (A, \cdot)$ 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 5.2.1(ii) on peut trouver des primitifs $P^*, Q^* \in A[X]$ tels que $P = \mathscr{C}(P) \cdot P^*$ et $Q = \mathscr{C}(Q) \cdot Q^*$. En particulier

$$P * Q = \mathscr{C}(P) \cdot \mathscr{C}(Q) \cdot P^* * Q^*$$

et donc par remarque 5.1.9(xi)

$$\mathscr{C}(P * Q) = \mathscr{C}(P) \cdot \mathscr{C}(Q) \cdot \mathscr{C}(P^* * Q^*) \quad .$$

Il reste donc à montrer que $P^* * Q^*$ est primitif. On va utiliser la caractérisation 5.2.3. 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 π. Comme P^*, Q^* sont primitifs, on sait que $\overline{P}, \overline{Q} \neq 0$. Par remarque 5.2.2(i) $\pi A[X]$ est premier et donc $A[X]/\pi A[X]$ intègre, d'où on déduit

$$\overline{P^* * Q^*} \overset{5.2.2}{=} \overline{P^*} * \overline{Q^*} \neq 0 \quad .$$

Par conséquence, $P^* * Q^*$ est primitif.

□

5.2.5 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 $\mathscr{C}(C) = 1$. Soient $a, b \in R$ tels que $aA, bB \in R[X]$. Alors

$$\mathscr{C}(aA) \cdot \mathscr{C}(bB) = \mathscr{C}(aA * bB) = ab\mathscr{C}(A * B) = ab\mathscr{C}(C) = ab \quad .$$

On a donc

$$C = \frac{aA * bB}{ab} = \underbrace{\frac{aA}{\mathscr{C}(aA)}}_{=:\widetilde{A}} \cdot \underbrace{\frac{bB}{\mathscr{C}(bB)}}_{=:\widetilde{B}} \quad ,$$

avec $\widetilde{A}, \widetilde{B} \in R[X]$. Comme le coefficient dominant de C, égal à 1, est produit des coefficients dominants des $\widetilde{A}, \widetilde{B}$, il faut que les derniers sont inversibles dans A. Donc, A et $\widetilde{A}$ 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 $\mathbb{K} = \mathbb{Q}$.

5.2.6 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 5.2.1(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

$$b \cdot \mathscr{C}(F) = \mathscr{C}(bF) = \mathscr{C}(aP * Q^*) = a \cdot \underbrace{\mathscr{C}(P)}_{\sim 1} \cdot \underbrace{\mathscr{C}(Q^*)}_{\sim 1} = a \pmod{\sim} \ ,$$

   d'où on déduit $b \mid a$. Donc, comme $\operatorname{pgcd}(b, a) = 1$, d'après remarque 5.1.9(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 5.2.1(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 4.1.12 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 5.2.1(iii) il existe primitifs $F^*, G^* \in A[X]$ et $a, b, c, d \in A$ tels que $\operatorname{pgcd}(a, b) = 1 = \operatorname{pgcd}(c, d)$ et

$$F = \frac{a}{b} \cdot F^* \quad , \quad G = \frac{c}{d} \cdot G^* \quad .$$

   Donc $bdP = acF^* * G^*$ et par conséquence

$$bd = bd \cdot \overbrace{\mathscr{C}(P)}^{1} = \mathscr{C}(bdP) = \mathscr{C}(acF^* * G^*) = ac \cdot \underbrace{\mathscr{C}(F^* * G^*)}_{1} = ac \pmod{\sim} \ ,$$

   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 4.1.12 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 4.1.12 G est une constante. Comme

$$1 = \mathscr{C}(P) = \mathscr{C}(G) \cdot \mathscr{C}(H) \ ,$$

   on trouve que $\mathscr{C}(G)$ et $\mathscr{C}(H)$ contient des inversibles, donc G est en fait une constante inversible dans A, c'est-à-dire P est irréductible.

□

5.2.7 Théorème : Factorialité de $A[X_1, .., X_n]$

Si A est un anneau factoriel, alors $A[X_1, .., X_n]$ est également pour tout $n \in \mathbb{N}$.

Preuve : Il suffit par récurrence et théorème 4.1.8 de montrer que $A[X]$ est factoriel si A est factoriel. Soit $\mathbb{K}$ le corps quotient de A.

Proposition : Les irréductibles constantes de $A[X]$ sont premiers.

Soit $\pi \in A[X]$ un polynôme constant irréductible. Alors, par remarque 5.2.2(i) il suffit de montrer que π est aussi irréductible dans A. Evidement π 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 4.1.12 aussi dans A, c'est-à-dire π et vraiment irréductible.

Proposition : Les irréductibles non-constantes de $A[X]$ sont premiers.

Par 5.2.6(2), ces sont exactement les irréductibles, primitifs dans $\mathbb{K}[X]$. Soit $P \in A[X]$ un tel polynôme. Par remarque 5.1.3(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 5.1.5(i) on sait que $\mathbb{K}[X]$ et 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 5.2.6(1).

Il reste à voir, que tout $0 \neq F \in A[X]$ est un produit fini d'irréductibles. Par 5.2.1(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 $\pi_1, .., \pi_n \in A$ tels que $a = \pi_1..\pi_n \pmod{A^\times}$. Noter que par remarque 5.2.2(i) les $\pi_1, .., \pi_n$ 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

$$1 = \mathscr{C}(F^*) = \mathscr{C}(G) \cdot \mathscr{C}(H) \quad ,$$

on trouve que $\mathscr{C}(G), \mathscr{C}(H)$ sont inversibles, c'est-à-dire G, H sont primitives. Donc, $\mathrm{dg}(G) \geq 1$ (car sinon $G = \mathrm{const} \in A^\times$). De même $\mathrm{dg}(H) \geq 1$ et par conséquence $\mathrm{dg}\, G < \mathrm{dg}\, F^*$, $\mathrm{dg}\, H < \mathrm{dg}\, F^*$. 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 5.1.5, tout corps $\mathbb{K}$ est factoriel. Donc, $\mathbb{K}[X_1, .., X_n]$ est factoriel.

(ii) Par 5.1.5, $\mathbb{Z}$ est factoriel. Donc $\mathbb{Z}[X_1, .., X_n]$ est factoriel.

(iii) Soit $p \in \mathbb{Z}$ premier et $P \in \mathbb{Z}[X]$ tel que sa réduction $\overline{P}$ 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,

$$\mathbb{Z}[X]/\mathfrak{M} \overset{\substack{2.2.14\ \&\\ 2.2.5(1)}}{\cong} \underbrace{\mathbb{Z}[X]/p\mathbb{Z}[X]}_{\substack{\cong(\mathbb{Z}/p\mathbb{Z})[X]\\ \text{par } 4.2.11}} \Big/ \langle \overline{P} \rangle \cong \underbrace{\mathbb{F}_p[X]/\langle \overline{P} \rangle}_{\substack{\text{corps}\\ \text{par lemme } 6.1.7}}$$

où on a utilisé le fait que $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps. Donc, par 2.2.18 $\mathfrak{M}$ est maximal dans $\mathbb{Z}[X]$.

(iv) Soit A un anneau intègre et $P \in A[X]$ irréductible. Alors, P est soit de degré ≤ 1 soit de degré plus grand que 1 et sans racines.
Preuve : Supposer $\mathrm{dg}(P) \geq 2$ et P irréductible. Si P avait la racine $x \in A$, alors par 4.1.14 il se décomposerait comme $P = Q * (X - x)$, où $\mathrm{dg}(Q) \geq 1$. Par 4.1.12 Q et $(X - x)$ ne sont pas inversibles, une contradiction à l'irréductibilité de P.

(v) L'inverse de (iv) n'est pas forcement 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, $P_1, .., P_n \in A[X]$ irréductibles et $Q_1, .., Q_m \in A[X]$ quelconques tels que $Q_1..Q_m = P_1..P_n$. Alors, il existe une partition $\{1, .., n\} = \biguplus_{i=1}^m I_i$ telle que $Q_i = \prod_{j\in I_i} P_i$ de multiplication par inversibles près. Cela est simplement un cas spécial de 5.1.8, appliqué à l'anneau factoriel $A[X]$.

5.2.8 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 $\mathrm{dg}(R) < \mathrm{dg}(B)$ ou $R = 0$, alors $Q, R \in \mathbb{K}[X]$.

Preuve : Noter que par 4.2.12 $\mathbb{K}[X]$ et $\mathbb{L}[X]$ sont anneaux euclidiens avec division euclidienne unique et $\mathbb{K}[X] \subseteq \mathbb{L}[X]$, avec la même valuation $\mathrm{val}() := \mathrm{dg}()$. Donc, l'affirmation est juste un cas spécial de lemme 2.1.15 sur anneaux euclidiens.

□

5.2.9 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).

5.2.10 Le critère d'Eisenstein pour l'irréductibilité dans $\mathbb{Q}[X]$

1. Si $P \in \mathbb{Z}[X]$ est de degré ≥ 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 $a_0, .., a_{n-1}$.
   (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 $P(X) := X^{p-1} + \cdots + X^1 + X^0$ 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 $P/\mathscr{C}(P) \in \mathbb{Z}[X]$, on peut supposer que P est primitif, c'est-à-dire $\mathscr{C}(P) = 1$. Il existe deux $U, V \in \mathbb{Q}[X]$ de degré ≥ 1 tels que $P = U * V$. Soient $a, b \in \mathbb{Z}$ tels que $aU, bV \in \mathbb{Z}[X]$. Alors
$$\mathscr{C}(aU)\mathscr{C}(bV) = \mathscr{C}(abU * V) = \mathscr{C}(abP) = ab\mathscr{C}(P) = ab \quad . \tag{5.2.10.1}$$
Par conséquence
$$P = \frac{1}{ab}(aU) * (bV) \overset{(5.2.10.1)}{=} \underbrace{\frac{aU}{\mathscr{C}(aU)}}_{\in \mathbb{Z}[X]} * \underbrace{\frac{bV}{\mathscr{C}(bV)}}_{\in \mathbb{Z}[X]} \quad .$$
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 reduction des polynômes par p, c'est-à-dire le morphisme d'anneaux
$$\pi : \mathbb{Z}[X] \to \underbrace{(\mathbb{Z}/p\mathbb{Z})}_{\mathbb{F}_p}[X] \quad , \quad \sum_i b_i X^i \mapsto \overline{b}_i X^i \quad .$$
On a
$$\pi(P) = \sum_{i=1}^{n} \overline{a}_i X^i \overset{\text{(ii)}}{=} \overline{a}_n X^n \quad ,$$
avec $\overline{a}_n \neq 0$ par hypothèse (i). En particulier $\mathrm{dg}(\pi(P)) = \mathrm{dg}(P)$ et donc
$$\mathrm{dg}(Q) + \mathrm{dg}(R) = \mathrm{dg}(Q * R) = \mathrm{dg}(P) = \mathrm{dg}(\pi(P)) = \mathrm{dg}(\pi(Q) * \pi(R)) = \mathrm{dg}(\pi(Q)) + \mathrm{dg}(\pi(R)) \quad , \tag{5.2.10.2}$$
où on a utilisé le fait que $\mathbb{Z}$ et $\mathbb{F}_p$ sont intègres. Comme $\mathrm{dg}(\pi(Q)) \leq \mathrm{dg}(Q)$ et $\mathrm{dg}(\pi(R)) \leq \mathrm{dg}(R)$, on conclut de (5.2.10.2) que
$$\mathrm{dg}(\pi(Q)) = \mathrm{dg}(Q) \quad \wedge \quad \mathrm{dg}(\pi(R)) = \mathrm{dg}(R) \quad . \tag{5.2.10.3}$$
Noter que $\overline{a}_n X^n = \overline{a}_n X * .. * X$ donne une décomposition de $\pi(P)$ en irréductibles dans $\mathbb{F}_p$. Par 5.1.5(i) et 5.2.7 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 $\pi(Q) = \overline{q}X^{\varkappa}$ et $\pi(R) = \overline{r}X^{\rho}$ pour quelques $\overline{q}, \overline{r} \in \mathbb{F}_p$ et $\varkappa := \mathrm{dg}(Q) \geq 1$, $\rho := \mathrm{dg}(R) \geq 1$. 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 $q_0, .., q_{\varkappa-1}$ et $r_0, .., r_{\rho-1}$. 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 5.2.9 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 voir que p divise $\binom{p}{k}$ pour tout $k \in \{1, .., p-1\}$, 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 5.2.10(2). De plus, P est primitif dans $\mathbb{Z}[X]$ et donc par 5.2.6(3) aussi irréductible dans $\mathbb{Z}[X]$.

5.2.11 Le critère d'Eisenstein pour le cas général

Soit A un anneau factoriel et $P(X) = a_0 + .. + a_{n-1}X^{n-1} + X^n \in A[X]$. Supposer que $\pi \in A$ est irréductible tel que :
- π divise les $a_0, .., a_{n-1}$.
- π^2 ne divise pas a_0.

Alors, $P(X)$ est irréductible.

5.2.12 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.

□

6 Extensions de corps

6.1 Préliminaires

6.1.1 Definition: 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

$$[\mathbb{E} : \mathbb{K}] = [\mathbb{E} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}] \quad .$$

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 5.2.8).

6.1.2 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 5.1.9(viii)) on a $\operatorname{pgcd}(P, Q) = 1$ 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 $\operatorname{pgcd}(P, Q) = 1$ 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 $\overline{P}$ de P dans $V := \mathbb{K}[X]/\langle Q\rangle$ est inversible. Noter que par 4.2.13, V est un $\mathbb{K}$-espace vectoriel munit de la base $\overline{X}^0, .., \overline{X}^{m-1}$, où $m := \operatorname{dg}(Q)$. Donc, $\overline{P}$ est inversible ssi l'opérateur $\mathbb{K}$-linéaire $V \to V$ donné par $\overline{R} \mapsto \overline{P} * \overline{R}$, est inversible, c'est-à-dire sa matrice $(p_{ij})_{i,j=0}^{m-1}$ par rapport à la base $\overline{X}^0, .., \overline{X}^{-1}$ possède déterminante non-nule. Noter qu'elle est donnée par

$$\overline{P} * \overline{X}^j = \sum_{i=0}^{m-1} p_{ji} \cdot \overline{X}^i \quad , \quad j \in \{0, .., m-1\} \quad .$$

Si on passe au espace $V' := \mathbb{L}[X]/\langle Q\rangle$, la matrice de $(\overline{R} \mapsto \overline{P} * \overline{R})$ 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 $\mathbb{K}$.

□

6.1.3 Lemme : Caractéristique d'un anneau intègre

Soit A un anneau non-trivial intègre et $\chi : \mathbb{Z} \to A$ 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 χ 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 2.2.15(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 6.5.1 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 forcement première ou zéro. Par exemple, tout anneau de la forme $\mathbb{Z}/n\mathbb{Z}$, où $n \in \mathbb{N}$, est de caractéristique n.

6.1.4 Definition: Corps engendré

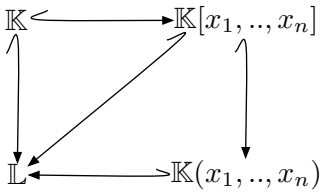
Soit B un anneau et A un sous-anneau de B. Pour éléments $x_1, .., x_n \in B$ on pose

$$A[x_1, .., x_n] := \{P(x_1, .., x_n) : P \in A[X_1, .., X_n]\} \quad .$$

Alors, $A[x_1, .., x_n]$ est le plus petit sous-anneau de B contenant A et les éléments $x_1, .., x_n$. Si $\mathbb{K}$ est un sous-corps du corps $\mathbb{L}$ et $x_1, .., x_n \in \mathbb{L}$, on note $\mathbb{K}(x_1, .., x_n)$ le plus petit corps contenant l'anneau $\mathbb{K}[x_1, .., x_n]$. Il est exactement le corps des fractions de $\mathbb{K}[x_1, .., x_n]$ (voir 3.1.20) et on a

$$\mathbb{K} \hookrightarrow \mathbb{K}[x_1, .., x_n] \hookrightarrow \mathbb{K}(x_1, .., x_n) \hookrightarrow \mathbb{L} \quad .$$

où le diagramme ci-dessous commute :



6.1.5 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

$$\varkappa : (\mathbb{K}[X], +, *) \to (\mathbb{L}, +, \cdot) \quad , \quad P(X) \mapsto P(x) \quad .$$

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 4.2.5 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 2.2.18 que $\ker(\varkappa)$ est un idéal

maximal dans $\mathbb{K}[X]$. En particulier, par 2.2.20 $\ker(\varkappa)$ 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 [28] 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 4.2.13, $\mathbb{K}[X]/\langle P_x\rangle$ est un $\mathbb{K}$-espace vectoriel de dimension égale à $\mathrm{dg}(P_x)$, donc

$$\mathrm{dg}(P_x) = \mathrm{dg}_{\mathbb{K}}(x) \quad .$$

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 $X^n - 1 = (X-1)*(X^{n-1}+..+X+1)$ est produit de deux non-inversibles, donc réductible. En fait, comme on verra dans 6.5.6, son polynôme minimal est donné par le n-ième polynôme cyclotomique et

$$\mathrm{dg}_{\mathbb{Q}}\left(e^{2\pi i/n}\right) = \varphi(n) \quad ,$$

où $\varphi : \mathbb{N} \to \mathbb{N}$ est l'indicatrice d'Euler, donnée par

$$\varphi(n) := |\{m \in \{1,..,n\} : \mathrm{pgcd}(m,n) = 1\}| \quad . \tag{6.1.5.1}$$

(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 $\mathrm{dg}_{\mathbb{K}}(x) \leq n$.

(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 $x_1,..,x_n \in \mathbb{L}$ algébriques sur $\mathbb{K}$. Alors $\mathbb{K}[x_1,..,x_n]$ est aussi un corps, en fait une extension de $\mathbb{K}$ de degré fini. Cela suit de la décomposition

$$\mathbb{K} \subseteq \mathbb{K}[x_1] \subseteq \mathbb{K}[x_1,x_2] \subseteq .. \subseteq \mathbb{K}[x_1,..,x_n] \subseteq \mathbb{L}$$

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 $\mathbb{L}$**.

6.1.6 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-nule de $\mathbb{K}$.
5. $\mathrm{pgcd}(P_x, P'_x) \neq 1$ (se rappeler à 6.1.2).

Preuve :

1 $\Leftrightarrow$ 2 **:** Cas spécial de remarque 4.1.15(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, $\mathrm{dg}(P'_x) \geq \mathrm{dg}(P_x)$, une contradiction !

28. Voir aussi 4.1.12(2).

3 ⇒ 4 : Noter que comme x est algébrique, $P_x \neq 0$ et donc $P_x \neq$ 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 $j \in \{1, .., n-1\}$ 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 ⇒ 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 ⇒ 5 : Si $P_x' \equiv 0$ alors par convention $\operatorname{pgcd}(P_x, P_x') = P_x$. Mais P_x est irréductible, donc pas associé à 1.

5 ⇒ 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 $P_x'(x) = 0$.

□

6.1.7 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 $\operatorname{dg}(P)$.

Preuve : Par 4.2.13 on sait que $\mathbb{K}[X]/\langle P \rangle$ est un $\mathbb{K}$-espace vectoriel de dimension $m := \operatorname{dg}(P) < \infty$. Noter que

$$\mathbb{K}[X]/\langle P \rangle = \mathbb{K}[\overline{X}] := \left\{ Q(\overline{X}) : Q \in \mathbb{K}[X] \right\} \quad .$$

Par 5.2.7 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 2.2.15(ii), $\mathbb{K}[X]/\langle P \rangle$ est intègre. Par 3.1.20, 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 6.1.5 $\mathbb{K}[\overline{X}]$ est un corps.

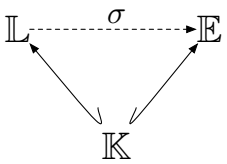
□

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 $\operatorname{dg}(P)$ 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 $\mathbb{K}$.

6.2 Morphismes et Automorphismes

6.2.1 Definition: $\mathbb{K}$-morphisme

Soit $\mathbb{K}$ un corps et $\mathbb{L}, \mathbb{E}$ deux corps-extensions de $\mathbb{K}$. Un **$\mathbb{K}$-morphisme de corps** $\sigma : \mathbb{L} \to \mathbb{E}$ est un morphisme de corps qui rend commutatif le triangle :



Dans un certain façon, σ est *l'identité sur* $\mathbb{K}$. En cas que $\mathbb{L} = \mathbb{E}$ et $\sigma : \mathbb{L} \to \mathbb{L}$ est bijective, on appelle σ un **$\mathbb{K}$-automorphisme de corps** de $\mathbb{L}$.

6.2.2 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 $\mathbb{L} \to \mathbb{L}$ 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.

□

6.2.3 Théorème : Éléments algébriques et $\mathbb{K}$-morphismes $\mathbb{K}[x] \to \mathbb{E}$

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 $\mathbb{K}$-morphismes de corps $\sigma : \mathbb{K}[x] \to \mathbb{E}$ sont en bijection avec les racines (distinctes) de P_x dans $\mathbb{E}$, via l'association $\sigma \mapsto \sigma(x)$.

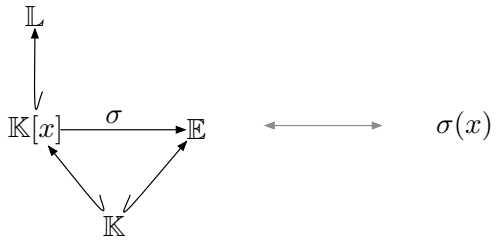


Figure 15: Sur théorème 6.2.3 : Les $\mathbb{K}$-morphismes de corps $\sigma : \mathbb{K}[x] \to \mathbb{E}$ sont en bijection avec les racines de P_x dans $\mathbb{E}$.

Preuve : Se rappeler que $\mathbb{K}[X]/\langle P_x \rangle \cong \mathbb{K}[x]$, via l'isomorphisme $\overline{Q} \mapsto Q(x)$. Soit P_x de la forme $P_x = \sum_i p_i \cdot X^i$, avec $p_i \in \mathbb{K}$. Soit $\mathscr{R}_{\mathbb{E}}(P_x)$ l'ensemble des racines de P_x dans $\mathbb{E}$. Tout $\mathbb{K}$-morphisme de corps $\mathbb{K}[x] \to \mathbb{E}$ 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 $\mathscr{R}_{\mathbb{E}}(P_x)$: Pour tout $y \in \mathbb{E}$ on peut choisir le morphisme d'anneaux $\sigma_0 : \mathbb{K}[X] \to \mathbb{E}$ comme la *spécification* $Q(X) \overset{\sigma_0}{\mapsto} Q(y)$. Si $y \in \mathscr{R}_{\mathbb{E}}(P_x)$, alors

$$\sigma_0(P_x) \overset{\text{def}}{=} P_x(y) = 0 \quad ,$$

c'est-à-dire σ_0 passe au quotient $\mathbb{K}[X]/\langle P_x \rangle \cong \mathbb{K}[x]$ comme le $\mathbb{K}$-morphisme de corps $\sigma : \mathbb{K}[x] \to \mathbb{E}$, donné par $\sigma : Q(x) \mapsto Q(y)$. En particulier $\sigma(x) = y$.

□

6.2.4 Corollaire sur le nombre de $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$

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 $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$ est plus petit ou égal à $\mathrm{dg}_{\mathbb{K}}(x) = \mathrm{dg}(P_x)$, avec égalité ssi P_x est scindé dans $\mathbb{E}[X]$ avec racines (dans $\mathbb{E}$) simples.

Preuve : Suit de 6.2.3.

6.2.5 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 $\mathbb{L} \to \mathbb{E}$ (pas unique). Autrement dit, $\mathbb{L}$ se plonge [29] par un $\mathbb{K}$-morphisme dans tout corps dans lequel P est scindé.

Preuve : Si $\mathrm{dg}(P) = 0$ il n'y a rien à faire, supposons donc $\mathrm{dg}(P) \geq 1$. On écrit $P = \prod_{i=1}^{r} P_i$ pour irréductibles $P_1, .., P_r \in \mathbb{K}[X]$. Alors $\mathrm{dg}(P) = \sum_{i=1}^{r} \mathrm{dg}(P_i)$. La preuve consiste d'une récurrence décroisante en $r \leq \mathrm{dg}(P)$.

Dans le cas $r = \mathrm{dg}(P)$, il faut $\mathrm{dg}(P_i) = 1$ 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 $\mathrm{dg}(P_i) \geq 2$, supposons $i = 1$. Comme P_1 est irréductible, $\mathbb{K}_1 := \mathbb{K}[X]/\langle P_1 \rangle$ est par 6.1.7 un corps extension de $\mathbb{K}$, de la forme $\mathbb{K}_1 = \mathbb{K}[x]$ avec $x := \overline{X}$ 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 5.2.7(vii) P_1 est aussi scindé dans $\mathbb{E}$, c'est-à-dire possède dans $\mathbb{E}$ une racine. Par théorème 6.2.3, il existe donc un $\mathbb{K}$-morphisme de corps $\mathbb{K}_1 \to \mathbb{E}$.

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 $\mathbb{L} \to \mathbb{E}$.

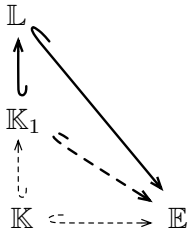


Figure 16: Sur la preuve de théorème 6.2.5. Le sous-diagramme indiqué fortement commute, de même pour le diagramme *coupé*. Par conséquence, tout le diagramme commute.

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 6.1.1 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 $\mathbb{L}, \widetilde{\mathbb{L}}$ satisfont tous les deux les affirmations ci-dessus, alors il existe $\mathbb{K}$-morphismes de corps $f : \mathbb{L} \to \widetilde{\mathbb{L}}$ et $\widetilde{f} : \widetilde{\mathbb{L}} \to \mathbb{L}$. Par conséquence, $\widetilde{f} \circ f : \mathbb{L} \to \mathbb{L}$ est un $\mathbb{K}$-morphisme de corps et par 6.2.2 un $\mathbb{K}$-automorphisme de corps. Par la surjectivité de $\widetilde{f} \circ f$ et l'injectivité de $\widetilde{f}$ on conclut que f est surjective, donc un $\mathbb{K}$-isomorphisme de corps entre $\mathbb{L}$ et $\widetilde{\mathbb{L}}$.

On appelle $\mathbb{L}$ le **corps de décomposition** de P **sur** $\mathbb{K}$.

(ii) Si $x_1, .., x_n \in \mathbb{L}$ sont les racines de P dans $\mathbb{L}$, alors la *minimalité* de $\mathbb{L}$ implique $\mathbb{L} = \mathbb{K}[x_1, .., x_n]$.

(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 $\mathbb{L}$.

6.2.6 Definition: 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 $\mathbb{K}$.

6.2.7 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 $n \in \mathbb{N}$.

6.2.8 Definition: 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 6.1.2 $\text{pgcd}(P, P') = 1$ dans $\mathbb{K}[X]$ ssi $\text{pgcd}(P, P') = 1$ dans $\mathbb{E}[X]$. Par 6.2.5 et remarque 5.2.7(vi), P est séparable ssi tous ses racines sont simples dans son corps de décomposition.

6.2.9 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 6.1.6 on a donc une équivalence entre $P' \neq 0$ et $\text{pgcd}(P, P') = 1$. Evidement, comme P est non-constant, si $\mathbb{K}$ est de caractéristique 0 alors toujours $P' \neq 0$. □

6.2.10 Théorème d'Artin sur l'indépendance des $\mathbb{K}$-morphismes 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 $\mathbb{K}$-morphismes de corps $\mathbb{L} \to \mathbb{E}$ sont $\mathbb{E}$-linéairement indépendants dans $\mathcal{L}_{\mathbb{K}}(\mathbb{E}, \mathbb{L})$.

Preuve : Soient $\sigma_1, .., \sigma_r : \mathbb{L} \to \mathbb{E}$ $\mathbb{K}$-morphismes de corps distinctes et supposer qu'il existe $a_1, .., a_r \in \mathbb{E} \setminus \{0\}$ tels que

$$0 = \sum_{i=1}^{r} a_i \cdot \sigma_i \quad . \tag{6.2.10.1}$$

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 de corps trivial

$$\sum_{i=1}^{r} a_i \sigma_i(x) \cdot \sigma_i = 0 \quad . \tag{6.2.10.2}$$

En combinant (6.2.10.1) et (6.2.10.2) on obtient

$$0 = \sigma_1(x) \cdot \sum_{i=1}^{r} a_i \cdot \sigma_i - \sum_{i=1}^{r} a_i \sigma_i(x)\sigma_i(y) = \sum_{i=2}^{r} [\sigma_1(x) - \sigma_i(x)] \cdot a_i \cdot \sigma_i \quad . \tag{6.2.10.3}$$

Comme les $\sigma_1, .., \sigma_r$ sont distinctes, on peut choisir $x \in \mathbb{L}$ tel que $\sigma_1(x) \neq \sigma_2(x)$. En ce cas, dans (6.2.10.3) on trouve une relation de dépendance $\mathbb{E}$-linéaire plus courte que (6.2.10.1), une contradiction à la minimalité de r. □

6.2.11 Corollaire sur le nombre des $\mathbb{K}$-morphismes 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 $[\mathbb{L} : \mathbb{K}]$ $\mathbb{K}$-morphismes de corps de $\mathbb{L}$ dans $\mathbb{E}$.

Preuve : Soit $\dim_{\mathbb{K}} \mathbb{L} =: n$ et $l_1, .., l_n \in \mathbb{L}$ 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 $f_1, .., f_n \in \mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$ satisfaisant $f_i(l_j) = \delta_{ij}$. Par 6.2.10, les $\mathbb{K}$-morphismes de corps de $\mathbb{L}$ dans $\mathbb{E}$ forment un système $\mathbb{E}$-linéairement indépendant dans $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \mathbb{E})$.

□

6.2.12 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 $\mathbb{L} \to \mathbb{E}$ égales 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 σ_i fait de $\mathbb{K}$ un sous-corps de $\mathbb{E}$ par l'injection $\sigma_i\big|_{\mathbb{K}} : \mathbb{K} \hookrightarrow \mathbb{E}$. Comme tous $\sigma_1, .., \sigma_r$ sont égales sur $\mathbb{K}$, cette injection est *globale* dans le contexte actuel. Par rapport à elle, tout σ_i est un $\mathbb{K}$-morphisme de corps $\mathbb{L} \to \mathbb{E}$. Par 6.2.11, il existe au maximum $[\mathbb{L} : \mathbb{K}]$ $\mathbb{K}$-morphismes de corps $\mathbb{L} \to \mathbb{E}$.

□

6.3 Extensions de corps séparables

6.3.1 Definition: 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 $\mathbb{K}$-morphismes de corps $\mathbb{L} \to \mathbb{E}$ est égal à n.

6.3.2 Lemme : Transitivité de la separabilité 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.

6.3.3 Théorème : Caractérisation de la separabilité 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 6.1.6 équivalent à la separabilité de P_x.

6.3.4 Théorème : Caractérisation de separabilité 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[30] $P_x \in \mathbb{K}[X]$, c'est-à-dire ssi tout $\mathbb{K}[x]/\mathbb{K}$ (avec $x \in \mathbb{L}$) est séparable.

Preuve :

Direction "⇒" : Soit $\mathbb{E}$ une extension de $\mathbb{K}$ quelconque et $\sigma : \mathbb{L} \to \mathbb{E}$ un $\mathbb{K}$-morphisme de corps. De même façon comme dans la preuve de 6.2.3, on montre que $\sigma(x)$ est une racine de P_x dans $\mathbb{E}$. Par 4.1.15(ii), x est une racine simple de P_x dans $\mathbb{L}$ ssi $P'_x(x) \neq 0$ et par injectivité de σ ssi $\sigma(P'_x(x)) \neq 0$. Comme $P'_x \in \mathbb{K}[X]$ et σ 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 6.2.3 on sait que les racines de P_x dans $\mathbb{E}$ sont en bijection avec les $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$. D'autre part, $\mathrm{dg}(P_x) = [\mathbb{K}[x] : \mathbb{K}] =: q$, 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 $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$, 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 $\mathbb{K}$-morphismes de corps $\sigma_1, .., \sigma_n : \mathbb{L} \to \mathbb{E}$ pour un $\mathbb{E}$ convenant. Chaque σ_i induit un $\mathbb{K}$-morphisme de corps $\mathbb{K}[x] \to \mathbb{E}$ par restriction $\sigma_i\big|_{\mathbb{K}[x]}$. Par 6.2.12, pour tout $i \in \{1, .., n\}$, il existe au maximum $p := [\mathbb{L} : \mathbb{K}[x]]$ indices $j \in \{1, .., n\}$ satisfaisant $\sigma_j\big|_{\mathbb{K}[x]} = \sigma_i\big|_{\mathbb{K}[x]}$. D'autre part, par 6.2.11 il existe au maximum q distinctes $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$. 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 $\mathbb{K}$-morphismes de corps $\mathbb{K}[x] \to \mathbb{E}$, chacun induit par la restriction de p $\mathbb{K}$-morphismes de corps σ_i. Donc $\mathbb{K}[x]/\mathbb{K}$ est séparable. De même façon comme dans la preuve de 6.2.12, on conclut de plus que $\mathbb{L}/\mathbb{K}[x]$ est aussi séparable.

Direction "⇐" : De même façon.

□

Remarques :

30. Se rappeler que par 6.1.5 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 6.1.6 on sait que x est nécessairement racine simple de son polynôme minimal $P_x \in \mathbb{K}[X]$, donc par 6.3.3 l'extension $\mathbb{K}[x]/\mathbb{K}$ est séparable.

(ii) Cela se généralise par théorème 6.3.4 à toute extension $\mathbb{L}/\mathbb{K}$ de degré finie : Si $\mathbb{K}$ est de caractéristique nulle, alors $\mathbb{L}/\mathbb{K}$ est séparable.

6.3.5 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 $\mathbb{L} = \mathbb{K}[x]$.

6.4 Groupes de Galois

6.4.1 Definition: Groupe de Galois

Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de $\mathbb{K}$. Notons $\mathrm{Aut}(\mathbb{L}/\mathbb{K})$ 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 6.2.11 on sait que $|\mathrm{Aut}(\mathbb{L}/\mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]$. Si $|\mathrm{Aut}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$, l'extension $\mathbb{L}/\mathbb{K}$ est dit **galoisienne** et $\mathrm{Aut}(\mathbb{L}/\mathbb{K})$ est appelé le **groupe de Galois** de $\mathbb{L}/\mathbb{K}$, souvent noté $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Remarques

(i) Toute extension $\mathbb{L}/\mathbb{K}$ galoisienne est séparable.

(ii) Par lemme 6.2.2, une extension $\mathbb{L}/\mathbb{K}$ de degré fini est Galoisienne ssi il existe $[\mathbb{L} : \mathbb{K}]$ $\mathbb{K}$-morphismes de corps $\mathbb{L} \to \mathbb{L}$.

Exemples

(i) Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$ galoisienne de degré 2, avec

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id},\ (\text{conjugaison complexe})\} \cong \mathbb{Z}/2\mathbb{Z}$$

comme groupe de Galois.

6.4.2 Théorème : Correspondance galoisienne

Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de $\mathbb{K}$ galoisienne. Pour tout sous-groupe $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ on note

$$\mathbb{L}^H := \{x \in \mathbb{L} \mid g(x) = x\ \forall g \in H\} \quad .$$

Alors :

1. Pour tout $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, l'ensemble $\mathbb{L}^H$ est un corps satisfaisant $\mathbb{K} \subseteq \mathbb{L}^H \subseteq \mathbb{L}$.
2. $\mathbb{L}^{\{\mathrm{Id}\}} = \mathbb{L}$ et $\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$.
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
$$\mathrm{Aut}(\mathbb{L}/\mathbb{E}) \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \quad .$$
4. La correspondance $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \mapsto \mathbb{L}^H$ est une bijection décroisante entre sous-groupes H de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ et corps $\mathbb{E}$ entre $\mathbb{K}$ et $\mathbb{L}$. La correspondance inverse est donnée par $\mathbb{E} \mapsto \mathrm{Aut}(\mathbb{L}/\mathbb{E})$.
5. Les degrés des extensions sont reliées aux ordres des sous-groups via
$$[\mathbb{L} : \mathbb{L}^H] = |H| \quad , \quad [\mathrm{Gal}(\mathbb{L}/\mathbb{K}) : H] = [\mathbb{L}^H : \mathbb{K}] \quad .$$

6. Soit $\mathbb{E}$ un corps entre $\mathbb{K}$ et $\mathbb{L}$. Alors $\mathrm{Aut}(\mathbb{L}/\mathbb{E}) \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ ssi $\mathbb{E}/\mathbb{K}$ est galoisienne et ssi $g(\mathbb{E}) = \mathbb{E}$ pour tout $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. En ce cas on a un isomorphisme

$$\mathrm{Aut}(\mathbb{E}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{K})/\mathrm{Aut}(\mathbb{L}/\mathbb{E}) \quad ,$$

induit via la restriction des automorphismes de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ sur $\mathbb{E}$.

6.4.3 Théorème : Génération de sous-corps galoisiens

Soit $\mathbb{L}$ un corps quelconque et $G \leq \mathrm{Aut}(\mathbb{L})$ un groupe fini d'automorphismes de corps $\mathbb{L} \to \mathbb{L}$. 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.

6.4.4 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[31] $\mathbb{K}[X]/\langle P\rangle$. Le groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est dit **groupe de Galois de** P.

6.4.5 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 $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Alors, $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ agit fidèlement, transitivement sur les racines $x_1, .., x_n$ de P dans $\mathbb{L}$.

Preuve : Soit $n := \mathrm{dg}(P)$ et $x_1, .., x_n \in \mathbb{L}$ les racines de P dans $\mathbb{L}$. Noter que par 6.2.8 ils sont deux à deux inégales. Soit $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, alors

$$0 = g(P(x_i)) = P(g(x_i)) \quad \forall i \in \{1, .., n\} \quad ,$$

c'est-à-dire $g(x_i)$ est une racine de P. Donc, g agit vraiment sur $\{x_1, .., x_n\}$ comme permutation et on a un morphisme de groupes $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to \mathrm{Sym}(n)$. Ce morphisme est injectif, car si $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ fixe tous les racines x_i, alors il fixe tout $\mathbb{L} = \mathbb{K}[x_1, .., x_n]$, c'est-à-dire $g = \mathrm{Id}$. Soit $\mathrm{Orb}(x_1)$ l'orbite de la racine x_1 sous $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ et poser

$$Q(X) := \prod_{y \in \mathrm{Orb}(x_1)} (X - y) \ \in \mathbb{L}[X] \quad .$$

Alors pour tout $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ on a

$$g(Q(X)) = \prod_{y \in \mathrm{Orb}(x_1)} (X - g(y)) = Q(X) \quad ,$$

c'est-à-dire Q a des coefficients $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$-invariants. Par 6.4.2 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 6.1.1(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, $\mathrm{Orb}(x_1) = \{x_1, .., x_n\}$.

□

Interprétation : Via restriction des $\mathbb{K}$-automorphismes de corps $\mathbb{L} \to \mathbb{L}$ sur les racines $x_1, .., x_n \in \mathbb{L}$ de P, on obtient une représentation fidèle de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ comme sous-groupe transitive de $\mathrm{Sym}(x_1, .., x_n)$.

31. Se rappeler que par remarque 6.2.5(iii) le corps de décomposition de P sur $\mathbb{K}$ contient toujours une copie du corps $\mathbb{K}[X]/\langle P\rangle$.

6.5 Corps finis

6.5.1 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 6.1.3 l'anneau $\mathbb{Z}/n\mathbb{Z}$ ne serait pas intègre, donc pas un corps. Soit inversement n premier. Alors, par la caractérisation 2.2.18, il faut montrer que l'idéal $n\mathbb{Z}$ est maximal dans $\mathbb{Z}$. Supposer $I \subseteq \mathbb{Z}$ 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.

□

6.5.2 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 6.1.3, 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 6.5.1 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 6.1.3 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 $\mathbb{Z} \to \mathbb{K}$, $n \mapsto n_{\mathbb{K}}$ 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

$$x^{p^n} = x \quad \forall x \in \mathbb{K} \quad . \tag{6.5.2.1}$$

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 $\mathrm{dg}(P) = p^n$. D'autre part, $P(X)$ est scindé dans $\mathbb{K}$ car par (6.5.2.1) tous p^n éléments de $\mathbb{K}$ sont racines de $P(X)$. Donc par 6.2.5, 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

$$F := \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \quad , \quad x \mapsto x^p \quad ,$$

(voir 2.1.16) est un élément de $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ d'ordre n, donc $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

Preuve : Par Fermat-Euler on a $x^p = x$ pur tout $x \in \mathbb{F}_p$. Évidement $(xy)^p = x^p y^p$ 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 $k \in \{1, .., p-1\}$. Donc $F : x \mapsto x^p$ est un $\mathbb{F}_p$-morphisme de corps $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, donc par 6.2.2 dans $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Soit $s \in \{1, .., n\}$ son ordre [32]. Comme

$$F^n(x) = x^{p^n} \overset{(6.5.2.1)}{=} x \quad \forall x \in \mathbb{F}_{p^n} \quad ,$$

il faut que $s \mid n$. D'autre part, par définition

$$x = \mathrm{Id}(x) = F^s(x) = x^{p^s} \quad \forall x \in \mathbb{F}_{p^n} \quad ,$$

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. □

6.5.3 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 "⇒" : Par théorème 6.5.2 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 6.1.1 $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$ divise $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$.

Direction "⇐" : Noter que par théorème 6.5.2, $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne avec groupe de Galois cyclique $\mathbb{Z}/n\mathbb{Z}$. Pour $m \mid n$ il existe donc par Lagrange un (unique) sous-group $H \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ d'ordre n/m. Par la correspondance galoisienne 6.4.2, il existe donc un sous-corps $\mathbb{K}$ entre $\mathbb{F}_p$ et $\mathbb{F}_{p^n}$, tel que

$$[\mathbb{K} : \mathbb{F}_p] = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : H| = m \quad .$$

Par 6.5.2, $\mathbb{K}$ est exactement $\mathbb{F}_{p^m}$.

□

6.5.4 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

$$(Q(X))^p = Q(X^p) \quad .$$

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

$$(P_1 + P_2)^p = \sum_{k=0}^{p} \binom{p}{k} (P_1)^k (P_2)^{p-k} = (P_1)^p + (P_2)^p \quad ,$$

car p divise tout $\binom{p}{k}$ avec $k \in \{1, .., p-1\}$. Donc, pour $Q = \sum_i q_i X^i \in \mathbb{F}_p[X]$ on a

$$(Q(X))^p = \sum_i (q_i X^i)^p = \sum_i q_i^p (X^i)^p = \sum_i q_i (X^p)^i = Q(X^p) \quad .$$

□

32. Noter que $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

6.5.5 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 $m \mid n$, alors $(\mathcal{P}_m(A))_{m|n}$ est une partition de $\mathbb{U}_n(A)$.
4. Si $|\mathbb{U}_m| = m$ pour tout $m \mid n$, 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 $\mathbb{U}_n(\mathbb{C}) = \left\{e^{2\pi i \frac{m}{n}}\right\}_{m=1}^{n}$ et en particulier $|\mathbb{U}_n(\mathbb{C})| = n$.
7. Pour n'importante quel $r \in \mathcal{P}_n(\mathbb{C})$, on a $\mathcal{P}_n(\mathbb{C}) = \{r^m \mid m \in \{1, .., n\},\ \operatorname{pgcd}(m, n) = 1\}$. En particulier
$$|\mathcal{P}_n(\mathbb{C})| = \varphi(n) \quad ,$$
où $\varphi : \mathbb{N} \to \mathbb{N}$ 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 4.1.15, $X^n - 1$ possède au maximum n racines, donc $|\mathbb{U}_n| \leq n$.
2. Si $m \mid n$ et $x \in \mathcal{P}_m$, on a évidement $x^n = 1$ 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 $m \mid n$. Donc
$$\mathbb{U}_n = \bigcup_{\substack{m \in \mathbb{N} \\ m|n}} \mathcal{P}_m \quad . \tag{6.5.5.1}$$
3. Par hypothèse, $\mathcal{P}_m \neq \mathcal{P}_{m'}$ pour tout $m \neq m'$. Donc, l'union dans (6.5.5.1) est une union de parties disjoints.
4. Par (2) on sait que le groupe $\mathbb{U}_n$ est fini. Tout $r \in \mathbb{U}_n$ est donc racine du polynôme $X^{|U_n|} - 1$. Donc, par 4.1.15, $\prod_{r \in \mathbb{U}_n}(X - r)$ 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
$$X^{|\mathbb{U}_n|} - 1 = \prod_{r \in \mathbb{U}_n} (X - r) \overset{(3)}{=} \prod_{m|n} \prod_{r \in \mathcal{P}_m} (X - r) = \prod_{m|n} \Phi_m$$
5. Supposons que $\operatorname{pgcd}(P, P') \neq 1$, alors il existerait un irréductible $\alpha \in \mathbb{K}[X]$ tel que $\alpha \mid P$ et $\alpha \mid P' = nX^{n-1}$. Comme $n \neq 0$ dans $\mathbb{K}$ il est inversible, donc X^{n-1} est une décomposition de P' en irréductibles $X, .., X$. Par unicité d'une cette décomposition (modulo multiplication par inversibles), il faudrait que $\alpha = X$, donc $X \mid P$, une contradiction ! Se rappeler que par 6.2.8 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 separabilité 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 $\text{pgcd}(n,m) = 1$. Donc
$$|\mathcal{P}_n(\mathbb{C})| = |\{1 \leq m \leq n : \text{pgcd}(m,n) = 1\}| = \varphi(m) \quad .$$
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 5.2.5 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 5.2.8 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 6.5.6(i), l'extension $\mathbb{Q}(\mathbb{U}_n(\mathbb{C}))/\mathbb{Q}$ est de degré $\varphi(n)$. Par 6.5.6(ii) elle est Galoisienne. La dernière affirmation ne sera pas prouvée.

□

Exemple : Considérons les racines 12-ièmes de l'unité dans $\mathbb{C}$. Alors
$$\mathbb{U}_{12}(\mathbb{C}) = \left\{e^{i2\pi\frac{m}{12}} : m \in \{1,..,12\}\right\} \quad .$$
Une racine primitive est donnée par $r := e^{i2\pi\frac{1}{12}}$. Donc, par 6.5.5(7) on obtient tous les autres racines primitives comme
$$\mathcal{P}_{12}(\mathbb{C}) = \{r^m : m \in \{1,..,12\},\ \text{pgcd}(12,m) = 1\} = \left\{r^1, r^5, r^7, r^{11}\right\} \quad .$$
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 6.5.5(8), il se trouve dans $\mathbb{Z}[X]$.

6.5.6 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 $\Phi_{n,\mathbb{C}}$ et 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 6.5.5).

(ii) Par 6.2.3, les $\mathbb{Q}$-morphismes de corps $\mathbb{Q}(r) \to \mathbb{Q}(r)$ 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 6.5.5(9) en fait dans $\mathbb{Q}(r)$. Donc, il y a $|\mathcal{P}_n(\mathbb{C})| = \varphi(n)$ $\mathbb{Q}$-morphismes de corps $\mathbb{Q}(r) \to \mathbb{Q}(r)$. Par remarque 6.4.1(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'importante quelle 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 5.2.5 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 5.2.5 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 $\overline{P}$ le polynôme à coefficients dans $\mathbb{F}_p$ obtenu en réduisant les coefficients de P modulo p. En utilisant lemme 6.5.4, on montre que $\overline{h}(X^p) = \overline{f} * \overline{g}$.
- Soit $\widetilde{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. On montre qu'il existe $z \in \widetilde{\mathbb{F}}_p$ tel que $\overline{f}(z) = 0 = \overline{h}(z)$,
- On en déduit que $X^n - 1 = \overline{f} * \overline{h} \in \mathbb{F}_p[X]$ a une racine $z \in \widetilde{\mathbb{F}}_p$ au moins double.
- On en déduit que $\frac{d}{dX}(X^n - 1)\big|_z = 0$ 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, $\left\{r^k : k \in \mathbb{N},\ \text{pgcd}(k, n) = 1\right\} \overset{6.5.5(7)}{=} \mathcal{P}_n$ sont tous racines de f. Donc, par 4.1.15 on conclut que le produit

$$\prod_{\rho \in \mathcal{P}_n(\mathbb{C})} (X - \rho) = \Phi_{n,\mathbb{C}} \overset{6.5.5(8)}{\in} \mathbb{Q}[X]$$

divise $f \in \mathbb{Q}[X]$ dans $\mathbb{C}[X]$ et par 5.2.8 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 $\mathbb{Q}[X]$.

□

7 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 $m_1, .., m_n \in M$ tels que

$$M = \mathrm{span}_A\{m_1, .., m_n\} = \sum_{i=1}^{n} Am_i \quad ,$$

c'est-à-dire le morphisme

$$\varphi : A^n \to M \quad , \quad (a_i)_{i=1}^n \mapsto \sum_{i=1}^{n} a_i m_i$$

et surjectif. En général, M n'est pas nécessairement libre, c'est-à-dire les $(m_i)_i$ ne forment pas une base.

7.0.7 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 $A \to J$, $\alpha \mapsto \alpha a$ est donc surjective. Comme A est intègre, il est aussi injectif. Donc J est libre avec base $\{a\}$.

Supposons l'affirmation valide pour $A^1, .., A^n$. Soit $M \subseteq A^n$ un sous-A-module de A^n. Considérons la projection

$$\Pi : A^n \to A \quad , \quad (a_1, .., a_n) \mapsto a_1 \quad ,$$

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 3.1.22(iv), cela implique que la somme est directe.

Par récurrence, $M \cap \ker(\Pi) \subseteq A^{n-1}$ possède une base de $m_2, .., m_k \in M \cap \ker(\Pi)$, avec $k \leq n$. Comme Am possède la base $\{m\}$, leur somme directe possède la base $\{m, m_2, .., m_k\}$.

□

Conséquence : Soit M un A-module de type fini, engendré par les $m_1, .., m_n \in M$. Alors, comme on sait, il existe un morphisme de A-modules surjectif $\varphi : A^n \to M$. 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 $\leq n$.

7.0.8 Definition: 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 $\det : M_n(A) \to A$ comme

$$\det((B)_{i,j}) := \sum_{\sigma \in \mathrm{Sym}(n)} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} B_{i,\sigma(i)} \quad , \quad B = (B_{i,j})_{i,j=1}^n$$

On note $\mathrm{GL}_n(A) := M_n(A)^\times$ 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 $B \in \mathrm{GL}_n(A)$. Le cas échéant, on a

$$B^{-1} = \frac{\mathrm{com}(B)}{\det(B)} \quad ,$$

où $\mathrm{com}(B)$ est la comatrice de B.

(ii) Toute matrice $B \in M_{n,m}(A)$ peut être vue comme application A-linéaire $A^m \to A^n$, via

$$(a_j)_{j=1}^m \mapsto \left(\sum_{j=1}^m B_{i,j} a_j \right)_{i=1}^n \quad .$$

Inversement, toute application A-linéaire $\Phi : A^m \to A^n$ est *induit* une telle matrice. Comme Φ est déterminé par les images de la base canonique $e_1, .., e_m \in A^m$, représentés par la base canonique $e_1, .., e_n \in A^n$, il existe une unique matrice $B \in M_{n,m}(A)$ associée, donnée par

$$B_{i,j} := (\Phi e_j)_i \quad .$$

L'association induit

$$(M_{n,m}(M), +, \cdot) \to (\mathrm{Hom}_A(A^m, A^n), +, \circ) := \{A^m \to A^n \ A\text{-linéaires}\}$$

est un isomorphisme de A-algèbres.

(iii) Le groupe $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ opère sur $M_{n,m}(A)$ par

$$(P, Q) \cdot B := PBQ^{-1} \quad , \quad B \in M_{n,m}(A), \ (P, Q) \in \mathrm{GL}_n(A) \times \mathrm{GL}_m(A) \quad .$$

(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 $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$, ssi ils possèdent le même *rang*. Autrement dit, $B \in M_{n,m}(\mathbb{K})$ possède le rang $r \in \{0, .., \min\{n, m\}\}$ ssi elle est dans l'orbite de

$$\begin{pmatrix} 1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & \ddots & \vdots \\ 0 & & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} 1_{r\times r} & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix} \quad .$$

Cela donne une indication pour une généralisation de la théorie du rang au delà les corps (voir 7.0.10).

7.0.9 Lemme : Extensions à bases

Soit A un anneau intègre, principal et $x_1, .., x_n \in A$. Alors, les suivants sont équivalents :

1. Il existe une matrice dans $\mathrm{GL}_n(A)$ dont la première ligne est $(x_1, .., x_n)$.
2. $\mathrm{pgcd}(x_1, .., x_n) \sim 1$. Noter que par 5.1.5, A est factoriel.
3. $(x_1, .., x_n)$ appartient à une A-base du A-module A^n.

7.0.10 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 $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ sur $M_{n,m}(A)$ introduit dans remarque 7.0.8(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 $0 \neq a_1 \mid a_2 \mid \cdots \mid a_r$. Les $a_i \in A$ sont uniques à multiplication par inversibles près, c'est-à-dire les idéaux principaux $Aa_1, .., Aa_r$ sont uniques. On dit r le **rang** de la matrice B.

7.0.11 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 [33]

$$M \cong_A A/(Aa_1) \oplus \cdots \oplus A/(Aa_n) \oplus A \oplus \cdots \oplus A$$

avec $0 \neq a_1 \mid a_2 \mid .. \mid a_n \in A \setminus A^\times$. De plus, les idéaux (Aa_i) sont déterminés de manière unique pour M.

33. Se rappeler que par remarque 3.1.9(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 $f : U \to W$ une application linéaire.

1. Si $F : U \to V$ est une application linéaire telle que $\ker(F) \subseteq \ker(f)$, alors il existe une application linéaire $g : V \to W$ telle que $f = g \circ F$.
2. Si $F : V \to W$ est une application linéaire telle que $f(U) \subseteq F(V)$, alors il existe une application linéaire $g : U \to V$ telle que $f = F \circ g$.

Preuve :

1. Soit $e_1, .., e_n$ une base de U telle que $e_1, .., e_l$ est une base de $\ker(f)$ et $e_1, .., e_k$ une base de $\ker(F)$, $k \leq l \leq n$. Alors $F(e_{k+1}), .., F(e_n) \in V$ 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 $e_1, .., e_k$ une base de $f(U)$ et $b_1, .., b_k \in V$ tels que $F(b_i) = e_i$. Soient $U_i \in f^{-1}(\{e_i\})$, alors

$$U = \operatorname{span} \bigcup_{i=1}^{k} U_i \quad .$$

   Définissons l'application linéaire $g : U \to V$ 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 $\sum_{i=1}^{k} \sum_j \lambda_{ij} a_{ij} = \sum_{i=1}^{k} \sum_j \mu_{ij} a'_{ij}$ pour $a_{ij}, a'_{ij} \in U_i$ on a

$$\sum_j \lambda_{ij} = \sum_j \mu_{ij} \quad \forall\ i = 1, .., k$$

   et donc

$$\sum_i \sum_j \lambda_{ij} \underbrace{g(a_{ij})}_{b_i} = \sum_i \sum_j \mu_{ij} \underbrace{g(a'_{ij})}_{b_i} \quad .$$

   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 finit.

1. Soient $f, f_1, .., f_m \in \operatorname{End}_{\mathbb{K}}(V)$ endomorphismes tels que

$$\bigcap_{i=1}^{m} \ker(f_i) \subseteq \ker(f) \quad .$$

   Alors il y a $g_1, .., g_m \in \operatorname{End}_{\mathbb{K}}(V)$ tels que $f = \sum_{i=1}^{m} g_i \circ f_i$.

2. Soient $f, f_1, .., f_m \in \operatorname{End}_{\mathbb{K}}(V)$ endomorphismes tels que

$$f(V) \subseteq \sum_{i=1}^{m} f_i(V) \quad .$$

   Alors il y a $g_1, .., g_m \in \operatorname{End}_{\mathbb{K}}(V)$ tels que $f = \sum_{i=1}^{m} f_i \circ g_i$.

Preuve :

1. Considérons l'application linéaire $F : V \to \bigoplus_{i=1}^m V$ défini par $F(x) := (f_1(x), .., f_m(x))$. Alors

$$\ker(F) = \bigcap_{i=1}^m \ker(f_i) \subseteq \ker(f) \quad ,$$

donc selon lemme A.0.12(1) il y a une application linéaire $g : \bigoplus_{i=1}^m V \to V$ telle que $g \circ F = f$. Définissons $g_i(x) := g(0, .., x_i, .., 0),\ x_i \in V$, alors $g_i \in \mathrm{End}_{\mathbb{K}}(V)$ et on a

$$f = g \circ F = \sum_{i=1}^m g_i \circ f_i \quad ,$$

comme affirmé.

2. Considérons l'application linéaire $F : \bigoplus_{i=1}^m V \to V$ défini par $F(x_1, .., x_m) := \sum_{i=1}^m f_i(x_i)$. Alors

$$F(V) = \sum_{i=1}^m f_i(V) \supseteq f(V) \quad ,$$

donc selon lemme A.0.12(2) il y a une application linéaire $g = (g_1, .., g_m) : V \to \bigoplus_{i=1}^m V$ telle que $F \circ g = f$. Donc

$$f = F \circ g = \sum_{i=1}^m f_i \circ g_i \quad .$$

□

A.0.14 Lemme de Zorn

Soit $\mathcal{F} \neq \emptyset$ un ensemble ordonnée dans lequel toute partie totalement ordonnée admet un majorant [34] dans $\mathcal{F}$. Alors $\mathcal{F}$ a un élément maximal [35].

34. Un élément $x \in \mathcal{F}$ est un majorant du $F \subseteq \mathcal{F}$ 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 5.1.3.
$\mathbb{F}_{p^n}$: Le corps de cardinalité p^n et caractéristique p. Voir 6.5.2.
$Z(G)$: Centre du groupe G.
$Z(A)$: Centre de l'anneau A. Voir 2.1.10.
$\mathcal{Z}(I)$: Les idéaux premiers contenant l'idéal bilatère I. Voir la topologie Zariski 2.2.16.
e_i : Base canonique dans le module libre $A^{(I)}$. Voir 3.2.1.
$\mathrm{End}_{\mathbb{K}}(V)$: Anneau des $\mathbb{K}$-endomorphismes sur un $\mathbb{K}$-espace vectoriel V.
$\ker(f)$: Noyau du homomorphisme f.
δ_{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 2.1.7.
$\bigtimes_{i \in I} A_i$: L'anneau produit d'une famille $(A_i)_{i \in I}$ d'anneaux. Voir 2.1.4.
$\bigtimes_{i \in I} G_i$: Le module produit directe d'une famille $(G_i)_{i \in I}$ de modules. Voir 3.1.21.
$\bigoplus_{i \in I} G_i$: La somme directe des modules $(G_i)_{i \in I}$. Voir 3.1.21.
$\mathrm{Spec}(A)$: Famille des idéaux premiers dans l'anneau A. Voir 2.2.15.
$\mathrm{Specmax}(A)$: Famille des idéaux maximaux dans l'anneau A. Voir 2.2.17.
$\mathrm{span}_A(X)$: Sous-A-module engendré par X. Voir 3.1.9.
$\cong$: Isomorphisme de groupes ou anneaux. Voir 2.1.12.
$\cong_A$: Isomorphisme de A-modules. Voir 3.1.3.
$A^{(I)}$: Module libre engendré par l'anneau A sur l'ensemble I. Voir 3.2.1.
$\mathrm{Ann}_A(g)$: Annulateur de l'élément $g \in G$ du A-module G. Voir 3.1.19.
$A[S]$: L'algèbre des polynômes sur l'anneau commutatif A, où S est un monoide commutatif. Voir 4.1.4.
$A[X]$: $A[\mathbb{N}]$. Voir exemple 4.1.4(i).
$A\left[X^{\pm 1}\right]$: $A[\mathbb{Z}]$. Voir exemple 4.1.4(ii).
$A[[S]]$: L'algèbre des séries formelles sur l'anneau commutatif A, où S est un monoide commutatif. Voir 4.5.1.
$A[[X]]^\times$: Le sous-groupe des séries formelles inversibles sur l'anneau A par rapport à "$*$". Voir 4.5.7.
$A[[X]]^\circ$: Le sous-groupe des séries formelles inversibles sur l'anneau A par rapport à "$\circ$". Voir 4.5.13.
$\mathcal{F}(B^n, B)$: Algèbre des fonctions polynomiales $B^n \to B$ sur la A-algèbre B. Voir 4.2.7.
$\mathbb{K}(X)$: Corps quotient de $\mathbb{K}[X]$. Voir 4.5.19.
$\mathbb{K}((X))$: Corps quotient de $\mathbb{K}[[X]]$. Voir 4.5.19.
$\leq_l$: Ordre lexicographique sur $\mathbb{R}^n$. Voir 4.1.9.
$\leq$: Ordre monômial sur $\mathbb{R}^n$. Voir 4.1.9.
$\mathcal{P}_n$: Ensemble des partitions dans $\mathbb{N}_0^n$. Voir 4.4.4.
λ^* : Partition duale de la partition λ. Voir 4.4.4.
$M_\lambda(X)$: Monôme symétrique complet associé à la partition $\lambda \in \mathbb{N}_0^n$. Voir 4.4.5.
$\sigma_k(X)$: Polynôme symétrique élémentaire de degré k. Voir 4.4.5.
$\mathscr{C}(P)$: Contenu d'un polynôme P. Voir 5.2.1.
$[\mathbb{L} : \mathbb{K}]$: Dimension de l'extension $\mathbb{L}$ d'un corps $\mathbb{K}$ comme $\mathbb{K}$-espace vectoriel. Voir 6.1.1.
$\mathrm{Aut}(\mathbb{L}/\mathbb{K})$: Groupe des $\mathbb{K}$-automorphismes de corps de $\mathbb{L}$. Voir 6.4.1.
$\mathbb{L}^H$: Le sous corps entre $\mathbb{K}$ et $\mathbb{L}$ point par point stable sous $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Voir 6.4.2.
$M_{n,m}(A)$: A-module des matrices $n \times m$ à coefficients dans l'anneau A. Voir 7.0.8.
$M_{n,n}(A)$: La A-algèbre des matrices $n \times n$ à coefficients dans l'anneau A. Voir 7.0.8.
$\mathrm{GL}_n(A)$: Le groupe multiplicatif des matrices inversibles dans $M_n(A)$. Voir 7.0.8.

Index