SOUTENANCE DE MÉMOIRE DE MASTER OPTION: ALGÈBRE COMMUTATIVE ET CRYPTOGRAPHIE SPÉCIALITÉ: THÉORIE DES FILTRATIONS

KABLAM Edjabrou Ulrich Blanchard

Université NANGUI ABROGOUA
UFR Sciences Fondamentales Appliquées

10 Juillet 2024

THÈME :

SOUTENANCE DE MÉMOIRE DE MASTER OPTION: ALGÈBRE COMMUTATIVE ET CRYPTOGRAPHIE SPÉCIALITÉ: THÉORIE DES FILTRATIONS

KABLAM Edjabrou Ulrich Blanchard

Université NANGUI ABROGOUA
UFR Sciences Fondamentales Appliquées

10 Juillet 2024

THÈME : DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATIONS BONNES

SOUTENANCE DE MÉMOIRE DE MASTER OPTION: ALGÈBRE COMMUTATIVE ET CRYPTOGRAPHIE SPÉCIALITÉ: THÉORIE DES FILTRATIONS

KABLAM Edjabrou Ulrich Blanchard

Université NANGUI ABROGOUA
UFR Sciences Fondamentales Appliquées

10 Juillet 2024

THÈME : **DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATIONS BONNES**

Directeur de Mémoire : Mr. ASSAN Abdoulaye

Encadrant scientifique : Mr. BROU Kouadjo Pierre

PLAN DE PRÉSENTATION

INTRODUCTION

La notion d'élément entier sur un idéal I d'un anneau noethérien A a été introduit par Prüfer dans les années 1930. Un élément $x \in A$ est dit entier sur l'idéal I de A s'il vérifie une équation de la forme $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$ où a_j appartient à I^j pour tout entier j. La clôture intégrale de l'idéal I est l'idéal I' des éléments $x \in A$ qui sont entiers sur I. L'idéal J de A est dit entier sur l'idéal I si $J \subseteq I'$.

INTRODUCTION

Northcott D.G. et Rees D. ont défini dans un anneau local noethérien la notion de réduction d'un idéal sur un autre qui est voisine de la notion d'élément entier sur un idéal introduit par Prüfer. L'idéal I est une réduction de l'idéal J si I est contenu dans J et s'il existe un entier $N \geqslant 1$ tel que $J^N = IJ^{N-1}$. Les réductions de l'idéal J sont exactement les idéaux de I contenus dans J et ayant la même clôture intégrale que J.

INTRODUCTION

Une filtration de l'anneau A est une suite $f = (I_n)_{n\in\mathbb{Z}}$ d'idéaux de A, décroissante pour l'inclusion et vérifiant $I_0 = A$ et $I_nI_m \subseteq I_{n+m}$. On note $\mathbb{F}(A)$ l'ensemble des filtrations de l'anneau A. Soit I un idéal de A, une filtration $f = (I_n)_{n\in\mathbb{Z}}$ est dite $I - bonne$ si pour tout $n \in \mathbb{N}, \quad II_n \subseteq I_{n+1}$ et s'il existe k un entier tel que pour tout $n \geqslant k$, $II_n = I_{n+1}$. Les filtrations les plus courantes sont les filtrations *adiques*. En particulier, toute filtrations $I - adiques$ est $I - bonne$ pour tout I idéal de A.

INTRODUCTION

Comment étendre de manière rigoureuse les résultats obtenus dans le contexte restreint de la filtration I-adique à des filtrations de nature plus générale, telles que les filtrations bonnes ? Comment ces notions interagissent-elles dans des environnements mathématiques variés, et quelles applications peuvent en découler dans des domaines tels que la géométrie algébrique ou encore la théorie des nombres ?

INTRODUCTION

Afin de répondre à ces interrogations, notre démarche s'articulera autour de trois axes majeurs. Dans un premier temps, nous plongerons dans l'étude approfondie de la dépendance intégrale, en explorant ses origines historiques et en analysant ses implications dans le contexte des anneaux commutatifs. Nous poursuivrons ensuite notre exploration en examinant la réduction au sein de la filtration I-adique, avant d'élargir notre perspective à des filtrations bonnes, mettant en lumière les liens conceptuels et les différences inhérentes à ces contextes variés.

1.1. Définition

Soit A un ensemble non vide muni de deux lois de compositions interne, $(A, +, \times)$. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien

(ii) La loi $\times$ est distributive par rapport à la loi $+$

(iii) La loi $\times$ est associative.

L'anneau est dit commutatif si la loi $\times$ est commutatif.

Exemple : $(\mathbb{Z}, +, .), (\mathbb{R}, +, .), \cdots$ sont des anneaux commutatifs unitaires.

DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATION I-BONNE

ANNEAU

1.1. Définition

Soit A un ensemble non vide muni de deux lois de compositions interne, $(A, +, \times)$. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien

(ii) La loi $\times$ est distributive par rapport à la loi $+$

(iii) La loi $\times$ est associative.

L'anneau est dit commutatif si la loi $\times$ est commutatif.

Exemple : $(\mathbb{Z}, +, .), (\mathbb{R}, +, .), \cdots$ sont des anneaux commutatifs unitaires.

DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATION I-BONNE

ANNEAU

1.1. Définition

Soit A un ensemble non vide muni de deux lois de compositions interne, $(A, +, \times)$. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien

(ii) La loi $\times$ est distributive par rapport à la loi $+$

(iii) La loi $\times$ est associative.

L'anneau est dit commutatif si la loi $\times$ est commutatif.

Exemple : $(\mathbb{Z}, +, .), (\mathbb{R}, +, .), \cdots$ sont des anneaux commutatifs unitaires.

1.1. Définition

Soit A un ensemble non vide muni de deux lois de compositions interne, $(A, +, \times)$. On dit que $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien

(ii) La loi $\times$ est distributive par rapport à la loi $+$

(iii) La loi $\times$ est associative.

L'anneau est dit commutatif si la loi $\times$ est commutatif.

Exemple : $(\mathbb{Z}, +, .), (\mathbb{R}, +, .), \cdots$ sont des anneaux commutatifs unitaires.

1.2. Remarque

L'élément neutre de la loi $+$ dans A est noté 0_A. Si de plus il existe un élément neutre pour la loi $\times$ dans A, cet élément est appelé l'élément unité et est noté 1_A. On dit alors que l'anneau A est unitaire.

1.3. Définition **(Élément Entier)**

Soient B un anneau et A un sous-anneau de B ($A \subseteq B$).
Un élément x de B est dit **entier** sur A s'il est **racine d'un polynôme unitaire à coefficient dans** A.
En d'autres termes, s'ils existent $a_1, a_2, \cdots, a_n$ éléments de A tels que :

$$x^n + a_1 x^{n-1} + \cdots + a_i x^{n-i} + \cdots + a_n = x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0, \; n \in \mathbb{N}^* \quad (1)$$

1.4. Remarque

Cette équation (1) est appelée **équation de dépendance intégrale** de x sur A.
On dit que B est entier sur A lorsque tous les éléments de B sont entiers sur A.

DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATION I-BONNE

DÉPENDANCE INTÉGRALE SUR LES ANNEAUX

1.5. Exemple

Posons $B = \mathbb{R}$ et $A = \mathbb{Z}$. A est un sous-anneau de B.

(i) $x = \sqrt{5}$ est solution de l'équation $x^2 - 5$. Donc $\sqrt{5}$ est entier sur $\mathbb{Z}$.

(ii) $x = \sqrt{2} + 1$ est solution de l'équation $x^2 - 2x - 1$. Donc $x = \sqrt{2} + 1$ est entier sur $\mathbb{Z}$.

(iii) $\frac{1}{2}$ n'est pas entier sur $\mathbb{Z}$.

1.5. Exemple

Posons $B = \mathbb{R}$ et $A = \mathbb{Z}$. A est un sous-anneau de B.

(i) $x = \sqrt{5}$ est solution de l'équation $x^2 - 5$. Donc $\sqrt{5}$ est entier sur $\mathbb{Z}$.

(ii) $x = \sqrt{2} + 1$ est solution de l'équation $x^2 - 2x - 1$. Donc $x = \sqrt{2} + 1$ est entier sur $\mathbb{Z}$.

(iii) $\frac{1}{2}$ n'est pas entier sur $\mathbb{Z}$.

1.5. Exemple

Posons $B = \mathbb{R}$ et $A = \mathbb{Z}$. A est un sous-anneau de B.

(i) $x = \sqrt{5}$ est solution de l'équation $x^2 - 5$. Donc $\sqrt{5}$ est entier sur $\mathbb{Z}$.

(ii) $x = \sqrt{2} + 1$ est solution de l'équation $x^2 - 2x - 1$. Donc $x = \sqrt{2} + 1$ est entier sur $\mathbb{Z}$.

(iii) $\frac{1}{2}$ n'est pas entier sur $\mathbb{Z}$.

Preuve

En effet, si $\frac{1}{2}$ est entier sur $\mathbb{Z}$ alors $\frac{1}{2}$ est solution d'une équation de dépendance intégrale. Alors :

$\exists$ n ≥ 1, $\left(\frac{1}{2}\right)^n + \sum_{i=1}^n a_i \left(\frac{1}{2}\right)^{n-i} = 0$, $a_i \in \mathbb{Z}$

D'où $\left(\frac{1}{2}\right)^n \left[1 + \sum_{i=1}^n a_i \left(\frac{1}{2}\right)^{-i}\right] = 0$

Comme $\left(\frac{1}{2}\right)^n \neq 0$ alors $1 + \sum_{i=1}^n a_i 2^i = 0 \Longrightarrow 1 + \sum_{i=1}^n a_i 2^i = 0 \Longrightarrow$ $1 = 2\left(\sum_{i=1}^n -a_i 2^{i-1}\right) \Longrightarrow 1 \in 2\mathbb{Z}$. Ce qui est **Absurde**.

1.6. Définition (Module)

Soit A un anneau commutatif unitaire.
Un A-module ou module sur A est un groupe abélien $(M, +)$ muni d'une multiplication externe $A \times M \to M, (a, x) \mapsto ax$ vérifiant les propriétés suivantes :

(i) $\forall a, b \in A, \forall x \in M, (a + b)x = ax + bx$;

(ii) $\forall a \in A, \forall x, y \in M, a(x + y) = ax + ay$;

(iii) $\forall x \in M,\ 1_A x = x$;

(iv) $\forall a, b \in A, \forall x \in M,\ a(bx) = (ab)x$.

1.6. Définition **(Module)**

Soit A un anneau commutatif unitaire.
Un A-module ou module sur A est un groupe abélien $(M, +)$ muni d'une multiplication externe $A \times M \to M, (a, x) \mapsto ax$ vérifiant les propriétés suivantes :

(i) $\forall a, b \in A, \forall x \in M, (a+b)x = ax + bx$;

(ii) $\forall a \in A, \forall x, y \in M, a(x+y) = ax + ay$;

(iii) $\forall x \in M,\ 1_A x = x$;

(iv) $\forall a, b \in A, \forall x \in M,\ a(bx) = (ab)x$.

1.6. Définition **(Module)**

Soit A un anneau commutatif unitaire.
Un A-module ou module sur A est un groupe abélien $(M, +)$ muni d'une multiplication externe $A \times M \to M, (a, x) \mapsto ax$ vérifiant les propriétés suivantes :

(i) $\forall a, b \in A, \forall x \in M, (a+b)x = ax + bx$;
(ii) $\forall a \in A, \forall x, y \in M, a(x+y) = ax + ay$;
(iii) $\forall x \in M,\ 1_A x = x$;
(iv) $\forall a, b \in A, \forall x \in M,\ a(bx) = (ab)x$.

1.6. Définition **(Module)**

Soit A un anneau commutatif unitaire.
Un A-module ou module sur A est un groupe abélien $(M, +)$ muni d'une multiplication externe $A \times M \to M, (a, x) \mapsto ax$ vérifiant les propriétés suivantes :

(i) $\forall a, b \in A, \forall x \in M, (a + b)x = ax + bx$;

(ii) $\forall a \in A, \forall x, y \in M, a(x + y) = ax + ay$;

(iii) $\forall x \in M,\ 1_A x = x$;

(iv) $\forall a, b \in A, \forall x \in M,\ a(bx) = (ab)x$.

1.7. Exemple

(i) $M = 0$ est un $A-$ *module* pour tout Anneau A, appelé **module nul**

(ii) L'anneau A est un $A-$ *module*. Les sous $A-$ *modules* sont les idéaux de A.

(iii) Si $A = \mathbb{Z}$, tout sous groupe abélien peut être vu comme un $\mathbb{Z}-$ *module*

(iv) Soit k un corps. Alors tout $k-$ *espace vectoriel* est un $k-$ *module*.

1.7. Exemple

(i) $M = 0$ est un $A - module$ pour tout Anneau A, appelé **module nul**

(ii) L'anneau A est un $A - module$. Les sous $A - modules$ sont les idéaux de A.

(iii) Si $A = \mathbb{Z}$, tout sous groupe abélien peut être vu comme un $\mathbb{Z} - module$

(iv) Soit k un corps. Alors tout $k - espace\ vectoriel$ est un $k - module$.

1.7. Exemple

(i) $M = 0$ est un $A - module$ pour tout Anneau A, appelé **module nul**

(ii) L'anneau A est un $A - module$. Les sous $A - modules$ sont les idéaux de A.

(iii) Si $A = \mathbb{Z}$, tout sous groupe abélien peut être vu comme un $\mathbb{Z} - module$

(iv) Soit k un corps. Alors tout $k - espace\ vectoriel$ est un $k - module$.

1.7. Exemple

(i) $M = 0$ est un $A - module$ pour tout Anneau A, appelé **module nul**

(ii) L'anneau A est un $A - module$. Les sous $A - modules$ sont les idéaux de A.

(iii) Si $A = \mathbb{Z}$, tout sous groupe abélien peut être vu comme un $\mathbb{Z} - module$

(iv) Soit k un corps. Alors tout $k - espace\ vectoriel$ est un $k - module$.

1.8. Définition (Module de type fini)

Soit M un A-module. M est dit de type fini s'il admet un système générateur fini, $\exists\ x_1, \cdots, x_r \in M$ tel que $\forall\, x \in M, x = \sum_{i=1}^{r} a_i x_i,\ a_i \in A$.

1.9. Définition (A-algèbre de type fini)

Soit A un anneau.
On dit que B est une $A-alg bre$ de type fini si :

(i) B est un $A-module$

(ii) B est un anneau

(iii) $B = A[b_1, \cdots, b_r] \simeq \frac{A[X_1, \cdots, X_r]}{J}$, $b_i \in B$, J idéal de $A[X_1, \cdots, X_r]$

1.9. Définition (A-algèbre de type fini)

Soit A un anneau.
On dit que B est une $A - alg bre$ de type fini si :

(i) B est un $A - module$

(ii) B est un anneau

(iii) $B = A[b_1, \cdots, b_r] \simeq \frac{A[X_1, \cdots, X_r]}{J}, \quad b_i \in B, \quad J$ idéal de $A[X_1, \cdots, X_r]$

1.9. Définition (A-algèbre de type fini)

Soit A un anneau.
On dit que B est une $A - algbre$ de type fini si :

(i) B est un $A - module$

(ii) B est un anneau

(iii) $B = A[b_1, \cdots, b_r] \simeq \dfrac{A[X_1, \cdots, X_r]}{J}$, $b_i \in B$, J idéal de $A[X_1, \cdots, X_r]$

1.10 Proposition

Soient B un anneau et A un sous-anneau de B ($A \subseteq B$).
Soit $x \in B$.
Les assertions suivantes sont équivalentes :

i) x est entier sur A ;
ii) $A[x]$ est un A-module de type fini ;
iii) Il existe C un sous-anneau de B contenant $A[x]$ tel que C soit un A-module de type fini.

1.10 Proposition

Soient B un anneau et A un sous-anneau de B ($A \subseteq B$).
Soit $x \in B$.
Les assertions suivantes sont équivalentes :

i) x est entier sur A ;
ii) $A[x]$ est un A-module de type fini ;
iii) Il existe C un sous-anneau de B contenant $A[x]$ tel que C soit un A-module de type fini.

1.10 Proposition

Soient B un anneau et A un sous-anneau de B ($A \subseteq B$).
Soit $x \in B$.
Les assertions suivantes sont équivalentes :

i) x est entier sur A ;
ii) $A[x]$ est un A-module de type fini ;
iii) Il existe C un sous-anneau de B contenant $A[x]$ tel que C soit un A-module de type fini.

1.11 Corollaire

Soient A et B deux anneaux tels que $A \subseteq B$ et $x_1, x_2, \cdots, x_n \in B$. Alors les assertions suivantes sont équivalentes :

i) $\forall\ 1 \leqslant i \leqslant n, x_i$ est entier sur A,

ii) $A[x_1, x_2, \cdots, x_n]$ est un A-module de type fini,

iii) Il existe un $A-module$ de type fini $C \subseteq B$ tel que $x_i C \subseteq C, \forall\ 1 \leqslant i \leqslant n$.

1.11 Corollaire

Soient A et B deux anneaux tels que $A \subseteq B$ et $x_1, x_2, \cdots, x_n \in B$. Alors les assertions suivantes sont équivalentes :

i) $\forall\ 1 \leqslant i \leqslant n, x_i$ est entier sur A,

ii) $A[x_1, x_2, \cdots, x_n]$ est un A-module de type fini,

iii) Il existe un $A-$*module* de type fini $C \subseteq B$ tel que $x_i C \subseteq C, \forall\ 1 \leqslant i \leqslant n$.

1.11 Corollaire

Soient A et B deux anneaux tels que $A \subseteq B$ et $x_1, x_2, \cdots, x_n \in B$.
Alors les assertions suivantes sont équivalentes :

i) $\forall\ 1 \leqslant i \leqslant n, x_i$ est entier sur A,

ii) $A[x_1, x_2, \cdots, x_n]$ est un A-module de type fini,

iii) Il existe un $A - module$ de type fini $C \subseteq B$ tel que $x_i C \subseteq C, \forall\ 1 \leqslant i \leqslant n$.

1.12. Proposition (Clôture intégrale d'anneaux)

Soit $A \subseteq B$ une inclusion d'anneaux.
L'ensemble des éléments de B entiers sur A est un sous anneau de B contenant A appelé **clôture intégrale** de B dans A notée A'.

1.13. Proposition

Soit $A \subseteq B$ une inclusion d'anneaux tel que B entier sur A.

$$B \text{ corps} \Longleftrightarrow A \text{ corps}$$

Preuve

$i) \implies ii)$ Supposons B corps.
Soit $x \in A \backslash \{0\}$.
Comme $A \subseteq B$ alors $x \in B \backslash \{0\}$. Donc x est inversible d'inverse $x^{-1} \in B$.
De plus B entier sur A, alors il existe $n \in \mathbb{N}^*, (x^{-1})^n + \sum_{i=1}^{n} a_i (x^{-1})^{n-i} = 0$,
pour tout $a_i \in A, i \in [\![1, n]\!]$.
Ainsi $(x^{-1})^n = \sum_{i=1}^{n} (-a_i)(x^{-1})^{n-i}$, pour tout $a_i \in A, i \in [\![1, n]\!]$.
$(x^{-1}) \times (x^{-1})^{n-1} = \sum_{i=1}^{n} (-a_i)(x^{-1})^{n-i}$, pour tout $a_i \in A, i \in [\![1, n]\!]$.

Preuve

$(x^{-1}) = \sum_{i=1}^{n}(-a_i)(x^{-1})^{n-i}(x^{-1})^{-n+1}$, pour tout $a_i \in A, i \in [\![1, n]\!]$.

$x^{-1} = \sum_{i=1}^{n}(-a_i)x^{i-1}$, pour tout $a_i \in A, i \in [\![1, n]\!]$.

Comme $1 \leq i \leq n$ alors $0 \leq i-1 \leq n-1$

Donc $x^{i-1} \in A$.

Par stabilité $x^{-1} \in A$

Donc A corps.

Preuve

$ii) \implies i)$ Supposons que A corps.
Soit $x \in B \backslash \{0\}$.
Comme B entier sur A, alors il existe $n \in \mathbb{N}^*, x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$,
pour tout $a_i \in A, i \in [\![1, n]\!]$.
Par récurrence sur n, montrons que $x \in A$.
<u>Initialisation</u> $(n = 1)$
l'équation de dépendance intégrale devient,
$x + a_1 = 0 \Rightarrow x = -a_1 \in A \backslash \{0\}$
Donc x est inversible dans $A \subset B$. Donc x est inversible dans B.

Preuve

<u>Hérédité</u> $(n \geq 1)$

Supposons que la propriété est vraie jusqu'à l'ordre n.

Alors $x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0 \Rightarrow x \in A$.

Ainsi $x^{n+1} + \sum_{i=1}^{n+1} a_i x^{n+1-i} = 0 \Rightarrow x(x^n + \sum_{i=1}^{n} a_i x^{n-i}) + a_{n+1} = 0 \Rightarrow$ $x(x^n + \sum_{i=1}^{n} a_i x^{n-i}) = -a_{n+1}$

* Si $-a_{n+1} \neq 0$ alors x est inversible dans $A \subset B$. Donc x est inversible dans B.

* Si $-a_{n+1} = 0$, alors $x(x^n + \sum_{i=1}^{n} a_i x^{n-i}) = 0 \Rightarrow x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0$ (car $x \neq 0$ et B intègre)

Preuve

Ainsi $x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0 \Rightarrow x(x^{n-1} + \sum_{i=1}^{n-1} a_i x^{n-1-i}) = -a_{n+2}$

* Si $-a_{n+2} \neq 0$ alors x est inversible dans $A \subset B$. Donc x est inversible dans B.

* Sinon de proche en proche, il vient $x + a_1 = 0 \Rightarrow x = -a_1 \in A \backslash \{0\}$

Donc x est inversible dans $A \subset B$. Donc x est inversible dans B

Dans tous les cas, il vient B corps. D'où l'équivalence.

2.1. Définition

Soit A un anneau.
Un idéal de A est une partie I de A vérifiant les propriétés suivantes :

(i) $0_A \in I$,

(ii) *Pour tout* $x, y \in I, x + y \in I$

(iii) *Pour tout* $a \in A$ et $x \in I, ax \in I$.

Exemple : Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

2.1. Définition

Soit A un anneau.
Un idéal de A est une partie I de A vérifiant les propriétés suivantes :

(i) $0_A \in I$,

(ii) *Pour tout* $x, y \in I, x + y \in I$

(iii) *Pour tout* $a \in A$ et $x \in I, ax \in I$.

Exemple : Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

2.1. Définition

Soit A un anneau.
Un idéal de A est une partie I de A vérifiant les propriétés suivantes :

(i) $0_A \in I$,

(ii) *Pour tout* $x, y \in I, x + y \in I$

(iii) *Pour tout* $a \in A$ et $x \in I, ax \in I$.

Exemple : Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

2.1. Définition

Soit A un anneau.
Un idéal de A est une partie I de A vérifiant les propriétés suivantes :

(i) $0_A \in I$,

(ii) *Pour tout* $x, y \in I, x + y \in I$

(iii) *Pour tout* $a \in A$ et $x \in I, ax \in I$.

Exemple : Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

2.2. Définition

Soient A un anneau commutatif unitaire et I un idéal de A.
Un élément x de A est dit entier sur I s'il existe un entier $m \in \mathbb{N}$ tel que :

$$x^m + a_1 x^{m-1} + \cdots + a_m = 0, \text{ avec } a_i \in I^i, \forall i = 1, \cdots, m.$$

2.2. Définition

Soient A un anneau commutatif unitaire et I un idéal de A.
Un élément x de A est dit entier sur I s'il existe un entier $m \in \mathbb{N}$ tel que :

$$x^m + a_1 x^{m-1} + \cdots + a_m = 0, \text{ avec } a_i \in I^i, \forall i = 1, \cdots, m.$$

2.2. Définition

Soit A un anneau.
Une **graduation sur A** est une famille $(A_n)_{n\in\mathbb{Z}}$ de sous-groupes stables de $(A,+)$ vérifiant :

i) $A_pA_q \subset A_{p+q}$

ii) $A = \bigoplus_{n\in\mathbb{Z}} A_n$

2.2. Définition

Soit A un anneau.
Une **graduation sur A** est une famille $(A_n)_{n\in\mathbb{Z}}$ de sous-groupes stables de $(A,+)$ vérifiant :

i) $A_pA_q \subset A_{p+q}$

ii) $A = \bigoplus_{n\in\mathbb{Z}} A_n$

2.3. Remarque

Si $\forall n < 0, A_n = \{0_A\}$, on dit que **A est positivement gradué** ou que **A est gradué de type n**. Ainsi $A = \bigoplus_{n\in\mathbb{N}} A_n$. Les éléments de A_n, pour tout $n \in \mathbb{N}$ sont dits de degré n.

De plus $A = \bigoplus_{n\in\mathbb{N}} A_n$ si et seulement si :

$$\forall x \in A, \exists x_i \in A, \text{tel que } x = \sum_{finie} x_i \text{ (Existence et Unicité).}$$

DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATION I-BONNE

FILTRATION

2.4. Définition

Soit A un anneau. On appelle filtration de A toute famille $f = (I_n)_{n\in\mathbb{Z}}$ d'idéaux de A telle que :

(i) $I_0 = A$

(ii) Pour tout $n \in \mathbb{Z}$, $I_{n+1} \subseteq I_n$.

(iii) Pour tout $p, q \in \mathbb{Z}$, $I_p I_q \subseteq I_{p+q}$.

L'ensemble des filtrations de l'anneau A est noté $\mathbb{F}(A)$.
Pour tout $f, g \in \mathbb{F}(A)$, cet ensemble est ordonné par :

$$\forall n \in \mathbb{Z}, f = (I_n) \leqslant g = (J_n) \implies I_n \subseteq J_n$$

2.4. Définition

Soit A un anneau. On appelle filtration de A toute famille $f = (I_n)_{n\in\mathbb{Z}}$ d'idéaux de A telle que :

(i) $I_0 = A$

(ii) Pour tout $n \in \mathbb{Z}$, $I_{n+1} \subseteq I_n$.

(iii) Pour tout $p, q \in \mathbb{Z}$, $I_p I_q \subseteq I_{p+q}$.

L'ensemble des filtrations de l'anneau A est noté $\mathbb{F}(A)$.
Pour tout $f, g \in \mathbb{F}(A)$, cet ensemble est ordonné par :

$$\forall n \in \mathbb{Z}, f = (I_n) \leqslant g = (J_n) \implies I_n \subseteq J_n$$

2.4. Définition

Soit A un anneau. On appelle filtration de A toute famille $f = (I_n)_{n\in\mathbb{Z}}$ d'idéaux de A telle que :

(i) $I_0 = A$

(ii) Pour tout $n \in \mathbb{Z}$, $I_{n+1} \subseteq I_n$.

(iii) Pour tout $p, q \in \mathbb{Z}$, $I_pI_q \subseteq I_{p+q}$.

L'ensemble des filtrations de l'anneau A est noté $\mathbb{F}(A)$.
Pour tout $f, g \in \mathbb{F}(A)$, cet ensemble est ordonné par :

$$\forall n \in \mathbb{Z}, f = (I_n) \leqslant g = (J_n) \implies I_n \subseteq J_n$$

2.4. Définition

Soit A un anneau. On appelle filtration de A toute famille $f = (I_n)_{n \in \mathbb{Z}}$ d'idéaux de A telle que :

(i) $I_0 = A$

(ii) Pour tout $n \in \mathbb{Z}$, $I_{n+1} \subseteq I_n$.

(iii) Pour tout $p, q \in \mathbb{Z}$, $I_p I_q \subseteq I_{p+q}$.

L'ensemble des filtrations de l'anneau A est noté $\mathbb{F}(A)$.
Pour tout $f, g \in \mathbb{F}(A)$, cet ensemble est ordonné par :

$$\forall n \in \mathbb{Z}, f = (I_n) \leqslant g = (J_n) \implies I_n \subseteq J_n$$

2.4. Définition

Soit A un anneau. On appelle filtration de A toute famille $f = (I_n)_{n\in\mathbb{Z}}$ d'idéaux de A telle que :

(i) $I_0 = A$

(ii) Pour tout $n \in \mathbb{Z}$, $I_{n+1} \subseteq I_n$.

(iii) Pour tout $p, q \in \mathbb{Z}$, $I_p I_q \subseteq I_{p+q}$.

L'ensemble des filtrations de l'anneau A est noté $\mathbb{F}(A)$.
Pour tout $f, g \in \mathbb{F}(A)$, cet ensemble est ordonné par :

$$\forall n \in \mathbb{Z}, f = (I_n) \leqslant g = (J_n) \implies I_n \subseteq J_n$$

FILTRATION

2.5. Exemple

1. Soit I un idéal de A et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_{3n} = I_{3n-1} = I_{3n-2} = I^n$$

2. Soit $A = \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_1 = I_2 = (\bar{2})$$

$$I_n = (\bar{0}) \text{ pour tout } \quad n \geqslant 3$$

FILTRATION

2.5. Exemple

1. Soit I un idéal de A et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_{3n} = I_{3n-1} = I_{3n-2} = I^n$$

2. Soit $A = \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_1 = I_2 = (\bar{2})$$

$$I_n = (\bar{0}) \text{ pour tout } \quad n \geqslant 3$$

FILTRATION

2.5. Exemple

1. Soit I un idéal de A et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_{3n} = I_{3n-1} = I_{3n-2} = I^n$$

2. Soit $A = \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_1 = I_2 = (\bar{2})$$

$$I_n = (\bar{0}) \text{ pour tout } \quad n \geqslant 3$$

FILTRATION

2.5. Exemple

1. Soit I un idéal de A et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_{3n} = I_{3n-1} = I_{3n-2} = I^n$$

2. Soit $A = \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ et $f = (I_n)_{n\in\mathbb{Z}}$ telle que pour tout $n \in \mathbb{Z}$:

$$I_1 = I_2 = (\bar{2})$$

$$I_n = (\bar{0}) \text{ pour tout } \quad n \geqslant 3$$

2.6. Définition **(Anneau de Rees)**

Soit $f = (I_n)_{n\in\mathbb{Z}}$ une filtration de l'anneau A.
X est une indéterminée.
On appelle **anneau de Rees** de f, l'anneau gradué noté R(A,f) tel que :

$$R(A, f) = \bigoplus_{n\in\mathbb{N}} I_n X^n$$

2.6. Définition (Anneau de Rees)

On appelle **anneau de Rees généralisé** de f, l'anneau gradué noté $\mathcal{R}(A, f)$ tel que :

$$\mathcal{R}(A, f) = \bigoplus_{n \in \mathbb{Z}} I_n X^n$$

DÉPENDANCE INTÉGRALE, RÉDUCTION ET FILTRATION I-BONNE

DÉPENDANCE INTÉGRALE SUR LES IDÉAUX

2.7. Remarque

On munit $R(A, f)$ et $\mathcal{R}(A, f)$ d'une structure de sous-anneau gradué de $A[X]$, l'ensemble des polynômes d'indéterminée X à coefficients dans A dont les opérations sont définies par :

1. la multiplication : $(\sum_{n=0}^{r} a_n X^n)(\sum_{k=0}^{s} b_k X^k) = \sum_{p=0}^{r+s} c_p X^p = \sum_{p=0}^{r+s} \sum_{q=0}^{p} a_{p-q} b_q X^p$
2. l'addition : $\sum_{n=0}^{r} a_n X^n + \sum_{k=0}^{s} b_k X^k = \sum_{j=0}^{r} (a_j + b_j) X^j$

2.7. Remarque

On munit $R(A, f)$ et $\mathcal{R}(A, f)$ d'une structure de sous-anneau gradué de $A[X]$, l'ensemble des polynômes d'indéterminée X à coefficients dans A dont les opérations sont définies par :

1. la multiplication : $(\sum_{n=0}^{r} a_n X^n)(\sum_{k=0}^{s} b_k X^k) = \sum_{p=0}^{r+s} c_p X^p = \sum_{p=0}^{r+s} \sum_{q=0}^{p} a_{p-q} b_q X^p$
2. l'addition : $\sum_{n=0}^{r} a_n X^n + \sum_{k=0}^{s} b_k X^k = \sum_{j=0}^{r} (a_j + b_j) X^j$

2.8. Proposition

Soient A un anneau, I un idéal de A. Soient $f = (I_n)_{n\in\mathbb{Z}} \in \mathbb{F}(A)$ et X une indéterminée.

(i) $A \subseteq R(A, f) \subseteq A[X]$

(iii) $\mathcal{R}(A, f) = R(A, f)[u]$ où $u = \dfrac{1}{X} = X^{-1}$

(iii) $R(A, I) = R(A, f_I)$

2.8. Proposition

Soient A un anneau, I un idéal de A. Soient $f = (I_n)_{n\in\mathbb{Z}} \in \mathbb{F}(A)$ et X une indéterminée.

(i) $A \subseteq R(A, f) \subseteq A[X]$

(iii) $\mathcal{R}(A, f) = R(A, f)[u]$ où $u = \dfrac{1}{X} = X^{-1}$

(iii) $R(A, I) = R(A, f_I)$

2.8. Proposition

Soient A un anneau, I un idéal de A. Soient $f = (I_n)_{n\in\mathbb{Z}} \in \mathbb{F}(A)$ et X une indéterminée.

(i) $A \subseteq R(A, f) \subseteq A[X]$

(iii) $\mathcal{R}(A, f) = R(A, f)[u]$ où $u = \dfrac{1}{X} = X^{-1}$

(iii) $R(A, I) = R(A, f_I)$

2.9. Proposition

Soient A un anneau et I un idéal de A.

x *entier sur* $I \Longleftrightarrow$ *Le* monôme $xX \in A[x]$ *est entier sur* $R(A, I) = \bigoplus_{n \in \mathbb{N}} I^n X^n$

Preuve

$i) \implies ii)$

Supposons x entier sur I. Alors il existe $n \in \mathbb{N}^*, x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0,\ a_i \in I^i$.

Ainsi il existe $n \in \mathbb{N}^*, (xX)^n + \sum_{i=1}^{n} a_i X^i (xX)^{n-i} = 0,\ a_i X^i \in I^i X^i \in R(A, I)$.

D'où xX est entier sur $R(A, I)$.

Preuve

$ii) \implies i)$

Supposons que $xX \in A[X]$ est entier sur $R(A, I)$.

Ainsi il existe $n \in \mathbb{N}^*, (xX)^n + \sum_{i=1}^{n} a_i(xX)^{n-i} = 0,\ a_i \in R(A, I)$.

Alors il existe $n \in \mathbb{N}^*, (xX)^n = \sum_{i=1}^{n} (-a_i)(xX)^{n-i},\ a_i \in R(A, I)$.

Comme $(xX)^n$ est homogène de degré n, alors pour tout $i \in [\![1, n]\!]$, $\deg[a_i(xX)^{n-i}] = n \Rightarrow \deg(a_i) + n - i = n \Rightarrow \deg(a_i) = i$.

Preuve

Donc $a_i \in I^i X^i \Rightarrow a_i = \alpha_i X^i$, avec $\alpha_i \in I^i$.

D'où, il existe $n \in \mathbb{N}^*, (xX)^n + \sum_{i=1}^{n} \alpha_i X^i (xX)^{n-i} = 0$,

il existe $n \in \mathbb{N}^*, X^n[x^n + \sum_{i=1}^{n} \alpha_i x^{n-i}] = 0$,avec $\alpha_i \in I^i$.

Par identification des polynômes, il existe $n \in \mathbb{N}^*, x^n + \sum_{i=1}^{n} \alpha_i x^{n-i} = 0$,avec $\alpha_i \in I^i$.

Donc x est entier sur I.

2.10. Corollaire **(Clôture intégrale d'idéaux)**

Soient A un anneau et I un idéal de A.L'ensemble noté :

$$I' = \{x \in A, x \text{ } entier \text{ } sur \text{ } A\} = \overline{I}$$

est un idéal de A appelé **clôture intégrale de I**.

2.11. Définition (Radical d'un idéal)

Soient A un anneau, I un idéal de A. On appelle radical de I

$$\sqrt{I} = \{a \in A, \exists n \in \mathbb{N}, a^n \in I\}$$

2.12. Remarque

Soient A un anneau et I et J des idéaux de A.

1) $I \subseteq J \implies I' \subseteq J'$.

2) $I \subseteq I' \subseteq \sqrt{I}$.

3) $\sqrt{I} = \sqrt{I'}$.

2.12. Définition (Intégralement fermé)

Un idéal I de A est dit **intégralement fermé** si $I = I'$.

3.1. Définition (Réduction d'un idéal)

Soient A un anneau commutatif unitaire, I et J deux idéaux de A. On dit que I est une réduction de J si :

i) I $\subseteq$ J,

ii) $\exists\, r \in \mathbb{N}^*$, tel que $J^{r+1} = IJ^r$.

3.1. Définition **(Réduction d'un idéal)**

Soient A un anneau commutatif unitaire, I et J deux idéaux de A. On dit que I est une réduction de J si :

i) $\mathrm{I} \subseteq \mathrm{J}$,

ii) $\exists\, r \in \mathbb{N}^*$, tel que $J^{r+1} = IJ^r$.

3.2. Exemple (Réduction d'un idéal)

1) I est une réduction de I lui-même.
2) $A = \mathbb{K}[X, Y]$ avec $\mathbb{K}$ corps.
   $I = (X^2, Y^2)$
   $J = (X, Y)^2 = (X^2, Y^2, XY)$ D'où $I \subseteq J$.

$$\begin{aligned} IJ &= (X^2, Y^2)(X, Y)^2 \\ &= (X^2, Y^2)(X^2, XY, Y^2) \\ &= (X^4, Y^4, X^3Y, XY^3, X^2Y^2) \end{aligned}$$

3.2. Exemple (Réduction d'un idéal)

Et,

$$
\begin{aligned}
J^2 &= (X^2X^2, X^2Y^2, X^3Y, Y^2Y^2, Y^3X) \\
&= (X^4, Y^4, X^2Y^2, X^3Y, XY^3)
\end{aligned}
$$

Donc $J^{1+1} = J^2 = IJ$ avec $r = 1$.
Par suite I est une réduction de J.

3.3. Remarque

$\forall\, r \geq n$, on a $J^{r+1} = IJ^r$.
D'une manière générale, $I^m J^n = J^{n+m},\ \forall\, m \in \mathbb{N}$.

MERCI POUR VOTRE AIMABLE ATTENTION