Université Cadi Ayyad
Faculté Polydsiciplinaire de Safi

Département de Mathématiques et Informatique

==========

Algèbre Commutative et Applicatons

==========

SMA-S6

Par : Mohammed Karmouni

Année Universitaire : 2019-2020

Préface

Ce ploycopie a été écrit pour des étudiants de troisième année de Licence Fondamentale Sciences Mathématiques et Applications(SMA). L'objectif de ce cours est d'approfondir les notions des structures algébriques, notamment les anneaux, avoir une vision plus générale sur les espaces vectoriels à travers l'étude des modules sur un anneau tout en distinguant les particularités de chacune de ces notions et initier l'étudiant à la géométrie algébrique et topologie algébrique.

http://cimas.uca.ma/karmouni/karmouni.html
(mohammed.karmouni@uca.ma)

Table des matières

CHAPITRE 1

Anneaux

1.1 Notion d'anneau

Définition 1.1. *Un anneau est un ensemble non vide A muni de deux lois de composition internes, une notée additivement $+$ et l'autre multiplicativement . telles que :*

1. *$(A, +)$ est un groupe abélien.*
2. *. est une loi de composition interne associative dans A.*
3. *. est distributive par rapport à la loi $+$: $(x+y)z = xz+yz$ et $z(x+y) = zx+zy$ pour tous $x, y \in A$.*

✓ Si la loi . est commutative, on dit que l'anneau A est commutatif.
✓ Si la loi . admet un élément neutre distinct de 0, noté 1_A ou 1 s'il n'y a pas d'ambiguité, on dit que l'anneau A est unitaire. On conveint que l'on a toujours $0 \neq 1$. Donc, un anneau unitaire a au moins deux éléments, à savoir 1 et 0.
✓ A est dit nul, si $A = \{0\}$. Cet anneau n'est pas unitaire.

Définition 1.2. *Soient $(A, +, .)$ un anneau et B un sous ensemble non vide de A. B est dit un sous-anneau de A si $(B, +, .)$ est un anneau. D'une autre manière :*

1. *$(B, +)$ est un sous groupe de A.*
2. *B est stable par la multiplication : $\forall x, y \in B$, $x.y \in B$.*

✓ Si A est un anneau unitaire, on dit que B est sous-anneau unitaire de A si on a en oùtre $1_A \in B$.
✓ Si A est commutatif, alors tout sous-anneau de A est commutatif.
Pratiquement, pour montrer qu'un sous-ensemble non vide B d'un anneau A est un sous-anneau de A, il suffit de vérifie que : pour tous $x, y \in B$, on a $x - y \in B$ et $xy \in B$. Si de plus $1_A \in B$, B est un sous-anneau unitaire.

Exemple 1.3. 1. *$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs unitaires.*

2. *L'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans un corps K est un anneau commutatif unitaire.*
3. *Soit A un anneau unitaire. L'ensemble $M_n(A)$ des matrices $n \times n$ à coefficients dans A muni des régles de calcul habituelle, la somme de deux matrices et le produit des matrices est un anneau*

unitaire. Si $n \geqslant 2$, ou si A n'est pas commutatif, $M_n(A)$ n'est pas commutatif.

4. *Si A est un anneau, alors $\{0\}$ et A lui-même sont des sous-anneau de A.*
5. *$Z(A) = \{x \in A, ax = xa$ pour tout $a \in A\}$ est un sous-anneau de A. $Z(A) = A \iff A$ est commutatif*
6. *Pour tout $n \geqslant 2$, $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$ est un sous anneau non unitaire de $\mathbb{Z}$.*
7. *Dans $F(I, \mathbb{R})$ les fonctions continues forment un sous anneau unitaire.*
8. *A_1 et A_2 étant deux anneaux, on considère l'ensemble produit direct :*

$$A_1 \times A_2 = \{(a, b); a \in A_1 \text{ et } b \in A_2\}.$$

$A_1 \times A_2$ est muni d'une structure d'anneau, grâce à l'addition et à la multiplication respectivement définies par les applications suivantes :

$$((x_1, x_2), (y_1, y_2)) \longrightarrow (x_1 + y_1, x_2 + y_2) \qquad ((x_1, x_2), (y_1, y_2))) \longrightarrow (x_1 y_1, x_2 y_2).$$

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

Définition 1.4. *Soient A et B deux anneaux. Une application $\varphi : A \longrightarrow B$ est dite un homomorphisme d'anneaux, et on note $\varphi \in Hom(A, B)$, si φ vérifie :*

⋆ $\varphi(x + y) = \varphi(x) + \varphi(y)\ \forall\ x, y \in A$.

⋆ $\varphi(x.y) = \varphi(x).\varphi(y)\ \forall\ x, y \in A$. *Si de plus,*

⋆ $\varphi(1_A) = 1_B$, *on dit que φ est un homomorphisme d'anneaux unitaires*

Nous avons, $\varphi(0_A) = 0_B$, $\varphi(x - y) = \varphi(x) - \varphi(y)$ et $\varphi(-x) = -\varphi(x)$.

Définition 1.5. *On dit que $\varphi \in Hom(A, B)$ est un isomorphisme d'anneaux, s'il existe $g \in Hom(B, A)$ tel que $g \circ \varphi = id_A$ et $\varphi \circ g = id_B$. Ce qui équivalent à $\varphi \in Hom(A, B)$ et φ est bijectif. On note, dans ce cas, $\varphi \in Iso(A, B)$.*
A et B sont dits isomorphes, s'il existe un isomorphisme d'anneaux de l'un sur l'autre, dans ce cas, on écrit $A \simeq B$.
Un isomorphisme de A sur lui-même est appelé un automorphisme de A.

⋆ $\varphi \in Iso(A, B) \Longrightarrow \varphi^{-1} \in Iso(B, A)$.

Notons par U_A l'ensemble des éléments inversibles de A, qui sont aussi appelés les unités de A.

1.2 Diviseurs de zéro, Eléments nilpotents, Eléments unités

Soit A un anneau unitaire, non nécessairement commutatif, soit $x \in A$.
On dit que x est inversible à gauche s'il existe $z \in A$ tel que $zx = 1$.
On dit que x est inversible à droite s'il existe $y \in A$ tel que $xy = 1$.
On dit que x est inversible s'il est inversible à gauche et à droite, ie $\exists a \in A$ tel que $ax = xa = 1$.
L'inverse d'un élément x de A sera noté x^{-1}.

Définition 1.6. *Un corps est un anneau unitaire commutatif tel que tout élément non nul est inversible.*

Remarque 1.7. *1. Dans tout anneau unitaire A, on a $U_A \neq \emptyset$ car 1 et -1 sont dans U_A.*

2. U_A est un groupe multiplicative.

3. U_A est un groupe abélien si et seulement si A est commutatif.

4. $U_{\mathbb{Z}} = \{-1, 1\}$.

5. Si $\mathbb{K}$ est un corps, alors $U_{\mathbb{K}} = \mathbb{K}^*$.

Exercice 1.8. *Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Définition 1.9. *Un élément non nul $a \in A$ est dit un diviseur de zéro à gauche(resp. à droite) si $\exists\, b(\neq 0) \in A$ tel que $ba = 0$ (resp. $ab = 0$).*
Dans un anneau commutatif on parlera seulement de diviseur de zéro.

Exemple 1.10. *Dans $\mathbb{Z}/8\mathbb{Z}$, $\overline{2}$ et $\overline{4}$ sont des diviseurs de zéro.*

Notons que x invesible implique que x n'est pas un diviseur de zéro. Donc un corps n'a pas de diviseur de zéro

Définition 1.11. *Un anneau est dit intègre s'il est non nul et sans diviseur de zéro.*
On appellera domaine d'intégrité tout anneau unitaire, commutatif intègre.

Pour x et y dans un anneau intègre, on a : $xy = 0 \Longrightarrow x = 0$ ou $y = 0$.

Exemple 1.12. *1. Tout corps est un domaine d'intégrité.*

2. $\mathbb{Z}/n\mathbb{Z}$ est un domaine d'intégrité si et seulement si n est premier.

3. Tout domaine d'intégrité fini est un corps (Exercice).

1.3 Notion d'idéaux et d'anneaux quotients

Définition 1.13. *Soient A un anneau et I un sous ensemble de A. On dit que I est un idéal à gauche (resp. à droite) de A si :*

i) *$(I, +)$ est un sous groupe de A.*

ii) *$\forall\, x \in I$, $\forall\, a \in A$, $ax \in I$, (resp. $xa \in I$) càd $A.I \subseteq I$ (resp. $I.A \subseteq I$).*

On dit que I est un idéal bilatère ou simplement un idéal de A si I est à la fois un idéal à gauche et à droite de A. Dans le cas commutatif, on parle alors tout simplement d'idéal.

Exemple 1.14. *1. $\{0\}$ et A sont des idéaux de A.*

2. Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$.

3. Dans l'anneau $F(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions continues qui s'annulent en 0 est un idéal.

4. Soient A et B deux anneaux unitaires, $\varphi \in Hom(A, B)$. Alors $\ker\varphi$ est un idéal de A

Définition 1.15. *Soit S une partie non vide d'un anneau A. On appelle idéal de A engendré par S, l'intersection de tous les idéaux de A contenant S. On notera (S), c'est le plus petit idéal de A contenant S.*

1. *I est un idéal principal s'il est engendré par un seul élément.*
2. *I est de type fini s'il est engendré par un nombre fini d'éléments.*

Nous avons,

$$(S) = \{ \sum_{1 \leqslant i \leqslant n} a_i x_i b_i, m \in \mathbb{N}^*, a_i, b_i \in A, x_i \in S\}.$$

Définition 1.16. *Un anneau unitaire commutatif A est dit principal, si tout idéal de A est principal.*
On appellera domaine principal, tout domaine d'intégrité dans lequel tout idéal est principal.

Exemple 1.17. *$\mathbb{Z}$ est un domaine principal.*

1.3.1 Construction d'anneau quotient

Rappelons qu'une relation $\mathcal{R}$ sur un ensemble X est dite relation d'équivalence si elle est réflexive (pour tout $x, x\mathcal{R}x$), symétrique (si $x\mathcal{R}y$, alors $y\mathcal{R}x$) et transitive (si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$). L'ensemble des classes d'équivalence de X pour la relation $\mathcal{R}$ est noté $X/\mathcal{R}$.
Soient A un anneau et I un idéal de A. En particulier I est un sous-groupe normal puisque A est un groupe abélien pour la somme. On peut considérer le groupe quotient A/I dont les éléments sont les classes pour la relation d'équivalence $\mathcal{R}$ définie par :

$$x\mathcal{R}y \Longleftrightarrow x - y \in I.$$

On note $\overline{x} = x + I$ la classe de l'élément x de A.
-On va munir A/I d'une structure d'anneau.
On définit sur A/I l'addition et la multiplication de la façon suivante :

$$(a + I) + (b + I) = a + b + I, \qquad (a + I)(b + I) = ab + I, a, b \in A.$$

Notons que la somme et la multiplication sont compatibles avec cette relation.
On dit que A/I est l'anneau quotient de A par l'idéal I.
Si A est unitaire, $1 + I$ est l'élément unité pour la multiplication pour A/I. De méme, si A est commutatif alors A/I est commutatif.
La surjection canonique $\pi : A \longrightarrow A/I$ est un morphisme d'anneaux. Ce morphisme est surjectif de noyau I.

Remarque 1.18. *Si $I = \{0\}$, $A/(0)$ s'identifie à A($\pi(a) = a$ pour tout $a \in A$).*
Si $I = A$, A/A est l'anneau nul, car $\pi(a) = \overline{0}$ pour tou $a \in A$.

Lemme 1.19. *Soit A un anneau commutatif unitaire.*

1. *Si I est un idéal de A qui contient 1, alors $I = A$.*
2. *Si I est un idéal de A qui contient un élément de U_A, alors $I = A$.*

Démonstration. Supposons que $1 \in I$, soit $a \in A$, $a = 1a \in I$. On a alors $A \subseteq I$, donc $A = I$.
Si I contienne un élément $x \in U_A$, alors $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$. On applique 1) donc $A = I$.

□

Proposition 1.20. *Si I est une partie non vide d'un anneau A. Pour que I est un idéal bilatère de A, il faut et il suffit qu'il existe un anneau A' et un morphisme d'anneux f de A dans A' tel que* $\ker f = I$.

Démonstration. Si A' est un anneau et $f \in Homm(A, A')$, on a $\ker f$ est un idéal bilatère de A. Inversement, si I est un idéal bilatère de A, en prenant $A' = A/I$, on a $I = \ker \pi$, où $\pi : A \longrightarrow A/I$ est la surjection canonique. □

On a la caractérisation suivante des corps :

Proposition 1.21. *Soit A un anneau unitaire commutatif. Les assertions suivantes sont équivalentes :*

i) *A est un corps ;*

ii) *Les seuls idéaux de A sont (0) et A ;*

iii) *Tout homomorphisme non nul d'anneaux de $A \longrightarrow B$ est injectif, où B est un anneau quelconque.*

Démonstration. *i)* $\Longrightarrow$ *ii)*, Supposons que A est un corps. Soit I un idéal de A tq $I \neq \{0\}$. Montrons que $I = A$. En effet, $I \neq \{0\}$ implique qu'il existe un a no nul tq $a \in I \subset A$. A est un corps implique qu'il existe $b \in A$ tq $ab = 1$. Or I est un idéal donne $1 = ab \in I$ donc $A = I$ par le lemme **??**.
ii) $\Longrightarrow$ *i)*, Soit $x \in A$ non nul. Montrons que x est inversible.
On a xA est un idéal non nul de A, donc $A = xA$, ie il existe $y \in A$ non nul tq $xy = 1$, d'où x est inversible.
ii) $\Longrightarrow$ *iii)*, Soit $\varphi : A \longrightarrow B$, $\varphi \in Hom(A, B)$. On a $\varphi \neq 0$ donc $\ker \varphi \neq A$ et $\ker \varphi$ est un idéal de A d'où $\ker \varphi = \{0\}$.
iii) $\Longrightarrow$ *ii)*, Soit I un idéal de A tq $I \neq A$. Nous avons $I = \{0\}$. En effet, soit $\varphi : A \longrightarrow A/I$ $x \longrightarrow \overline{x}$ non nul. On a $\ker \varphi = I$ et φ est injectif donc $I = \{0\}$

□

Théorème 1.22. *Soit I un idéal bilatère d'un anneau A.*

1. *Tout sous-anneau(resp. idéal) de A/I est l'image par π d'un unique sous anneau(resp. idéal) contenant I. D'une autre manière, si $\overline{J}$ est un sous anneau(resp. idéal) de A/I, alors $\overline{J} =$*

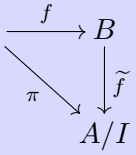
$\pi(J)$, où $J = \pi^{-1}(\overline{J}) \supseteq I$ ainsi $\overline{J} = J/I$.

2. *Si F est un sous anneau(resp. idéal) de A tel que $I \nsubseteq F$, alors $I + F$ est le plus petit sous anneau(resp. idéal) de A contenant I et $\pi(F) = (I + F)/I$.*

Exemple 1.23. *Pour $n \geqslant 2$; dans $\mathbb{N}$, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$ tels que $k \mid n$ dans $\mathbb{N}$. Ce sont aussi les seuls sous anneau de $\mathbb{Z}/n\mathbb{Z}$.*

L'importance de la structure d'anneau quotient vient notamment du théorème de factorisation que nous démontrons maintenant :

Théorème 1.24. *Soient A et B deux anneaux et $f \in Hom(A, B)$ un morphisme d'anneaux. Si I est un idéal de A contenu dans $\ker f$, il existe un unique homomorphisme d'anneaux $\widetilde{f} \in Hom(A/I, B)$ tel que $f = \widetilde{f} \circ \pi$. On a le diagramme commutatif suivant :*



Démonstration. Unicité, on a $\widetilde{f}(\pi(a)) = f(a)$ pour tout $a \in A$.
$\forall x \in A/I$, $x = \pi(a)$ avec $a \in A$ ce qui montre l'unicité de $\widetilde{f} : A/I \longrightarrow B$. Sinon, si $\exists \widetilde{f}_1, \widetilde{f}_2$, on a $\widetilde{f}_1(x) = \widetilde{f}_1(\pi(a)) = f(a)$ et $\widetilde{f}_2(x) = \widetilde{f}_2(\pi(a)) = f(a)$ pour tout $x \in A/I$. D'où, $\widetilde{f}_1 = \widetilde{f}_2$.
Existence, soit $x \in A/I$, alors il existe $a \in A$ tel que $x = \pi(a)$. Si a' un autre représentant de x tel que $x = \pi(a')$, alors $\pi(a - a') = 0 \Longrightarrow a - a' \in I$. On a $I \subseteq \ker f$ donc $f(a - a') = 0 \Longrightarrow f(a) = f(a')$.
On peut poser $\widetilde{f}(x) = f(a)$. Le résultat est indépendant de représentant choisi.
Montrons que $\widetilde{f}$ est un homomorphisme d'anneaux. Comme $\pi(0_A) = 0_{A/I}$ et $\pi(1_A) = 1_{A/I}$ on a $\widetilde{f}(0_{A/I}) = 0_B$ et $\widetilde{f}(1_{A/I}) = 1_B$.
Soient $x = \pi(a)$ et $y = \pi(b) \in A/I$ on a $x + y = \pi(a + b)$,

$$\begin{aligned} \widetilde{f}(x + y) &= \widetilde{f}(\pi(a + b)) = f(a + b) \\ &= f(a) + f(b) \\ &= \widetilde{f}(\pi(a)) + \widetilde{f}(\pi(b)) = \widetilde{f}(x) + \widetilde{f}(y). \end{aligned}$$

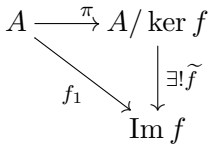
et $\widetilde{f}(xy) = f(ab) = f(a)f(b) = \widetilde{f}(x)\widetilde{f}(y)$. D'où, $\widetilde{f}$ est un homomorphisme d'anneaux.

□

Corollaire 1.25. – *f est surjectif $\Longrightarrow$ $\widetilde{f}$ est surjectif.*
– *$I = \ker f \Longrightarrow \widetilde{f}$ est injectif.*
– *f est surjectif et $I = \ker f \Longrightarrow \widetilde{f}$ est isomorphisme.*

Théorème 1.26. *(1er Théorème d'isomorphisme)*
Pour tout morphisme f d'un anneau A dans un anneau B, on a : $\operatorname{Im} f \simeq A/\ker f$.

Démonstration. Soit f_1 la restriction surjectif de f, définie par $f_1 : A \longrightarrow \operatorname{Im} f$, $x \longrightarrow f_1(x) = f(x)$. $\ker f_1 = \ker f$, d'après le Théorème 1.24, il existe un unique morphisme $\widetilde{f} \in Hom(A/\ker f, \operatorname{Im} f)$ tel que le diagramme suivant commute

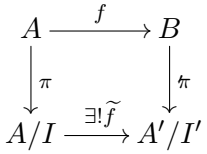


Donc, $\widetilde{f} \circ \pi = f_1$.
Comme f_1 est surjectif, alors $\widetilde{f}$ est surjectif et $\ker f_1 = \ker f \Longrightarrow \widetilde{f}$ injectif, par suite $\widetilde{f}$ est un isomorphisme de $A/\ker f$ sur $\operatorname{Im} f$ et $\widetilde{f}(\overline{x}) = \widetilde{f}(\pi(x)) = f(x)$, pour tout $\overline{x} = \pi(x) \in A/\ker f$.

□

Lemme 1.27. *Soit deux anneaux A et A' et deux idéaux bilatères I dans A et I' dans A' ; alors, pour tout morphisme $f \in Hom(A, A')$ tel que $f(I) \subseteq I'$, il existe un unique morphisme $\widetilde{f} \in Hom(A/I, A'/I')$ tel que $\widetilde{f} \circ \pi = \pi' \circ f$, où $\pi et \pi'$ sont les surjections canoniques $A \longrightarrow A/I$ et $A' \longrightarrow A'/I'$.*

Démonstration. $f(I) \subseteq I' \Longleftrightarrow I \subseteq f^{-1}(I')$, d'autre part, on a $\ker(\pi' \circ f) = f^{-1}(I')$. D'après le théorème 1.24, $I \subseteq \ker(\pi' \circ f)$ implique l'existence d'un unique morphisme d'anneaux $\widetilde{f} \in Hom(A/I, A'/I')$ tel que le diagramme suivant commute :

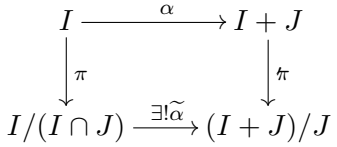


Donc, $\widetilde{f} \circ \pi = \pi' \circ f$. □

Remarque 1.28. – *Si $\pi' \circ f$ est surjectif, alors $\widetilde{f}$ est surjectif. On notera que $\pi' \circ f$ peut être surjectif, sans que f le soit.*
– *Si $\ker(\pi' \circ f) = I (\Longleftrightarrow f^{-1}(I') = I)$, alors f est injectif.*

Théorème 1.29. *(2em Théorème d'isomorphisme)*
Soient I et J deux idéaux bilatères d'un anneaux A, on a : $I/(I \cap J) \simeq (I + J)/J$.

Démonstration. Soit α l'injection canonique de I dans $I + J$, alors, $\alpha(I \cap J) = I \cap J \subseteq J$. D'après le lemme 1.27, il existe un unique $\widetilde{\alpha} \in Hom(I/(I \cap J), (I + J)/J)$ tel que le diagramme suivant :



commute, $\widetilde{\alpha} \circ \pi = \pi' \circ \alpha$.
On a $\pi' \circ \alpha(I) = \pi'(I) = (I + J)/J$, donc $\pi' \circ \alpha$ est surjectif. D'autre part, $\alpha^{-1}(J) = I \cap J$, donc $\widetilde{\alpha}$ est injectif par suite $\widetilde{\alpha}$ est un isomorphisme. □

Remarque 1.30. *Si $I \cap J = \{0\}$, alors $J \simeq (I + J)/I$ et $I \simeq (I + J)/J$.*

Théorème 1.31. *(3em Théorème d'isomorphisme)*
Soient I et J deux idéaux bilatères d'un anneau A tel que $I \subseteq J$, on a : $A/J \simeq (A/J)/(J/I)$.

Démonstration. Soit σ la surjection canonique $A \longrightarrow A/I$. $I \subseteq J \Longrightarrow \sigma(J) = J/I$. Il existe alors un unique morphisme $\sigma \in Hom(A/J, (A/J)/(J/I))$ tel que le diagramme suivant commute

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

$\widetilde{\sigma} \circ \pi = \pi' \circ \sigma$.
$\pi' \circ \sigma$ surjectif $\Longrightarrow$ et $\ker(\pi' \circ \sigma) = J \Longrightarrow \widetilde{\sigma}$ surjectif donc $\widetilde{\sigma}$ est un isomorphisme. □

Soit A un anneau unitaire. Soit $\phi : \mathbb{Z} \longrightarrow A$, $n \longrightarrow n1_A$.

Définition 1.32. *On appelle caractéristique de A, l'unique entier $k \in \mathbb{N}$ tel que $\ker \phi = k\mathbb{Z}$. On écrit alors : $carA = k$.*

Exemple 1.33. *1) L'anneau $\mathbb{Z}$, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0.*
2) Pour $n > 1$ dans $\mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

1.4 Idéaux premiers d'un anneau unitaire commutatif

1.4.1 Opérations sur les idéaux d'un anneau

Dans ce qui suit, A est un anneau unitaire commutatif.
Soit $\{I_\lambda\}_{\lambda\in\Lambda}$ une famille non vide d'idéau de l'anneau A, alors :

1. $\bigcap_{\lambda\in\Lambda} I_\lambda$ est un idéal de A.
2. $\bigcup_{\lambda\in\Lambda} I_\lambda$ n'est pas, en général, un idéal de A. (l'est, la famille est totalement ordonnée par l'inclusion, en particulier, tous les idéaux sont inclus dans un idéal I_β).

   Soient I et J deux idéaux de A.
3. Somme : La somme de I et J est définie par :

   $$I + J = \{a + b, a \in I, b \in J\}.$$

   $I + J$ est un idéal de A et c'est l'idéal engendré par $I \cup J$.(C-à-d $I + J$ est le plus petit idéal contenant $I \cup J$.)
4. Produit : Le produit de I par J est défini par :

   $$IJ := \{\sum_{fini} a_i b_i, a_i \in I, b_i \in J\}.$$

   IJ est un idéal de A.

Nous avons, $IJ \subseteq I \cap J$.
Si $I + J = A$ (I et J sont étrangés), alors $IJ = I \cap J$.

Définition 1.34. *Soit P un idéal de A. On dit que P est premier si :*

1. *P est un idéal propre de A ($P \neq A$).*
2. *$\forall\, x, y \in A$ on a : $xy \in P \Longrightarrow x \in P$ ou $y \in P$.*

Théorème 1.35. *Dans A, I est premier si et seulement si A/I est un domaine d'intégrité.*

Démonstration. Supposons I premier ; alors $I \neq A$ et par suite A/I est non nul. A/I est un anneau unitaire commutatif, montrons qu'il est intègre. Soit $\overline{x}, \overline{y} \in A/I$, tels que $\overline{xy} = \overline{0}$. $\overline{xy} = \overline{0} \Longleftrightarrow \overline{xy} = \overline{0} \Longleftrightarrow xy \in I$. I étant premier, donc $x \in I$ ou $y \in I$ donc A/I est intègre. On en conclut que A/I est un domaine d'intégrité.
Réciproquement, on suppose que l'anneau A/I est un domaine d'intégrité, nécessairement, A/I est non nul, donc I est un idéal propre de A. Soient x et y dans A tels que $xy \in I$. Dans A/I : $\overline{xy} = \overline{0} \Longrightarrow \overline{x} = \overline{0}$ ou $\overline{x} = \overline{0}$; par suite : $x \in I$ ou $y \in I$. Donc I est premier. □

Corollaire 1.36. *Si A est un anneau unitaire et commutatif, alors A est un domaine d'intégrité si et seulement si (0) est un idéal premier.*

Exemple 1.37. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $n = 0$ ou n est premier. On déduit que les idéaux premiers de $\mathbb{Z}$ sont (0) et les $p\mathbb{Z}$, p premier.*

Définition 1.38. *Le Spectre premier ou seulement Spectre de A, noté par $Spec(A)$, est l'ensemble de tous les idéaux premiers de A.*

Lemme 1.39. *Soient I, J et P des idéaux de A. Si P est premier et si $IJ \subseteq P$, alors $I \subset P$ ou $J \subset P$.*

Démonstration. Si $I \nsubseteq P$, il existe $x \in I$ tel que $x \notin P$. De même, si $J \nsubseteq P$, soit $y \in J$ tel que $y \notin P$. Alors, $xy \in IJ$ mais P étant premier, $xy \notin P$. Par suite $IJ \nsubseteq P$. □

Proposition 1.40. *Soit A un anneau. Alors on a :*

1. *Soient $P_1, ..., P_n$ des idéaux premiers de A et I un idéal de A. Si $I \subseteq \bigcup_{i=1}^{n} P_i$ pour un certain $n \in \mathbb{N}^*$, alors $I \subseteq P_{i_0}$ pour un certain $i_0 = 1, ..., n$.*
2. *Soient $I_1, ..., I_n$ des idéaux de A et P un idéal premier de A. Si $\bigcap_{i=1}^{n} I_i \subseteq P$, alors $I_{i_0} \subseteq P$ pour un certain $i_0 = 1, ..., n$.*

Démonstration. 1. Par induction sur n sous la forme : $I \nsubseteq P_i\ \forall i \Rightarrow I \nsubseteq \bigcup_{i=1}^{n} P_i$.

– $n = 1$, c'est clair.

– Supposons que l'hypothèse de récurrence est vraie pour $n-1$. On a $\forall i = 1, ..., n$ et $\forall j \neq i$ (avec $j = 1, ..., n$), on peut supposer que $I \nsubseteq \bigcup_{j=1, j\neq i}^{n} P_j$ (car sinon, l'hypothèse de récurrence donne le résultat). Ainsi $\exists x_i \in I \setminus \bigcup_{j=1, j\neq i}^{n} P_j$ pour tout $i = 1, ..., n$. Deux cas se posent :

– Cas 1. $x_i \notin P_i$ pour un certain i. Dans ce cas, on a $x_i \notin \bigcup_{j=1}^{n} P_j$ puisque $x_i \notin P_i$ et $x_i \notin \bigcup_{j=1, j\neq i}^{n} P_j$. Ainsi on a $x_i \in I \setminus \bigcup_{j=1}^{n} P_j$ puisque $x_i \in I$.

– Cas 2. $x_i \in P_i$, $\forall i = 1, ..., n$. Alors soit $y = \sum_{i=1}^{n} x_1...x_{i-1}x_{i+1}...x_n = x_2...x_n + x_1x_3x_4...x_n + x_1x_2...x_{n-1}$. On a $y \notin P_i$ et par suite $y \notin \bigcup_{i=1}^{n} P_i$. D'où $y \in I \setminus \bigcup_{i=1}^{n} P_i$.
Ainsi, dans tous les cas on a $I \nsubseteq \bigcup_{i=1}^{n} P_i$.

2. Par contraposée sous la forme : $I_i \nsubseteq P \ \forall i = 1, ..., n \Rightarrow \bigcap_{i=1}^{n} I_i \nsubseteq P$.
Soit $x_i \in I_i \setminus P$ pour tout $i = 1, ..., n$. On a $\prod_{i=1}^{n} x_i \in I_1I_2...I_n \subseteq \bigcap_{i=1}^{n} I_i$, or $\prod_{i=1}^{n} x_i \notin P$ (puisque $x_i \notin P \ \forall i = 1, ..., n$ et P est un idéal premier). D'où le résultat. ■

□

Corollaire 1.41. *P étant un idéal premier de A, pour tout $n \in \mathbb{N}*$:*
1) $(x \in A$ et $x^n \in P) \Longrightarrow x \in P$.
2) (I idéal de A et $I^n \subseteq P \Longrightarrow$) $I \subseteq P$.

1.4.2 Idéaux maximaux d'un anneau unitaire

Définition 1.42. *I est un idéal bilatère maximal d'un anneau A, si*

1. *I est un idéal bilatère propre de A.*
2. *(J idéal bilatère de A et $I \subseteq J \subseteq A) \Longrightarrow J = I$ ou $J = A$.*

Théorème 1.43. *Dans un anneau unitaire et commutatif A, on a :*
I est un idéal maximal si et seulement si A/I est un corps.

Démonstration. Si A/I est un corps, on a nécessairement $I \neq A$. D'autre part, supposons J idéal de A tel que $I \subsetneq J$; alors J/I est un idéal non nul du corps A/I, donc $J/I = A/I$. Par suite $J = A$, donc I est un idéal maximal de A. Réciproquement, soit I un idéal maximal de A, alors A/I est non nul et c'est un anneau unitaire commutatif ; la maximalité de I implique que A/I n'a pas d'autre idéal que (0) et A/I, donc A/I est un corps. □

$\longrightarrow$ Dans tout corps K, (0) est le seul idéal maximal.

Corollaire 1.44. *Pour un idéal I d'un anneau unitaire commutatif A, on a I maximal $\Longrightarrow I$ premier.*

Démonstration. Il suffit de voir que I maximal $\Longrightarrow A/I$ est un coprs $\Longrightarrow A/I$ est un domaine d'intégrité $\Longrightarrow I$ est premier.

□

$\longrightarrow$ La réciproque du corollaire est fausse. Par exemple, dans $\mathbb{Z}$, (0) est un idéal premier qui n'est pas maximal.
Nous avons le résultat suivant :

Théorème 1.45. *(Exercice) Dans un domaine principal tout idéal premier non nul est maximal.*

Lemme 1.46. *(Axiome de Zorn) Tout ensemble non vide, partiellement ordonné et inductif, a au moins un élément maximal.*

Théorème 1.47. *Tout anneau unitaire a au moins un idéal bilatère (resp. à gauche, à droite) maximal.*

Démonstration. Soit Σ l'ensemble de tous les idéaux propres de A. Σ est ordonné par inclusion.
Soit $\{I_\alpha\}_\alpha$ une chaîne d'éléments de Σ et posons $I = \cup_\alpha I_\alpha$. On a $I \in \Sigma$, en effet :
• $I \neq A$ car si $I = A$, alors $1 \in I = \cup_\alpha I_\alpha$ et par suite il existe α tel que $1 \in I_\alpha$ de sorte que $I_\alpha = A$, absurde. Donc $I \neq A$.
• I est un idéal, en effet :
Soient x et $y \in I$. Alors il existe α_1, α_2 tels que $x \in I_{\alpha_1}$ et $y \in I_{\alpha_2}$. Comme $\{I_\alpha\}_\alpha$ est une chaîne, alors $x, y \in I_{sup(\alpha_1,\alpha_2)}$ et par suite $x - y \in I_{sup(\alpha_1,\alpha_2)} \subseteq I$.
Soient $x \in I$ et $a \in A$. Alors $x \in I_\alpha$ pour un certain α et par suite $ax \in I_\alpha \subseteq I$.
• Ainsi $\Sigma \neq \emptyset$ (car $(0) \in \Sigma$) et toute chaîne de Σ admet un élément maximal.
D'après le lemme de Zorn, Σ admet un élément maximal de A. Si M est cet élément maximal, il est naturellement un idéal maximal de A. □

Corollaire 1.48. *Tout idéal propre de A est contenu dans un idéal maximal.*

Démonstration. Soit I un idéal propre de A. Considèrons l'anneau quotient A/I. D'après le théorème 1.47, A/I admet au moins un idéal maximal N. Or, $N = M/I$, où M est un idéal de A contenant I. Ainsi, M est un idéal maximal contenant I (car sinon, $N = M/I$ ne serait pas maximal dans A/I). □

Définition 1.49. *On appellera anneau local tout anneau unitaire commutatif n'ayant qu'un seul idéal maximal.*

$\longrightarrow$ Tout corps est un anneau local. La réciproque est fausse.

1.5 Nilradical et Radical de Jacobson

***A* est un anneau unitaire commutatif.** Un élément non nul $a \in A$ est dit nilpotent si $a^n = 0$ pour un certain $n \in \mathbb{N}^*$.

Remarque 1.50. *Tout élément nilpotent est un diviseur de zéro. La réciproque est fausse car* 3 *est un diviseur de zéro dans* $\mathbb{Z}/6\mathbb{Z}$ *mais n'est pas nilpotent.*

Proposition 1.51. *L'ensemble $N(A)$ de tous les éléments nilpotents de A est un idéal de A et $A/N(A)$ n'admet aucun élément nilpotent autre que zéro.*

Démonstration. Montrons que $N(A)$ est un idéal de A.
- On a $N(A) \neq \varnothing$ car $0 \in N(A)$.
- Soient $x \in N(A)$ et $a \in A$. Alors il existe $n \in \mathbb{N}^*/x^n = 0$. Ainsi on a, $(ax)^n = a^n x^n = 0$ (car A est commutatif) et par suite $ax \in N(A)$.
- Soient x et $y \in A$. Alors il existe $n_1 \in \mathbb{N}^*/x^{n_1} = 0$ et $n_2 \in \mathbb{N}^*/y^{n_2} = 0$. Ainsi on a $(x-y)^{n_1+n_2} = \sum_{p=0}^{n_1+n_2} C^p_{n_1+n_2} x^p (-y)^{n_1+n_2-p} = 0$.
  Dés lors, $N(A)$ est un idéal de A. Montrons que $A/N(A)$ n'admet aucun élément nilpotent.

- Soit $\overline{a}$ un élément nilpotent de $A/N(A)$, où $a \in A$. Il existe alors $n \in \mathbb{N}^*$ tel que $\overline{a}^n = \overline{0}$; c'est à dire que $a^n \in N(A)$. Dés lors, il existe $m \in \mathbb{N}^*$ tel que $(a^n)^m (= a^{nm}) = 0$ de sorte que $a \in N(A)$ et $\overline{a} = \overline{0}$ dans $A/N(A)$.

□

Proposition 1.52. *On a :*

$$N(A) = \bigcap_{P \in Spec(A)} P$$

est appelé le nilradical de A.

Démonstration. Soient $x \in N(A)$ et $P \in Spec(A)$. Comme il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$ $(\in P)$ et P est premier, alors $x \in P$.
Inversement, soit $x \in \bigcap_{P \in Spec(A)} P$. Supposons que $x \notin N(A)$ et considèrons :
$\Sigma = \{\text{Idéaux } I \text{ de } A / n \geqslant 1 \Rightarrow x^n \notin I\}$.
En appliquant le lemme de Zorn à Σ, l'élément (c'est à dire l'idéal) maximal de Σ donne la contradiction. D'où le résultat. □

Remarque 1.53. *Si A est un domaine d'intégrité, alors son nilradical est nul, car (0) étant un idéal premier, $\bigcap_{P \in Spec(A)} P = (0)$; mais la réciproque est fausse.*
En effet, $N(A/N(A)) = (0)$ est nul, cependant $A/N(A)$ n'est pas nécessairement intègre, car $N(A)$ n'est pas nécessairement premier.

Définition 1.54. *Le radical de Jacobson, noté $J(A)$, est défini comme étant l'intersection de tous les idéaux maximaux de A :*

$$J(A) = \bigcap_{\mathcal{M} \in max(A)} \mathcal{M}.$$

Proposition 1.55. *On a :*

$$[x \in J(A)] \Longleftrightarrow [1 - xy \in \mathrm{U}(A),\ \forall y \in A]$$

où $\mathrm{U}(A)$ *est le groupe multiplicatif des éléments inversibles de* A.

Démonstration. Soit $x \in J(A)$. Supposons qu'il existe $y \in A$ tel que $1-xy \notin U(A)$. Donc $(1-xy)A \subsetneq A$ et par suite il existe un idéal maximal M tel que $(1-xy)A \subseteq M \subsetneq A$. Ainsi on a $1-xy \in M$ et donc $1 \in M$ (car $x \in M$ puisque $x \in J(A)$) ; c'est à dire que $M = A$, absurde. Et on a $(1-xy) \in U(A)$ pour tout $y \in A$.

Inversement, supposons que $(1-xy) \in U(A)$, pour tout $y \in A$. Par absurde, supposons que $x \notin J(A)$. Donc, il existe $M \in max(A)$ tel que $x \notin M$. Dès lors, on a $M + Ax = A$ car $M \subsetneq M + Ax$ et M est maximal . Ainsi, il existe $y \in A$ et $m \in M$ tels que $1 = m + yx$ et par suite $1 - xy(= m) \notin U(A)$, absurde. Par conséquent, $x \in J(A)$ est cela termine la preuve de la proposition. □

Définition 1.56. *Un anneau* A *est dit* <u>local</u> *s'il admet un seul idéal maximal.*
Dans un anneau local, on a $J(A) = M$ *et :*

$$x \in M \Leftrightarrow (1 - xy \in U(A)\ \forall y \in A)$$

1.6 Anneau de fraction

Dans ce qui suit, A est un anneau unitaire commutatif.

Définition 1.57. *Soit* S *une partie non vide de l'anneau* A*, on dit que* S *est une partie multiplicative de* A *si :*

1. $\forall a, b \in S, ab \in S$.
2. $1 \in S$ *et* $0 \notin S$.

Exemple 1.58.

1. *Si* A *est un domaine d'intégrité, alors* $A^* = A\ \{O\}$ *est une partie multiplicative de* A.
2. *Les éléments réguliers (non diviseurs de zéro) de* A *est une partie multiplicative de* A*. Lorsque* A *est intègre, les éléments réguliers sont les éléments non nuls.*
3. *Si* P *est un idéal premier de* A*, alors* $S = A\ P$ *est une partie multiplicative de* A.
4. *Pour tout* $x \in A^*$, $S = \{x^n; n \in \mathbb{N}\}$ *est une partie multiplicative de* A.
5. *Pour tout idéal non nul* I *de* A, $S = 1 + I = \{1 + x; x \in I\}$ *est une partie multiplicative de* A.
6. U_A *est une partie multiplicative de* A.

Soit S une partie multiplicative de A, on définie une relation sur $S \times A$ par :

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

C'est une relation d'équivalence. En effet :
Il est visible que $\sim$ est réflexive et symétrique. Pour la transitivité, si $(a, s) \sim (\acute{a}, \acute{s})$ et $(\acute{a}, \acute{s}) \sim (a'', s'')$ alors on a :
$(as' - a's)t = 0$, et$(a's'' - a''s')t' = 0$ pour certains $t, t' \in S$. On a donc :

$$(as'' - sa'')s't't' = as's''tt' - sa's''tt' + sa's''tt' - sa''s'tt' = 0 + 0 = 0.$$

On obtient alors une relation d'équivalence.
On note par $\frac{a}{s}$ la classe d'équivalence de (a, s) qu'on appelle fraction. L'ensemble quotient $A \times S := \{\frac{a}{s}, a \in A, s \in S\}$ sera noté $S^{-1}A$. On définit l'addition et la multiplication par :

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'}$$

et

$$\frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'}.$$

On vérifie facilement que + et $\times$ sont bien définies :
Puisque S et une partie multiplicative, $\frac{as'+sa'}{ss'}$ et $\frac{aa'}{ss'}$ sont des élément de $S^{-1}A$.
Si $\frac{a}{s} = \frac{b}{c}$, $\frac{a'}{s'} = \frac{b'}{c'}$, on doit montrer que : $\frac{as'+sa'}{ss'} = \frac{bc'+cb'}{cc'}$ et $\frac{aa'}{ss'} = \frac{bb'}{cc'}$.
$\frac{a}{s} = \frac{b}{c}$ et $\frac{a'}{s'} = \frac{b'}{c'} \Longrightarrow \exists t, t' \in S$ tel que $t(ac - bs) = 0$ et $t'(s'c' - s'b') = 0$ donc $ts'c'(ac - bs) = 0$ et $t'sc(s'c' - s'b') = 0$ donc

$$tt'(cc'(as' + sa') - ss'(bc' + cb')) = c's'tt'(ac - sb) + cstt'(c'a' - s'b') = 0 + 0 = 0.$$

Montrons qu'il existe $\lambda \in S$ tq $\lambda(aa'cc' - ss'bb') = 0$. Prenons $\lambda = tt'$,

$$tt'(aa'cc' - ss'bb') = tt'((ac(a'c' - s'b) + (acs'b' - sbs'b')) = tt'(ac(a'c' - s'b')) + tt'(s'b'(ac - sb)) = 0 + 0 = 0.$$

Ainsi, + et $\times$ définissent deux lois de composition internes dans $S^{-1}A$. Les éléments $\frac{0}{1}$ et $\frac{1}{1}$ sont, respectivement, éléments neutres pour l'addition et la multiplication dans $S^{-1}A$. L'ensemble $S^{-1}A$ muni d'une structure d'anneau unitaire et commutatif induite par celle de A.
L'homomorphisme

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & S^{-1}A \\ & a & \longrightarrow & a/1 \end{array}$$

applique les éléments de S sur les unités de $S^{-1}A$, on dit que φ est $\underline{S - inversant}$. ($\forall s \in S, \varphi(s) = \frac{s}{1}$ est inversible dans $S^{-1}A$)

Définition 1.59. *L'anneau $S^{-1}A$ est appelé $\underline{anneau\ des\ fractions\ de\ A\ par\ rapport}$ à $\underline{S}$.*

$S^{-1}A$ possède la propriété universelle suivante :

L'homomorphisme

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & S^{-1}A \\ & a & \longrightarrow & a/1 \end{array}$$

applique les éléments de S sur les unités de $S^{-1}A$, on dit que φ est $\underline{S - inversant}$.

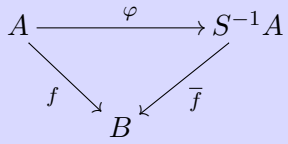
Définition 1.60. *L'anneau $S^{-1}A$ est appelé $\underline{anneau\ des\ fractions\ de\ A\ par\ rapport}$ à $\underline{S}$.*

$S^{-1}A$ possède la propriété universelle suivante :

Théorème 1.61. *Soient A un anneau et S une partie multiplicative de A. Pour tout anneau unitaire, commutatif B et le morphisme d'anneaux unitaires $f : A \longrightarrow B$ vérifiant $f(S) \subseteq U_B$, il existe un unique homomorphisme :*

$$\overline{f} : S^{-1}A \longrightarrow B$$

tel que $\overline{f} o \varphi = f$.



Démonstration. Soit $f : A \longrightarrow B$ un homomorphisme $S-$inversant. Considèrons :

$$\begin{array}{rccc} \overline{f} : & S^{-1}A & \longrightarrow & B \\ & \frac{a}{s} & \longrightarrow & \dfrac{f(a)}{f(s)} = f(a).(f(s))^{-1}. \end{array}$$

• Montrons que $\overline{f}$ est bien défini :
Soit $\frac{a}{s} = \frac{a^{'}}{s^{'}} \in S^{-1}A$. On doit montrer que $\overline{f}(\frac{a}{s}) = \overline{f}(\frac{a^{'}}{s^{'}})$.

Comme on a $\frac{a}{s} = \frac{a^{'}}{s^{'}}$, alors $(as^{'} - a^{'}s)t = 0$ pour un certain $t \in S$ de sorte que $(f(a)f(s^{'}) - f(a^{'})f(s))f(t) = 0$. Or, comme $f(t)$ est inversible (car f est un homomorphisme S-inversant et $t \in S$), alors $f(a)/f(s) = f(a^{'})/f(s^{'})$ et par suite $f(a)f(s)^{-1} = f(a^{'})f(s^{'})^{-1}$. D'où $\overline{f}(a/s) = \overline{f}(a^{'}/s^{'})$.

• Pour tout $x \in A$, on a $\overline{f} \circ \varphi(x) = \overline{f}(\varphi(x)) = \overline{f}((x/1) = f(x)f(1)^{-1} = f(x)1_B = f(x)$. D'où $\overline{f} \circ \varphi = f$.
• Montrons que $\overline{f}$ est unique :

Supposons qu'il existe deux homomorphismes $\overline{f}$ et $\overline{g}$ tels que $\overline{f} \circ \varphi = \overline{g} \circ \varphi = f$. Alors on a :
$* \; \forall\, x \in A$, $\overline{f}(x/1) = \overline{f} \circ \varphi(x) = \overline{g} \circ \varphi(x) = \overline{g}(x/1)$.
$* \; \forall\, s \in S$, $\overline{f}(1/s) = f(1)f(s)^{-1} = 1_B(f(s))^{-1} = (f(s))^{-1}$.
D'où :

$$\begin{aligned} \overline{f}(x/s) &= \overline{f}((x/1)(1/s)) \\ &= \overline{f}((x/1))(f(s))^{-1} \\ &= \overline{g}((x/1))(f(s))^{-1} \\ &= \overline{g}(x/1)(\overline{g} \circ \varphi(s))^{-1} \\ &= \overline{g}(x/1)(\overline{g}(s/1))^{-1} \\ &= \overline{g}(x/1)\overline{g}(1/s) \\ &= \overline{g}(((x/1)(1/s)) \\ &= \overline{g}(x/s). \end{aligned}$$

D'où $\overline{g} = \overline{f}$.
Montrons que $\overline{f}$ est un morphisme d'anneaux unitaire.

Soient $\frac{a}{s}$, $\frac{a'}{s'} \in S^{-1}A$, on a

$$\begin{aligned}\overline{f}(\frac{a}{s}+\frac{a'}{s'}) &= \overline{f}(\frac{as'+a's}{ss'}) = f(as'+a's)f(ss')^{-1}\\ &= f(a)f(s)^{-1}+f(a')f(s')^{-1}\\ &= \overline{f}(\frac{a}{s})+\overline{f}(\frac{a'}{s'}).\end{aligned}$$

$$\begin{aligned}\overline{f}(\frac{a}{s}\frac{a'}{s'}) &= f(aa')f(ss')^{-1} = f(a)f(a')f(s)^{-1}f(s')^{-1}\\ &= f(a)f(s)^{-1}f(a')f(s')^{-1}\\ &= \overline{f}(\frac{a}{s})\overline{f}(\frac{a'}{s'}).\end{aligned}$$

D'autre part, $\overline{f}(\frac{1}{1}) = f(1)f(1)^{-1} = 1_B$. □

Remarque 1.62. *1. Il est clair que l'homomorphisme $\varphi : A \longrightarrow S^{-1}A$ est injectif si et seulement si S ne contient pas de diviseurs de zéro.*

2. Si A est un domaine d'intégrité et $S = A\backslash\{0\}$, alors $S^{-1}A$ est le corps des fractions de A.

3. Si S est la partie des éléments non diviseurs de zéro, alors $S^{-1}A$ s'appelle l'anneau total des fractions de A noté $T(A)$.

Exemple 1.63. *1. <u>Localisation :</u>*

Soit P un idéal premier de A. On a $S = A\backslash P$ est une partie multiplicative de A. Dans ce cas on note $S^{-1}A$ par A_P. Les éléments de a/s où $a \in P$ et $s \in S$ forment un idéal M de A_P. Si $a/s \notin M$ alors $a \notin P$ et par suite $1/a \in A_P$ et donc $s/a \in A_P$. Donc $a/s \in U(A_P)$ de sorte que M est l'unique idéal maximal de A_p. Ainsi on a :

$$M = PA_P = \{a/s \, telque \, a \in P \, et \, s \in S = A\backslash P\}.$$

A_P est appelé <u>anneau local en P</u> ou <u>localisation de A en P</u>.

▶ Ne pas confondre A/P qui annule tous les éléments de P et A_P qui inverse tous les éléments de $A\backslash P$.

2. Soit $0 \neq s \in A$ tel que s est non nilpotent (sinon $0 \in S$). L'ensemble $S = \{s^n / \, n \in \mathbb{N}\}$ est une partie multiplicative de A. En particulier si $A = \mathbb{Z}$ et $s = 10$, alors $S^{-1}A = \mathbb{D}$ est l'anneau des nombres décimaux.

Proposition 1.64. *Soient A un anneau et S une partie multiplicative de A.*

1. Si I est un idéal de A, l'ensemble des fractions a/s où $a \in I$ et $s \in S$ est l'idéal de $S^{-1}A$ engendré par $\varphi(I)$ et est noté $S^{-1}I$ (ou I_S) :

$$S^{-1}I = \{\frac{a}{s}; a \in I \, et \, s \in S\}.$$

2. *Soit I un idéal propre de A. On a :*

$$I_S \neq S^{-1}A \Longleftrightarrow S \cap I = \emptyset.$$

3. *Soient I_1 et I_2 deux idéaux de A. Alors on a :*

$$S^{-1}(I_1 I_2) = S^{-1}I_1 . S^{-1}I_2.$$

4. *Pour tout idéal J de $S^{-1}A$, on a :*

$$S^{-1}(\varphi^{-1}(J)) = J.$$

5. *Pour tout idéal I de A, on a :*

$$(I_S)_S \supseteq I.$$

On obtient l'égalité si et seulement si aucun élément de S n'est diviseur de zéro modulo A/I.

6. *Les idéaux premiers de $S^{-1}A$ sont en correspondance bijective avec les idéaux premiers de A ne rencontrant pas S.*

Démonstration. 1) Soient $\frac{a}{s}$ et $\frac{a'}{s'}$ dans I_S, $a, a' \in I$. On a $\frac{0}{1} \in I_S$ et $\frac{a}{s} - \frac{a'}{s'} = \frac{as'-a's}{ss'} \in I_S$. Soit $\frac{a''}{s''} \in S^{-1}A$, $\frac{a}{s}.\frac{a'}{s'} = \frac{aa'}{ss'} \in I_S$, donc I_S est un idéal de $S^{-1}A$.
Montrons que $I_S = (\varphi(I)) = \{_{finie}\frac{a_i}{1}\frac{x_i}{s_i}, a_i \in I, \frac{x_i}{s_i} \in S^{-1}A\}$. Soit $\frac{a}{s} \in I_S$, alors $\frac{a}{s} = \frac{a}{1}.\frac{1}{s}$, $\frac{a}{1} = \varphi(a)$ et $\frac{1}{s} \in S^{-1}A$, d'où $I_S \subseteq (\varphi(I))$
Soit $x \in (\varphi(I))$, alors $x = \sum\limits_{finie} \frac{a_i}{1}\frac{x_i}{s_i}$, $\frac{a_i}{1} \in (\varphi(I))$ et $\frac{b_i}{s_i} \in S^{-1}A$. On a $a_i \in I$ et $b_i \in A \Longrightarrow a_i b_i \in I$ donc $\frac{a_i b_i}{s_i} \in I_S$, d'où $x \in I_S$ donc $\varphi(I) \subseteq I_S$.
2) Montrons que $I_S \neq S^{-1}A \Longleftrightarrow S \cap I = \emptyset$. $I_S \neq S^{-1}A \Longrightarrow S \cap I = \emptyset$. Sinon $\exists s \in I \cap S$ donc $\frac{s}{s} \in I_S$ c-à-d $1 \in I_S$. D'où, $I_S = S^{-1}A$. Inversement, si $S \cap I = \emptyset \Longrightarrow I_S \not= S^{-1}A$. Sinon, $I_S = S^{-1}A$ implique que $\frac{1}{1} \in S^{-1}I \Longleftrightarrow \exists (a, s) \in S \times A, \frac{a}{s} = \frac{1}{1}.\ \frac{a}{s} = \frac{1}{1} \Longleftrightarrow \exists t \in S, ta = ts$ donc $ts \in I \cap S \Longrightarrow I \cap S \neq \emptyset$, absurde.
3) Soit $\frac{a}{s} \in (IJ)_S$. On suppose $a \in IJ$ donc $a = \sum\limits_{finie} x_i y_i$ $\frac{a}{s} = \sum\limits_{finie} \frac{x_i y_i}{1s} \in I_S J_S \Longrightarrow (IJ)_S \subseteq I_S J_S$.
Soit $x \in I_S J_S$ tel que $x = \sum_{finie} \frac{a_i b_i}{s_i t_i}$, $\frac{a_i}{s_i} \in I_S$ et $\frac{b_i}{t_i} \in J_S$. On alors $x = \frac{\sum_{finie} a_i b_i \prod s_i t_i}{\prod s_i t_i} \in (IJ)_S$, donc $I_S J_S \subseteq IJ)_S$.
4) Montrons que pour tout idéal J de $S^{-1}A$, on a $S^{-1}(\varphi^{-1}(J)) = J$. $S^{-1}(\varphi^{-1}(J)) = (\varphi\varphi^{-1}(J))$, or $\varphi \circ \varphi^{-1}(J) \subseteq J$, donc $S^{-1}(\varphi^{-1}(J)) = (\varphi \circ \varphi^{-1}(J)) \subseteq J$. Inversement, soit $\frac{x}{b} \in J$, alors $\frac{x}{1} = \frac{x}{1}.\frac{b}{1} \in J$. Ainsi, $x = \varphi^{-1} \in \varphi^{-1}(J)$, d'où $\frac{x}{b} \in S^{-1}\varphi(J))$. Ainsi, $J \subseteq S^{-1}\varphi^{-1}(J)$.
6) Soit

$$\begin{array}{rccc} f: & \{\textit{idéaux premiers } Q \textit{ de } A \ / \ S \cap Q = \emptyset\} & \longrightarrow & \{\textit{idéaux premiers de } S^{-1}A\} \\ & Q & \longmapsto & S^{-1}Q \end{array}$$

• On vérifie que f est une application. En effet, $S^{-1}Q$ est un idéal de $S^{-1}A$ d'après 1). D'autre part, comme on a $Q \cap S = \emptyset$, alors $S^{-1}Q \neq S^{-1}A$; c'est à dire que $S^{-1}Q$ est un idéal propre de $S^{-1}A$ d'après 2).
• Montrons que f est bien définie :

Soit Q un idéal premier de A tel que $S \cap Q = \emptyset$. On doit montrer que $S^{-1}Q$ est un idéal premier de $S^{-1}A$. Soient $x, y \in S^{-1}A$ tels que $xy \in S^{-1}Q$ et montrons que x ou $y \in S^{-1}Q$. Posons $x = a/s$ et $y = b/t$ où $a, b \in A$ et $s, t \in S$. On a $(a/s)(b/t) \in S^{-1}Q$ c'est à dire que $(ab)/(st) \in S^{-1}Q$, et par suite on a $(ab)/(st) = c/\mu$ où $c \in Q$ et $\mu \in S$.
Donc $(\mu ab - cst)\lambda = 0$ pour un certain $\lambda \in S$ de sorte que $\lambda\mu ab = cst\lambda \in Q$. Or $Q \cap S = \emptyset$, d'où λ et $\mu \notin Q$. Ainsi $ab \in Q$ et donc $a \in Q$ ou $b \in Q$ puisque Q est un idéal premier de A. Ainsi on a $x = a/s \in S^{-1}Q$ ou $y = b/t \in S^{-1}Q$, et donc $S^{-1}Q$ est premier. Cela implique que f est bien définie.
• f est clairement surjective. En effet, soit N un idéal premier de $S^{-1}A$ et $\varphi^{-1}(N)$ l'idéal premier de A. On a $S^{-1}(\varphi^{-1}(J)) = N$ d'après 4). Posons alors. $Q = \varphi^{-1}(N)$. On a donc $f(Q) = S^{-1}Q = S^{-1}(\varphi^{-1}(N)) = N$.
• f est injective :
Soient P et Q deux idéaux premiers de A tels que $P \cap S = Q \cap S = \emptyset$ et $f(P) = f(Q)$; c'est à dire que $S^{-1}P = S^{-1}Q$. On doit montrer que $P = Q$.
Soit $x \in P$. On a $x/1 \in S^{-1}P = S^{-1}Q$, et par suite on a $x/1 = a/s$ où $a \in Q$ et $s \in S$. Donc $(sx - a)t = 0$ pour un certain $t \in S$, d'où $stx = at \in Q$. Or $s, t \notin Q$, alors $x \in Q$, ce qui montre que $P \subseteq Q$. De même on montre que $Q \subseteq P$ et par suite $P = Q$, d'où f est injective. Enfin f est bijective et cela achève la preuve. ■

□

Théorème 1.65. *Soit P un idéal premier d'un anneau unitaire commutatif A alors le localisé de A en P, noté A_P est un anneau local, dont l'unique idéal maximal est P_S, où $S = A\backslash P$.*

Démonstration. P est premier dans A et $P \cap S = \emptyset$, donc $S^{-1}P \in Sepc(A_P)$. A_P est un anneau unitaire, commutatif donc il contient au moins un idéal maximal M. M est premier, donc il existe $Q \in Spec(A)$, $Q \cap S = \emptyset$ tel que $M = Q_S$ or $Q \cap S = \emptyset$ et $S = A\backslash P \Longrightarrow Q \subseteq P \Longrightarrow M = Q_S \subseteq P_S$. Donc, $M = P_S$.
Soit $\frac{a}{s} \in A_p \setminus M \Longrightarrow a \notin P \Longrightarrow a \in S$. $\frac{a}{s} = \frac{a}{1}.\frac{1}{s}$ inversible car $\varphi(S) \subseteq U_{S^{-1}A}$ ($\frac{a}{s}\frac{s}{a} = \frac{1}{1}$).

□

Proposition 1.66. *Soient I un idéal d'un anneau commuatif unitaire A et S une partie multiplicative de A. Alors $\pi(S) = \overline{S}$ est une partie multiplicative de A/I et $S^{-1}A/S^{-1}I \simeq \overline{S^{-1}}(A/I)$.*

CHAPITRE 2

Modules

Le concept de Module est une généralisation de la notion d'espace vectoriel sur un corps $\mathbb{K}$ en remplaçons le corps $\mathbb{K}$ par un anneau A.
Soit A un anneau unitaire.

Définition 2.1. *un A-module à gauche est un ensemble non vide muni*

1. *d'une loi de composition interne notée, en général, additivement et telle que $(M,+)$ est un groupe abélien ;*
2. *d'une loi de composition externe à opérateurs dans l'anneau A :*

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,x) & \longrightarrow & a.x \end{array}$$

vérifiant les conditions suivantes :

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

ii) $\forall x \in M, \forall (a,b) \in A \times A,\ a.(bx) = (ab).x,$ *noté* $abx.$

iii) $\forall a \in A, \forall (x,y) \in M, \times M\ a(x+y) = ax + ay.$

iv) $\forall x \in M,\ 1_A x = x.$

On définit de même la notion de module à droite.

Définition 2.2. *un A-module à droite est un ensemble non vide muni*

1. *d'une loi de composition interne notée, en général, additivement et telle que $(M,+)$ est un groupe abélien ;*
2. *d'une loi de composition externe à opérateurs dans l'anneau A :*

$$\begin{array}{ccc} M \times A & \longrightarrow & M \\ (x,a) & \longrightarrow & x.a \end{array}$$

vérifiant les conditions suivantes :

i) $\forall x \in M, \forall (a,b) \in A \times A,\ x.(a+b) = xa + xb.$

ii) $\forall x \in M, \forall (a,b) \in A \times A,\ (xb).a = x(ba),$ *noté* $xba.$

iii) $\forall a \in A, \forall (x,y) \in M, \times M\ (x+y)a = xa + ya.$

iv) $\forall x \in M,\ x1_A = x.$

Définition 2.3. *A et B étant deux anneaux unitaires, on dira que M est un $A-B$-bimodule, si M est à la fois un A-module à gauche et un B-module à droite vérifiant la condition :*

$$\forall x \in M, \forall (a,b) \in A \times B,\ (ax)b = a(xb),\ \textit{noté } axb.$$

Lemme 2.4. *Si A est commutatif, alors A-module à droite est aussi un A-module à gauche, et réciproquement. Dans ce cas, on dit seulement que M est un A-module.*

Démonstration. Supposons que M est un A-module à droite, muni de la loi externe

$$\begin{array}{ccc} M \times A & \longrightarrow & M \\ (x,a) & \longrightarrow & x.a = ax. \end{array}$$

Montrons que ceci définit une structure de A-module à gauche sur M. On a $i), iii) et iv)$ sont évidents. Soient $a, b \in A$ et $x \in M$: $a.(bx) = a.(xb) = (xb).a = x(ba) = x(ab) = (ab)x$. La réciproque se démontre de façon analogue. □

Exemple 2.5.

1. *Tout anneau unitaire A est un A-module à gauche et à droite ($a.x = ax$ et $x.a = xa$).*
2. *Si $A := k$ est un corps, la structure de A-module est exactement celle de A-espace vectoriel. Les propriétés élémentaires des espaces vectoriels s'étendent aux A-modules ($0.x = 0$, $(-a)x = -ax$, ...).*
3. *Si $A = \mathbb{Z}$ et $(M, +)$ est un groupe abélien, M est muni d'une structure de $\mathbb{Z}$-module à travers la loi externe :*

$$\begin{array}{ccc} \mathbb{Z} \times M & \longrightarrow & M \\ (n,x) & \longrightarrow & nx = \underbrace{x + ... + x.}_{n fois} \end{array}$$

   Ainsi, il n'y a aucune différence entre la structure de $\mathbb{Z}$-module et celle du groupe abélien, par suite tout anneau unitaire A est un $\mathbb{Z}$-module à gauche, tout A-module à gauche est un $\mathbb{Z}$-module à gauche.
4. *Si I est un idéal de A, alors I est un A-module à travers la loi externe :*

$$\begin{array}{ccc} A \times I & \longrightarrow & I \\ (a,x) & \longmapsto & ax. \end{array}$$

5. *Soient B un anneau et A un sous-anneau de B. L'anneau B est de manière naturelle un A-module à travers la loi externe :*

$$\begin{array}{ccc} A \times B & \longrightarrow & B \\ (a,b) & \longrightarrow & ab. \end{array}$$

6. *Soient K un corps et E un K-e.v. Soit $A = End(E)$. A est un anneau non commutatif si $dimE > 1$. E est un A-module à gauche via :*

$$\begin{array}{ccc} A \times E & \longrightarrow & E \\ (\phi, v) & \longmapsto & \phi(v). \end{array}$$

2.1 Sous-Module

Définition 2.6. *Soit M un A-module à gauche. une partie non vide N de M est un sous-module (plus précisément, un sous-A-module) de M, si*

1. *N est un sous groupe de $(M,+)$;*
2. *Pour tout $x \in N$ et tout $a \in A$, $ax \in N$.*

Exemple 2.7. *1. (0) et M sont des sous-modules de M.*

2. Les sous-modules du A-module à gauche A (resp. à droite) sont les idéaux à gauche (resp. à droite) de l'anneau A.

Proposition 2.8. – *Soit $(N_i)_{i\in I}$ une famille non vide de sous-modules d'un A-module M ; alors, $\bigcap_{i\in I} N_i$ est un sous-module de M.*
– *$\bigcup_{i\in I} N_i$ n'est pas, en général, un sous-module de M. Si la famille $(N_i)_{i\in I}$ est totalement ordonnée par l'inclusion, alors $\bigcup_{i\in I} N_i$ est un sous-module de M.*

Démonstration. - On a $(N_i,+)$ est un groupe pour tout $i \in I$ donc $0 \in N_i$ pour tout $i \in I$, ainsi $0 \in \bigcap_{i\in I} N_i$. Donc $\bigcap_{i\in I} N_i \neq \emptyset$.
Soient $x, y \in \bigcap_{i\in I} N_i \Longrightarrow x \in N_i$ pour tout $i \in I$. Donc $x - y \in N_i$ pour tout $i \in I \Longrightarrow x - y \in \bigcap_{i\in I} N_i$.
Soient $a \in A$ et $x \in \bigcap_{i\in I} N_i \Longrightarrow a \in A$ et $x \in N_i$ pour tout $i \in I \Longrightarrow ax \in N_i$ pour tout $i \in I$. Donc $ax \in \bigcap_{i\in I} N_i$. D'où, $\bigcap_{i\in I} N_i$ est un sous-module de A.

- Si la famille $(N_i)_{i\in I}$ est totalement ordonnée par l'inclusion, alors $\bigcup_{i\in I} N_i \neq \emptyset$.
Soient $x, y \in \bigcup_{i\in I} N_i$ donc il existe $j, k \in I$ tel que $x \in N_i$ et $y \in N_k$. Or $(N_i)_{i\in I}$ est totalement ordonnée par l'inclusion ce qui donne que $N_i \subset N_k$ ou $N_k \subset N_i$.
Si $N_i \subset N_k$ alors $x, y \in N_k \Longrightarrow x - y \in N_k \Longrightarrow x - y \in \bigcup_{i\in I} N_i$.
Si $N_k \subset N_i$ alors $x, y \in N_i \Longrightarrow x - y \in N_i \Longrightarrow x - y \in \bigcup_{i\in I} N_i$.
Donc $\bigcup_{i\in I} N_i$ est un sous-groupe de M.
Soient $a \in A$, $x \in \bigcup_{i\in I} N_i$, alors $a \in A$ et $x \in N_{i_0}$ avec $i_0 \in I \Longrightarrow ax \in N_{i_0} \Longrightarrow ax \in \bigcup_{i\in I} N_i$.

□

Définition 2.9. *Soit S un sous-ensemble non vide d'un A-module M. L'intersection de tous les sous-modules contenant S est appelé le sous-module engendré par S, souvent noté (S) ou $< S >$. Si M est un A-module à gauche (resp. à droite), on notera ${}_A(S)$ (resp. $(S)_A$).*

Proposition 2.10.

$$_A(S) = \{ \sum_{1\leqslant i\leqslant n} a_i x_i, n \in \mathbb{N}^*; \quad \forall i \in \{1, ..., n\} \quad a_i \in A, \quad x_i \in S\}$$

Démonstration. Notons par $N(S) = \{ \sum_{1\leqslant i\leqslant n} a_i x_i, n \in \mathbb{N}^*; \quad \forall i \in \{1, ..., n\} \quad a_i \in A, \quad x_i \in S\}$.
$N(S)$ est un sous-ensemble de M. $N(S) \neq \emptyset$ car $0_M \in N(S)$.
Soient $x, y \in N(S)$, alors $x = \sum_{1\leqslant i\leqslant n} a_i x_i$ et $y = \sum_{1\leqslant i\leqslant n} a'_i y_i$.
$x + y = \sum_{1\leqslant i\leqslant n} a_i x_i + \sum_{1\leqslant i\leqslant n} a'_i y_i \in N(S)$, donc c'est un sous-groupe de $(M, +)$.
Soit $a \in A$ et $x \in N(S)$, on a $ax = a \sum_{1\leqslant i\leqslant n} a_i x_i = \sum_{1\leqslant i\leqslant n} a a_i x_i \in N(S)$, donc $N(S)$ est un sous-module de M, donc il contient S, ainsi $_A(S) \subseteq N(S)$.
Soit $x \in N(S)$, alors $x = \sum_{1\leqslant i\leqslant n} a_i x_i$ avec $a_i \in A$ et $x_i \in S \subseteq N \Longrightarrow x \in N$ pour tout idéal $N \supset S \Longrightarrow x \in_A (S)$. D'où, $N(S) \subseteq_A (S)$. □

Définition 2.11. *Soit M un A-module à gauche et $x_1, x_2, ..., x_n$ sont des éléments de M ($n \in \mathbb{N}^*$), on appelle combinaison linéaire sur A des x_i ($1 \leqslant i \leqslant n$), tout élément $x \in M$ de la forme $x = \sum_{1\leqslant i\leqslant n} a_i x_i$ avec $a_i \in A$, $i = 1, ..., n$.*

Remarque 2.12. *$_A(S)$ est l'ensemble des combinaisons linéaires sur A de toutes les parties finies(non-vides) de S.*

Définition 2.13. *Une partie non vide S d'un A-module à gauche M est une partie génératrice de M, si $_A(S) = M$. On dit aussi, dans ce cas, que S engendre le A-module M ou que S est un ensemble de générateurs de M.*

Définition 2.14. *Soit M un A-module à gauche.*

1. *On dit que M est de type fini, s'il possède une partie génératrice finie. Dans ce cas, si $S = \{x_1, x_2, ..., x_n\}$ engendre M, alors*

$$x \in M \Longleftrightarrow x = \sum_{1\leqslant i\leqslant n} a_i x_i, a_i \in A \text{ pour tout } i = 1, ..., n.$$

2. *M est dit monogène, s'il est engendré par un seul élément x ; alors $M = Ax = \{ax; a \in A\}$.*

2.1.1 Somme de sous-modules

Soit $(N_i)_{1\leqslant i\leqslant n}$, $n \in \mathbb{N}$, une famille finie de sous-modules d'un A-module M. On pose

$$\sum_{1\leqslant i\leqslant n} N_i = \{ \sum_{1\leqslant i\leqslant n} x_i, \quad x_i \in N_i, 1 \leqslant i \leqslant n\}.$$

$\sum_{1\leqslant i\leqslant n} N_i$ est un sous-module de M et appelé somme de sous-modules N_i, $1 \leqslant i \leqslant n$.

Proposition 2.15. *Soit $(N_i)_{1\leqslant i\leqslant n}$ une famille de sous-modules d'un A-module M. $\sum_{1\leqslant i\leqslant n} N_i$ est le sous-module de M engendré par $\bigcup_{1\leqslant i\leqslant n} N_i$.*

Démonstration. Pour $n=2$ $(N_1\cup N_2)\supseteq N_1+N_2=\{n_1+n_2, n_1\in N_1, n_2\in N_2\}$. On a $(N_1\cup N_2)=\{\sum_{1\leqslant i\leqslant n} a_ix_i,\quad x_i\in N_1\cup N_2,\quad a_i\in A\quad 1\leqslant i\leqslant n\}$.
Soit $z\in(N_1\cup N_2)$, alors $z=\sum_{1\leqslant i\leqslant n_1} a_ix_i+\sum_{1\leqslant k\leqslant n_2} b_kx_k$, $a_i,b_k\in A$, $x_i,\in N_1$ $1\leqslant i\leqslant n_1$ et $x_k\in N_2$ $1\leqslant k\leqslant n_2$. On a donc $\sum_{1\leqslant i\leqslant n_1} a_ix_i\in N_1$ et $\sum_{1\leqslant k\leqslant n_2} b_kx_k\in N_2\Longrightarrow z\in N_1+N_2$, d'où $(N_1\cup N_2)\subseteq N_1+N_2$.
Pour $n>2$, on démontre la propriété par réccurence. □

Soit $(N_i)_{i\in I}$ une famille non vide de sous-modules d'un A-module M. On note

$$\sum_{i\in I} N_i=\{\sum_{1\leqslant j\leqslant m} x_{\lambda_j},\quad m\in\mathbb{N}^*,\lambda_i\in I,\quad x_{\lambda_j}\in N_{\lambda_j}, 1\leqslant j\leqslant m\}.$$

Nous avons : $\sum_{i\in I} N_i$ est un sous-module de M, appelé somme des sous-modules N_i, $i\in I$ et c'est le sous-module de M engendré par $\bigcup_{i\in I} N_i$.

Remarque 2.16. *1. Pour tout $j\in I$, N_j est un sous-module de $\sum_{i\in I} N_i$.*

2. L'expression des éléments de $\sum_{i\in I} N_i$, montre que si l'ensemble I est de cardinal infini, alors $x\in\sum_{i\in I} N_i\Longleftrightarrow$ il existe une partie finie $\{\lambda_1,\lambda_2,...,\lambda_m\}$ de I telle que $x\in\sum_{1\leqslant j\leqslant m} N_j$. On pourra écrire : $x=\sum_{i\in I} x_i$, où pour tout $i\in I$, $x_i\in N_i$, les x_i étant "presque tous nuls" (c'est à dire nuls sauf un nombre fini d'entre eux), car tout $x\in\sum_{i\in I} N_i$ est une somme finie d'éléments de $\bigcup_{i\in I} N_i$.

2.1.2 Somme directe de sous-modules

Définition 2.17. *Soit $(N_i)_{i\in I}$ une famille non vide de sous-modules d'un A-module M. On dit que la somme $\sum_{i\in I} N_i$ est une somme (interne) directe si tout $x\in\sum_{i\in I} N_i$ s'écrit de façon unique : $x=\sum_{i\in I} x_{i_j}$; où $m\in\mathbb{N}^*$, $i_j\in I$, $x_{i_j}\in N_{i_j}$ $1\leqslant j\leqslant m$. Dans ce cas, la somme est noté $\bigoplus_{i\in I} N_i$.*

Proposition 2.18. *Soit $(N_i)_{i\in I}$ une famille non vide de sous-modules d'un A-module M. Les conditions suivantes sont équivalentes :*

1. La somme des sous-modules N_i, pour $i\in I$, est directe ;

2. $(\sum_{i\in I} x_i = 0$ *dans* $\sum_{i\in I} N_i \Longrightarrow) \; x_i = 0$, *pour tout* $i \in I$;
3. $\forall j \in I,\ N_j \bigcap (\sum_{i\in I\setminus\{j\}} N_i) = \{0\}$.

Démonstration. 1) $\Longrightarrow$ 2). si la somme est directe, alors 0 s'écrit de façon unique, $0 = \sum_{i\in I} x_i$, d'où $x_i = 0$ pour tout $i \in I$.
2) $\Longrightarrow$ 3). Soit $x \in N_j \bigcap (\sum_{i\in I\setminus\{j\}} N_i$, si $x \neq 0$ alors $x = x_j = \sum_{1\leqslant j\leqslant m} x_{i_j}$, $\lambda_j \in I \setminus \{j\}$, donc $x_j - \sum_{1\leqslant j\leqslant m} x_{i_j} = 0$, d'après 2) on a $x = x_j = 0$.
3) $\Longrightarrow$ 1). Supposons que $x \in \sum_{i\in I} N_i$ tel que $x = \sum_{1\leqslant i\leqslant m} x_i = \sum_{1\leqslant i\leqslant m} y_i$ où les x_i et y_i sont presque tous nuls dans N_i. S'il existe $j \in I$ tel que $x_j \neq y_j$ alors $x_j - y_j = \sum_{i\in I\setminus\{j\}}(y_i - x_i)$. D'après 3) on a $x_j - y_j = 0$, contradiction. On en conclut que $x_i = y_i$ pour tout $i \in I$. □

Définition 2.19. *Soit M un A-module à gauche.*

1. *Deux sous-modules N_1 et N_2 de M sont dits supplémentaires dans M, si $M = N_1 \oplus N_2$.*
2. *Un sous-module N de M est dit facteur direct dans M, s'il existe un sous-module N' de M tel que $M = N \oplus N'$.*

Remarque 2.20. 1. $M = N_1 \oplus N_2 \Longleftrightarrow M = N_1 \oplus N_2$ *et* $N_1 \cap N_2 = \{0\}$.

2. *Un sous-module N' d'un A-module M n'est pas, en général, un facteur dans M. On sait cependant que dans un $\mathbb{K}$.e-v tout s.e.v a un supplémentaire, donc facteur direct.*
3. *Un A-module est dit semi-simple si tous sous-modules soient facteurs directs.*

2.1.3 Morphismes de A-modules

Définition 2.21. *Soient M et N deux A-modules. On appelle un morphisme de A-modules (homorphisme ou application A-linéaire) de M dans N toute application $f : M \longrightarrow N$ telle que :*

1. $f(x + y) = f(x) + f(y)$ *pour tout* $x, y \in M$,
2. $f(ax) = af(x)$ *pour tout* $a \in A, x \in M$.

L'ensemble des A-homomorphismes se note $Hom_A(M, N)$.

Soient u et $v \in Hom_A(M, N)$ et $a \in A$. Notons par :

$$\begin{array}{ccc} u+v : M & \longrightarrow & N \\ x & \longmapsto & (u+v)(x) = u(x) + v(x) \end{array}$$

et

$$\begin{array}{ccc} au : M & \longrightarrow & N \\ x & \longmapsto & (au)(x) = au(x). \end{array}$$

$Hom_A(M, N)$ a ainsi la structure d'un A-module à travers la loi externe :

$$\begin{array}{ccc} A \times Hom_A(M,N) & \longrightarrow & Hom_A(M,N) \\ (a, u) & \longmapsto & au. \end{array}$$

Si $N = A$, $Hom_A(M, A)$ qui est l'ensemble des formes A-linéaires de M dans A s'appelle <u>le dual</u> de M.

Exemple 2.22. *1) Si N est un sous-module d'un A-module M, alors l'injection*

$$\begin{array}{ccc} i : N & \longrightarrow & M \\ x & \longmapsto & x \end{array}$$

est un A-morphisme.
2)

$$\begin{array}{ccc} M & \longrightarrow & M' \\ x & \longmapsto & 0. \end{array}$$

est un morphisme de A-modules, appelé morphisme nul.

Proposition 2.23. *Soient M et M' deux A-modules et $f \in Hom_A(M, M')$, N un sous-module de M et N' un sous-module de M'. Alors on a :*

1. *$f(N)$ est un sous-module de M', en particulier $Imf := \{f(x)/\ x \in M\}$ est un sous module de N.*
2. *$f^{-1}(N')$ est un sous-module de M, en particulier $\ker f := \{x \in M/\ f(x) = 0_N\}$ est un sous-module de M.*
3. *f est surjectif si et seulement si $Imf = M$.*
4. *f est injectif si et seulement si $\ker f = \{0\}$.*
5. *Si $f \in Hom_A(M, M')$ et $g \in Hom_A(M', M'')$ alors $g \circ f \in Hom_A(M, M'')$.*

Démonstration. Exercice.

□

Définition 2.24. *Soient M et M' deux A-modules, une application f de M dans M' est un isomorphisme de A-modules, si $f \in Hom_A(M, M')$ et s'il existe $g \in Hom_A(M', M)$ tel que $g \circ f = id_M$ et $f \circ g = id_{M'}$.*

Proposition 2.25. *1) f isomorphisme de M sur $M' \iff f \in Hom_A(M, M')$ et f bijectif.*
2) f isomorphisme M sur $M' \Longrightarrow f^{-1}$ isomorphisme de M' sur M.

Définition 2.26. *a) Deux A-modules M et M' sont dits isomorphes (ou A-isomorphes) s'il existe un isomorphisme de A-modules de l'un sur l'autre ; on écrit alors, symboliquement, $M \simeq M'$.*

Définition 2.27. *Soient M un A-module et N un sous-module de M. Sur le groupe quotient abelien M/N, on considère la loi de composition externe à opérateurs dans A, définie par :*

$$\begin{array}{ccc} A \times M/N & \longrightarrow & M/N \\ (a, \overline{x}) & \longmapsto & \overline{ax} = ax + N. \end{array}$$

La loi est compatible avec la relation : $x \sim y \iff x - y \in N$. En effet $x \sim y \iff x - y \in N \implies a(x-y) \in N \implies ax \sim ay$.

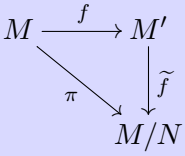
Ainsi, $\overline{x} = \overline{y} \implies \overline{ax} = \overline{ay}, x, x' \in M$ et $a \in A$.

On peut donc poser, dans M/N, $a\overline{x} = \overline{ax}$.

M/N a une structure de A-module appelé module quotient de M par N.

L'application canonique $\pi : M \longrightarrow M/N$ est un morphisme de A-modules surjectif avec $\ker \pi = N$, appelé surjection canonique. Nous avons :

Théorème 2.28. *(Propriété universelle)*
Soient A un anneau, M et M' deux A-modules et $f \in Hom_A(M, M')$ un morphisme de modules. Si N est un sous-module de M contenu dans $kerf$, il existe un unique homomorphisme $\widetilde{f} \in Hom(M/N, M')$ tel que $f = \widetilde{f} \circ \pi$. On a le diagramme commutatif suivant :



Théorème 2.29. *(1er théorème d'isomorphisme)*
Soient M et M' deux A-modules et $f \in Hom_A(M, M')$. Alors on a :

$$E/Ker(f) \simeq Im(f).$$

Théorème 2.30. *(2em théorème d'isomorphisme)*
Soient N_1 et N_2 deux sous-modules d'un A-module M. Alors on a :

$$(N_1 + N_2)/N_2 \simeq N_1/(N_1 \cap N_2).$$

Corollaire 2.31. *Si $M = N_1 \oplus N_2$, alors $M/N_1 \simeq N_2$ et $M/N_2 \simeq N_1$*

Théorème 2.32. *(3em théorème d'isomorphisme)*
Soient N_1 et N_2 deux sous-modules d'un A-module M tels que $N_2 \subseteq N_1$. Alors on a :

$$M/N_1 \simeq (M/N_2)/(N_1/N_2).$$

Dans toute la suite du cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.

2.2 Produit et somme de modules

Définition 2.33. *1. Soient $(M_i)_{i\in I}$ une famille de R-modules et $M = \prod_{i\in I} M_i$ le produit au*

sens ensembliste des M_i. On munit M d'une structure de A-module en posant :

$$\begin{cases} (x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \\ \lambda(x_i)_{i\in I} = (\lambda x_i)_{i\in I} \end{cases}$$

Muni d'une telle structure, M est appelé module produit de la famille des modules $(M_i)_{i\in I}$.

2. *On appelle somme directe de la famille des modules $(M_i)_{i\in I}$ qu'on note $\bigoplus_{i\in I} M_i$, le sous module de $M = \prod_{i\in I} M_i$, formé des $(x_i)_{i\in I}$ tels que $x_i = 0$ sauf pour un nombre fini d'indices.*

– *Notons que lorsque I est fini, on a :*

$$\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i.$$

– *Pour chaque $j \in I$, on appelle projection canonique le A-morphisme surjectif :*

$$\begin{array}{ccc} P_j : \prod_{i\in I} M_i & \longrightarrow & M_j \\ (x_i)_{i\in I} & \longmapsto & x_j. \end{array}$$

On appelle injection canonique le A-morphisme :

$$\begin{array}{ccc} e_j : M_j & \longrightarrow & \prod_{i\in I} M_i \\ x_j & \longmapsto & (y_i)_{i\in I} \end{array}$$

avec

$$\begin{cases} y_j = x_j \\ y_i = 0 \quad \forall\, i \neq j. \end{cases}$$

Remarque 2.34. *1. Soit M un A-module, le produit de modules où tous les facteurs sont identiques à M n'est autre que M^I (l'ensemble des applications de I dans A : $I \longrightarrow A$).*
Notation :

$$\prod_{i\in I} M_i = M^I, \bigoplus_{i\in I} M_i = M^{(I)}.$$

2. *Soient $(M_i)_{i\in I}$, $(N_i)_{i\in I}$ deux familles de A-modules et $f_i : M_i \longrightarrow N_i$ $(i \in I)$ une famille de morphismes. Alors :*

a) *L'application*

$$\begin{array}{ccc} f : M = \prod_{i\in I} M_i & \longrightarrow & N = \prod_{i\in I} N_i \\ (x_i)_{i\in I} & \longmapsto & (f_i(x_i))_{i\in I} \end{array}$$

est un A-morphisme.

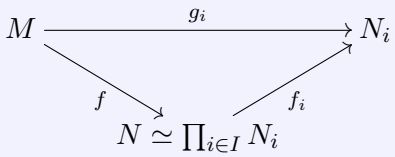
b) *$Ker(f) = \prod_{i\in I} Ker(f_i)$ et $Im(f) = \prod_{i\in I} Im(f_i)$.*
Par conséquent : f est injectif (resp., surjectif) si et seulement si f_i est injectif (resp., surjectif) $\forall i \in I$.
a) et b) restent valables si on remplace le module produit par la somme directe.

Lemme 2.35. *Soit M un module et soit $(N_i)_i$ une famille de modules. Les assertions suivantes*

sont équivalentes :

i) $N \simeq \prod_{i\in I} N_i$.

ii) *Il existe une famille de morphismes* $f_i : N \longrightarrow N_i$ $(i \in I)$ *tels que pour tout module* M *et toute famille de morphismes* $g_i : M \longrightarrow N_i$ $(i \in I)$, *il existe un unique* $f \in Hom_R(M, N)$ *tel que :* $f_i o f = g_i \ \forall i \in I$.



Démonstration. Supposons que $i)$ est vraie et montrons $ii)$. Si $N = \prod_{i\in I} N_i$, on considère la famille des projections canoniques $(p_i)_{i\in I}$. Pour l'existence de f prenons $f(x) = (g_i(x))_{i\in I}$ on a $p_i o f(x) = p_i(g_i(x)) = g_i(x)$ pour tout $i \in I$ et $x \in M$, d'où $p_i o f = g_i$.
unicité : Supposons qu'il existe $f' \in Hom_R(M, N)$ tel que $p_i o f' = g_i$. On a $f'(x) = (f'_i(x))_{i\in I}$,
$\begin{cases} p_i o f' = g_i \\ p_i o f = g_i \end{cases} \Longrightarrow f'_i(x) = f_i(x)$ pour tout $i \in I$, d'où $f = f'$.
Inversement, supposons que $ii)$ est vraie et montrons $i)$. D'après les hypothèses, nous avons les diagrammes commutatifs :

(1) $M = N \xrightarrow{f_i} N_i$, $\exists! f$, p_i, $\prod_{i\in I} N_i$ (2) $M = \prod_{i\in I} N_i \xrightarrow{p_i} N_i$, $id(M)$, p_i, $\prod_{i\in I} N_i$

(3) $M = \prod_{i\in I} N_i \xrightarrow{p_i} N_i$, $\exists! g$, f_i, N (4) $M = N \xrightarrow{f_i} N_i$, $id(N)$, f_i, $N \simeq \prod_{i\in I} N_i$

Il en résulte d'après (1) et (3), que pour tout $i \in I$ on a :

$$\begin{cases} p_i o f = f_i & (1) \ \forall i \in I \\ f_i o g = p_i & (2). \end{cases}$$

Par conséquent, pour tout $i \in I$ on a :

$$\begin{cases} p_i o f o g = p_i \\ f_i o g o f = f_i. \end{cases}$$

D'après l'unicité de (2) et (4) on a :

$$\begin{cases} f o g = id(\prod_{i\in I} N_i) \\ g o f = id(N). \end{cases}$$

D'où, $A \simeq \prod_{i\in I} A_i$. Ce qui achève la preuve du lemme. □

On peut maintenant énoncer le théorème d'isomorphisme suivant :

Théorème 2.36. *On a l'isomorphisme :*

$$Hom_A(M, \prod_{i\in I} N_i) \cong \prod_{i\in I} Hom_A(M, N_i)$$

Démonstration. Soit

$$\begin{array}{ccc} \varphi : Hom_A(M, \prod_{i\in I} N_i) & \longrightarrow & \prod_{i\in I} Hom_A(M, N_i) \\ f & \longmapsto & (p_i o f)_{i\in I}. \end{array}$$

On peut facilement vérifier que φ est un A-morphisme. En vertu du lemme précédent, φ est bijectif. □

Corollaire 2.37. *Etant donné deux familles non vides de A-modules $(M_i)_{i\in I}$ et $(M'_i)_{i\in I}$, alors*

$$(\forall i \in I, M'_i \simeq M_i) \Longrightarrow \prod_{i\in I} M'_i \simeq \prod_{i\in I} M_i.$$

Lemme 2.38. *Soient N un module et $(N_i)_{i\in I}$ une famille de modules. Les assertions suivantes sont équivalentes :*

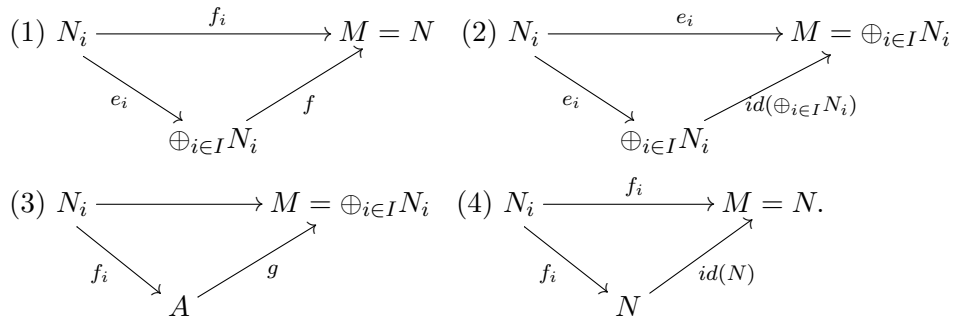
i) $N \simeq \bigoplus_{i\in I} N_i$.

ii) *Il existe une famille de morphismes $f_i : N_i \longrightarrow N$ $(i \in I)$ tels que pour tout module M et toute famille de morphismes $g_i : N_i \longrightarrow M$ $(i \in I)$, il existe un unique $f \in Hom_A(N, M)$ tel que $f o f_i = g_i$ $\forall i \in I$.*

Démonstration. Supposons que $i)$ est vraie et montrons $ii)$. Si $N \simeq \bigoplus_{i\in I} N_i$, on considère alors la famille des injections canoniques $(e_i)_{i\in I}$ et on vérifie que : $f o e_i = g_i$ $\forall i \in I$ si et seulement si $f((x_i)_{i\in I}) = \sum_{i\in I} f(e_i(x))_{i\in I} = \sum_{i\in I} g_i(x_i)$. Il est possible de prendre f défini par :

$$f((x_i)_{i\in I}) = \sum_{i\in I} f(e_i(x))_{i\in I}$$

puisque les x_i sont nuls sauf pour un nombre fini.
Inversement, supposons que $ii)$ est vraie. D'après l'étude directe et par hypothèses, nous avons les diagrammes commutatifs :



Nous avons donc pour tout $i \in I$:

$$\begin{cases} f o e_i = f_i \\ g o f_i = e_i. \end{cases}$$

Par conséquent, on a pour tout $i \in I$:

$$\begin{cases} gofoe_i = e_i \\ fogof_i = f_i. \end{cases}$$

D'après l'unicité de $id(\oplus_{i\in I}N_i)$ et $id(N)$ on a :

$$\begin{cases} fog = id(N) \\ gof = id(\bigoplus_{i\in I} N_i). \end{cases}$$

D'où $N \simeq \bigoplus_{i\in I} N_i$. □

Théorème 2.39. *On a l'isomorphisme suivant :*

$$Hom_A(\bigoplus_{i\in I} N_i, M) \cong \prod_{i\in I} Hom_A(N_i, M).$$

Démonstration. Soit

$$\begin{array}{rccc} \varphi : Hom_A(\bigoplus_{i\in I} N_i, M) & \longrightarrow & \prod_{i\in I} Hom_A(N_i, M) \\ f & \longmapsto & (foe_i)_{i\in I}. \end{array}$$

On peut vérifier facilement que φ est un A-morphisme bijectif. En effet, Soit $(g_i)_{i\in I} \in \prod_{i\in I} Hom_A(A_i, B)$, d'après le lemme précédent il existe un unique $G \in Hom_A(\bigoplus_{i\in I} N_i, M)$ tel que $G \circ e_i = g_i$ pour tout $i \in I$ i.e, $\varphi(G) = (g_i)_{i\in I} \Longrightarrow \varphi$ est bijectif. □

Remarque 2.40. *Il existe des exemples où on a :*

1. $Hom_A(\prod_{i\in I} N_i, M) \ncong \bigoplus_{i\in I} Hom_A(N_i, M)$.
2. $Hom_A(\prod_{i\in I} N_i, M) \ncong \prod_{i\in I} Hom_A(N_i, M)$.
3. $Hom_A(N, \bigoplus_{i\in I} M_i) \ncong \bigoplus_{i\in I} Hom_A(N, M_i)$.
4. $Hom_A(N, \bigoplus_{i\in I} M_i) \ncong \prod_{i\in I} Hom_A(N, M_i)$.

Proposition 2.41. *Soient $(M_i)_{i\in I}$ une famille de modules et N_i un sous module de M_i pour chaque $i \in I$. On a :*

$$\frac{\oplus_{i\in I} M_i}{\oplus_{i\in I} N_i} = \oplus_{i\in I} \frac{M_i}{N_i}$$

Démonstration. L'application

$$\begin{array}{rccc} f : & \oplus_{i\in I} M_i & \longrightarrow & \oplus_{i\in I} \frac{M_i}{N_i} \\ & (x_i)_{i\in I} & \longmapsto & (x_i + N_i)_{i\in I} \end{array}$$

est un homomorphisme surjectif de modules. De plus $Ker(f) = \oplus_{i\in I} N_i$. Dés lors, le premier théorème d'isomorphisme termine la preuve. □

2.3 Suites exactes de A-modules

Définition 2.42. *1. Une suite de A-modules et d'homomorphismes*

$$...M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} Mi+1 \xrightarrow{f_{i+1}} ...$$

est dite suite exacte en M_i si $\ker f_i = Imf_{i-1}$. Cette suite est dite exacte si elle est exacte en chaque M_i.

2. Une suite exacte courte est une suite exacte de la forme

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0;$$

c'est à dire que u est injectif, v est surjectif, et $Im(u) = Ker(v)$.

Notamment on a :

Proposition 2.43. *Soit $u : M \longrightarrow N$ un morphisme de A-modules. Alors on a :*

1. *u est injectif si et seulement si la suite $0 \longrightarrow M \longrightarrow N$ est exacte.*
2. *u est surjectif si et seulement si la suite $M \longrightarrow N \longrightarrow 0$ est exacte.*
3. *u est bijectif si et seulement si la suite $0 \longrightarrow M \longrightarrow N \longrightarrow 0$ est exacte.*

Exemple 2.44. *Soit N un sous-module d'un A-module M, alors la suite*

$$0 \longrightarrow N \xrightarrow{j} M \xrightarrow{\pi} M/N \longrightarrow 0$$

où j est l'injection canonique et π la surjection canonique, est une suite exacte courte.

Proposition 2.45. *Toute suite exacte courte de A-modules à gauche*

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

est "isomorphe" à la suite exacte courte suivante

$$0 \longrightarrow Imf \xrightarrow{j} M \xrightarrow{\pi} M/Imf \longrightarrow 0$$

Autrementdit, il existe des isomorphismes de A-modules, $Imf \xrightarrow{u} N$ et $M/Imf \xrightarrow{v} P$ tels que le diagramme suivant commute.

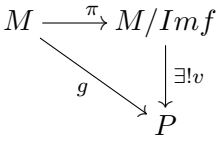
$$\begin{array}{ccccccc} 0 & \longrightarrow & Imf & \xrightarrow{j} & M & \xrightarrow{\pi} & M/Imf \longrightarrow 0 \\ & & u\downarrow & & Id_M\downarrow & & \downarrow v \\ 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P \longrightarrow 0 \end{array}$$

donc $f \circ u = j$ et $v \circ \pi = g$.

Démonstration. On a f est injectif, g est surjectif et $Imf = \ker g$.
Soit f_1 la restriction surjective de f

$$\begin{array}{rccc} f_1 : & A & \longrightarrow & Imf \\ & x & \longrightarrow & f_1(x) = f(x) \end{array} .$$

Le morphisme f_1 est surjectif et il est injectif, car f est injectif, donc f_1 est un isomorphisme. On en déduit que $u = f_1^{-1}$ est un isomorphisme de Imf sur N et $f \circ u = id_{Imf} \Longrightarrow f'ou = j = id_M \circ j$. D'autre part, d'après la propriété universelle du module quotient, la condition $Imf = \ker g$ implique $\exists! v \in Hom_A(M/Imf, P)$ tel que le diagramme suivant commute



d'où $v \circ \pi = g = g \circ id_M$. De plus, $\ker g = lmf$ implique v injectif, g surjectif entraîne v surjectif, donc v est un isomorphisme de M/Imf sur P.

□

2.4 A-module libre et de type fini

2.4.1 Module de type fini

Soient M un module et S une partie de M. Le plus petit sous module de M contenant S, noté $< S >$, est exactement l'ensemble des éléments de la forme $\sum_{i=1}^{n} a_i s_i$, avec $a_i \in A$, $s_i \in S$ et $n \in \mathbb{N}^*$.

Définition 2.46. *1. Un module M est dit de type fini s'il existe une partie finie $\{x_1, \ldots, x_n\}$ de M telle que $M =< x_1, \ldots, x_n >$. Dans ce cas, nous avons :*

$$M = \sum_{i=1}^{n} Ax_i.$$

2. Un module M est dit cyclique (ou monogène) s'il existe $x \in M$ tel que $M =< x >$; c'est à dire que $M = Ax$.

Exemple 2.47. *1. Si $A = K$ est un corps, les A-modules de type fini sont les espaces vectoriels de dimension finie.*

2. A^m est un A-module de type fini.

Remarque 2.48. *Un sous module d'un A-module de type fini n'est pas nécessairement de type fini. En effet, soient $A = K[X_1, ..., X_n, ...]$, où K est un corps, $(X_i)_{i\in\mathbb{N}}$ sont des indéterminées sur K et $I :=< X_1, ..., X_n, ... >$ l'idéal de A engendré par $(X_i)_{i\in\mathbb{N}}$. L'idéal I n'est pas de type fini et pourtant A est de type fini.*

Le résultat suivant caractérise les modules de type fini.

Théorème 2.49. *Soit M un A-module. Les assertions suivantes sont équivalentes :*

1. *M est de type fini ;*
2. *Il existe $n \geqslant 1$ tel que M est isomorphe à un quotient d'un module libre de type fini A^n(:=*

$\underbrace{A \times A \times ... \times A}_{nfois}$).

Démonstration. Supposons que M est de type fini engendré par $x_1, ..., x_n$: $M = \sum_{i=1}^{n} Ax_i$. Considèrons l'homorphisme :

$$\begin{array}{rcl} f : A^n & \longrightarrow & M \\ (a_1, ..., a_n) & \longmapsto & \sum_{i=1}^{n} a_i x_i. \end{array}$$

L'homomorphisme f est surjectif par construction. Par le 1er théorème d'isomorphisme on a $M = Imf \simeq A^n/Kerf$.
Inversement, supposons qu'il existe $r \in \mathbb{N}^*$ et un sous module N de A^r tels que $M \simeq A^r/N$. Si $(e_1, ..., e_r)$ est une base de A^r, alors $(e_1 + N, ..., e_r + N)$ engendre M. □

Proposition 2.50. *1. Soient M un module et N un sous module de M. Si M est de type fini, alors M/N est aussi un module de type fini.*
2. Soit $0 \to A \to^{\mu} B \to^{\nu} C \to 0$ une suite exacte de modules. Si A et C sont de type fini, alors B est aussi de type fini.

Démonstration. 1. Soit $M =< x_1, \ldots, x_n >$. Il est clair que $M/N =< \bar{x_1}, \ldots, \bar{x_n} >$, où $\bar{x_i} = x_i + N$.
2. Supposons que $A =< a_1, \ldots, a_n >$ et $C =< c_1, \ldots, c_m >$. Le morphisme ν étant surjectif, il existe $b_i \in B$ tel que $\nu(b_i) = c_i$, pour tout $i = 1, \ldots, m$. On a aussi $C =< \nu(b_1), \ldots, \nu(b_m) >$. Dés lors, on a $< \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m > \subseteq B$. Montrons que : $B \subseteq < \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m >$.

Soit $b \in B$, on a :

$$\nu(b) = \sum_{i=1}^{m} \lambda_i c_i = \sum_{i=1}^{m} \lambda_i \nu(b_i) = \sum_{i=1}^{m} \nu(\lambda_i b_i).$$

D'où $b - \sum_{i=1}^{m} \lambda_i b_i \in Ker(\nu) = Im(\mu)$ car (μ, ν) est exacte, de sorte que $b - \sum_{i=1}^{m} \lambda_i b_i = \mu(\sum_{j=1}^{n} \mu_j a_j)$ pour un certain $\mu_j \in R$. Dés lors, $b = \sum_{j=1}^{n} \mu_j \mu(a_j) + \sum_{i=1}^{m} \lambda_i b_i \in < \mu(a_1), \ldots, \mu(a_n), b_1, \ldots, b_m >$. D'où le résultat. □

Remarque 2.51. *L'hypothèse "A et C sont de type fini" est nécessaire pour avoir B de type fini dans la proposition précédente. En effet :*

1. Soient $R = K[X_1, \ldots, X_n, \ldots]$ l'anneau des polynômes à une infinité d'indeterminées sur un corps K, $B =< X_1, \ldots, X_n, \ldots >$ l'idéal engendré par $\{X_1, \ldots, X_n, \ldots\}$ et $A =< X_1 >$ l'idéal engendré par $\{X_1\}$.

On a A est de type fini, B n'est pas de type fini et on a la suite exacte :

$$0 \to A =< X_1 > \to B =< X_2, \ldots, X_n, \ldots > \to B/A \simeq < X_1, \ldots, X_n, \ldots > \to 0$$

où B/A n'est pas de type fini.

2. Soient B un module qui n'est pas de type fini et $C = 0$ le module nul. On a C est de type fini, B n'est pas de type fini et on a la suite exacte de A-modules :

$$0 \to A(= B) \to B \to C(= 0) \to 0.$$

Concernant les modules cycliques, on a :

Proposition 2.52. *Un module M est cyclique si et seulement si $M \simeq A/I$ pour un certain idéal I de R.*

Démonstration. Supposons que $M =< x >$. L'application :

$$\begin{array}{ccc} f : A & \longrightarrow & M \\ \lambda & \longmapsto & \lambda x \end{array}$$

est un morphisme de A-modules surjectif. Donc, $M \simeq A/\ker(f)$, où $Ker(f)$ est un idéal de R. Réciproquement, si I est un idéal de A, alors $A/I =< \overline{1} >$ est un A-module cyclique et cela achève la preuve. □

Théorème 2.53. *[Lemme de Nakayama]*
Soient I un idéal de A et $J(A)$ le radical de Jacobson de l'anneau A. Les assertions suivantes sont équivalentes :
i. $I \subseteq J(A)$;
ii. Pour tout module de type fini M tel que $IM = M$, on a $M = 0$;
iii. Pour tout module M de type fini et tout sous module N de M tel que $M = IM + N$, on a $M = N$;
iv. Pour tout module M tel que $M/IM =< \bar{x_1}, \ldots, \bar{x_n} >$, on a $M =< x_1, \ldots, x_n >$.

La preuve de ce théorème se base sur le lemme suivant :

Lemme 2.54. *Soient M un A-module de type fini et I un idéal de A. Si $IM = M$ alors il existe $a \in A$ tel que $(1 + a) \in I$ et $aM = 0$.*

Démonstration. Posons $M = \sum_{i=1}^{n} Ax_i$. L'égalité $IM = M$ implique que $x_i \in IM$ pour tout $i = 1, ..., n$; c'est à dire que $x_i = \sum_{j=1}^{n} a_{ij}x_j$ où $a_{ij} \in I$ et $x_j \in M$. Ainsi, on a $(-1+a_{ii})x_i+\sum_{j=1,j\neq i}^{n} a_{ij}x_j = 0$. Posons

$$B = (a_{ij})_{1\leqslant i,j\leqslant n} \text{ et } X = \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix}.$$

On a $(B - I_n)X = 0$ où I_n est la matrice identité d'ordre n. Posons $a = det(B - I_n)$. Modulo I, on a $\overline{a} = \overline{1}$; c'est à dire que $1 + a \in I$. Il est clair que $aM = 0$ et cela termine la preuve de ce lemme. □

Preuve du théorème 2.53.

$i \Rightarrow ii$. Comme $IM = M$, alors d'après le lemme précédent, il existe $a \in A$ tel que $1+a \in I$ et $aM = 0$. Or $I \subseteq J(A)$. Dés lors, $1 + a \in J(A)$ et donc $1 - (1 + a) = -a \in U(A)$; c'est à dire que $a \in U(A)$. Ainsi $aM = 0$ et par suite $M = a^{-1}aM = a^{-1}0 = 0$. D'où ii).

$ii \Rightarrow iii$. Soient M un R-module de type fini et N un sous module de M tel que $M = IM + N$. Ainsi, le A-module M/N est de type fini et $I(M/N) = M/N$ (car $M = IM + N$). Dés lors on a $M/N = 0$; c'est à dire que $M = N$.

$iii \Rightarrow iv$. Il suffit d'appliquer iii) à $N =< x_1, \ldots, x_n >$.

$iv \Rightarrow i$. Soient $x \in I$ et $\lambda \in A$. On a : $A/IA = A/I =< \bar{1} >=< 1 + \bar{\lambda x} >$, ceci implique que $A =< 1 + \lambda x >$ et $1 + \lambda x$ est donc inversible pour tout $\lambda \in A$.

Soit maintenant m un idéal maximal de A. On veut montrer que $x \in m$.
Supposons que $x \notin m$, alors $< x > +m = A$. Il existe donc $\lambda \in A$ et $a \in m$ tels que $1 = \lambda x + a$. Ainsi on a $a = 1 - \lambda x \in I$ est inversible, absurde. Donc $I \subseteq m$ pour tout idéal maximal m de A ; c'est à dire que $I \subseteq J(R)$ et cela termine la preuve du théorème. ■

2.5 A-algèbre

Définition 2.55. *A étant un annneau unitaire et commutatif, on dit que M est une A-algèbre à gauche si :*

1. *M est un anneau unitaire(éléments unité 1_M).*
2. *M est un A-module à gauche ;*
3. *$\forall (x, y) \in M \times M$, $\forall a \in A$, $a(xy) = (ax)y = x(ay)$.*

$\longrightarrow$ On définit de même, une A-algèbre à droite.
$\longrightarrow$ Une A-algèbre M est dite commutative si l'anneau M est commutatif.
$\longrightarrow$ Une A-algèbre M est dite libre si le A-module M est libre.
Donc, si K est un corps, toute K-algèbre est libre.

Exemple 2.56. 1. *Tout anneau unitaire est une $\mathbb{Z}$-algèbre.*

2. *Un anneau unitaire et commutatif A est une A-algèbre à droite et à gauche.*

Définition 2.57. *M étant une A-algèbre, une partie N de M est une sous-algèbre de M si S est à la fois un sous-anneau unitaire et un sous-A-module de M.*

Remarque 2.58. *Pour $n > 1$, $n\mathbb{Z}$ n'est pas une sous $\mathbb{Z}$-algèbre de $\mathbb{Z}$, car $1 \notin n\mathbb{Z}$.*

Définition 2.59. *Pour deux A-algèbres M et M', une application f de M dans M' est un morphisme de A-algèbres, si f est à la fois un morphisme d'anneau unitaires et un morphisme de A-modules.*

2.5.1 Module libre

Définition 2.60. *M étant un A-module. On dit qu'une partie non vide S de M est libre si pour toute partie finie T de S, la relation $\sum_{s\in T} a_s s = 0$ avec les $a_s \in A$, entraîne $a_s = 0$ pour tout $s \in T$.*

Remarque 2.61.
1. *Par convention, on considère la partie vide d'un A-module quelconque, comme une partie libre.*
2. *D'après la définition 2.60., quel que soit le A-module M, $\{0\}$ n'est pas une partie libre de M.*
3. *Si S est une partie libre non vide d'un A-module M, alors $S' \subseteq S \Longrightarrow S'$ partie libre de M. Par suite, $\{0\}$ n'appartient à aucune partie libre de M.*

Définition 2.62. *Un A-module M est dit libre s'il possède une partie génératrice, libre sur A. Dans ce cas, toute partie libre et génératrice du A-module M est appelée une base de M sur A.*

Remarque 2.63. *a) Le A-module $\{0\}$ est considéré comme libre, de base l'ensemble vide.*
b) Tout K-espace vectoriel est un K-module libre.
c) Le A-module A est libre de base $\{1\}$.
d) Si A n'est pas un corps, un A-module n'est pas nécessairement libre. Par exemple, $\mathbb{Z}/6\mathbb{Z}$ en tant que $\mathbb{Z}$-module n'a pas de base. Sinon, si $\overline{x} \in \mathbb{Z}/6\mathbb{Z}$ dans une base, on a $6\overline{x} = \overline{0}$, alors que 6 n'est pas nul dans $\mathbb{Z}$.
e) Les A-modules n'ont pas les mêmes comportements que les espaces vectoriels. Un sous-module d'un A-module libre n'est pas forcément libre : soit $A = \mathbb{Z}/n^2\mathbb{Z}$ et $I = n\mathbb{Z}/n^2\mathbb{Z}$, idéal de A comme sous-module de A n'est pas libre, $n \in \mathbb{N}^*$. En effet, pour tout $x \in I$, on a $nx = 0$ avec $n \neq 0$ dans A, donc aucune partie de I ne peut être libre et donc une base de I.
(Le $\mathbb{Z}/4\mathbb{Z}$-module $\mathbb{Z}/4\mathbb{Z}$ est libre de base $\{\overline{1}\}$ mais le sous-module $2\mathbb{Z}/4\mathbb{Z}$ n'est pas libre car $\{\overline{2}\}$ est génératrice mais n'est pas libre.)

Proposition 2.64. *Soit M un A-module, les conditions suivantes sont équivalentes :*
1. *M est libre de base $X = \{x_i\}_{i\in I}$,*
2. *Tout $x \in M$ s'écrit de façon unique : $x = \sum_{i\in I} a_i x_i$, les a_i étant presque tous nuls dans A,*
3. *$M \simeq A^{(I)}$.*

Démonstration. (1) $\Longleftrightarrow$ (2), d'après la définition.
(2) $\Longleftrightarrow$ (3), on a 2) $\Longleftrightarrow M \simeq \bigoplus_{i\in I} Ax_i$, or $Ax_i \simeq A$ pour tout $i \in I$, d'où le résultat.

□

Corollaire 2.65. *M est un A-module libre de base $\{x_1, x_2, ..., x_n\}, n > 0$, si et seulement si M est isomorphe au A-module A^n.*

Remarque 2.66.
1. *On a $X = \{x_i\}_{i\in I}$, donc $card(X) = card(I)$; d'où $A^{(X)} = A^{(I)}$,*
2. *Si A est un anneau unitaire, commutatif, alors toutes les bases d'un A-module libre M ont le même cardinal (que celui-ci soit fini ou non), lorsque ce cardinal est fini, il est appelé le rang de M, sinon on dit que M est libre de rang infini.*
3. *Lorsque l'anneau unitaire n'est pas commutatif, un tel A-module peut avoir des bases finies n'ayant pas le même cardinal.*
4. *Soit A un anneau principal. Alors tout idéal non nul A est libre de rang 1. En effet, soit I un idéal non nul de A, alors il existe $a \in A$ tel que $I = aA$, (a) est une base de I car A est un D.I.*
5. *Par convetion, le module $\{0\}$ est libre de rang 0.*
6. *Libre n'implique pas une base : $\{\overline{2}\}$ est une famille libre du $\mathbb{Z}$-module $\mathbb{Z}$ mais n'est pas une base. De même, famille génératrice n'implique pas une base : $\{\overline{1}\}$ est une famille génératrice du $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ mais n'est pas une base car $\overline{1}.\overline{2} = \overline{0}$ mais $\overline{2} \neq \overline{0}$.*

Exemple 2.67.
1. *Soit K un corps. Tout K-espace vectoriel est un K-module libre.*
2. *L'anneau des polynômes $A[X]$ est un A-module libre admettant pour base $\{1, X, X^2, X^3, \ldots\}$.*
3. *Le module $\mathbb{R}^n$ est un $\mathbb{R}$-module libre de type fini admettant pour base la famille $\{(1, 0, ..., 0), \ldots, (0, 0, ..., 1)\}$.*

2.6 Modules Noethériens

Nous avons vu qu'en général un sous-module d'un module de type fini n'est pas de type fini. Nous allons maintenant étudier une classe de modules pour lesquels cette propriété est vérifiée.

Théorème 2.68. *Soient A un anneau et M un A-module. Les assertions suivantes sont équivalentes :*

i) *(Max) Toute famille non vide de sous modules de M admet un élément maximal (Max : condition du maximum) ;*

ii) *(C.C.A) Toute suite croissante de sous modules de M est stationnaire, (i.e, constante à partir d'un certain rang) (C.C.A : condition des chaines ascendantes) ;*

iii) *(C.F) Tout sous module de M est de type fini (C.F : condition de finitude).*

Démonstration. $i) \Longrightarrow ii)$ Soit $M_1 \subseteq M_2 \subseteq ...$ une suite de sous modules de M. D'après $i)$, $\{M_i\}_{i\in I}$ admet un élément maximal, soit M_r cet élément. Il est clair que $\forall\, n \geqslant r$, $M_n = M_r$.

$ii) \Longrightarrow i)$ Supposons qu'il existe un ensemble $\mathbb{E} \neq \emptyset$ de sous modules de M qui n'admet pas d'élément maximal.

$\star$ $\mathbb{E} \neq \emptyset$, donc il existe $M_1 \in \mathbb{E}$. Puisque $\mathbb{E}$ n'admet pas d'élément maximal, il existe $M_2 \in \mathbb{E}$ tel que $M_1 \subsetneq M_2$. De même pour M_2, il existe $M_3 \in \mathbb{E}$ tel que $M_1 \subsetneq M_2 \subsetneq M_3$. Ainsi, on construit une suite strictement croissante de sous modules de M qui n'est pas stationnaire, ce qui contredit $ii)$. D'où $i)$.

ii) $\Longrightarrow$ *iii*) Supposons qu'il existe un sous module N de M qui n'est pas de type fini. Soit $a_1 \in N$, alors $a_1A \subsetneq N$ (puisque N n'est pas de type fini). Donc il existe $a_2 \in N$ tel que $M_1 := Aa_1$, $M_2 := Aa_1 + Aa_2$ et $M_1 \subsetneq M_2 \subsetneq N$. De même, il existe $a_3 \in N \backslash M_2$ tel que $M_3 = Aa_1 + Aa_2 + Aa_3$ et $M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq N$. Ainsi, on construit une suite strictement croissante de sous modules de M qui n'est pas stationnaire, ce qui est absurde. D'où *iii*).

iii) $\Longrightarrow$ *ii*) Soit $M_1 \subseteq M_2 \subseteq ... \subseteq M_n \subseteq ...$ une suite croissante de sous modules de M. Soit $N := \bigcup_{j \in I} M_j$. Alors N est un sous module de M, et d'après (*iii*), N est de type fini : $N = Aa_1 + Aa_2 + ... + Aa_n$, où $a_i \in N$ et n est un entier naturel non nul. Il existe n_0 un entier naturel tel que $a_i \in M_{n_0}$ pour tout $i = 1, ..., n$. Ainsi on a $N = M_{n_0}$ et $N = M_{n_0} = M_n$ pour tout $n \geqslant n_0$. Cela termine la preuve du Théorème 2.68. □

Définition 2.69. *On dit qu'un A-module M est Noethérien s'il vérifie les conditions équivalentes du Théorème 2.68.*

Remarque 2.70. *On considère aussi dans l'autre sens la condition de minimum (Min) et celle des chaines descendantes (C.C.D) :*

(Min) Toute famille non vide de sous modules de M admet un élément minimal.

(C.C.D) Toute suite décroissante de sous modules de M est stationnaire.

Il est facile de vérifier que $(Min) \Longleftrightarrow (C.C.D)$*. Un A module vérifiant l'une des deux conditions est dit un module Artinien.*

Définition 2.71. *On dit que l'anneau A est noethérien s'il est noethérien comme A-module, c-à-d si tout idéal de A est de type fini.*

Exemple 2.72.

1. *Les espaces vectoriels de type fini ; c'est à dire de dimension finie, sont Noethériens.*
2. *Un groupe abelien fini est un $\mathbb{Z}$-module Noethérien.*
3. *Soit k un corps, l'anneau des polynômes $A = k[X_1, ..., X_n, ...]$ avec un nombre infini d'indéterminées n'est pas noethérien. En effet, on a la suite croissante non stationnaire d'idéaux suivante : $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq ... \subsetneq (X_1, ..., X_n) \subsetneq ...$*
4. *Tout anneau principal (et en particulier un corps) est noethérien puisque tous ses ideaux sont principaux donc de type fini.*

Théorème 2.73. *Soit A un anneau, M un A-module et N un sous-module de M. M est noethérien si et seulement si, N et M/N sont noethériens.*

Démonstration. Les sous-modules de N sont des sous-modules de M contenus dans N. Donc, N est noethérien.

D'autre part, $Q = M'/N$, où $M' = \pi^{-1}(Q)$ est un sous-module de M. M est noethérien implique que M' est de type fini, donc Q l'est aussi(car si R de type fini, alors R/S l'est aussi).
Inversement, si, N et M/N sont noethériens. Soit M' un sous-module de M, alors $M' \cap N$ est un sous-module de N donc de type fini. Nous avons $M'/(M' \cap N) \simeq (M' + N)/N$ (sous-module de M/N) or M/N est noethérien donc $M'/(M' \cap N)$ est de type fini, ce qui donne que M' est de type fini(car R et S/R de type finis $\Longrightarrow$ S de type fini). □

Corollaire 2.74. *Soit* $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ *une suite exacte de A-modules. Alors M est Noethérien si et seulement si L et N sont Noethériens.*

Démonstration. Imf est un sous-module de M tel que $Imf \simeq L/\ker f = L$(car f est injectif et g surjectif). Aussi, $N = Img \simeq M/\ker g = M/Imf$(car $\ker g = Imf$). On conclut à l'aide du théorème 2.73. □

Corollaire 2.75. *Soit M un A-module, et soient N et N′ deux sous-modules noethériens de M tels que* $M = N + N'$. *Alors M est noethérien.*

Démonstration. On a une suite exacte $0 \longrightarrow N \xrightarrow{i} N + N' \xrightarrow{\pi} (N + N')/N \longrightarrow 0$. Or N est noethérien, et $(N + N')/N \simeq N'/(N \cap N')$. Comme N' est noethérien alors $(N + N')/N$, par le corollaire 2.74 $M = N' + N$ qui est noethérien. □

Corollaire 2.76. *Soient M et N des A-modules. Alors* $M \oplus N$ *est noethérien si et seulement si M et N sont noethériens.*

Démonstration. On utilise la suite exacte $0 \longrightarrow M \xrightarrow{q} M \oplus N \xrightarrow{p} N \longrightarrow 0$. □

Dans les anneaux noethérien, nous avons la caractérisation simple suivante des modules noethérien.

Proposition 2.77. *Soient A un anneau noethérien et M un A-module. Alors M est un A-module noetherien si et seulement s'il est de type fini.*

Démonstration. $\Longrightarrow$ Toujours vrai car M est un sous-module de M.
$\Longleftarrow$ M est de type fini donc M est isomorphe à un quotient d'un module libre de base fini : $M \simeq A^n/N$ avec N un sous-module de A^n. On a $A^n = A \oplus A \oplus ... \oplus A$, n fois, A est noethérien, donc A^n l'est, d'où M est noethérien. □

Exercice 2.78. *Soient A un anneau noethérien et S une partie multiplicative de A. Montrer que* $S^{-1}A$ *est noethérien.*

L'autre sens n'est pas juste.

Exercice 2.79. *A est noethérien si et seulement si tout idéal premier de A est de type fini.*

Théorème 2.80. *[Théorème de Hilbert]*

Soient A un anneau Noethérien et X une indeterminée sur A. Alors $A[X]$ *est Noethérien.*

Démonstration. Soit I un idéal de $A[X]$. Pour tout $n \in \mathbb{N}^*$, on pose J_n l'idéal de A engendré par les coefficients dominants des polynômes de degré inférieur ou égal à n dans I. La suite $\{J_n\}_{n\in N^*}$ est une famille croissante d'idéaux de A. Soit $J := \biguplus_n J_n$ qui est un idéal de A, et qui sera de type fini puisque A est Noethérien. Posons $J = (a_1, ..., a_r)$ et soient $f_1, ..., f_r$ les polynômes de I dont les coefficients dominants sont les a_i. Alors chaque $f_i = a_i X^{n_i} + g_i$, avec $n_i = deg(f_i)$ et $deg(g_i) \leqslant n_i - 1$.
Soit $\omega = max\{n_i / 1 \leqslant i \leqslant r\}$. Soit f un élément quelconque de I, alors $f = aX^m + g$ où $m = deg(f)$ et $deg(g) \leqslant m - 1$. Par construction $a \in J$ (coefficient dominant de f), donc $a = \sum_{i=1}^{r} a_i u_i$ où $u_i \in A$. Si $m > \omega$, soit $f' = f - \sum_{i=1}^{r} u_i f_i X^{m-n_i} \in I$ (car f et $f_i \in I$). Ainsi on a $f \equiv f' mod(f_1, ..., f_r)$. Il suffit donc de traiter les polynômes de degré inférieur ou égal à ω.
Soit B le A-module des polynômes de degré inférieur à ω. Ainsi $(1, X, ..., X^\omega)$ est une base du A-module libre de type fini B.
Comme A est Noethérien, alors B est Noethérien puisque B est un A-module de type fini. Dés lors, $I \bigcap B$ est de type fini comme idéal de B. Soit $(g_1, ..., g_s)$ un systéme générateur de $I \bigcap B$. On a $f' = \sum_{i=1}^{s} h_i g_i$, $h_i \in B \subseteq A[X]$ et $f = f' + \sum_{i=1}^{r} u_i f_i X^{m-n_i}$, d'où $f \in (g_1, ..., g_s, f_1, ..., f_r)$. Donc $I \subseteq (g_1, ..., g_s, f_1, ..., f_r)$. Or on a tous les $g_i \in I \bigcap B \subseteq I$ et tous les $f_i \in I$, par suite $(g_1, ..., g_s, f_1, ..., f_r) \subseteq I$. Dés lors on a $I = (g_1, ..., g_s, f_1, ..., f_r)$, ce qui termine la preuve du Théorème. □

Corollaire 2.81. *Soient A un anneau noethérien alors $A[X_1, ..., X_n]$ est un anneau noethérien.*

Démonstration. Par récurrence sur n et en utilisant le Théorème de Hilbert. □

CHAPITRE 3

Introduction à la géométrie algébrique

Une des applications les plus importantes et les plus intéressantes de la théorie des modules(anneaux) se trouve dans l'étude de la géométrie algébrique, c'est à dire l'étude des solutions d'un système d'équations algébrique dans l'espace affine.

3.1 Elément entier sur un anneau

Dans tout ce qui suit, les anneaux seront commutatifs.

Définition 3.1. *Soit B un anneau, A un sous-anneau de B. Un élément $x \in B$ est dit entier sur A, s'il est racine d'un polynôme unitaire à coefficients dans A c-à-d. s'il existe $a_1, a_2, ..., a_n \in A$ tel que : $x^n + a_1x^{n-1} + ... + a_n = 0$; une telle relation est appelée relation de dépendance intégrale de x sur A.*

$\longrightarrow$ Les éléments de A sont entier sur A.
$\longrightarrow$ Lorsque A est un corps, un élément est entier sur A s'il est algébrique sur A.

Proposition 3.2. *Soit A un sous-anneau d'un anneau B et x un élément de B. Les conditions suivantes sont équivalentes :*

1. *x est entier sur A ;*
2. *le sous-anneau $A[x]$ engendré par A et x est un A-module de type fini ;*
3. *il existe un sous-anneau C de B, tel que $A[x] \subseteq C$ et C est un A-module de type fini.*

Démonstration. 1) $\Longrightarrow$ 2) x est entier sur A, donc $\exists a_1, a_2, ..., a_n \in A$ tel que $x^n + a_1x^{n-1} + ... + a_n = 0$. Montrons que $A[x] =< 1, x, x^2, ..., x^{n-1} >$. En effet, on a $x^n = -a_1x^{n-1} - ... - a_n$ donc $\forall r \geqslant n$ $x^r \in < 1, x, x^2, ..., x^{n-1} >$ d'où $A[x]$ est engendré par $\{1, x, x^2, ..., x^{n-1}\}$.
2) $\Longrightarrow$ 3) Il suffit de prendre $C = A[x]$.
3) $\Longrightarrow$ 1) Soit C un sous-anneau de B tel que C est un A-module de type fini engendré par $\{y_1, y_2, ..., y_n\}$ et $A[x] \subseteq C$, alors $y_ix \in C$, pour tout $i = 1, ..., n$. Donc, il existe $(a_{i,j})_{1 \leqslant j \leqslant n}$ tel que $y_ix = \sum_{j=1}^{n} a_{ij}y_j$, $a_{i,j} \in A$. Nous avons

$$(x - a_{1,1})y_1 - a_{1,2}y_2 - ..... - a_{1,n}y_n = 0$$

$$a_{2,1}y_1 - (x - a_{2,2})y_2 - ..... - a_{2,n}y_n = 0$$

.....

$$a_{n,1}y_1 - ..... - a_{n,n-1}y_{n-1} - (x - a_{n,n})y_n = 0$$

Si on note α_{ij} le cofacteur de l'élément (i, j) de la matrice de ce système, si l'on multiplie par α_{ij} la i-ème ligne et que l'on somme on obtiendra :

$$det[\delta_{ij}x - a_{ij}].y_j = 0$$

où δ_{ij} est le symbole de Kronecker et $[\delta_{ij}x - a_{ij}]$ est la matrice du système précédent. Posons $d = det[\delta_{ij}x - a_{ij}]$; on aura donc $dy_j = 0$, $1 \leqslant j \leqslant n$. D'où $dC = 0$ et $d = d.1 = 0$. En développant le déterminant d, on obtient une équation de la forme : $f(x) = 0$ où $f \in A[x]$ est un polynôme unitaire de degré n. □

Corollaire 3.3. *Soit A un sous-anneau d'un anneau B, soient $x_1, x_2, ..., x_n \in B$; on suppose x_i entier sur A et pour $2 \leqslant i \leqslant n$, x_i entier sur l'anneau $A[x_1, ..., x_n]$. Alors l'anneau $A[x_1, ..., x_n]$ est un A-module de type fini.*

Démonstration. Par récurrence sur n. Pour $n = 1$, $A[x]$ est un A-module de type fini d'après la proposition 3.2.
Supposons $n > 1$ et tel que $A[x_1, ..., x_{n-1}]$ soit un A-module de type fini. Prenons $\{y_1, ..., y_n\}$ un système générateur de $A[x_1, ..., x_{n-1}]$. On a x_n entier sur $A[x_1, ..., x_{n-1}]$ donc $A[x_1, ..., x_n] = A[x_1, ..., x_{n-1}][x_n]$ est un $A[x_1, ..., x_{n-1}]$-module de type fini.
Soit $\alpha \in A[x_1, ..., x_n]$, il existe $(\lambda_i) \subseteq A[x_1, ..., x_{n-1}]$ tel que $\alpha = \sum_{i=1}^{r} \lambda_i z_i$ d'autre part, $\forall 1 \leqslant i \leqslant r$, $\exists (\alpha_{ij})_{1 \leqslant i,j \leqslant n} \subseteq A$ tel que $\lambda_i = \sum_{j=1}^{n} \alpha_{ij} y_j$ donc $\alpha = \sum_{i=1}^{r} \sum_{j=1}^{n} \alpha_{ij} z_i y_j$ d'où $\{z_i y_j, 1 \leqslant i, j \leqslant n\}$ engendre $A[x_1, ..., x_n]$ comme un A-module. □

Corollaire 3.4. *Soit A un sous-anneau d'un anneau B. L'ensemble C des éléments de B entiers sur A est un sous-anneau de B qui contient A.*

Démonstration. $\forall x \in A$, x est entier sur A donc $A \subseteq C$.
Soient $x, y \in C$, alors $A[x, y]$ est un A-module de type fini d'après le corollaire 3.3. On a xy et $x + y$ dans $A[x, y]$, or $A[xy] \subseteq A[x, y] \subseteq C$ et $A[x \pm y] \subseteq A[x, y] \subseteq C$ par 3) du proposition 3.2, donc $xy \in C$ et $x - y \in C$. □

Définition 3.5. *Soit A un sous-anneau d'un anneau B. L'anneau C de tous les éléments entier sur A, est appelé la fermeture intégrale de A dans B. On la note $\overline{A}^B$.*

Si $A = \overline{A}^B$, on dit que A est intégralement fermé dans B.
Si $B = \overline{A}^B$, on dit que B est entier sur A, ou que B est une extension entière de A. C-à-d, B est entier sur A, ou que B est une extension entière de A si tout élément de B est entier sur A.
D'après la proposition 3.2 : On a si B est un A-module de type fini alors B est entier sur A.

Proposition 3.6. *(Transitivité) Soit A, B deux sous-anneaux d'un anneau C tels que $A \subseteq B$. Si C est entier sur B et B est entier sur A, alors C est entier sur A.*

Démonstration. Soit $x \in C$, alors il existe $(b_i)_{1 \leqslant i \leqslant n} \in B$ tels que : $x^m + b_1 x^{m-1} + ... + b_m = 0$. Donc x est entier sur $A[b_1, ..., b_m]$, d'autre part $b_1, ..., b_m$ sont entier sur A, donc $A[b_1, ..., b_n, x]$ est un A-module de type fini, d'où x est entier sur A. □

Corollaire 3.7. *Soit A un sous-anneau d'un anneau C et soit B la fermeture intégrale de A dans C. Alors B est intégralement fermé dans C, i.e $B = \overline{B}^C = \overline{A}^C$.*

Démonstration. Soit $x \in C$, entier sur B i.e $x \in \overline{B}^C$, donc x entier sur $A \Longrightarrow x \in B = \overline{A}^C = \{x \in C, x \text{ entier sur } A\} \Longrightarrow \overline{B}^C \subseteq B$. Comme $B \subseteq \overline{B}^C$ est toujour vrai, nous avons $B = \overline{B}^C$. □

Proposition 3.8. *Soit A un sous-anneau d'un anneau B, tel que B est entier sur A. Soit I un idéal de B et $J = I \cap A$, alors B/I est entier sur A/J.*

Démonstration. Soit $\overline{x} \in B/J$, alors il existe $a_1, ..., a_n \in A$ tels que $x^n + a_1 x^{n-1} + ... + a_n = 0$ on en déduit $\overline{x}^n + \overline{a_1}.\overline{x}^{n-1} + ... + \overline{a_n} = \overline{0}$, c-à-d, $\overline{x}$ est entier sur A/J. □

Proposition 3.9. *Soit A un sous-anneau d'un anneau B sur lequel B est entier. Soit S une partie multiplicative de A. Alors $S^{-1}B$ est entier sur $S^{-1}A$.*

Démonstration. Soit $\frac{b}{s} \in S^{-1}B$, $b \in B$ $s \in S$, nous avons $b^n + a_1 b^{n-1} + ... + a_n = 0$, $a_i \in A \Longrightarrow \frac{b^n}{s^n} + \frac{a_1}{s}(\frac{b}{s})^{n-1} + ... + \frac{a_n}{s^n} = \frac{0}{1} \in S^{-1}B$.

□

Lemme 3.10. *(de normalisation de Noether)*
Soient K un corps et A une K-algèbre de type fini. Il existe alors un entier d et un homomorphisme injectif $K[X_1, X_2, ..., X_d] \longrightarrow A$ tel que A soit entier sur $K[X_1, ..., X_d]$.

Corollaire 3.11. *Soit K un corps. Si une K-algèbre de type fini est un corps, alors c'est une extension algébrique de K.*

3.2 Théorème de montée

Proposition 3.12. *Soit A un sous-anneau d'un dommaine d'intégrité B sur lequel B est entier. Alors B est un corps si et seulement si A est un corps.*

Démonstration. Supposons que B est un corps, soit $a \in A$ non nul, alors $a^{-1} \in B$ et a^{-1} entier sur A. Soit $(a_i)_{1\leqslant i\leqslant n} \subseteq A$ tel que $(a^{-1})^n + a_1(a^{-1})^{n-1} + ... + a_n = 0$ donc $(a^{-1})^n(1 + a_1a + a_2a^2 + ... + a_na^n) = 0$, d'où $1 + a_1a + a_2a^2 + ... + a_na^n = 0$(B est un D.I) $\Longrightarrow 1 = a(-a_1 - a_2a - ... - a_na^{n-1})$ donc a est inversible dans A d'inverse $a^{-1} = -a_1 - a_2a - ... - a_na^{n-1}$.
Supposons que A est un corps, soit $b \in B$. Montrons que b est inversible dans B.
$b \in B \Longrightarrow b$ est entier sur $A \Longrightarrow \exists a_1, ..., a_n \in A$ tels que $b^n + a_1b^{n-1} + ... + a_n = 0 \Longrightarrow b^n + a_1b^{n-1} + ... + a_{n-1}b = -a_n \Longrightarrow b(b^{n-1} + a_nb^{n-2} + ... + a_{n-1}) = -a_n \Longrightarrow b(-a_n^{-1}(b^{n-1} + a_nb^{n-2} + ... + a_{n-1})) = 1$
d'où b est inversible dans B. □

Corollaire 3.13. *Soit A un sous-anneau d'un anneau B sur lequel B est entier. Soit Q un idéal premier de B. Posons $P = A \cap Q$. Alors Q est un idéal maximal de B si et seulement si P est un idéal maximal de A.*

Démonstration. B/Q un domaine d'intégrité entier sur A/P. Q maximal $\Longleftrightarrow B/Q$ corps $\Longleftrightarrow A/P$ corps $\Longleftrightarrow P$ maximal □

Corollaire 3.14. *Soit A un sous-anneau d'un anneau B sur lequel B est entier. Soient Q et Q' deux idéaux premiers de B tels que $Q \subseteq Q'$. Si $Q' \cap A = Q' \cap A$ alors, $Q = Q'$.*

Démonstration. Posons $P = Q \cap A = Q' \cap A$ et $S = A \setminus P$ donc $S \cap Q = S \cap Q' = \emptyset$ il suffit de montrer que $S^{-1}Q = S^{-1}Q'$.
On a $S^{-1}B$ est entier sur $S^{-1}A = A_P$ donc $S^{-1}Q \cap A_P = S^{-1}(Q \cap A) = S^{-1}P$ qui est maximal dans A_P d'où $S^{-1}Q$ est maximal dans $S^{-1}B$.
$S^{-1}Q' \cap A_P = S^{-1}P$, donc $S^{-1}Q'$ est maximal dans $S^{-1}B$. Or $Q \subseteq Q'$ donc $S^{-1}Q \subseteq S^{-1}Q'$ d'où $S^{-1}Q = S^{-1}Q'$, ce qui montre que $Q = Q'$. □

Théorème 3.15. *(Théorème de montée)*
Soit A un sous-anneau de B tel que B est entier sur A. Si P est un idéal premier de A, il existe Q un idéal premier de B tel que $P = Q \cap A$.

Démonstration. Soit $S = A \setminus P$ on a $S^{-1}B$ est entier sur $S^{-1}A = A_P$. Soit N un idéal maximal de $S^{-1}B$, alors il existe $Q \in Spec(B)$ tel que $Q \cap S = \emptyset$ et $N = S^{-1}Q$ et $S^{-1}Q \cap A_P = N \cap A_P$ est un idéal maximal de A_P (Corollaire 3.13). Or A_P est local d'idéal maximal $S^{-1}P$ donc $S^{-1}Q \cap S^{-1}A = S^{-1}P$ c-à-d $S^{-1}(Q \cap A) = S^{-1}P \Longrightarrow Q \cap A = P$. □

Théorème 3.16. *(2em Théorème de montée) Soit A un sous-anneau d'un anneau B sur lequel B est entier. Si $P_1 \subseteq P_2$ sont deux idéaux premiers de A et si Q_1 est un idéal premier de B tel que $P_1 = A \cap Q_1$, il existe un idéal premier Q_2 de B tel que : $Q_1 \subseteq Q_2$ et $P_2 = A \cap Q_2$.*

3.3 Théorème des zéros de Hilbert

Dans la suite, on fixe un corps algébriquement clos K. Soit n un entier positif et posons $A = k[X_1, ..., X_n]$. Pour tout sous-ensemble S de A, considérons l'ensemble

$$Z(S) = \{(x_1, ..., x_n) \in K^n; f(x_1, x_2, ..., x_n) = 0 \quad \forall f \in S\}.$$

Définition 3.17. *Un sous-ensemble V de K^n est un ensemble algébrique s'il existe un sous-ensemble S de A tel que $V = Z(S)$.*
$\longrightarrow$ $Z(S)$ est un idéal de K^n.

Réciproquement, pour tout sous-ensemble V de K^n, on définit l'idéal de A suivant

$$I(V) = \{f \in A; f(x_1, ..., x_n) = 0 \quad \forall (x_1, ..., x_n) \in V\}.$$

Exemple 3.18. *1. L'ensemble vide est un ensemble algébrique, $V(\{1\}) = \emptyset$.*

2. $Z(\{X\}) =$ Droite.

3. $Z(\{X^2 + Y^2 - 1\}) =$ Cercle.

4. $Z(\{X, Y\}) = \{(0, 0)\}$.

5. Un point $(a_1, ..., a_n) \in K^n$ est toujours un ensemble algébrique. En effet,

$$\{(a_1, ..., a_n)\} = Z(X_1 - a_1, ..., X_n - a_n) \text{ (Voir le lemme 3.23) .}$$

6. Deux sous-ensembles de A peuvent définir les mêmes ensembles algébriques. Par exemple, on a $Z(X) = Z(X^2) = Z(X^k), k \in \mathbb{N}^*$.

Proposition 3.19. *1. Soient S et T des parties de A.*

a) *Si $S \subset T$, alors $Z(T) \subset Z(S)$.*

b) *$Z(A) = \emptyset$ et $Z(\{0\}) = K^n$*

c) *Soit $< S >$ l'idéal de A engendré par S. On a $Z(< S >) = Z(S)$.*

d) *Si J et L sont deux idéaux de A, on a :*

$$Z(J + L) = Z(J) \cap Z(L) \text{ et } Z(JL) = Z(J \cap L) = Z(J) \cup Z(L).$$

2. Si U et V sont deux sous-ensembles de K^n.

a) *$I(U) \cap I(V) = I(U \cap V)$.*

b) *Si $U \subset V \subset K^n$ alors $I(V) \subset I(U)$.*

c) *$I(K^n) = \{0\}$ et $I(\emptyset) = A$.*

d) *Pour tout idéal J de A, $J \subset I(Z(J))$.*

e) *Pour tout sous-ensemble V de K^n, on a une inclusion $V \subset Z(I(V))$.*

On a égalité si et seulement si Z est un ensemble algébrique. En effet, si $V = Z(I(V))$ alors V est un ensemble algébrique. Inversement, supposons que V soit un ensemble algébrique et soit $S \subset A$ tel que $V = Z(S)$, on a $S \subset I(V)$ (car $I(V) = I(Z(S)) \supset S$) $\Longrightarrow Z(I(V)) \subset Z(S) = V$, d'où $Z(I(V)) \subset V$.

Corollaire 3.20. *Tout sous-ensemble fini de K^n est un ensemble algébrique.*

Démonstration. On a vu que tout point est un ensemble algébrique (Exemple). On conclue par la proposition. □

Remarque 3.21. *1. Si V n'est pas algébrique, on a pas l'égalité $V = Z(I(V))$. Par exemple, $K = \mathbb{R}$ et $V = \{x \in \mathbb{R}, 0 < x < 1\}$. Alors $I(V) = \{0\}$: un élément $P \in I(V) \subset \mathbb{R}[X]$ a une infinité de racines et est donc nul. Par contre, on a $Z(I(V)) = Z(\{0\}) = \mathbb{R} \supsetneq V$.*

2. L'inclusion $J \subset I(Z(J))$ est en général une inclusion stricte. Il y a deux raisons à celà :

a) *Si K n'est pas algébriquement clos, alors les ensembles algébriques ne voient pas toutes les solutions. Par exemple soit $K = \mathbb{R}$ et $J = (X^2+Y^2+1)$. On a $Z(J) = Z(\{X^2+Y^2+1\}) = \emptyset$; et donc $J \subsetneq R[X, Y] = I(Z(J))$.*

b) *$Z()$ ne voit pas les puissances supérieures. Par exemple, soit $I = (X^2) \subset K[X]$. On a $Z(I) = \{0\}$ et $I(Z(I)) = (X) \supsetneq (X^2) = I$.*

Ce sera notamment le sujet des différents théorèmes de Hilbert(les fameuse "Hilbert Nullstellensätze"), où nous étudierons plus en détail le lien entre J et $I(Z(J))$.

Définition 3.22. *L'anneau des fonctions régulières d'un ensemble algébrique $V \subset K^n$ est le quotient $K[V] = A/I(V)$.*

Soit $P = (x_1, ..., x_n) \in K^n$ tel que $P \in V$ avec V un ensemble algébrique.
On définit un homomorphisme d'évaluation $e_P : A \longrightarrow K$ qui associe à un polynôme $f \in A$ sa valeur en P.

$$\begin{array}{rccc} e_P & : & A & \longrightarrow & K \\ & & f & \longrightarrow & e_P(f) = f(p) \end{array}$$

On a $I(V) \subset \ker e_p$, on obtient un homomorphisme $e_P : K[V] \longrightarrow K$. De plus, $e_P(c) = c$, pour tout $c \in K$.

Lemme 3.23.

$$I(P) =< X_1 - x_1, X_2 - x_2, ..., X_n - x_n > .$$

Démonstration. Pour tout $i = 1, .., n$, $X_i - x_i \in I(P)$, d'où $< X_1 - x_1, X_2 - x_2, ..., X_n - x_n > \subseteq I(\{P\})$.
Réciproquement, soit $f \in I(P)$, on fait une division euclidienne de f par $X - x_1$: $f = (X - x_1)q_1 + r_1$ avec $q_1 \in A$ et $r_1 \in K[X_2, ..., X_n]$. En itérant ce procédé, on arrive finalement à l'identité

$$f = (X - x_1)q_1 + ... + (X - x_n)q_n + c, \qquad c \in K$$

$f \in I(P) \Longrightarrow f(x_1, ..., x_2) = 0 \Longrightarrow c = 0$.
Donc, $f = (X - x_1)q_1 + ... + (X - x_n)q_n \in < X_1 - x_1, X_2 - x_2, ..., X_n - x_n >$.
D'où, $I(P) \subseteq < X_1 - x_1, X_2 - x_2, ..., X_n - x_n >$. □

Remarque 3.24. *L'écriture correcte serait $I(\{P\})$, afin de ne pas alourdir les notations, nous avons néanmoins préféré omettre les accolades.*

Théorème 3.25. *Les trois propriétés équivalentes suivantes sont vérifiées :*

1. (forme faible). Si M est un idéal maximal de A alors il existe un point $P \in K^n$ tel que

$M = I(P)$.

2. *(Existence des zéros). Pout tout idéal propre J de A, l'ensemble algébrique $Z(J)$ est non vide.*
3. *(forme forte). Pour tout idéal J de A, on a l'identité $I(Z(J)) = \sqrt{J}$.*

Démonstration. Commençons par montrer l'équivalence des trois formulations, en démontrant les implications 1) $\Longrightarrow$ 2) $\Longrightarrow$ 3) $\Longrightarrow$ 1).
1) $\Longrightarrow$ 2). Soit J un idéal propre de A, il existe un idéal maximal M tel que $J \subset M$. D'après 1), $\exists P \in \mathbb{K}^n$ tel que $M = I(P) \Longrightarrow Z(M) = Z(I(P)) \subset Z(J) \Longrightarrow Z(M) \neq \emptyset$. Donc, $Z(J) \neq \emptyset$.
2) $\Longrightarrow$ 3). Soit J un idéal de A. A est noethérien, l'idéal J possède un système de générateur fini. Soit $f_1, ..., f_m$ des générateurs.
Il s'agit de prouver que

$$\sqrt{J} = I(Z(J)) = \{g \in A, f_i(a_1, ..., a_n) = 0 \Longrightarrow g(a_1, ..., a_n) = 0, \quad i = 1, ..., m\}.$$

On a $\sqrt{J} \subset I(Z(J))$: si $f \in \sqrt{J} \Longrightarrow \exists r \geqslant 1$ tel que $f^r \in J \Longrightarrow \forall (x_1, ..., x_n) \in Z(J), f^r(x_1, ..., x_n) = f(x_1, ..., x_n)^r = 0 \Longrightarrow f(x_1, ..., x_n) = 0$, donc $f \in I(Z(J))$.
Réciproquement, soit $g \in J$ et $R =< f_1, ..., f_m, Yg - 1 >$ on a :

$$\{(a_1, ..., a_n, b) \in K^{n+1}, h(a_1, ..., a_n, b) = 0 \quad \forall h \in R\} = \emptyset$$

car $(1 - Xg)h(a_1, ..., a_n, b) \neq 0$.
D'après 2) $R = K[X_1, X_2, .., X_n, Y]$ donc on a $1 = \sum_{i=1}^{m} h_i(X_1, X_2, .., X_n, Y)f_i + l(X_1, X_2, .., X_n, Y)(Yg - 1)$ où $h_i, l \in K[X_1, X_2, .., X_n, Y]$. L'égalité précédente est fortiori vraie dans $K(Y)[X_1, X_2, .., X_n]$.
Posons $Z = \frac{1}{Y}$, on obtient pour un entier N, $N \geqslant 1$. $Z^N = \sum_{i=1}^{m} k_i(X_1, X_2, .., X_n, Z)f_i + m(X_1, X_2, .., X_n, Z)(g - Z)$ dans $K[X_1, X_2, .., X_n, Z]$. On substituant g à Z, on a

$$g^N \in J \Longrightarrow g \in \sqrt{J}.$$

3) $\Longrightarrow$ 1). Soit M un idéal maximal de A. $Z(M) \neq \emptyset$ car si $Z(M) = \emptyset \Longrightarrow I(Z(M)) = A$. Or $M = \sqrt{M} = I(Z(M)) = A$ et $M \neq A$ absurde. D'où, $Z(M) \neq \emptyset$. Il existe $P \in Z(M)$ tel que $M = \sqrt{M} = I(Z(M)) \subset I(P) \subset M$ (car $I(P)$ un idéal de A) et M maximal de A, d'où $I(P) = M$.
Nous terminons en démontrant la forme faible. Si M est un idéal maximal de A, on a A/M est une extension algèbrique de K ($\overline{A}^K = K$), le corps K étant algébriquement clos, on obtient $A/M = K$.
Si $x_1, x_2, ..., x_n$ les images respectives de $X_1, ..., X_n$ dans A/M, ce qui donne $< X_1 - x_1, ..., X_n - x_n >= I(P) \subset M$ or d'après le lemme 3.23 $A/I(P) \simeq K \Longrightarrow I(P)$ est maximal d'où $M = I(P)$.

□

Remarque 3.26. *Si K n'est pas algébriquement clos, les trois formulations de Hilbert ne sont plus vraies.*

Exemple 3.27. *(forme faible)*
Pour $K = \mathbb{R}$, on a $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ et $< X^2 + 1 >$ est un idéal maximal mais n'est pas de la forme $< X - a >= I(a)$ quelque soit $a \in \mathbb{R}$.

Exemple 3.28. *(Existence des zéros) Pour* $K = \mathbb{R}$ *:* $Z(< X^2 + Y^2 + 1 >) = \emptyset$.

Exemple 3.29. *(forme forte)*
Pour $K = \mathbb{R}$ *et* $J =< X^2 + Y^2 + 1 >$*, nous avons* $Z(J) = \emptyset$ *donc* $I(Z(J)) = \mathbb{R}[X, Y] \supsetneq \sqrt{J} = J$.

Bibliographie

[1] M. F. Atiyah, I. G. Macdonald (1969), Introduction to commutative algebra, Addison-Wesley.

[2] Josette Calais(2006), Eléments de théorie des anneaux-Anneaux commutatifs, Ellipses.

[3] Najib Mahdou(2013), Introduction à l'Algèbre Homologique, IPNPUB Fez, Morocco.

[4] M-P Malliavin(1985), Algèbre commutative. Applications en géométrie et théorie des nombres, Elsevier Masson.