UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES
Département des Mathématiques

Licence Sciences et Techniques (LST)

CALCUL SCIENTIFIQUE ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Localisations Des Anneaux Et Des Modules

Présenté par :

- **Rabie El Hanaoui**

Encadré par :

- **Pr. Najib Mahdou**

Soutenu Le Lundi 10 Juin 2013 devant le jury composé de:

- **Pr. Fatima Ezzaki**
- **Pr. Aziza Rahmouni Hassani**
- **Pr. Abdelmajid Hilali**
- **Pr. Chahrazade Bakkari (FS Ain Chock)**
- **Pr. Najib Mahdou**

Stage effectué à FST FES

Année Universitaire 2012 / 2013

Remerciement

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

En second lieu, nous tenons à remercier notre encadreur Mr : Najib Mahdou, pour son précieux conseil et son aide durant toute la période du travail.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

SOMMAIRE :

CHAPITRE 1
PRELIMINAIRES

1 Loi de composition interne.

1.1- DEFINITION

On appelle loi de composition interne sur un ensemble E toute application de $E\times E$ dans E.

Notation :

A tout couple $(a,b) \in E^2$; la loi associe un élément unique c dans E : a se nomme le premier terme, b le second terme et c le composé de a et b . Il y a plusieurs notation de ce composé ; parmis eux :

Notation additive : $a+b=c$;

Notation multiplicative : $ab=c$;

Autre notations : $a\top b=c$; $a\perp b=c$; $a*b=c$; ……

- **PROPRIETES SPECIALES :**

La loi de composition peut présenter certaines qualités, que l'on va étudier.

1.2- ASSOCIATIVITE :

La loi T est dite associative si :

$$(\forall a,b,c \in E)\ ;\ \ (aTb)Tc=aT(bTc).$$

Exemples :

i. L'addition et la multiplication dans $\mathbb{N}$ ou $\mathbb{Z}$ sont associatives.
ii. La réunion et l'intersection dans $P(E)$ sont associatives.

1.3- COMMUTATIVITE :

La loi T est dite commutative si :

$$(\forall a,b,c \in E)\ ;\ aTb=bTa$$

Exemples :

i. L'addition et la multiplication dans $\mathbb{N}$ sont commutatives.
ii. La réunion et l'intersection dans $P(E)$ sont commutatives.
iii. Soit dans E la loi de composition interne suivante :

$$E\times E \rightarrow E$$

$$(a,b) \rightarrow aTb=a\ .$$

Dite le premier projecteur.
Si E contient plus de deux éléments, (E,T) n'est pas commutatif.

1.4- ELEMENT NEUTRE :

On dit qu'un élément $e \in E$ est neutre pour la loi T si :

$$\forall a \in E\ ,\ aT\,e= eTa=a$$

On dit alors que la loi est unifère ou unitaire.

Exemples :

i. L'addition dans $\mathbb{N}$ possède l'élément neutre 0. La multiplication à l'élément neutre 1.
ii. Le premier projecteur sur E : $aTb = a$; n'a pas d'élément neutre si E contient plus de deux éléments.
iii. La réunion dans $P(E)$ à l'élément neutre $\emptyset$:

$$(\forall A\in P(E))\ :\ \emptyset\cup A=A\cup\emptyset=A$$

iv. L'intersection dans $P(E)$ à l'élément neutre E :

$$(\forall A\in P(E))\ :\ E\cap A=A\cap E=A$$

Proposition :
Si l'élément neutre existe ; il est unique.

Preuve :
Supposons que la loi T ait deux éléments neutres e et e' dans E; alors on a :
e neutre et $e' \in E \Rightarrow e'\,T\,e= e\,T\,e'= e'$,
et e' neutre et $e \in E \Rightarrow e\,T\,e'= e'\,T\,e= e$.
Donc $e= e'$.

1.5- ELEMENT SIMPLIFIABLE :

On dit qu'un élément *$a \in E$ est simplifiable à gauche* si :

$$(\forall\, b,c \in E)\ ;\ aTb=aTc \Rightarrow b=c.$$

On dit que $a \in E$ *est simplifiable à droite* si :

$$(\forall\, b,c \in E)\ ;\ bTa=cTa \Rightarrow b=c.$$

Si a est simplifiable à droite et à gauche ; on dit qu'il est *simplifiable.*

Remarque :
Pour une loi commutative, un élément simplifiable d'un côté est simplifiable.
Si la loi est unitaire dans E, l'élément neutre est évidemment simplifiable.

Exemples :

i. Tout nombre naturel , sauf 0, est simplifiable pour la multiplication :

$$(\forall\, x \in \mathbb{N}\ ;\ x\neq 0)\ ;\ ax=bx \Longrightarrow a=b$$

ii. Pour le premier projecteur , tout élément est simplifiable à droite :

$$a*b=b*c \Longrightarrow a=b$$

Mais aucun élément n'est simplifiable à gauche, car :

$$a*b=a*c=a\ ;\ \forall a,b,c$$

iii. Dans $P(E)$ aucun élément, sauf E, n'est simplifiable pour l'intersection et aucun élément, sauf $\emptyset$, n'est simplifiable pour la réunion.

2- Groupe :

Définition :
Un ensemble G muni d'une loi de composition interne T noté (G,T) est dit un groupe si les axiomes suivantes sont vérifiées :

i. La loi T est associative.
ii. Il existe un élément neutre.
iii. Tout élément est symétrisables. (T est symétrique si : $xTy \Longrightarrow y\,Tx\ ;\ \ \forall\, x,y \in G$)

Exemples :
$(\mathbb{Z},+)$, $(\mathbb{R}^*,\times)$.

Exemples :
Un groupe peut être fini ou infini.

- On appelle ordre d'un groupe G le nombre de ses éléments et on le note *$ord(G)$* ou $|G|$.
- Soit (G,T). Un groupe. On dit que G est abélien(ou commutatif) si la loi est commutative.

3- SOUS GROUPE D'UN GROUPE :

3.1- SOUS- GROUPE :

Dans tout ce qui suit, on va adopter la notion multiplicative d'un groupe. Ainsi on désigne dans la suite par G un groupe muni d'une loi de composition interne notée . , admettant 1 pour élément neutre, et le symétrique d'un élément x est l'élément x^{-1}.

Définition :
Un groupe H est appelé un sous groupe d'un groupe G s'il est contenu dans G, et si la loi de H est la restriction de celle de G.

Exemple fondamentale :
Tous les sous groupes non nuls de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}^*$.

Preuve :
Soit G un sous groupe de $(\mathbb{Z},+)$ et n le plus petit entier naturel non nul de G. Alors on a $n\mathbb{Z} \subset G$.
Soit $m \in G$; la division euclidienne de m par n montre qu'il existe $a \in \mathbb{N}$; $r \in \mathbb{N}$ telque : $m=an+r$ et $0 \leq r < n$. Comme on a $r = m-an \in G$, $0 \leq r < n$, et n le plus petit naturel non nul appartenant à G, alors on a nécessairement $r=0$ et $m=an \in n\mathbb{Z}$. D'où on a : $G=n\mathbb{Z}$.

Théorème (Caractérisation d'un sous groupe).
Un sous ensemble H d'un groupe G est un sous-groupe de G si et seulement si :

$$\begin{cases} H \neq \phi \\ (x,y) \in H \Rightarrow xy^{-1} \in H \quad ; \quad (\forall x, y) \end{cases}$$

Preuve :
La condition est nécessaire : si H est un groupe, l'inverse y^{-1} de y et le produit xy^{-1} de x et de y^{-1} appartenant à H.
La condition est aussi suffisante :
$x \in H \Rightarrow (x,x) \in H^2 \Rightarrow xx^{-1} = 1 \in H,$

$x \in H \Rightarrow (1,x) \in H^2 \Rightarrow 1.x^{-1} = x^{-1} \in H,$
$(x,y) \in H^2 \Rightarrow (x,y^{-1}) \in H^2 \Rightarrow x(y^{-1})^{-1} = xy \in H.$

Intersection de sous groupes :
Proposition :
Soit G un groupe. L'intersection de toute famille de sous-groupe de G est un sous groupe de G.

Preuve :
Soit $H = \bigcap_{i \in I} H_i$ l'intersection d'une famille de sous groupe H_i d'un groupe G.
H n'est pas vide car $1_G \in H$.
De plus si : $x, y \in H = \bigcap_{i \in I} H_i \Rightarrow \forall i; \quad xy^{-1} \in H_i$

$$\Rightarrow \forall i; \quad xy^{-1} \in H_i \text{ (car } H_i \text{ sous groupe de G)}$$
$$\Rightarrow xy^{-1} \in H.$$

D'où le résultat.

3.2- MORPHISME DE GROUPE :
Soient G et G' deux groupe et $f : G \rightarrow G'$ une application. f un morphisme de groupe càd :

$$\forall x,y \in G \; ; \; f(x\, y) = f(x) \, . \, f(y)$$

Propriété :
Soit e l'élément neutre de G et e' l'élément neutre de G'. Alors on a :

1. $f(e) = e'$;
2. $f(x^{-1}) = (f(x))^{-1} \quad ; \quad \forall x \in G$.

Preuve :

1. On a $f(x)=f(xe)=f(x)f(e)$; et on composant à gauche par $(f(x))^{-1}$ on obtient $f(e)=e'$.
2. On a : $f(x)f(x^{-1})=f(xx^{-1})=f(e)=e'$ et $f(x^{-1})f(x)=f(x^{-1}x)=f(e)=e'$.

   Donc nécessairement on a : $f(x^{-1})=(f(x))^{-1}$.

<u>Exemples</u> :

1. Soit G un groupe, x un élément de G ; et $<x>$ le sous groupe de G engendré par x.

   L'application :

$$f:(\mathbb{Z},+)\to <x>$$
$$n\to x^n$$

Est un morphisme de groupes. En effet on a : $f(n+m)=x^{n+m}=x^n.x^m=f(n).f(m);\forall n,m\in\mathbb{Z}$

2. Soient G un groupe et H un sous groupe distingué de G. L'application :

$$G\to G/H$$
$$x\ \to\ \overline{x}$$

Est un homorphisme surjectif de groupes.

3. L'application $f:(\mathbb{R}_+^*,.)\to(\mathbb{R},+)$

$$x\to\log(x)$$

   Est un homorphisme de groupe bijective, càd un isomorphisme de groupes.

<u>Noyau et image d'un homorphisme :</u>

<u>Proposition</u> :

Soit $f:G\to G'$ un morphisme de groupes.

1. L'image de f d'un sous-groupe de G est un sous-groupe de G'.
2. L'image réciproque d'un sous groupe de G' est un sous groupe de G.

<u>Preuve</u> : Immédiat.

<u>Cas particulier</u>

$f(G)$ est un sous groupe de G', on appelle l'image de f et on la note <u>$\mathrm{Im}(f)$.</u>

$f^{-1}(\{e'\})=\{x\in G\ /\ f(x)=e'\}$ est un sous groupe de G ; on appelle <u>le noyau de f</u> et on le note <u>$\ker(f)$</u>. On vérifie facilement que $\ker(f)$ est un sous groupe distingué de G.

<u>Théorème</u> :

Soit $f:G\to G'$ un homorphisme de groupe, N son noyau. Alors :

1. Si $b=f(x_0)\in G'$; alors $f^{-1}(b)=x_0N$.
2. f injectif si et seulement si $N=\{e\}$.

<u>Preuve</u> :

1. $x \in f^{-1}(b) \Leftrightarrow f(x) = b (= f(x_0))$
$$\Leftrightarrow f(x_0^{-1}) f(x) = e'$$
$$\Leftrightarrow f(x_0^{-1}x) = e'$$
$$\Leftrightarrow x_0^{-1}x \in N$$
$$\Leftrightarrow x \in x_0 N.$$

2. f injective $\Leftrightarrow (\forall x, y \in G; f(x) = f(y) \Rightarrow x = y)$
$$\Leftrightarrow (\forall x, y \in G; y \in xN \Rightarrow x = y)$$
$$\Leftrightarrow [\forall x \in G; xN = \{x\}\ ]$$
$$\Leftrightarrow N = \{e\}.$$

CHAPITRE 2
ANNEAUX ET IDEAUX

N.B : Toutes les lois sont supposées commutatives.

1 ANNEAUX .

1.1- DEFINITION :

- On appelle anneau un ensemble A muni de deux lois de composition internes ; une addition et une multiplication telles que :
  i. A est un groupe commutatif pour l'addition.
  ii. La multiplication est associative.
  iii. La multiplication est distributive par rapport à l'addition ; càd :
  $$\forall x, y, z \in A : x(y+z) = xy + xz \quad \text{et} \quad (y+z)x = yx + zx.$$
- Si on outre ; la multiplication est commutative, on dit que A est un anneau commutatif.
- Si A possède un élément neutre pour la multiplication, on note 1 cet élément-unité et on dit que A est un anneau unitaire.

- Un anneau A est dit <u>anneau intègre</u> si $\forall x, y \in A$ on a : $xy = 0 \Rightarrow x = 0$ ou $y = 0$.

Soit A un anneau (commutatif et unitaire).

1. Un élément non nul $a \in A$ est dit <u>un diviseur de zéro</u> si $\exists\ b(= 0) \in A$ tel que $ab(= ba) = 0$. On note par $Z\ (A)$ l'ensemble des diviseurs de zéro de A.
2. Un élément non nul $a \in A$ est dit <u>nilpotent</u> si $a^n = 0$ pour un certain $n \in N^*$.
3. Un élément $x \in A$ est dit <u>une unité de A</u> (ou bien inversible) si $\exists\ y \in A/\ xy(= yx) = 1_A$.

1.2- EXEMPLES :

i. $(\square ,+,.);(\square ,+,.)et(\square ,+,.)$ sont des anneaux commutatifs unitaires et intègres.

ii. Soit A un anneau et E un ensemble. L'ensemble $F(E,A)$ des applications de $E \rightarrow A$ muni des deux lois :

$$(f,g) \rightarrow f+g \quad \text{tel que} \quad (f+g)(x) = f(x)+g(x)\ ;\ \forall x \in E\ ;$$
$$(f,g) \rightarrow f.g \quad \text{tel que} \quad (fg)(x) = f(x)g(x)\ ;\ \forall x \in E\ ;\ \text{est un anneau unitaire.}$$

A est commutatif ; alors $F(E,A)$ est commutatif.

1.3- PROPRIETES :

Soit A un anneau commutatif. On a :

1. $x\ (y\text{-}z) = xy - xz$ et $(y\text{-}z)\ x = yx - zx$; $\forall x,y \in A$.

   <u>preuve :</u>

   on a $x\ (y\text{-}z) + xz = x\ (y\text{-}z\text{+}z) = xz$

   d'où : $x\ (y\text{-}z) = xy - xz = yz - zx = (y - z)\ x$.

2. $x.0 = 0$; $\forall x \in A$.

   on dit que 0 est un élément absorbant.

   <u>Preuve :</u>

   Il suffit de prendre $y=z$ dans 1).

3. Si A est unitaire et $a,b \in A$; alors on a $\forall n \geq 1$:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

(Formule de Binôme de Newton) où $C_n^k = \dfrac{n!}{k!(n-k)!}$.

<u>Preuve</u> :

Par récurrence sur n.

$n = 1\ ;\ (a+b)^1 = a+b = C_1^0 a^{1-0} b^0 + C_1^1 a^{1-1} b^1.$

Supposons la formule juste jusqu'à l'ordre n et montrons la pour $n+1$.

Un calcul simple donne la relation de Pascal suivante :

$$C_{n-1}^{k}+C_{n-1}^{k-1}=C_{n}^{k}$$

Ainsi on a :

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^{n}(a+b)\\
&= \left(\sum_{k=0}^{n} C_n^k a^{n-k} b^k\right)(a+b) \quad \text{(Hypothèse de récurrence)}\\
&= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k=0}^{n} C_n^k a^{n-k} b^{k+1}\\
&= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k=0}^{n} C_n^k a^{(n+1)-(k+1)} b^{k+1}\\
&= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k'=1}^{n} C_n^{k'-1} a^{n+1-k'} b^{k'} \quad \text{(avec k'= k+1)}\\
&= a^{n+1} + \sum_{k=1}^{n} C_n^k a^{n+1-k} b^k + b^{k+1} + \sum_{k=1}^{n} C_n^{k-1} a^{n+1-k} b^k\\
&= a^{n+1} + \sum_{k=1}^{n} (C_n^k + C_n^{k-1}) a^{n+1-k} b^k + b^{k+1}\\
&= C_{n+1}^{0} a^{n+1} b_0 + \sum_{k=1}^{n} C_{n+1}^{k} a^{n+1-k} b^k + C_{n+1}^{n+1} a^0 b^{n+1} \quad (pascal)\\
&= \sum_{k=0}^{n+1} C_{n+1}^{k} a^{(n+1)-k} b^k\end{aligned}$$

→ alors on a : $\forall a,b \in A$:

$$(a+b)^n = \left(\sum_{k=0}^{n} C_n^k a^{n-k} b^k\right)$$

2- SOUS-ANNEAUX ; HOMOMORPHISME-ET-IDEAUX :

2.1- Sous anneau :

Une partie A d'un anneau B est un sous anneau de B si elle est un sous groupe additif et si elle est stable par le produit. Un sous anneau et un anneau.

Exemple :

1. $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$.
2. Les fonctions polynômes définies sur $\mathbb{R}^n$ à valeurs réelles forment un anneau de l'anneau des fonctions de $\mathbb{R}^n$ à valeurs réelles.

Sous anneau engendré par une partie :

On vérifie facilement que toute intersection de sous anneaux de A est un sous anneau de A.
Soient A un anneau et S une partie de A. On définit le sous anneau de A engendré par S par :

$B(S)$= intersections des sous anneaux de A contenant S.

C'est le plus petit sous anneau de A contenant S. on montre facilement qu'on a aussi :

$$B(S)=\left\{\sum_{fini}\pm(t_1t_2...t_n)\,/\,t_i\in S, n\in \mathbb{N}\right\}$$

→Sauf mention du contraire, tout les anneau considérés par la suite , sont supposés commutatifs et unitaires.

2.2- HOMOMORPHISME - IDEAUX :

- **Homomorphisme *:***

Une application f d'un anneau A dans un anneau B est un homomorphisme (ou morphisme) si elle satisfait aux relations :

$$f(a+b)=f(a)+f(b)$$

$$f(ab)=f(a).f(b)$$

Pour tout a,b dans l'anneau A.

Exemples :

L'injection canonique d'un sous anneau A d'un anneau B (càd $A\hookrightarrow B$) dans B est un morphisme d'anneaux.

Définition :

Un endomorphisme est un morphisme d'un anneau A dans lui-même. Un isomorphisme et un morphisme bijectif. Un automorphisme est un endomorphisme bijectif.

- **Idéal** :

Un ensemble I d'un anneau (A , + , .) est dit un idéal de A si on a :

$$(I,+) \text{ est un groupe}$$

$$\forall x\in I; \forall y\in A \text{ ; on a } xy\in I.$$

Théorème :

1. Le noyau d'un morphisme est un idéal.
2. Un morphisme est injectif si et seulement si son noyau est nul.

Preuve :

1. Soit f un morphisme d'un anneau A dans un anneau B. Le noyau est un groupe additif puisque le morphisme est aussi un morphisme de groupe additif. En outre, si $a\in\ker(f)$ et $b\in A$ alors on a : $f(ab)=f(a).f(b)=O_b.f(b)=O_B$; et donc $ab\in\ker(f)$.
2. Si le morphisme est injectif, le zéro a un seul antécédent : $\ker(f)=\{0\}$. Réciproquement ; l'égalité $f(x)=f(y)$ entraîne $f(x-y)=0$: càd : $x-y\in\ker(f)=\{0\}$ et par suite $x=y$ et f est injectif.

Proposition :

1. L'image d'un idéal par un morphisme est un idéal.
2. L'image réciproque d'un idéal par un morphisme est un idéal.

Preuve : Trivial.

- ***Anneau quotient :***

Soit I un idéal de A. On a A/I muni de la loi additive $(\bar{x},\bar{y}) \to \overline{x+y}$ est un groupe commutatif car $(A,+)$ est un groupe commutatif. On définit de même sur A/I la loi multiplicative suivante : $(\bar{x},\bar{y}) \to \overline{x.y}$.
En effet :

$$\left.\begin{array}{l}\bar{x}=\overline{x'} \Rightarrow x=x'+u \,/\, u\in I \\ \bar{y}=\overline{y'} \Rightarrow y=y'+v \,/\, v\in I\end{array}\right\} \Rightarrow xy=x'y'+\underbrace{uy'+vx'+uv}_{\in I}.$$

I étant un idéal ; alors $uy'+vx'\in I$ et par suite $xy-x'y'\in I$ càd : $\overline{xy}=\overline{x'y'}$.
A/I muni des deux lois citées précédemment est un anneau commutatif unitaire.
On appelle <u>l'anneau quotient de A par I</u>. L'homomorphisme d'anneau $A \to A/I$ est appelé <u>l'homomorphisme canonique.</u>

<u>Application</u> :
Soit $f: A \to B$ un homomorphisme d'anneaux. Alors la décomposition de f donne l'isomorphisme d'anneaux :

$$A/Ker(f) \cong \mathrm{Im}(f)$$

<u>Exemples</u> :
1. Soit $n\in \mathbb{Z}$. Comme on $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,.)$: alors $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire. On appelle l'anneau des entiers modulo n.
2. Soit A un anneau, comme $\{0\}$ et A sont des idéaux impropres de A ; on vérifie facilement que : $A/\{0\}\cong A$ et $A/A\cong\{0\}$.

<u>3- CORPS :</u>

3.1- DEFINITION :

- Un corps est un anneau unitaire dans lequel tout élément non nul est inversible ; càd que $A^*=A\setminus\{0\}$ est un groupe pour la multiplication.
- Si la multiplication d'un corps est commutative : on dit que le corps est commutatif.
- Tout corps est intègre : $ab=0$ et $a\neq 0 \Rightarrow a^{-1}ab=b=0$.
- Tout corps contient 1 et 0 avec $(1\neq 0)$.

3.2- CARACTERISATION D'UN CORPS :

Soit A un anneau non nul. 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 de A dans un anneau est injectif.

<u>Preuve</u> :

i.$\Longrightarrow$ ii. Soit $I\neq\{0\}$ un idéal. Soit $x\in I$ et $x\neq 0$ alors $1=x^{-1}x\in I$ et par suite

on a : $I=A$.

ii .⟹iii. Soit $f: A \to B$ un morphisme d'anneaux non nul avec $B \neq \{0\}$. Càd : $\exists x \in A / f(x) \neq 0$. Par suite $x \notin \ker(f)$ est un idéal : donc d'après ii. On a $\ker(f) = \{0\}$ et par suite f est injectif.

iii.⟹i. soit $x \in A$ et x non inversible. On veut montrer que $x = 0$. Comme x est non inversible, alors $B = A / xA \neq 0$ (car $A \neq xA$) : et par suite on a : $f: A \to B = A / xA$, où $f(z) = \overline{z} = z + xA$, qui est non nul (car $B \neq 0$) est un morphisme qui est injectif d'après iii. Or on a : $f(0) = \overline{0} = \overline{x} = f(x)$. Donc $x = 0$ car f est injectif.

<u>**Proposition :**</u>

Tout anneau unitaire intègre fini est un corps.

<u>**Preuve**</u> :

Soit A un tel anneau et soit $a \in A$; avec $a \neq 0$.

Soit

$$\begin{aligned} f: A &\to A \\ a &\to ax \end{aligned}$$

- f est une application injective car $a \neq 0$ et A est intègre.
- f est bijective car A fini. Donc $\exists b \in A$ tel que : $ab = 1 = ba$

Ainsi on a : $ab = ba = 1$ (car toutes les lois sont supposées commutatif) , et a est inversible.

<u>THEOREME DE WEDDERBURN (Admis).</u>

Tout corps fini est commutatif.

<u>4- IDEAUX PREMIERES – IDEAUX MAXIMAUX :</u>

Soit P un idéal d'un anneau commutatif (A , + , .).

- P est dit <u>premier</u> si $\forall x,y \in A,\ xy \in P \Rightarrow x \in P$ ou $y \in P$.
- P est dit <u>maximal</u> si $P \neq A$ et si les seules idéaux compris entre P et A sont P et A.

<u>**Théorème :**</u>

Soit A un anneau commutatif unitaire et P un idéal de A. Alors on a :

1. P premier $\Leftrightarrow$ A/P intègre.
2. P maximal $\Leftrightarrow$ A/P corps.

<u>**Prevue:**</u>

1. Supposons P premier et montrons que A/P intègre. Soit $a,b \in A$ tel que :

   $\overline{ab} = \overline{0}$ et $\overline{a} \neq \overline{0}$. Ces relations se traduisent dans A par $ab \in P$ et $a \notin P$.

   L'hypothèse P premier entraine que $b \in P$; càd $\overline{b} = \overline{0}$.

Réciproquement, supposons A/P intègre, et considérons deux éléments a et b de A tel que $ab \in P$. Par passage au quotient on obtient $\overline{ab} = \overline{a}\,\overline{b} = 0$.

Puis $\overline{a} = 0$ ou $\overline{b} = 0$; donc $a \in P$ ou $b \in P$. Ainsi P est un idéal premier.

2. Supposons que M est maximal et montrons que A/M est un corps. Soit $a \in A$ tel que $\overline{0} \neq \overline{a} \in A/M$. Montrons que $\overline{a}$ est inversible dans A/M. Pour cela considérons l'idéal $aA+M$ qui contient strictement l'idéal M (car $a \notin M$).
A cause de la maximalité de M on a $aA + M = A$. Ainsi il existe $t \in A$ et $u \in M$ tel que : $1 = at + u$. Par passage aux classes modulo M, On obtient $\overline{a}\overline{t} = \overline{1}$. Ainsi la classe de a est inversible dans A/M ; et l'anneau A/M est un corps.

Réciproquement, supposons que A/M et un corps ; et prenons un idéal I contenant strictement M. Soit $a \in I - M$. On a $\overline{a} \neq 0$ car $a \notin M$, et par suite $\overline{a}$ est inversible dans A/M ; càd $\exists t \in A$ tel que $\overline{1} = \overline{at}$ ou : $\overline{a - at} = \overline{0}$, ou $1 - at \in M \subseteq I$. Donc

$1 = \underbrace{(1 - at)}_{\in M \subseteq I} + \underbrace{at}_{\in I} \in I$ et par suite :

$I = A$. Ainsi on a M est un idéal maximal de A.

<u>Corollaire :</u>
Un idéal maximal est premier car un corps est un anneau intègre.

<u>Théorème de Krull : (Admit)</u>
Tout idéal propre de A est inclu dans un idéal maximal.

CHAPITRE 3

LES MODULES

1- Modules

Définition

Soit A un anneau. Un A-module est un ensemble M muni d'une loi de groupe abélien $(M, +)$ et d'une application (modulation) de $A \times M \longrightarrow M$
telles que :

$$\begin{cases} a(x+y) = ax+ay & \\ (ab)x = a(bx) & \forall x, y \in M \\ (a+b)x = ax+bx & \forall a,b \in A \\ 1_A.x = x & \end{cases}$$

Définition

1. 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 $(0.x = 0,\ (-a)x = -ax, \dots)$.

2. Si $A = \mathbb{Z}$ et $(M, +)$ est un groupe abélien, M est muni d'une structure de $\mathbb{Z}$-module à travers la modulation :

$$\begin{aligned} \mathbb{Z} \times M &\rightarrow M \\ (n, x) &\rightarrow nx = \underbrace{x + \dots + x}_{n\ fois} \end{aligned}$$

Ainsi, il n'y a aucune différence entre la structure de $\mathbb{Z}$-module et celle du groupe abélien.

3. Si I est un idéal de A, alors I est un A-module à travers la modulation :

$$\begin{aligned} A \times I &\rightarrow I \\ (a, x) &\rightarrow ax. \end{aligned}$$

4. Soient B un anneau et A un sous-anneau de B. L'anneau B est de manière naturelle un A-module à travers la modulation :

$$\begin{aligned} A \times B &\rightarrow B \\ (a, b) &\rightarrow \text{ab}. \end{aligned}$$

Exemple

Soient M et N deux A-modules. On appelle un A-homorphisme
(Ou application A-linéaire) de M dans N toute application $f : M \rightarrow N$ telle que :

$$f(x+y) = f(x) + f(y) \qquad \forall x, y \in M$$
$$f(ax) = af(x) \qquad \forall a \in A, \forall x \in M.$$

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 :

$$\begin{aligned} u + v : M &\to N \\ x &\to (u+v)(x) = u(x) + v(x) \end{aligned}$$

et

$$\begin{aligned} au : M &\to N \\ x &\to (au)(x) = au(x). \end{aligned}$$

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

$$\begin{aligned} A \times Hom_A(M, N) &\to Hom_A(M, N) \\ (a, u) &\to au. \end{aligned}$$

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

<u>Annulateur</u> : l'ensemble $\{a \in A / ax = 0\ ;\ \forall x \in M\}$ est un idéal de A appelé annulateur de M , noté $Ann(M)$:

$$Ann(M) := \{a \in A /\ ax = 0 ; \forall x \in M\}.$$

<u>2- Sous modules, Modules quotients.</u>

<u>Définition</u>

Soit M un A-module. Une partie N de M est un <u>sous module</u> de M si $(N, +)$ est un groupe abélien et $ax \in N$ pour tout $x \in N$ et $a \in A$.

L'injection canonique $N \hookrightarrow M$ est un homomorphisme de A-modules.

<u>Proposition</u>

Soient M et N deux A-modules et $f \in Hom_A(M, N)$. Alors on a :

1. Ker $f := \{x \in M / f(x) = 0_N\}$ est un sous-module de M .
2. Im $f := \{f(x) / x \in M\}$ est un sous module de N .

<u>Preuve</u>

La même que celle des espaces vectoriels.

<u>Définition</u>

Soient M un A-module et N un sous-module de M. Sur le groupe quotient abélien M/N , on considère la modulation :

$$\begin{aligned} A \times M/N &\to M/N \\ (a, \overline{x}) &\to \overline{ax} = ax + N. \end{aligned}$$

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

L'application canonique $\varphi : M \to M / N$ est un homorphisme de A-modules avec $\ker\varphi = N$.

On a le théorème suivant :

Théorème

Soient E et F deux A-modules et $f \in Hom_A(E, F)$. Alors on a :

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

(C'est le premier théorème d'isomorphisme).

En effet : si $\varphi : E \to E / Ker(f)$ est l'homomorphisme canonique, il existe un seul isomorphisme :

$$\overline{f} : E / \ker(f) \to \mathrm{Im}(f).$$

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ s\downarrow & & \uparrow i \\ E/\ker(f) & \xrightarrow{\overline{f}} & \mathrm{Im}(f) \end{array}$$

Tel que : $f = i \, o \, \overline{f} \, o \, s$

Preuve

Il est simple de voir que :

$$\begin{aligned} \overline{f} \; &: E / Ker(f) \to Im(f) \\ \overline{x} &= x + Ker(f) \to f(x) \end{aligned}$$

est un isomorphisme et que

$$f = i \, o \, \overline{f} \, o \, s.$$

- **Opérations sur les modules**

Proposition et Définition

1. Toute intersection de sous modules d'un A-module est un A-module.
2. Soient M un A-module et S une partie de M. L'intersection de tous les sous modules de M contenant S est le plus petit sous module de M contenant S appelé sous module engendré par S. C'est aussi l'ensemble des combinaisons A-linéaires des éléments de S. Il est noté $< S >$:

$$< S > = \{ \sum_{finie} a_i \, x_i \;\; / \;\; a_i \in A \; et \; x_i \in S \}.$$

Preuve .

1. Soit $M_1, \ldots, M_n$ des sous modules d'un A-module.

Il est facile de verifier les axiomes telque : $\bigcap_{k=1}^{n} M_k$ est un A-module

2. Soient M un A-module et S une partie de M, *et* Soit $M_1,\ldots,M_n$ tout les sous modules de M contenant S.

   simple a remarquer que $\forall x \in \bigcap_{k=1}^{n} M_i \Rightarrow x \in M_k$; $\forall k \in \{1,\ldots,n\}$

   D'où $\bigcap_{k=1}^{n} M_k$ est le plut petit sous module de M contenant S.

Proposition et Définition

Soit $(M_i)_{i\in I}$ une famille de sous-modules d'un A-module M . Le sous-module engendré par $\bigcup_{i\in I} M_i$ est l'ensemble des éléments de la forme $\sum_{finie} x_i$ tels que $x_i \in M_i$, on l'appelle la somme des M_i et on le note $\sum_{i\in I} M_i$.

Preuve (trivial).

CHAPITRE 4
ANNAEAUX ET MODULES DES FRACTIONS

1- Constructions et propositions élémentaires

1.1- Relation d'équivalence:

Soit E un ensemble et considérons une relation binaire $\Re$ sur E. Cette relation peut présenter des qualités particulières que nous allons étudier.

1.1.1- Réflexivité :

On dit qu'une relation binaire $\Re$ est réflexive si :

$$(\forall x \in E) \ ; \ x \Re x$$

Exemples :

1. L'égalité est réflexive : $(\forall a \in E)$; $a = a$.
2. L'inclusion dans $P(E)$ est réflexive : $\forall A \in P(E))$; $A \subset A$.

1.1.2- Symétrie :

On dit qu'une relation $\Re$ sur E est symétrique si :

$$x \Re y \Rightarrow y \Re x.$$

Exemples :

1. L'égalité est symétrique : $a = b \Rightarrow b = a$.
2. La relation d'inclusion n'est pas symétrique :

$A \subset B$ n'entraine pas, en général que $B \subset A$. On ne peut échanger A et B que dans le cas où $A = B$.

1.1.3- transitivité :

On dit qu'une relation binaire $\mathfrak{R}$ sur E est transitive si :

$$(x\mathfrak{R}y \text{ et } y\mathfrak{R}z) \Rightarrow x\mathfrak{R}z$$

Exemple :

L'inclusion est transitive :

$$(A \subset B \text{ et } B \subset C) \Rightarrow A \subset C$$

1.1.4- Relation d'équivalence :

On dit qu'une relation binaire $\mathfrak{R}$ sur E est une relation d'équivalence si elle est à la fois réflexive, symétrique et transitive.

1.2- Partie multiplicative :

Définition

Soient A un anneau et S une partie non vide de A. On dit que S est une partie multiplicative de A si :

i) $1 \in S$ et $0 \notin S$.

ii) $\forall\ a,\ b \in S$, $ab \in S$.

La construction du corps des nombres rationnels $\mathbb{Q}$ à partir de $\mathbb{Z}$ reste valable dans le cas des anneaux intègres et fournit le corps des fractions de l'anneau intègre.

Soient A un anneau intègre et $S = A \setminus \{0\}$ une partie multiplicative $(p.m)$ de A. Le corps des fractions de A peut être défini comme suit :

$$Frac(A) = \{a/s \text{ telsque } a \in A \ et\ s \in S\}.$$

L'anneau intègre A s'injecte dans son corps des fractions à travers l'homomorphisme :

$$\begin{array}{ccc} A & \hookrightarrow & Frac(A) \\ a & \rightarrow & a/1 \end{array}$$

Cette construction considère l'ensemble des couples $(a,\ s)$ tels que $a \in A\ et\ s \in S$, avec la relation d'équivalence :

$$(a,\ s) \sim (a',\ s') \iff as' - a's = 0.$$

Cette relation reste valable dans le cas des anneaux intègres puisque la transitivité utilise la simplification ; c'est à dire que A n'a pas de diviseurs de zéro. Toutefois, on peut généraliser cette méthode comme suit :

Soient A un anneau et S une partie multiplicative de A. On définit une relation de $A \times S$ par :

(1) $(a,\ s) \sim (a',\ s') \Leftrightarrow (as' - a's)t = 0$ pour un certain $t \in S$.

On veut montrer que $\sim$ est une relation d'équivalence. Il est visible que $\sim$ est réflexive et symétrique. Pour la transitivité, si $(a,\ s) \sim (a',\ s')$ et $(a',\ s') \sim (a'',\ s'')$ alors on a :

$$(as' - a' s)t = 0,$$

et

$$(a' s'' - a'' s')t' = 0$$

pour certains $t,\ t' \in S$. On a donc :

$$(as'' - sa'')s' tt' = as' s'' tt' - sa' s'' tt' + sa' s'' tt' - sa'' s' tt' = 0 + 0 = 0.$$

On obtient alors une relation d'équivalence.

On note par a/s la classe d'équivalence de $(a,\ s)$ qu'on appelle fraction. Sur l'ensemble de ces fractions noté $S^{-1}A$, on définit l'addition et la multiplication par :

$$(a/s) + (a'/s') = (as' + sa')/(ss')$$

et

$$(a/s) \times (a'/s') = (aa')/(ss').$$

On vérifie facilement que + et × sont bien définies et font de $S^{-1}A$ un anneau commutatif et unitaire d'élément nul $0/1$ et d'élément unité $1/1$.
L'homomorphisme:

$$\begin{aligned} \varphi :\ & \mathrm{A} \to \mathrm{S}^{-1}\mathrm{A} \\ & \mathrm{a} \to \mathrm{a}/1 \end{aligned}$$

Applique les éléments de S sur les unités de $S^{-1}A$, on dit que φ est <u>$S-$ inversant.</u>

<u>Définition</u>

L'anneau $\mathrm{S}^{-1}\mathrm{A}$ est appelé <u>anneau des fractions de A par rapport à S.</u>

<u>Remarque</u>

1. Il est clair que l'homomorphisme $\varphi : A \to S^{-1}A$ est injectif si et seulement si S ne contient pas de diviseurs de zéro.
2. Si A est intègre et $S = A \setminus \{0\}$, alors $\mathrm{S}^{-1}\mathrm{A}$ est le corps des fractions de A.
3. Si S_0 est le semi groupe des éléments non diviseurs de zéro, alors $S_0^{-1}A$ s'appelle <u>l'anneau total des fractions de A</u> noté $T(A)$.

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

Soit P un idéal premier de A. On a $S = A \setminus P$ 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 :

$$M = P A_P = \{a/s \text{ telque } a \in P \text{ et } s \in S = A \setminus P\}.$$

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

<u>Exemple : (A=ℤ)</u>

2ℤ est un idéal maximal de ℤ, est puisque ℤ/2ℤ est un corps, alors l'idéal 2ℤ est premier. Donc S=ℤ\2ℤ est un partie multiplicative de A. On note $S^{-1}\mathbf{Z}$ par $\mathbf{Z}_{2\mathbb{Z}}$. Les éléments a/s où $a \in 2\mathbb{Z}$ et $s \in S$ forme un idéal M tel que M est l'unique idéal maximal de $A_{2\mathbb{Z}}$. Ainsi on a :

$$\boxed{M = 2\mathbb{Z} A_{2\mathbb{Z}} = 2\mathbb{Z}(\mathbb{Z}\setminus 2\mathbb{Z})^{-1}\mathbb{Z} = 2\mathbb{Z}(\mathbb{Z}\setminus 2\mathbb{Z})^{-1} = \{a/s \text{ telque } a \in 2\mathbb{Z} \text{ et } s \in S = \mathbb{Z}\setminus 2\mathbb{Z}\}.}$$

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

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.

$S^{-1}A$ se note $A_{(s)}$.

3. Soit I un idéal de A. L'ensemble $S = 1 + I = \{1 + x \,/\, x \in I\}$ est une partie multiplicative de A.

<u>2- Modules des fractions</u>

On peut de manière analogue appliquer la construction de $S^{-1}A$ à un A-module M pour construire le module des fractions.

Soient M un A-module et S une partie multiplicative de A. On définit sur $M \times A$ la relation d'équivalence :

$$(m,\ s) \sim (m',\ s') \iff \exists t \in S \ / \ t(ms' - sm') = 0.$$

On désigne par m/s la classe de $(m,\ s)$ qu'on appelle <u>fraction</u>. L'ensemble de ces fractions est noté $S^{-1}M$.

En définissant de manière naturelle l'addition et la modulation par :

$$(m/s) + (m'/s') = (s'm + sm')/ss' ,$$

et

$$(a/t)(m/s) = (am)/(st)$$

Où $a/t \in S^{-1}A,\ S^{-1}M$ devient ainsi un $S^{-1}A$ -module (et aussi un A-module).

• Pour $S = A\setminus P$ où P est un idéal premier de A, on note $S^{-1}M$ par M_P .

• Tout homomorphisme de A-modules $\alpha : M \to N$ induit un homomorphisme de $S^{-1}A$ -modules :

$$\begin{aligned} S^{-1}\alpha : S^{-1}M &\to S^{-1}N \\ a/s &\to \alpha(a)/s. \end{aligned}$$

La formation de ces fractions commute avec l'intersection finie et l'addition ; c'est à dire que :

1. $S^{-1}(M + N) = S^{-1}M + S^{-1}N$.

2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$.

3. Si $N \subseteq M$, alors $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.

Proposition

Soit M un A-module, alors les assertions suivantes sont équivalentes :

i) $M = 0$;

ii) $M_P = 0$ pour tout idéal premier P de A ;

iii) $M_m = 0$ pour tout idéal maximal m de A.

Preuve

$i) \Rightarrow ii) \Rightarrow iii)$ sont triviales.

$iii) \Rightarrow i)$ Supposons que $M \neq 0$. Soient $x \in M\setminus\{0\}$ et $I = Ann(Ax)(=Ann(x) = \{a \in A/ax = 0\})$.

On a I est un idéal de A et $1 \notin I$, d'où I est un idéal propre de A. Ainsi I est inclus dans au moins un idéal maximal m_0 de A. D'après (iii) $M_{m_0} = 0$, et donc $x/1 = 0$ (car $x \in M$). Ainsi il existe $t \in A\setminus m_0$ tel que $tx = 0$, alors on a $t \in I\ (= Ann(x)) \subseteq m_0$, contradiction. D'où $M = 0$.

Proposition

Soit $\phi : M \to N$ un homomorphisme de A-modules. Alors les assertions suivantes sont équivalentes :

i) ϕ est injectif (respectivement surjectif) ;

ii) ϕ_P est injectif (respectivement surjectif) pour tout $P \in \mathrm{Spec}(A)$;

iii) ϕ_m est injectif (respectivement surjectif) pour tout $m \in Max(A)$.

Preuve

$i) \Rightarrow ii)$ Supposons que ϕ est injectif, alors

$$0 \longrightarrow M \xrightarrow{\phi} N$$

est une suite exacte. Soit $P \in Spec(A)$ et posons $S = A\setminus P$. Comme le foncteur S^{-1} est exact, alors la suite :

$$0 \longrightarrow S^{-1}M \xrightarrow{S^{-1}(\phi)} S^{-1}N$$

est exacte, et donc $\phi_P = S^{-1}\phi$ est injectif.

$ii) \Rightarrow iii)$ Triviale.

$iii) \Rightarrow i)$ Supposons que ϕ_m est injectif pour tout $m \in Max(A)$ et montrons que ϕ est injectif. Posons $M' = Ker\ \phi$ et on doit montrer que $M' = 0$. Il suffit de montrer, d'après la proposition précédente, que $M'_m = 0$ pour tout $m \in Max(A)$.

Comme

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\phi} N$$

est une suite exacte, alors pour tout $m \in Max(A)$, la suite :

$$0 \longrightarrow M'_m \xrightarrow{i_m} M_m \xrightarrow{\phi_m} N_m$$

est exacte. Dés lors on a $M'_m = Im(i_m) = Ker(\phi_m) = 0$. Notamment on a, $M' = 0$ et ϕ est donc injectif. Le cas où ϕ est surjectif est similaire et cela achève la preuve de la proposition.

<u>Proposition</u>

Soient A un anneau et S une partie multiplicative de A.

1. Supposons que M est un A-module de type fini. Alors $S^{-1}M = 0$ si et seulement s'il existe $s \in S$ tel que $sM = 0$.
2. L'hypothèse M est de type fini dans 1) est nécessaire.

<u>Preuve</u>

1. Considèrons un A-module de type fini $M := \langle x_1, \ldots, x_n \rangle$ engendré par le système $\{x_1,\ldots,x_n\}$ tel que $S^{-1}M = 0$. Pour tout $i = 1, \ldots, n$, il existe $s_i \in S$ tel que $s_i x_i = 0$. Dés lors, pour $s = \prod_{i=1}^n s_i \in S$, on a $sM = 0$.

Inversement, supposons qu'il existe $s \in S$ tel que $sM = 0$. Dés lors on a, pour tout $m \in M$, $sm = 0$ et par suite on a $m/1 = 0/1$. Ainsi $S^{-1}M = 0$.

2. Soient R un domaine qui n'est pas un corps, $K = Frac(R)$ le corps des fractions de R, $S = R - \{0\}$ une partie multiplicative de R, et $M = K/R$. On vérifie aussitôt que $S^{-1}M = 0$. De plus, s'il existe $s \in S$ tel que $sM \neq 0$, on aura $M = 0$; c'est à dire que $K = R$, absurde. Donc $sM \neq 0$ pour tout $s \in S$.

D'où le résultat.

Bibliographie

1) N. Bourbaki, Algèbre commutative, Chapitre 5 and 6, Herman (1964).

2) A. Jebli, Algèbre commutative. Scientifika, (1993).

3) M.P. Malliavin, Algèbre commutative, application en géométrie et théorie des nombres, Masson (1985).