Rappels

déf

Un anneau A est un ensemble muni de deux opérations (notées $+$ et $\cdot$) de sorte à ce que

(0) $(A,+)$ groupe abélien

(1) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$ $\forall a_1, a_2, a_3 \in A$: associativité

(2) $a_1 \cdot (a_2 + a_3) = a_1 \cdot a_2 + a_1 \cdot a_3$ $\forall a_1, a_2, a_3 \in A$: distributivité

$(a_1 + a_2) \cdot a_3 = a_1 \cdot a_3 + a_2 \cdot a_3$

def

A est un anneau unitaire s'il existe un élément appelé unité, noté 1, qui vérifie $1 \cdot a = 1$ $\forall a \in A$

def

A est un anneau commutatif si $\forall a_1, a_2 \in A$ $a_1 \cdot a_2 = a_2 \cdot a_1$

Exemples

* $\mathbb{Z}$ anneau unitaire commutatif
* $2\mathbb{Z}$ anneau non unitaire
* Un corps est un anneau : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ anneau commutatif et unitaire $(\bar{1})$
* Si A anneau $M_n(A) = \{$matrice carrées de tailles n à coeff dans $A\}$ est un anneau pour $+$ et $\cdot$

  mais si $n \geq 2$ $M_n(A)$ n'est pas commutatif

  si $n = 1$ $M_{1,1}(A) = A$

  par ex $A = \mathbb{Z}$ $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $b = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}$ $ab \neq ba$
* $\mathcal{O}$ = ens fonctions holomorphes sur $\mathbb{C}$

  $f : \mathbb{C} \to \mathbb{C}$ tq $\forall z_0 \in \mathbb{C}$ $\lim\limits_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$ existe

  $(\mathcal{O}, +, \cdot)$ anneau unitaire (fct cste $= 1$)
* Si A anneau, on a $A[X] = \{$poly en la variable $X\}$

  $A[X][Y] = A[X,Y] = A[Y][X]$
* $\mathbb{Z}[i]$ anneau de Gauss, $i^2 = -1$, $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$

Remarque

Soit A anneau unitaire

→ neutre pour $+$ noté 0

→ neutre pour $\cdot$ noté 1

On a alors

$0 \cdot a = 0$ en effet $a \cdot (0 + b) = ab \iff a0 + ab = ab$

$0 + a = a$

$(-1) \cdot a = -a$

$0 \neq 1$

déf

Un élément de $a \in A$ est inversible s'il existe $b \in A$ tel que $a \cdot b = 1 = b \cdot a$

$(A^*, \cdot)$ est le groupe des éléments inversible de A

Exemples

. $A = \mathbb{Z}$, $(\mathbb{Z}^*, \cdot) = (\{1, -1\}, \cdot) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$

. $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k}$ avec $0 \leq k < n$ tel que $PGCD(k,n) = 1\}$

Bézout $ak + bn = PGCD(k,n) = 1$ ie $\bar{a}\bar{k} = \bar{1}$ $(\mathbb{Z}/n\mathbb{Z})$

seuls elts inv de $\mathbb{Z}$

. $A = M_2(\mathbb{Z})$ $\quad A^* = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) , \quad ad - bc = \pm 1 \}$

. $A = \mathcal{O} = \{ f^t \text{ holo} : \mathbb{C} \to \mathbb{C}$

$z \longmapsto e^z$ inv d'inverse $g(z) = e^{-z}$

Déf

A commutatif

Un diviseur de A est un élément $a \in A$, $a \neq 0$ tel qu'il existe $b \in A$ $b \neq 0$ vérifiant $a.b = 0$

Exemple

. Si $A = \mathbb{Z}$,

il n'y a pas de div de zéro

pareil si $A = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (ou n'importe quel anneau intègre)

. Si $A = M_2(\mathbb{Z})$

M est un diviseur de zéro si $M \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\exists N \in M_2(\mathbb{Z}) \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ tq $MN = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

si $\det M = 0 \in \mathbb{Z}$

. $A = \mathcal{O} = \{ f^t \text{ holo} \}$ n'a pas de diviseur de zéro

en effet,

fct cste nulle

$f(z) \cdot g(z) = 0(z) = 0 \iff f(z) = 0$ ou $g(z) = 0$ $\forall z \in \mathbb{C}$

. $A = \mathbb{R}[X]$ n'a pas de diviseurs de zéros

déf

Soient A et B deux anneaux

$f : A \to B$ est un homomorphisme d'anneaux

si 1) $f : (A,+) \longrightarrow (B,+)$ homo de groupes

2) $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$ $\forall a_1, a_2 \in A$

Ex :

. $A = 2\mathbb{Z} \subset B = \mathbb{Z}$ homo d'anneaux

. $ev_{z_0} : \begin{array}{l} (\mathcal{O}, +, \cdot) \longrightarrow (\mathbb{C}, +, \cdot) \\ f \longmapsto f(z_0) \end{array}$ homo d'anneaux

$ev_{z_0}(f+g) = ev_{z_0}(f) + ev_{z_0}(g)$

$ev_{z_0}(f \cdot g) = ev_{z_0}(f) \cdot ev_{z_0}(g)$

. $\begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x \longmapsto x[n] = \bar{x} \end{array}$ homo d'anneau

$\bar{x} \cdot \bar{y} = \overline{xy}$ et $\bar{x} + \bar{y} = \overline{x+y}$

déf

Un isomorphisme de groupe est un homomorphisme bijectif

Exemple

. $\text{pgcd}(n,m) = 1$ alors $\begin{array}{l} \mathbb{Z}/nm\mathbb{Z} \xrightarrow{\text{iso}} (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \\ x[nm] \longmapsto (x[n], x[m]) \end{array}$

déf

La caractéristique d'un anneau unitaire A, noté car(A) est $car(A) = \min \{ n \in \mathbb{N}^* \mid i(n) = 0 \}$

où $i : \begin{array}{l} \mathbb{Z} \longrightarrow A \\ n \longmapsto \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}} \end{array}$ tq $i(0) = 0$

Rmq:
Si le min n'existe pas (ex $A = \mathbb{Z}$)
Alors on dit que $\mathrm{car}(A) = 0$

Ex:
si $A = \mathbb{Z}/n\mathbb{Z}$
$\mathrm{car}(A) = n$
en effet $1 : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$
$k \longmapsto \overline{k}$

déf
A un anneau unitaire
Un grpe abélien M est un A-module si $(M,+)$ est muni d'une opération de A sur M (multiplication des scalaires sur les vecteurs)
$A \times M \longrightarrow M$
$(a, m) \longmapsto a.m$
qui satisfait les conditions suivantes
1) $1_A . m = m \quad \forall m \in M$
2) $(a+b).m = a.m + b.m \quad \forall a,b \in A \ \forall m \in M$
3) $a.(m+n) = a.m + a.n$
4) $(a.b).m = a.(b.m)$

Rmq
. (1), (2), (3) et (4) $\Rightarrow$ $a.0_M = 0_M$ et $0_A.m = 0_M$ et $(-1).m = -m$
. si A est un corps, un A-module est un A-ev

Exemples
i) $A = \mathbb{Z}$, $M = \mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$
soit $a \in \mathbb{Z}$
soit $m \in \mathbb{Z}/n\mathbb{Z}$
$a.\overline{x} = \overline{ax}$
$\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module
$\mathbb{Z}^N$ est un $\mathbb{Z}$-module
ii) Un groupe abélien G n'est rien d'autre qu'un $\mathbb{Z}$-module
iii) Si $A = k$ est un corps, alors un A-module est un ev sur k
iv) pour $N \in \mathbb{N}^*$ $M = A^N = A \times A \times \dots \times A = \{(u_1, \dots, u_N) \text{ avec } u_i \in A\}$ est un A-module
v) n, m, $M = \mathcal{M}_{n,m}(A)$ est un A-module pour l'opération $a \in A$, $m = (a_{ij}) \in M$ $\Rightarrow$ $a.m = (a.a_{ij})$ multiplication ds A
rmq : si on définit $a.m = (a + a_{ij})$ ce n'est plus une structure de A-module
rmq: iv) est un cas part de v) $A^N = \mathcal{M}_{1,N}(A)$ ou $\mathcal{M}_{N,1}(A)$
vi) $A[X]$ est un A-module avec $a.P = \sum_{i=0}^{N} (a.a_i)X^i$
vii) $\mathcal{O} = \{$fonctions holomorphes : $\mathbb{C} \to \mathbb{C}\}$ est un $\mathbb{C}$-module et un $\mathbb{C}$-ev
viii) pour Λ un ens. qcq pas nécessairement fini
$A^\Lambda = \{(a_\lambda)_{\lambda \in \Lambda}$, avec $a_\lambda \in A\}$ est un A-module
$A^{(\Lambda)} = \{(a_\lambda)_{\lambda \in \Lambda}$ où $a_\lambda = 0$ sauf pour un nb fini de $\lambda_i\}$ est un A module
les deux pour l'opération $a.(a_\lambda)_{\lambda \in \Lambda} = (aa_\lambda)_{\lambda \in \Lambda}$
rmq: $A^{(N)} = A[X] \subsetneq A^N$ $A^{(N)} \ni m = (a_i)_{i \in N} \mapsto \sum_{i=0}^{N} a_i X^i$

Rem:
Si $f : A \to B$ est un homomorphisme d'anneaux
et si M est un B-module
Alors M est aussi un A-module
Explication: il faut définir une op de A sur M $a.m = \overset{\in B}{f(a)}.m$

Déf

Un homomorphisme de A-modules $f : M \to N$ est une application $f : M \to N$ qui vérifie

$\forall a \in A, \forall m \in M, \forall m' \in M \quad f(am+m') = af(m) + f(m') \iff \begin{cases} f(m+m') = f(m)+f(m') \\ f(am) = a \cdot f(m) \end{cases}$

Rmq :

(1) un homomorphisme de A-modules est aussi appellée une application A-linéaire

(2) la composée de 2 appli. A-linéaires est aussi A-linéaire

(3) si une application f A-lin est bijective alors son inverse f^{-1} est aussi A-linéaire

Question

Comment représenter une application A-linéaire ?

$f : \underset{A^m}{\overset{\shortparallel}{M}} \longrightarrow \underset{A^n}{\overset{\shortparallel}{N}}$

$f \longleftrightarrow \mathrm{mat}(f) \in \mathcal{M}_{m,n}(A)$

Exemples

1) $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^3$

$(a_1, a_2) \mapsto (a_1+a_2,\ 2a_1+a_2,\ -a_2) = f(a_1, a_2)$

f est bien $\mathbb{Z}$-linéaire : $f((a_1,a_2)+(b_1,b_2)) = f(a_1+b_1, a_2+b_2)$ et $f(a \cdot (a_1,a_2)) = a \cdot f(a_1,a_2)$

$M = \mathrm{mat}_{can}(f) = \begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$

2) $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$
$x \longmapsto \bar{x} = x[n]$

π est $\mathbb{Z}$-linéaire : $\pi(x+y) = \pi(x) + \pi(y)$ et $\pi(\lambda x) = \lambda \pi(x) = \bar{\lambda x}$

En revanche,

π ne peut pas être représentée par une matrice car $\mathbb{Z}/n\mathbb{Z} \neq \mathbb{Z}^{\mathbb{N}}$

3) $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \xrightarrow{f} \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$
$(a_1, a_2) \longmapsto (a_1+a_2, -a_2)$

On considère :

$A = \mathbb{Z}$

$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ est un A-module

Donc f est bien $\mathbb{Z}$-linéaire et représentée par $\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \overline{-1} \end{pmatrix} \in \mathrm{mat}_{2,2}(\mathbb{Z}/30\mathbb{Z})$

Rmq :

$\mathbb{Z}/30\mathbb{Z}$ est un A-module pour $A = \mathbb{Z}/30\mathbb{Z}, \mathbb{Z}$

4- $A[X]$ un A-module mais aussi un anneau unitaire où A est un anneau

$ev_{x_0} : A[X] \longrightarrow A$
$P = \sum_{i=1}^{N} a_i X^i \longmapsto \sum_{i=0}^{N} a_i x_0^i$

$ev_{x_0}(P+Q) = ev_{x_0}(P) + ev_{x_0}(Q)$ pour $P, Q \in A[X]$ et $\lambda \in A$

$ev_{x_0}(\lambda P) = \lambda ev_{x_0}(P)$

Donc ev_{x_0} est A-linéaire

A est aussi un $A[X]$-module

voir TD pour la $A[X]$-linéarité

5) $\partial : A[X] \longrightarrow A[X]$ et A-linéaire mais pas $A[X]$-linéaire (TD)
$P \longmapsto P'$

Déf
$f : M \to N$ A-linéaire entre deux A-modules
Alors le noyau est $\ker(f) = \{ m \in M \mid f(m) = 0_N \}$
Et l'image est $\mathrm{im}(f) = \{ n \in N \mid \exists m \in M \quad n = f(m) \}$

Déf
Soit M un A-module
Un sous-A-module $\tilde{M} \subset M$ est un sous-ens $\neq \emptyset$ de M qui vérifie
* $\tilde{m}_1 + \tilde{m}_2 \in \tilde{M}$ $\forall \tilde{m}_1, \tilde{m}_2 \in \tilde{M}$
* $a.\tilde{m} \in \tilde{M}$ $\forall a \in A, \tilde{m} \in \tilde{M}$

Prop
$\ker(f)$ sous-A-module de M
$\mathrm{Im}(f)$ ——————— N

Prop
Soit $f : M \longrightarrow N$ A-linéaire
soient $\tilde{M} \subset M$, $\tilde{N} \subset N$ deux sous-modules
Alors
* $f(\tilde{M})$ sous-A-module de N
* $f^{-1}(\tilde{N})$ sous-A-module de M

rmq :
ceci généralise la prop précédente $(\tilde{M} = M, \tilde{N} = \{0_N\})$

Déf
On se donne deux A-modules M et N tels que $N \subset M$
Alors le quotient M/N est un A-module avec l'opération $A \times (M/N) \to (M/N)$, $(a, \overline{m}) \mapsto a.\overline{m} = \overline{a.m}$

Rappel : description de l'ens M/N
Soient M, N deux groupes abéliens
si $m \in M$, on note $\overline{m} = \{ m + n \mid n \in N \} \subset M$ et $\overline{m} = \overline{m'} \iff m - m' \in N$
En d'autres mots, M/N correspond aux classes d'équivalences pour la relation d'eq $m \mathcal{R} m' \iff m - m' \in N$
On définit une opération de A sur M/N par la formule $a.\overline{m} := \overline{a.m} \in M/N$
il suffit de vérifier que l'elts $\overline{am} \in M/N$ ne dépend pas du représentant de la classe $\overline{m}$.
choisissons un autre représentant $m' \in M$
$\overline{m} = \overline{m'} \iff m - m' \in N \subset M$
comme N est un A-module, on a $a.(m - m') \in N$
$a(m - m') = a.m - am' \in N \iff \overline{am} = \overline{am'}$
si $\overline{m} = \overline{m'}$ alors $\overline{am} = \overline{am'}$

Rmq
L'application canonique $\pi : M \longrightarrow M/N$ est A-linéaire et surjective
$m \longmapsto \overline{m}$

Exemples
1) $A = \mathbb{Z}$, $M = \mathbb{Z}$, $N = n\mathbb{Z} \subset M$
$M/N = \mathbb{Z}/n\mathbb{Z}$
$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}$-linéaire
$x \longmapsto \tilde{x} = x[n]$

Exemples

1)

$I = n\mathbb{Z} \subset \mathbb{Z}$, I est un idéal de $\mathbb{Z}$

2)

$I = Tk[T] \subset \overbrace{k[T]}^{=A}$, k corps

I sous-A-module

en effet,

si $Q \in I$ et $P \in A$ alors $PQ \in I$ (clair car $Q \in I \iff Q(0) = 0$)

$PQ(0) = P(0)\,Q(0) = P(0) \cdot 0 = 0$

3.

$I = (T-1)\,k[T] \subset k[T]$ est un idéal

4

$I = k[T^2] \subset k[T]$ n'est pas un idéal

En effet, $Q \in I$ alors $TQ \notin I$

En revanche, I est un sous-anneau et un sous-k-module mais pas un sous-A-module

Prop

Si A est un anneau et $I \subset A$ un idéal

Alors A/I est un anneau (et aussi un A-module par quotient de 2 A-modules)

où la multiplication est définie par

$$\begin{aligned} A/I \times A/I &\longrightarrow A/I \\ (\bar{a}, \bar{b}) &\longmapsto \overline{ab} \end{aligned}$$

avec $a, b \in A$

preuve :

il suffit de montrer que c'est bien défini

si $\bar{a} = \bar{a}'$, $\bar{b} = \bar{b}'$

mq $\overline{ab} = \overline{a'b'}$

on a $\begin{cases} \bar{a} = \bar{a}' \\ \bar{b} = \bar{b}' \end{cases} \iff \begin{cases} a' - a \in I \\ b' - b \in I \end{cases} \iff \begin{cases} a' = a + i_1 \\ b' = b + i_2 \end{cases}$, $i_1 \in I$, $i_2 \in I$

Donc $a'b' = (a+i_1)(b+i_2) = ab + \underbrace{ai_2}_{\in I} + \underbrace{i_1 b}_{\in I} + \underbrace{i_1 i_2}_{\in I} \in I$

D'où $a'b' - ab \in I \iff \overline{ab} = \overline{a'b'}$

$\square$

Rmq :

si A unitaire, A/I est un anneau unitaire d'unité $\bar{1} = 1 \bmod I$

Exemple

1) $I = n\mathbb{Z}$, $A = \mathbb{Z}$: $A/I = \mathbb{Z}/n\mathbb{Z}$

2) $I = Tk[T]$, $A = k[T]$, $A/I = k$

3) $I = (T-1)k[T]$, $A = k[T]$, $A/I = k$

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ P &\longmapsto P(1) \end{aligned}$$

Rmq

$\pi : A \to A/I$ est un homomorphisme d'anneaux

$\pi(ab) = \pi(a)\,\pi(b)$

Déf

Un anneau commutatif A est intègre s'il n'a pas de diviseurs de zéro

ie $\forall\, a, b \in A$ $a \cdot b = 0 \implies (a = 0$ ou $b = 0)$

Poly qui s'annule en 0

2) A qcq , $M = A[T]$, $N = TA[T] \subset M$

M/N

$\pi : \underset{\underset{A[T]}{\parallel}}{M} \longrightarrow \underset{\underset{A}{\parallel}}{M/N}$ est A-linéaire

$P \longmapsto P(0)$ $\rightsquigarrow$ $\overline{P_1} = \overline{P_2} \iff P_1 - P_2 \in N = TA[T] \iff (P-P')(0) = 0 \iff P(0) = P'(0)$

Prop

Soit M un A-module

Soit $N \subset M$ un sous-A-module

Alors, on a la correspondance bijective suivante

$$\{N \subset L \subset M \mid L = \text{sous-}A\text{-module de } M\} \overset{Bij}{\longleftrightarrow} \{L' \subset M/N \ , \ L' = \text{sous-}A\text{-module de } M/N\}$$

$$L \longmapsto \pi(L) \subset M/N$$

$$\{l \in M \mid \pi(l) \in L'\} = \pi^{-1}(L') \longleftarrow\!\shortmid \ L' \subset M/N$$

Exemple :

$A = \mathbb{R}$, $M = \mathbb{R}^3$, $N = \mathbb{R}(1,1,1)$ dr^{te} vect. dans $\mathbb{R}^3$

la prop dit : les sev contenant la droite N correspondent bij aux sev de $\mathbb{R}^3/\mathbb{R}(1,1,1) = \mathbb{R}^2$

$P \longmapsto P/N \subset \mathbb{R}^2$

Preuve :

Rappels :

Si $f : E \to F$ A-lin , $E' \subset E$ et $F' \subset F$

Alors : * $f(E') \subset F$ sous-A-module de F

* $f^{-1}(F') \subset E$ sous-A-module de E

pour montrer que c'est une bijection, il suffit de montrer que :

① $\pi^{-1}(\pi(L)) = L$ $\forall L$ tq $N \subset L \subset M$

② $\pi(\pi^{-1}(L')) = L'$ $\forall L'$ tq $L' \subset M/N$

$\pi : M \longrightarrow M/N$

$\pi^{-1}(L') \longmapsto L'$

On a donc l'égalité ②, car il est clair que $\pi(\pi^{-1}(L')) \subset L'$ et comme π surj , on a l'égalité

Pour ① : $L \subset \pi^{-1}(\pi(L))$ est clair car si $x \in L$ alors $\pi(x) \in \pi(L)$ donc $x \in \pi^{-1}(\pi(L))$

il reste à montrer que $\pi^{-1}(\pi(L)) \subset L$

soit $x \in \pi^{-1}(\pi(L))$

$\iff \pi(x) \in \pi(L)$

$\iff \exists y \in L$ tel que $\pi(x) = \pi(y)$

$\iff \exists y \in L$ tel que $\pi(x-y) = 0$

$\iff \exists y \in L$ tel que $x - y \in N$

$\iff \exists y \in L$ et $\exists n \in N$ tel que $x = \underset{\in L}{y} + \underset{\in L}{n}$

Donc $x \in L$

$\boxtimes$

Déf :

Soit A un anneau unitaire

On dit que I est un idéal de A si I est un sous-A-module de A

En d'autres mots,

$I \subset A$ et I sous-A-module

Il existe une opération de A sur I qui est en fait la restriction de sur A : $\begin{array}{ccc} A \times I & & I \\ \cap & & \cap \\ A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a \cdot b \end{array}$

I ss-grpe de A stable par multiplication.

Exemples

1) $A = \mathbb{Z}/5\mathbb{Z}$ est intègre car 5 premier de $\mathbb{Z}/5\mathbb{Z}$ corps

2) $A = \mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : il y a des div de zéro $\bar{2}.\bar{3} = \bar{0}$

3) $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ n premier

* n premier $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ corps
* n pas premier $\Rightarrow$ $n = a.b$ avec $1 < a, b < n$ $\Rightarrow \bar{0} = \underset{\neq 0}{\bar{a}} \cdot \underset{\neq 0}{\bar{b}}$

4) $A = \mathbb{R}[X]$ est intègre

5) $A/I = \mathbb{R}[X,Y] / (XY)\mathbb{R}[X,Y]$ n'est pas intègre

$I = XY\,\mathbb{R}[X,Y] \subset \mathbb{R}[X,Y]$

$\pi : \begin{array}{l} A \longrightarrow A/I \\ X \longmapsto \bar{X} \\ Y \longmapsto \bar{Y} \end{array}$

$\underset{\neq 0}{\bar{X}} \cdot \underset{\neq 0}{\bar{Y}} = \overline{XY} = \bar{0}$

Def

Soit I un idéal de A

1) I est un idéal premier si A/I est intègre

2) I est un idéal maximal si A/I est un corps

Prop

I premier $\Leftrightarrow$ $xy \in I \Rightarrow (x \in I$ ou $y \in I)$

preuve :

$\Rightarrow$) on suppose A/I intègre

si $xy \in I$

Alors $\overbrace{\bar{x}\bar{y}}^{\bar{x}\bar{y}} = \bar{0}$ dans A/I

Comme A/I intègre, $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$ $\Leftrightarrow$ $x \in I$ ou $y \in I$

$\Leftarrow$) supposons $xy \in I \Rightarrow x \in I$ ou $y \in I$

mq A/I intègre

$\bar{x}\bar{y} = \bar{0} \Leftrightarrow xy \in I \Rightarrow x \in I$ ou $y \in I$ $\Leftrightarrow \bar{x} = 0$ ou $\bar{y} = 0$

Prop

I idéal maximal $\Leftrightarrow$ si I' ideal tq $I \subset I' \subset A$ alors $I' = I$ ou $I' = A$

preuve :

$\Rightarrow$) si on suppose que A/I est un corps

prenons $I \subset I' \subset A$

et supposons que $I \subsetneq I'$ ie $\exists i' \in I'$ avec $i' \notin I$

alors $\bar{i'} \neq \bar{0}$ dans A/I qui est un corps (tout elt non nul est inv)

alors $\exists \bar{x} \in A/I$ tq $\bar{x}.\bar{i} = \bar{1}$ dans A/I

$\Leftrightarrow \bar{x}.\bar{i} - \bar{1} = \bar{0}$

$\Leftrightarrow \overline{xi - 1} = \bar{0}$

$\Leftrightarrow xi - 1 \in I \subset I'$

$\Rightarrow \exists j' \in I'$ $xi - 1 = j'$

$\Leftrightarrow 1 = xi' - j' \in I'$

Rmq : si $1 \in I \subset A$ alors $I = A$ (comme I stable par multiplicat° a $1 \in I$ $\forall a \in A$)

$\Rightarrow I' = A$

$\Leftarrow$) si I vérifie $I \subset I' \subset A \Rightarrow I' = A$ ou $I = I'$

Alors, il faut mq A/I est un corps

Prenons $\bar{x} \in A/I$ avec $\bar{x} \neq \bar{0}$ $\Leftrightarrow x \in I$

il faut mq $\bar{x}$ est inv. dans A/I

Considérons I' engendré par I et x $I' = \langle I, x \rangle$

I' est le plus petit idéal contenant I et x $I' = I + \overbrace{\langle x \rangle}^{x \cdot A}$

$I \subsetneq I'$, par maximalité de I, on conclut que $I' = A \iff 1 \in I' \iff 1 = i + xa$, $\begin{smallmatrix} i \in I \\ a \in A \end{smallmatrix}$

$\iff \bar{1} = \bar{x}\bar{a}$ ds A/I

Donc $\bar{x}$ est inv donc A/I corps

$a \in A$ tel que $\bar{f}(a) = (\bar{a_1}, \bar{a_2})$

on peut alors prendre $a = a_2 i_1 + a_1 i_2$

car $a \bmod I_1 = a_1 i_2 \bmod I_1 = a_1 \bmod I_1$

$a \bmod I_2 = a_2 i_1 \bmod I_2 = a_2 \bmod I_2$

. Ensuite, on suppose par récurrence que le thm est vrai pour $k-1$ idéaux

et on veut le montrer pour k idéaux $I_1, I_2, \dots, I_{k-1}, I_k$

Il suffit de montrer que $A/(I_1 \cap \dots \cap I_{k-1}) \cap I_k \xrightarrow{\sim} A/I_1 \cap \dots \cap I_{k-1} \times A/I_k$

on se ramène au cas de deux idéaux $I = I_1 \cap \dots \cap I_{k-1}$ et I_k

mais il faut vérifier qu'on a l'hypothèse $I + I_k = A$

on a supposé que $I_j + I_k = A$ pour $j = 1, 2, \dots, k-1$

et on veut montrer que $I + I_k = A$ avec $I = I_1 \cap \dots \cap I_{k-1}$

On sait que $\forall j \in \{1, \dots, k-1\}$ $1 = i_j + m_j$ avec $i_j \in I_j$ et $m_j \in I_k$

on veut déduire que $1^{k-1} = 1 = \prod_{j=1}^{k-1} (\underbrace{i_j}_{\in I_j} + \underbrace{m_j}_{\in I_k}) = \prod_{j=1}^{k-1} i_k + (\text{tous les autres termes})$ ces termes contiennent au moins un facteur de la forme $m_j \in I_k$

$\cap$

$I_1 I_2 \dots I_{k-1} \subset I_1 \cap I_2 \cap \dots \cap I_{k-1} \in I_k$

ceci donne la relation de Bézout $1 = \underbrace{\alpha}_{\in I_1 \cap \dots \cap I_{k-1}} + \underbrace{\beta}_{\in I_k}$ entre $I_1 \cap \dots \cap I_{k-1}$ et I_k

Rmq:

Si on suppose que les k idéaux $I_1, \dots, I_k$ sont distincts et maximaux,

alors on a $I_i + I_j = A$ pour tout i, j avec $i \neq j$

en effet,

si I_i est maximal et $I_j \neq I_i$ on a $\underbrace{I_i \subsetneq}_{\text{max}} I_i + I_j \underbrace{=}_{\text{par maximalité de } I_i} A$

Déf

Soit M un A-module

. Une famille libre dans M est un ensemble (fini ou infini) $\{m_j\}_{j \in S}$ avec $m_j \in M$ et S un ensemble

vérifiant $\underbrace{\sum_{j \in S}}_{\text{somme finie}} a_j m_j = 0 \Rightarrow a_j = 0 \quad \forall j \in S$

avec seulement un nb fini de $a_j \neq 0$

. Une famille génératrice dans M est un ensemble $\{m_j\}_{j \in S}$

vérifiant $\forall m \in M$ $\exists \{a_j\}_{j \in S}$ avec $a_j = 0$ sauf un nb fini tel que $m = \sum_{j \in S} a_j m_j$

Exemple

$M = A[T]$ comme A-module

La famille $\{1, T, T^2, T^3, \dots, T^k, \dots\}_{k \in \mathbb{N} = S}$ est libre et génératrice.

déf

Une famille $\{m_j\}_{j \in S}$ de M est une base de M comme A-module

si la famille est libre et génératrice

Exemple

$A = \mathbb{Z}$

$M_1 = \mathbb{Z}/30\mathbb{Z}$ et $M_2 = \mathbb{Q}$ sont des $\mathbb{Z}$-modules

Y a-t-il des familles libres / génératrices ?

. Pour le $\mathbb{Z}$-module $M_1 = \mathbb{Z}/30\mathbb{Z}$, il y a une famille génératrice (à 1 elt), $S = \{0\}$, $m_0 = \bar{1}$ ou $-\bar{1}$ ou $\bar{7}$ ou.. tous les nb premiers avec 30 sont générateurs

car tout $\bar{m} \in \mathbb{Z}/30\mathbb{Z}$ peut s'écrire $\bar{m} = \underbrace{m}_{\in \mathbb{Z}} \cdot \underbrace{\bar{1}}_{\in \mathbb{Z}/30\mathbb{Z}}$

En revanche, la famille génératrice $\{m_0 = \bar{1}\}$ n'est pas libre

en effet, il existe un $a \in A$, $a \neq 0$ tel que $a \cdot m_0 = \bar{0}$ dans $\mathbb{Z}/30\mathbb{Z}$ ($a = 30$ par ex)

. Pour le $\mathbb{Z}$-module $M_2 = \mathbb{Q}$,

$m \in \mathbb{Q}$ si $m = \frac{n}{d}$ avec $n, \underbrace{d}_{\neq 0} \in \mathbb{Z}$

Opérations sur les sous-A-modules

Contexte

Soit A un anneau unitaire

Soit M un A-module

Soient $N_1, N_2 \subset M$ deux sous-A-modules

(1) $N_1 \cap N_2 = \{ m \in M \mid m \in N_1 \text{ et } m \in N_2 \}$ est un A-module

(2) $N_1 + N_2 = \{ m \in M \mid m = n_1 + n_2 \ , \ n_i \in N_i \}$ est un sous-A-module de M

(3) $N_1 \cup N_2$ n'est pas necessairement un sous-A-module (sauf si par ex $N_1 \subset N_2$)

(4) si $S \subset M$ est un sous-ensemble de M, alors on définit :

$\langle S \rangle = \{ m \in M \mid s_1, s_2, \dots, s_k \in S \ \ m = \sum_{i=1}^{k} a_i s_i \ ; \ a_i \in A \}$ le sous-A-module engendré par S

c'est le plus petit (au sens de l'inclusion.) sous-A-module qui contient S

Avec cette notation : $\langle N_1 \cup N_2 \rangle = N_1 + N_2$

(5) Cas particulier : $M = A$

ie N_1 et N_2 sont des idéaux de A

on peut considérer $N_1 \cap N_2$, $N_1 + N_2$, $N_1 \cdot N_2$ = idéal engendré par les $n_1 \cdot n_2$, $n_i \in N_i$

$= \{ \sum_{i=1}^{k} n_{1,i} n_{2,i} \mid n_{1,i} \in N_1 \text{ et } n_{2,i} \in N_2 \}$

Thm (restes chinois)

Rappels:

* Si $A = \mathbb{Z}$, on se donne k entiers $n_1, \dots, n_k$ et on suppose que $PGCD(n_i, n_j) = 1 \quad \forall i \neq j$

Alors on a un isomorphisme d'anneaux $\mathbb{Z}/n_1 \cdots n_k \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$

$a[n_1 \cdots n_k] \longmapsto (a[n_1], a[n_2], \dots, a[n_k])$

* $n_i \mathbb{Z} + n_j \mathbb{Z} = PGCD(n_i, n_j)\mathbb{Z}$

Cas général:

Soit A un anneau unitaire avec des idéaux $I_1, I_2, \dots, I_k$ de A tels que $I_i + I_j = A \quad \forall i \neq j$

Alors, on a un isomorphisme d'anneaux :

$A/_{I_1 \cap \cdots \cap I_k} \longrightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_k$

$a \longmapsto (a \bmod I_1, a \bmod I_2, \dots, a \bmod I_k)$

En part, c'est un homo de A-modules d'anneaux car $A \longrightarrow A/I_i$, $a \longmapsto a \bmod I_i$ homo d'anneaux

Preuve :

par construction, l'application $A \longrightarrow A/I_1 \times \cdots \times A/I_k$, $a \longmapsto (a \bmod I_1, \dots, a \bmod I_k)$ est un homo d'anneaux

et $\ker(f) = \{ a \mid a \bmod I_i = \bar{0} \} = I_1 \cap I_2 \cap \cdots \cap I_k$

Donc (par le TD) il existe une appli inj $\bar{f}$ $A \xrightarrow{\pi} A/_{I_1 \cap \cdots \cap I_k} \xrightarrow{\bar{f}} A/I_1 \times \cdots \times A/I_k$

Il reste à montrer que $\bar{f}$ est surjective

on le fait par récurrence sur k

- pour $k = 1$, c'est clair, car $\bar{f} : A/I_1 \longrightarrow A/I_1$ où $\bar{f}$ est l'identité
- pour $k = 2$, $A/_{I_1 \cap I_2} \xrightarrow{\bar{f}} A/I_1 \times A/I_2$

il faut montrer que pour tout $(\bar{a_1}, \bar{a_2}) \in A/I_1 \times A/I_2$, il existe un $a \in A$ tel que

$a \bmod I_1 = a_1$ et $a \bmod I_2 = \bar{a_2}$

un idéal est égal à A si il contient l'unité de A.

il faut utiliser l'hypothèse $I_1 + I_2 = A$

ie on a une relation $1_A = \overset{\in I_1}{i_1} + \overset{\in I_2}{i_2}$ ($\Leftrightarrow$ Bézout ds $\mathbb{Z}$ $1 = \underset{I_1}{n_1} x + \underset{I_2}{n_2} y$) $PGCD(n_1, n_2)$

$A \longrightarrow A/I_1 \times A/I_2$

$i_1 \longmapsto (\bar{0}, \bar{1})$ car $\bar{i_1} + \bar{i_2} = 1$

$i_2 \longmapsto (\bar{1}, \bar{0})$

On se donne deux éléments qcq $a_1, a_2 \in A$ et on souhaite construire un antécédant

$m \in \frac{1}{d}\mathbb{Z} \subset \mathbb{Q}$

On peut prendre $\{\frac{1}{n}\}_{n\in\mathbb{N}^*}$ comme famille génératrice $(S = \mathbb{N}^*)$

mais cette famille n'est pas libre car $1 \times \frac{1}{2} + (-2) \times \frac{1}{4} = 0$

On va donc trouver une condition sur $\{r_1, r_2\}$, $r_i \in \mathbb{Q}$ pour que $\{r_1, r_2\}$ soit libre dans $\mathbb{Q}$

mais $(d_1 n_2)\frac{n_1}{d_1} + (-d_2 n_1)\frac{n_2}{d_2} = 0$

Donc si $r_1 \neq r_2$ $\{r_1, r_2\}$ n'est jamais $\mathbb{Z}$-libre.

<u>def</u>

Un A-module M est de type fini s'il existe une famille génératrice finie

<u>Ex</u>

$\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module de type fini

$\mathbb{Z}[X]$

$M = \mathbb{Z}^n$ avec $n \in \mathbb{N}$ fixé, est un $\mathbb{Z}$-module de type fini

$\mathbb{Z} \times \dots \times \mathbb{Z}$ de base $m_1 = (1, 0, \dots, 0)$; … ; $m_i = (0, \dots, 0, 1, 0, \dots, 0)$ " base can de $\mathbb{Z}^n$

$\{m_i\}_{1 \leq i \leq n}$ libre et génératrice.

<u>Rmq</u>:

Une famille génératrice $\{m_1, \dots, m_n\}$ d'un A-module M est équivalente à une application A linéaire surjective :

$$A^n \longrightarrow M$$
$$(a_1, \dots, a_n) \longmapsto a_1 m_1 + \dots + a_n m_n$$

ϕ surjectif $\iff$ $\{m_1, \dots, m_n\}$ famille génératrice

<u>def</u>

- On dit qu'un A-module M est libre s'il existe une base (= famille libre et génératrice) de M
- On dit qu'un A-module M est libre de type fini s'il existe une base finie

<u>Exemples</u>

$M = A[X]$ est un A-module libre

base : $\{1, X, X^2, \dots, X^k, \dots \mid k \in \mathbb{N}\}$

Mais elle n'est pas libre de type-fini

En d'autres mots,

si M est un A-module libre de type fini,

il existe une base $\mathcal{B} = \{m_1, \dots, m_n\}$ qui correspond à une application A-linéaire surj et inj

$\mathcal{B}$ génératrice $\mathcal{B}$ libre

$\phi : A^n \longrightarrow M$

$(a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i m_i$

<u>Ccl</u>:

Les A-modules libres de type fini correspondent aux modules $M = A^n$

... mais il existe d'autres A-modules qui ne sont pas libres (par ex: A/I où I idéal $\neq \{0\}$, $\neq A$)

<u>Rmq</u>:

Certains résultats de la théorie des $\mathbb{K}$-esp vect ($\mathbb{K}$ corps) ne sont pas vrais pour les A-modules

<u>Ex</u>:

1) Chaque $\mathbb{K}$ev admet une base,
   faux pour les A-modules car seuls les A-modules libres de type fini admettent des bases
2) Thm de la base incomplète : tout famille libre peut être complété en une base.
   faux pour les A-modules
   par ex : $A = \mathbb{Z}$, $M = \mathbb{Z}$ famille libre $\{2\}$, $2 \in M$ qu'on ne peut pas compléter en une $\mathbb{Z}$-base

Anneaux Euclidien - Anneaux Principaux

déf

Un anneau A est dit euclidien

si * A est intègre

* il existe une division euclidienne dans A ie $\forall a,b \in A$ avec $b \neq 0_A$, $\exists q,r \in A$ tq $a = bq + r$

avec $\theta(r) < \theta(b)$ où θ est une application $A \longrightarrow \mathbb{N}$

Exemples

1)

$A = \mathbb{Z}$ avec $\theta : \mathbb{Z} \longrightarrow \mathbb{N}$, $\theta(n) = |n|$

2)

$A = \begin{cases} \mathbb{C}[X] \\ \mathbb{R}[X] \end{cases}$, $\theta : \begin{cases} \mathbb{C}[X] \\ \mathbb{R}[X] \end{cases} \longrightarrow \mathbb{N}$, $\theta(P) = \deg(P)$ et $\deg(0) = -1$ poly cste 0

3)

$A = \mathbb{Z}[i] = \mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\omega]$ où $\omega^3 = 1$, $1 \neq \omega = e^{2i\pi/3}$

def

Un anneau A est principal

si * A est intègre

* tout idéal I de A est engendré par un seul élément $a \in A$ ie I est principal

Dans ce cas, on écrit $I = (a)$ avec $a \in A$

Exemple

$\mathbb{Z}[X]$ et $\mathbb{R}[X,Y]$ ne sont pas des anneaux principaux.

Thm

Un anneau A euclidien est principal

preuve :

on se donne un idéal $I \subset A$

on veut mq $I = (a)$ pour $a \in A$

. si $I = \{0\} = (0)$ ok !!

. si $I \neq \{0\}$, il existe $b \in I$, $b \neq 0$

on choisit a un élément non nul ayant $\theta(a)$ minimal

alors, on va mq $I = (a)$

* $(a) \subset I$ clair

* si $x \in I$,

on peut faire la division euclidienne de x par a : $x = qa + r$ avec $\theta(r) < \theta(a)$, $q,r \in A$

$\Rightarrow r = \underbrace{x}_{\in I} - q\underbrace{a}_{\in I} \in I$

or par minimalité de $\theta(a)$, on obtient que $r = 0$

donc $x = qa \in (a)$

D'où $I = (a)$

$\boxtimes$

de $M = \mathbb{Z}$ car les seules bases de $\mathbb{Z}$ sont $\{1\}$ et $\{-1\}$

or $\{\underline{2}, \underline{1}\}$ n'est pas une base car non libre : $1 \cdot \underline{2} + (-2) \cdot \underline{1} = 0$

Structure des A-modules de type fini

Soit A anneau principal (par ex $A = \mathbb{Z}, \mathbb{Z}[i], \mathbb{K}[X]$ où $\mathbb{K}$ est un corps)

Rappel

A principal si A intègre et tout idéal de A est engendré par un seul elt $a \in A$

L'idéal est noté (a).

Prop

Si $(a) = (a')$

Alors $a' = c.a$ avec c inversible dans A ($\Leftrightarrow \exists c' \in A$ tq $cc' = 1$)

preuve

$a' = \alpha a$ pour $\alpha \in A$

et on a aussi $a = \beta a'$ pour $\beta \in A$

on compose alors $a = \beta(\alpha a) = \beta\alpha\, a$

$\Leftrightarrow a - \beta\alpha\, a = 0$

$\Leftrightarrow \underset{\neq 0}{a}(1 - \beta\alpha) = 0$

$\overset{\text{intègre}}{\Rightarrow} \alpha\beta = 1$

Donc α inversible

Déf (notion de divisibilité)

$a, b \in A$

On dit que a divise b, noté $a|b$, si $(b) \subset (a)$

ie $\exists c \in A \mid b = ac$

Déf

A anneau principal

Soient $a, b \in A$

On définit deux elts à inversibles près : $PGCD(a,b)$ et $PPCM(a,b)$ par les égalités suivantes :

i. $(a) + (b) = (PGCD(a,b)) = \{\lambda a + \mu b \mid \lambda, \mu \in A\}$

ii. $(a) \cap (b) = (PPCM(a,b))$

Rappel :

$A = \mathbb{Z}$

. $n_1\mathbb{Z} + n_2\mathbb{Z} = PGCD(n_1, n_2)\,\mathbb{Z}$

. $n_1\mathbb{Z} \cap n_2\mathbb{Z} = PPCM(n_1, n_2)\,\mathbb{Z}$

Propriétés

1) Identité de Bézout

$\exists u, v \in A$ $PGCD(a,b) = u.a + v.b$

2) Lemme de Gauss

Si $\underbrace{PGCD(a,b) = 1}_{\Leftrightarrow (PGCD(a,b)) = A}$ (à inversible près) et $a \mid bc$ alors $a \mid c$

3)

On a la relation dans A suivante : $PGCD(a,b) \cdot PPCM(a,b) = ab$ (à inversible près)

preuve :

2) Bézout $1 = au + vb$, $u, v \in A$

$\Leftrightarrow c = uac + vbc$

or $a \mid bc \Leftrightarrow bc = a.\alpha$

donc $c = uac + v a\alpha = a(uc + v\alpha)$

$L\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d_1 \\ 0 \end{pmatrix}$

Puis on itère ces opérations pour rendre la 1ère colonne $= \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}$

À la fin de ces opérations, on obtient une matrice de la forme $\underbrace{\tilde{L}_n \cdots \tilde{L}_1}_{L} P \underbrace{\tilde{R}_1 \cdots \tilde{R}_m}_{R} = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P_2 & \\ 0 & & & \end{pmatrix}$

Ensuite, on recommence avec la matrice P_2 qui a $n-1$ lignes et $m-1$ colonnes

Finalement, on obtient une matrice de la forme $\begin{pmatrix} \begin{matrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \ddots & \\ & & & \delta_k \end{matrix} & 0 \\ 0 & 0 \end{pmatrix}$ avec $\delta_i \in A$

Mais le δ_i ne vérifie pas nécessairement la relation de divisibilité $\delta_1 | \delta_2 | \cdots | \delta_k$

2ème étape : obtenir les facteurs invariants $d_1, \dots, d_k$ à partir de $\delta_1, \dots, \delta_k$

(Exemple : $P = \begin{pmatrix} 5 & 0 \\ 0 & 6 \end{pmatrix}$, $LPR = \begin{pmatrix} 1 & 0 \\ 0 & 30 \end{pmatrix}$)

Sur A anneau principal on peut trouver des matrices L et R inversibles telles que $L\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}R = \begin{pmatrix} PGCD(a,b) & 0 \\ 0 & PGCD(a,b) \end{pmatrix}$

On va construire L et R par étapes

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & b \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ 0 & b \end{pmatrix}\begin{pmatrix} u & -\frac{ab}{d} \\ v & -\frac{av}{d} \end{pmatrix} = \begin{pmatrix} d & 0 \\ bv & \frac{ab}{d} \end{pmatrix}$$

et on sait que $d | b$ donc $\exists \lambda \in A$, $d\lambda = bv$

$$\begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}\begin{pmatrix} d & 0 \\ bv & \frac{ab}{d} \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & \frac{ab}{d} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} u & -\frac{ab}{d} \\ v & \frac{ap}{d} \end{pmatrix} = \begin{pmatrix} PGCD(a,b) & 0 \\ 0 & PGCD(a,b) \end{pmatrix}$$

Pour une matrice diagonale avec k elts diagonaux $(\delta_1, \dots, \delta_k)$, on fait ces opérations en commençant par les 2 derniers elts

$$(\delta_1, \dots, \delta_{k-1}, \delta_k) \longmapsto (\delta_1, \delta_2, \dots, \delta_{k-2}, PGCD(\delta_{k-1}, \delta_k), PPCM(\delta_k, \delta_{k-1}))$$

$$\longmapsto (\delta_1, \delta_2, \dots, \delta_{k-3}, PGCD(\delta_{k-2}, \delta_{k-1}, \delta_k), \dots\dots)$$

$$\vdots$$

$$\longmapsto (\underbrace{PGCD(\delta_1, \dots, \delta_k)}_{d_1}, \delta_2', \dots, \delta_k') \quad \text{avec } d_1 | \delta_j' \ \forall j$$

Puis on itère ces opérations sur $(\delta_2', \dots, \delta_k')$

$\boxtimes$

Quelques définitions d'algèbre homologique

<u>déf</u> (suite exacte de A-module)

Une suite exacte de A-modules est la donnée de 3 A-modules L, M, N et deux applications A-linéaires $L \xrightarrow{i} M$ et $M \xrightarrow{p} N$.

qui vérifient :
1) i injectif
2) p surjectif
3) $\ker p = \operatorname{im} i$

Si cela est le cas on le note $0 \longrightarrow L \xrightarrow{i} M \xrightarrow{p} N \longrightarrow 0$

<u>Deux cas particulier</u>

- $f : M \to N$ surj : $0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} N \longrightarrow 0$
- $f : L \to M$ inj : $0 \longrightarrow L \longrightarrow M \longrightarrow \operatorname{coker}(f) \longrightarrow 0$

<u>def</u>

$\operatorname{coker}(f) = M/\operatorname{im}(f)$

<u>Rappels</u>

A anneau

$P \in \mathcal{M}_{n,m}(A)$

Alors il existe des $d_i \in A$ facteurs invariants

$$LPR = \left(\begin{array}{c|c} \begin{matrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$

$L \in \mathcal{M}_n(A)$, $R \in \mathcal{M}_m(A)$ inversibles et $d_i \in A$ tq $d_1 | d_2 | \cdots | d_k$

De plus, les $d_i \in A$ sont uniques (à inversibles près)

<u>Prop</u>

Soient M_1, M_2, M trois A-module

On considère une suite exacte $0 \longrightarrow M_1 \xrightarrow{i} M \xrightarrow{p} M_2 \longrightarrow 0$

Si M_1 et M_2 sont des A-modules de type fini,

Alors M est aussi un A-module de type fini (ie admet une famille génératrice finie $A^n \xrightarrow{surj} M$

<u>preuve</u>:

M_2 de type fini donc il existe $m_1, m_2, \dots, m_k \in M_2$ des générateurs de M_2.

Comme p est surj on peut trouver des elts $n_1, n_2, \dots, n_k \in M$ tq $p(n_i) = m_i$

M_1 est de type fini donc il existe une famille $l_1, l_2, \dots, l_s \in M_1$ génératrice de M_2

On va montrer que la famille $\{ i(l_1), i(l_2), \dots, i(l_s), n_1, n_2, \dots, n_k \}$ est une famille génératrice de M

Soit $x \in M$, on projette x dans M_2

On peut donc écrire $p(x) = a_1 m_1 + a_2 m_2 + \cdots + a_k m_k$ dans M_2

Alors $x - (a_1 n_1 + a_2 n_2 + \dots + a_k n_k) \in \ker(p) = \operatorname{im}(i)$

Donc on peut écrire $x - (a_1 m_1 + \dots + a_k m_k) = b_1 i(l_1) + \dots + b_s i(l_s)$

$\Rightarrow x = a_1 m_1 + \cdots + a_k m_k + b_1 i(l_1) + \cdots + b_s i(l_s)$, $a_i, b_j \in A$

$\boxtimes$

<u>Rmq</u>:

Si A est général (non-Noethérien),

alors il n'est pas vrai que si M et M_2 st de type fini alors M_1 de type fini

(ex td)

Retour sur les anneaux principaux

Prop

A un anneau principal

M un A-module de type fini

$N \subset M$ un sous-A-module

Alors, N est de type fini

Rmq

ce résultat est faux si A n'est pas noethérien (principal $\Rightarrow$ noethérien)

Preuve:

par récurrence sur le nb de générateurs de M

. Si M est engendré par un élément $m \in M$

$$A \xrightarrow{\rho} M \quad , \quad a \longmapsto am \quad \text{surj.}$$

$$\{a \in A \mid \rho(a) \in N\} = \rho^{-1}(N) \longrightarrow N$$

$\rho^{-1}(N)$ est un idéal de A (car sous-module de A)

Comme A est principal, on peut écrire $\rho^{-1}(N) = (\alpha)$, $\alpha \in A$

Donc N peut-être engendré par un elt $\rho(\alpha) \in M$

. On va démontrer la prop par récurrence sur n = nb de générateurs de M

on suppose $\{m_1, \dots, m_n\}$ famille génératrice de M

on choisit m_1 et on considère $\langle m_1 \rangle = M_1$ le sous-A-module engendré par m_1

et on considère $M_2 = M/M_1$ le quotient

Donc on a une suite exacte $0 \to \underset{\substack{\cup \\ m_1}}{M_1} \to \underset{m_1, \dots, m_n}{M} \xrightarrow{\rho} \underset{\substack{\rho(m_1), \rho(m_2), \dots, \rho(m_n) \\ \parallel \\ 0}}{M_2} \to 0$

Si on considère N un sous-A-module de M

$0 \to M_1 \to M \xrightarrow{\rho} M_2 \to 0$

$0 \to M_1 \cap N \to N \to \rho(N) \to 0$ qui est une suite exacte

Et par l'hypothèse de récurrence M_2 et M_1 ont moins de n générateurs

Donc $\underbrace{M_1 \cap N}_{\rho(N)}$ est de type fini

Donc d'après la prop précédente N est aussi de type fini

Thm

A anneau principal

M A-module libre de type fini

$N \subset M$ un sous-A-module de M

Alors, N est un A-module libre de type fini et on peut trouver une base $\{e_1, \dots, e_n\}$ de M

tq $\{d_1 e_1, \dots, d_k e_k\}$ soit une base de N et $k \leq n$ et $d_i \in A$ et $d_1 | d_2 | \dots | d_k$

preuve

M est un A-module libre de type fini

Cela veut dire qu'il existe un isomorphisme A-linéaire $A^n \to M$

Pour simplifier la notation on peut supposer que $M = A^n$

$N \subset A^n$ sous-A-module

D'après la prop précédente, comme A^n est de type fini et A principal

tout sous-A-module N est aussi de type fini

ie N admet un nb fini de générateurs

donc on a une appl. A-linéaire surjective $A^m \xrightarrow{f} N \subset A^n$

Donc on obtient une appli linéaire $f : A^m \to A^n$ tq $N = \operatorname{im}(f)$

On obtient ainsi une matrice $P = \operatorname{mat}_{can}(f) \in \mathcal{M}_{n,m}(A)$

On peut alors appliquer le thm des facteurs invariants $LPR = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_k & \\ \hline & 0 & & 0 \end{array}\right) = D$

3) on a définit PPCM (a,b) comme le générateur de l'idéal $(a)\cap(b)$

on peut écrire : $a = \alpha' \, PGCD(a,b)$ avec $\alpha' \in A$

$b = \beta' \, PGCD(a,b)$ avec $\beta' \in A$

$\Rightarrow PGCD(\alpha',\beta') = 1$ car $\cancel{PGCD(a,b)} = au + bv = \cancel{PGCD(a,b)}\,(\alpha' u + \beta' v) \Rightarrow \alpha' u + \beta' v = 1)$

on introduit $\delta = \alpha'\beta' \, PGCD(a,b) \in A$

il faut mq ce $\delta \in A$ est un générateur de l'idéal $(a)\cap(b)$.

vérifions d'abord que $\delta \in (a)\cap(b)$

on a par définition $\delta = \begin{cases} a\beta' \in (a) \\ b\alpha' \in (b) \end{cases}$ donc $\delta \in (a)\cap(b)$

Inversement, si $c \in (a)\cap(b)$

alors on va mq $c = \delta . \gamma$ avec $\gamma \in (A)$

$\begin{cases} c \in (a) \Leftrightarrow c = a.\tilde{\alpha} \\ c \in (b) \Leftrightarrow c = b.\tilde{\beta} \end{cases} \Rightarrow a\tilde{\alpha} = b\tilde{\beta} \Rightarrow \alpha\tilde{\alpha}\, PGCD(a,b) = \beta'\tilde{\beta}\, PGCD(a,b) \Rightarrow \alpha'\tilde{\alpha} = \beta'\tilde{\beta}$

Comme, par construction, on a : $PGCD(\alpha',\beta') = 1$

On peut appliquer le lemme de Gauss avec la relation $\alpha'\tilde{\alpha} = \beta'\tilde{\beta}$

On en déduit que $\alpha' \mid \tilde{\beta} \Rightarrow \tilde{\beta} = \alpha' . x$, $x \in A$

et $\beta' \mid \tilde{\alpha} \Rightarrow \tilde{\alpha} = \beta' . y$, $y \in A$

or $\delta = \alpha'\beta' \, PGCD(a,b)$ donc $c = a\tilde{\alpha} = a\beta' y = \alpha'\beta' \, PGCD(a,b) . y$

$c = b\tilde{\beta} = \beta' \, PGCD(a,b)\, \alpha' = \delta x$

$\square$

<u>Thm</u> (facteurs invariants d'une matrice à coeff ds A, anneau principal)

Soit P une matrice à coeff. dans un anneau principal A.

Alors, il existe deux matrices inversibles R, L tel que $LPR = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_k & \\ \hline & 0 & & 0 \end{array}\right)$ (m colonnes, n lignes)

avec $d_1, d_2, \dots, d_k \in A$ et $d_1 \mid d_2 \mid d_3 \mid \dots \mid d_k$

P correspond à une application A-linéaire : $A^m \longrightarrow A^n$

Les d_i sont appelés les facteurs invariantes de P

De plus, $k \in \mathbb{N}$ et les éléments $d_1, \dots, d_k$ sont uniques (à inv près)

k est appelé rayon de P.

<u>preuve</u> :

$$P = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & \vdots & \cdots & \\ a_{3,1} & \vdots & & \\ \vdots & \vdots & & \\ a_{n,1} & & & \end{pmatrix}, \quad a_{ij} \in A \quad \forall i,j$$

Nous allons faire des opérations sur les lignes et les colonnes.

Pour simplifier, regardons une matrice $P = (a \;\; b)$ 2 colonnes, 1 ligne

Trouvons L, R tq $LPR = (d_1 \;\; 0)$

$(x)(a \;\; b)\begin{pmatrix} x & x \\ x & x \end{pmatrix} = (d_1 \;\; 0)$

pour cela, on utilise la relation de Bézout sur $a = a_{1,1}$ et $b = a_{1,2}$: $ua + vb = PGCD(a,b) = d_1$

(1) $(a \;\; b)\underbrace{\begin{pmatrix} u & -\frac{b}{d_1} \\ v & \frac{a}{d_1} \end{pmatrix}}_{R} = (d_1 \;\; 0)$

$u\frac{a}{d_1} + v\frac{b}{d_1} = 1 \Rightarrow$ la matrice R est inversible.

On refait cette opération sur la première et troisième colonne, puis 1ère et 4ème .....

de sorte à rendre la première ligne sous la forme $(d \;\; 0 \;\; 0 \cdots 0)$

$(a_{1,1} \;\; a_{1,i})\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} = (d \;\; 0) \Rightarrow$

Ensuite, on fait les mêmes opérations sur la 1ère colonne en multipliant à gche avec $L = \begin{pmatrix} u & v \\ \frac{b}{d_1} & \frac{a}{d_1} \end{pmatrix} = {}^tR$

$$\begin{tikzcd} A^m \arrow[r] \arrow[rr, bend left, "L"] & N \subset A^n \\ A^m \arrow[u, "R"] \arrow[r, "D"] & A^n \arrow[u] \end{tikzcd}$$

ce diagramme est commutatif

Si on regarde $D : A^m \to A^n$ donnée par la matrice diagonale $\left(\begin{array}{ccc|c} d_1 & & & 0 \\ & \ddots & & \\ & & d_k & \\ \hline & 0 & & 0 \end{array}\right)$

Si on note $f_1, \dots, f_m$ la base can de A^m et A^n
$f_1, \dots, f_n$

$f_1, \dots, f_k \longmapsto d_1 f_1, \dots, d_k f_k$
$f_i \longmapsto 0 \quad i > k$

$\mathrm{Im}(D)$ a comme base $\{d_1 f_1, \dots, d_k f_k\}$
A^n a comme base $\{f_1, \dots, f_n\}$
Donc si on définit $e_i = L^{-1}(f_i)$ pour $i = 1, \dots, n$
Alors N a comme base $\{d_1 e_1, \dots, d_k e_k\}$
A^n ——————— $\{e_1, \dots, e_k\}$

<u>Thm</u> (structure d'un A-module de type fini, A principale)
Soit M un A-module de type fini
Alors, il existe un entier $l \in \mathbb{N}$ et des éléments $d_1, \dots, d_k \in A$ vérifiant $d_1 \mid d_2 \mid \dots \mid d_k$
tq $M \xrightarrow[\text{iso } A\text{-lin}]{\sim} A^l \times A/(d_1) \times A/(d_2) \times \dots \times A/(d_k)$
Les d_i sont appelés les facteurs invariants, ils sont uniques à inv près
<u>preuve</u>
comme M est de type fini,
on peut trouver n générateurs $m_1, \dots, m_n$
et une appli A-linéaire surjective $A^n \xrightarrow{p} M$
$(a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i m_i$
On considère le sous-A-module $N = \ker(p)$
Donc d'après la prop précédente, il existe une base $\{e_1, \dots, e_n\}$ de A^n et des $d_i \in A$ vérifiant $d_1 \mid \dots \mid d_k$
tels que $\{d_1 e_1, d_2 e_2, \dots, d_k e_k\}$ base de N $(k \leq n)$
Donc $M \xrightarrow{\sim} A^n/N = \dfrac{Ae_1 \times \dots \times Ae_k \times Ae_{k+1} \times \dots \times Ae_n}{Ad_1 e_1 \times \dots \times Ad_k e_k} = A/(d_1) \times A/(d_2) \times \dots \times A/(d_k) \times A^{n-k=l}$

<u>Rmq</u>:
si d_i inversible alors $A/(d_i) = 0$
en particulier, si tous les d_i sont inversibles alors $M \cong A^l$ est libre

<u>Applications</u>:
$\boxed{1}$ <u>Groupes abéliens finis</u> (classification)
Soit G un groupe abélien fini
Alors il existe des entiers $d_1, d_2, \dots, d_k \in \mathbb{N}$, $d_i \geq 2$ avec $d_1 \mid d_2 \mid \dots \mid d_k$ tq $G \xrightarrow[\text{iso en tant que grpe}]{\sim} \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$

De plus la suite des entiers $(d_1, \dots, d_k)$ détermine la classe d'iso de G
<u>preuve</u>:
Cas particulier de A-module
on a vu qu'un groupe abélien (= commutatif) est un $\mathbb{Z}$-module et $\mathbb{Z}$ est principal
Donc on peut appliquer le thm de str. de $\mathbb{Z}$-module
$G \xrightarrow{\sim} \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^l$
(G fini $\Rightarrow l = 0$)

Ex :

$G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Trouver les facteurs invariants de G

Application

$\boxed{2}$ K un corps commutatif qcq et V un K-ev de dim finie $(=n)$ $(V = K^n)$

$\Phi, \Phi' \in End(V)$

$V \xrightarrow{\Phi\Phi'} V$

déf : on dit que Φ' est semblable à Φ

s'il existe un iso $u : V \xrightarrow{\sim} V$

tq

$$\begin{tikzcd} V \arrow[r, "\Phi"] \arrow[d, "u"'] \arrow[dr, phantom, "\circlearrowleft"] & V \arrow[d, "u"] \\ V \arrow[r, "\Phi"] & V \end{tikzcd}$$

$u \circ \phi = \phi' \circ u \iff \phi' = u \circ \phi \circ u^{-1}$

idée : trouver des invariants de similitude de cette relation d'éq.

Φ semblable à $\Phi' \iff \phi$ et ϕ' ont même inv de similitude

idée : regarder V comme un $K[X]$-module en utilisant ϕ

$K[X] \times V \longrightarrow V$

$(P, v) \longmapsto P(\phi).(v)$

De manière explicite $P = \sum_{i=0}^{d} a_i X^i$ $a_i \in K$

$P(\phi) = \sum_{i=0}^{d} a_i \phi^i \subset End(V)$, $a_i \in K$

$\phi : V \to V$, $\phi^2(v) = \phi(\phi(v))$, $\phi^n(v) = \phi(\phi(\phi \dots (\phi(v))$

Cette définition munit V d'une structure de $K[X]$-module qui n'est en fait rien que

1) str. de K-module = str. de K-ev

2) str. de X sur V : $\phi : V \to V$

Si on note V_ϕ la str. de $K[X]$-module donnée par ϕ

$V_{\phi'}$ ϕ'

On a 2 $\underset{A}{\overset{\shortparallel}{K[X]}}$-modules V_ϕ et $V_{\phi'}$

Rmq :

V_ϕ et $V_{\phi'}$ sont iso en tant que $A = K[X]$-modules

s'il existe un iso A-lin $V_\phi \xrightarrow{u} V_{\phi'}$

u est $\overset{K[X]}{A}$-lin $\iff \forall a \in A \quad \forall v \in V \quad u(av) = a\,u(v)$

$a \in K \iff u$ est K-linéaire

$a = X \iff u(\overset{\in V_\phi}{X.v}) = X.\overset{\in V_{\phi'}}{u(v)} \quad \forall v$

$\iff u(\phi(v)) = \phi'(u(v)) \quad \forall v$

$\iff u \circ \phi = \phi' \circ u$

$\iff \phi'$ semblable à ϕ

$V = K[X]$-module

$V = \cancel{K[X]}^{\ell} \times K[X]/(P_1) \times \dots \times K[X]/(P_k)$