Séance du 14 octobre 2026

Not : $\hom_A(M,N) \underset{\text{DEF}}{=} \{ f : M \longrightarrow N \text{ morphisme de } A\text{-modules} \}$

① MORPHISMES

(si $A = \mathbb{F}$ un corps et E, F sont des $\mathbb{F}$-espaces vectoriels
$\hom_{\mathbb{F}}(E,F) = \{ f : E \longrightarrow F$ applications $\mathbb{F}$-linéaires$\}$)

Prop $\hom_A(M,N)$ est un A-module

- $(f+g)(m) = f(m) + g(m)$
- $(a \cdot f)(m) = a f(m)$

Exemple : $\hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ $a, b \geq 1$ est un groupe abélien.

il est isomorphe à $\mathbb{Z}/pgcd(a,b)\mathbb{Z}$.

Def $f \in \hom_A(M,N)$ est un isomorphisme

Conditions équivalentes :

$\Leftrightarrow$ f bijective

$\Leftrightarrow \exists g \in \hom_A(N,M)$ tel que

$$\begin{cases} g \circ f = Id_M \\ f \circ g = Id_N \end{cases}$$

Exemple. $a, b \in \mathbb{Z}$

$$f_{a,b} : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 50x + ay \\ 21x + by \end{pmatrix}$$

$f_{a,b}$ est un morphisme de groupe

$$f_{a,b}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

Prop : $f_{a,b}$ est isomorphisme de $\mathbb{Z}$-modules

$$\Updownarrow$$

$$\det \begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix} = 1 \text{ ou } -1$$

$\Downarrow$ si $f_{a,b}$ est un isomorphisme, alors $\exists \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$, $\exists \begin{pmatrix} x' \\ y' \end{pmatrix} \in \mathbb{Z}^2$

tel que $f_{a,b}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$f_{a,b}\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

identité matricielle

$$\begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix}\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\underbrace{\det \begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix}}_{\in \mathbb{Z}} \underbrace{\det \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}}_{\in \mathbb{Z}} = 1$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = (\alpha\delta - \beta\gamma)\, I_n$$

supposons que $\det\begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix} = \varepsilon \in \{\pm 1\}$

Inverse de $\begin{pmatrix} 50 & a \\ 21 & b \end{pmatrix}$ dans $GL_2(\mathbb{R})$

$$B = \frac{1}{\varepsilon}\begin{pmatrix} b & -a \\ -21 & 50 \end{pmatrix} \in M_2(\mathbb{Z})$$

On pose $g : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto B\begin{pmatrix} x \\ y \end{pmatrix}$$

Alors g est l'inverse de $f_{a,b}$.

2) QUOTIENTS

$N \subset M$ deux A-modules

Prop : M/N a une structure de A-module

déf : $a \cdot (m+N) = a \cdot m + N$

Exple : $E \subset F$ sont deux $\mathbb{F}$-ev alors F/E est un ev sur $\mathbb{F}$.

Exemple. $N \subset M \subset \mathbb{Z}^3$

$$N = \{ 2x + 3y - 10z = 0 \}$$

$$M = \{ 2x + 3y - 10z \in 8\mathbb{Z} \}$$

Prop :
- $\mathbb{Z}^3/N$ est isomorphe à $\mathbb{Z}$
- $\mathbb{Z}^3/M$ est un groupe fini

$v \in \mathbb{Z}^3$ et $\overline{v} \in \mathbb{Z}^3/M$

$v = (x,y,z) = (x',y',z') + 8v'$
(division euclidienne par 8)

où $x', y', z' \in \{0, 1, \dots, 7\}$

$$\overline{v} = \overline{(x',y',z')} + \overline{8v'} = \overline{(x',y',z')}$$

$8\mathbb{Z}^3 \subset M$

Donc $\boxed{\# \mathbb{Z}^3/M \leq 8^3}$

Autre type de quotient

I idéal de A

$$\pi : A \longrightarrow A/I$$

On déjà vu que si N est un A/I-module alors N est muni d'une structure de A-module

$$a \cdot m \underset{\text{DEF}}{=} \pi(a) \cdot m$$

$a \cdot m$: nouveau produit externe.

$\pi(a) \cdot m$: ancien produit externe.

Prop Soit M un A-module.

Supposons $\forall m \in M$, $\boxed{I \subseteq \mathrm{ann}_A(m)}$.

Alors M possède une structure de A/I-module

def $$\pi(a) \cdot m \underset{\text{DEF}}{=} a \cdot m$$

$\pi(a) \cdot m$: nouveau produit externe

$a \cdot m$: ancien produit externe.

Si $\pi(a) = \pi(a')$ alors $a = a' + b$ avec $b \in I$

et donc $a \cdot m = a' \cdot m + \underbrace{b \cdot m}_{=0}$.

Exemple : G un groupe abélien fini tel que $2x = 0$ $\forall x \in G$

Ex $(G, \cdot)$ tq $x^2 = 1$ $\forall x \in G \Rightarrow G$ est abélien ?

$\forall x \in G$, $2\mathbb{Z} \subset \mathrm{ann}_{\mathbb{Z}}(x)$ ↯

Conséquence : G possède une structure de $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel.

Conclusion : si $\dim_{\mathbb{Z}/2\mathbb{Z}} G = n$, alors

$$G = \left(\mathbb{Z}/2\mathbb{Z}\right)^n$$

M un A module ⟺ M est un A/I module

(⇒) $\forall m \in M$, $I \subset \mathrm{ann}_A(m)$

On pose $IM = \left\{ \sum_{k=1}^{\ell} a_k m_k \;/\; \begin{matrix} a_k \in I \\ m_k \in M \end{matrix} \right\}$

IM est un sous module de M.

On va considérer le module quotient

M/IM qui est un A-module

$\bar{m} \in M/IM$ et $b \in I$

alors $b \cdot \bar{m} = \overline{b \cdot m} = \bar{0}$ car $bm \in IM$

On a donc $I \subseteq \mathrm{ann}_A(\bar{m})$, $\forall \bar{m} \in M/IM$

Conclusion : M/IM est A/I module

Exemple : G un $\mathbb{Z}$-module, $p \geq 2$ un nombre premier

G/pG est $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel

③ Factorisation :

Soit $f : M \longrightarrow N$ un morphisme de A-modules

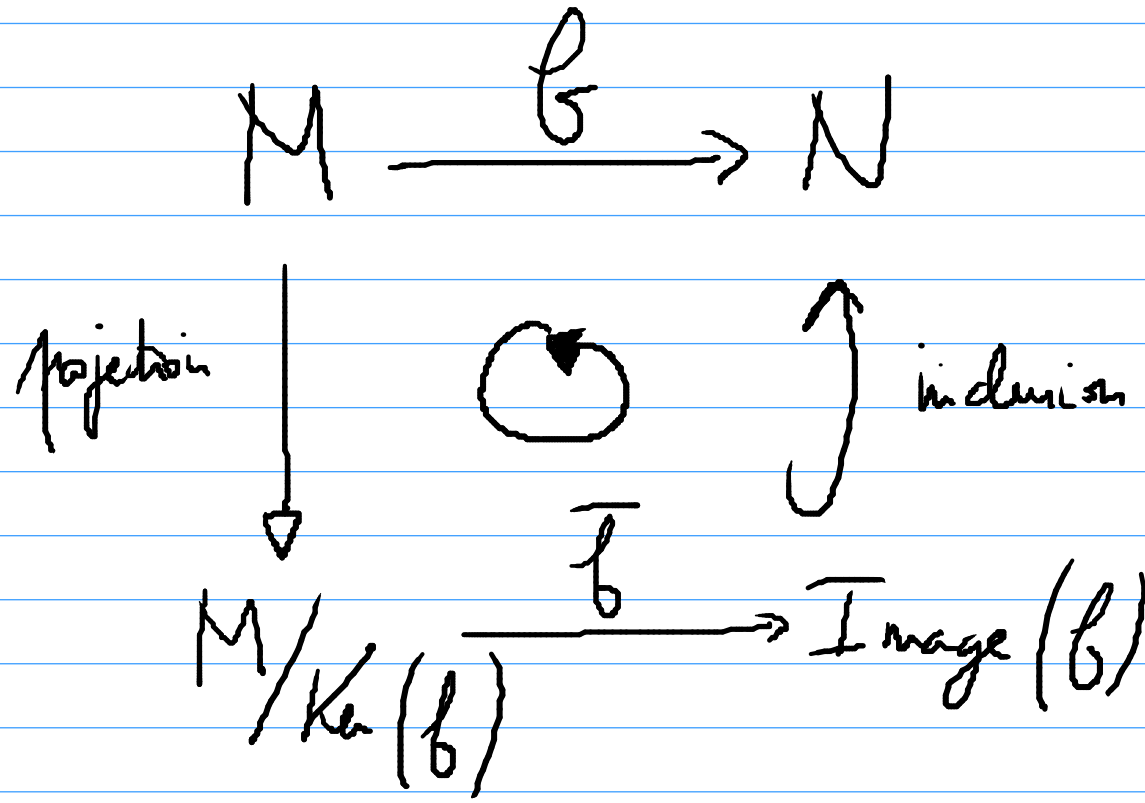
Alors • $\mathrm{Ker}(f) = \{ m \in M,\ f(m) = 0 \}$ est un sous-module de M.

• $\mathrm{Image}(f) = \{ f(m) \mid m \in M \}$ est un sous-module de N

On pose
$$\boxed{\begin{aligned} \bar{f} : M/\mathrm{Ker}(f) &\longrightarrow \mathrm{Image}(f) \\ \bar{m} &\longmapsto f(m) \end{aligned}}$$

Prop $\bar{f}$ est un isomorphisme de A-modules

Diagramme Commutatif :



Exemple : $N = \{2x+3y-10z=0\} \subset \mathbb{Z}^3$

on pose $f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto 2x+3y-10z$$

$$N = \mathrm{Ker}(f)$$

Image (f) est un sous groupe de $\mathbb{Z}$

Imag $(f) \ni 1 = f(-1, 1, 0)$

$\mathrm{Imag}(f) = \mathbb{Z}$

$$\overline{f} : \mathbb{Z}^3/N \xrightarrow{\sim} \mathbb{Z}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} + N \longmapsto 2x + 3y - 10z$$

On a montré que $\mathbb{Z}^3/N$ est isomorphe à $\mathbb{Z}$.

---

(4) Opération sur les modules.

- **Intersection** : soit $N_\alpha \subset M$ sous-module de M, $\alpha \in \mathcal{X}$

Alors $\bigcap_{\alpha \in \mathcal{X}} N_\alpha$ est un sous-module de M

- **Réunion croissante** : $N_k \subseteq M$, $k \in \mathbb{N}$

tel que $N_k \subseteq N_{k+1}$, $\forall k \in \mathbb{N}$.

Mon $\bigcup_{k \in \mathbb{N}} N_k$ est un sous A-module de M

• Module engendré : $X \subset M \ (X \neq \emptyset)$

M est un A-module

Def $\langle X \rangle$ le sous module de M engendré par X est défini par la relation

$$\langle X \rangle = \bigcap_{\substack{N \text{ sous-module de } M \\ X \subseteq N}} N$$

Définition bis : soit $m \in M$

$$m \in \langle X \rangle \iff \begin{cases} \exists\, x_1, \dots, x_k \in X \\ \exists\, a_1, \dots, a_k \in A \\ m = \sum_{i=1}^{k} a_i \cdot x_i \end{cases}$$

Lemme : Soit $N_\alpha \subset M$ $_{\alpha \in \mathcal{X}}$ des A-modules

Def
$$\sum_{\alpha \in \mathcal{X}} N_\alpha \underset{DEF}{=} \left\langle \bigcup_{\alpha \in \mathcal{X}} N_\alpha \right\rangle$$

Définition : $m \in \sum_{\alpha \in \mathcal{X}} N_\alpha$

$\Updownarrow$

- $\exists\ \alpha_1, \dots, \alpha_\ell \in \mathcal{X}$
- $\exists\ m_i \in N_{\alpha_i}$ pour tout $i \in \{1, \dots, \ell\}$

tels que $m = \sum_{i=1}^{\ell} m_i$.

- **Produit Cartesien :**

Première situation

$N_1, \dots, N_p \subseteq M$ sous A-modules

Def Les (N_i) sont en somme directe si

$\forall (n_1, \dots, n_p) \in N_1 \times \dots \times N_p$

$\sum_{i=1}^{p} n_i = 0 \Longrightarrow n_i = 0, \forall i$

Dans ce cas là le sous module

$N_1 + \dots + N_p$ est noté $N_1 \oplus \dots \oplus N_p$

Prop $\forall m \in N_1 \oplus \dots \oplus N_p$,

$\exists ! (n_1, \dots, n_p)$ tel que

$m = n_1 + \dots + n_p$

2ème situation : $N_1, \dots, N_p$ sont des A-modules

alors le produit cartésien $N_1 \times \dots \times N_p$

est muni d'une structure de A-module

$$a \cdot (m_1, \dots, m_p) \underset{\text{DEF}}{=} (a \cdot m_1, \dots, a \cdot m_p)$$

Rmq $X_1 \times \dots \times X_m$ sera noté $X_1 \oplus \dots \oplus X_m$

$$M = X_1 \times \dots \times X_m$$

$$M_i = \{ (0, \dots, 0, x_i, 0 \dots 0) \mid x_i \in X_i \}$$

$$M_i \simeq X_i$$

$$(m_1, \dots, m_p) = \sum_{i=1}^{p} (0, \dots, 0, m_i, 0 \dots 0)$$

$$M = M_1 \oplus \dots \oplus M_p$$

$$X_1 \times \dots \times X_p \simeq X_1 \oplus \dots \oplus X_p$$

$N_1, \dots, N_p$ des A-modules

$N_1 \oplus \dots \oplus N_p$ désigne le produit cartésien $N_1 \times \dots \times N_p$

Notation

si $N_1, \dots N_p$ sont des sous A-modules de M, dans ce cas $N_1 \oplus \dots \oplus N_p$ désigne la somme $N_1 + \dots + N_p$ lorsque celle-ci est **directe**

et ici $N_1 \oplus \dots \oplus N_p \simeq N_1 \times \dots \times N_p$

Module de type fini

M un A - module

Def : $X \subset M$ est dite génératrice $\Leftrightarrow \langle X \rangle = M$

$$A^X = \{ g : X \longrightarrow A \text{ application} \}$$ A-module

$$\left(A^X\right)_0 = \{ g : X \longrightarrow A \text{ application tel que } \{x \in X, f(x) \neq 0\} \text{ est fini} \}$$

Rq si X est fini $A^X = \left(A^X\right)_0$

Morphisme : $f : \left(A^X\right)_0 \longrightarrow M$

$$g \longmapsto \sum_{x \in X} g(x) \cdot x$$

l'image de f est $\langle X \rangle$

Def M est un module de type fini s'il admet une partie génératrice finie

$$X = \{m_1, \dots, m_p\}$$

$$\langle X \rangle = Am_1 + Am_2 + \dots + Am_p$$

Def bis : M est de type fini s'il existe $m_1, \dots, m_p \in M$ tq $M = Am_1 + \dots + Am_p$

Modules libres

$X \subset M$

$$f_X : (A^X)_0 \longrightarrow M$$
$$g \longmapsto \sum_{x \in X} g(x) \cdot x$$

Def. X génératrice ou f_X surjectif

- X est libre si f_X est injectif
- X est une **base** si f_X est un isomorphisme de A-Modules

Def | M est un A-Module libre s'il possède une base

Soit M un A-module :

① de type fini

② libre

Prop Alors M possède une base finie. Toutes les bases de M ont le même cardinal

↳ $\operatorname{rang}(M)$ = le cardinal d'une base de M.

Soit $\{b_1, \dots, b_p\}$ une famille finie génératrice

Soit $\{e_i, i \in I\}$ base de M.

$$\boxed{f_j = \sum_{i \in I} a_j(i) \cdot e_i}$$

Ici $\{ i \in I \mid a_j(i) \neq 0 \}$ est fini

I_j // Notation

$$\boxed{I_1 \cup \dots \cup I_p} \subseteq I$$

ensemble finie

$$\mathcal{F} = \{ e_i, \ i \in I_1 \cup \dots \cup I_p \}$$

famille libre

famille génératrice

car $f_j \in \langle \mathcal{F} \rangle$

On a démontré qu'un M admet une base finie.

Soient $(e_1, \dots, e_n)$ et $(e'_1, \dots, e'_m)$ bases de M

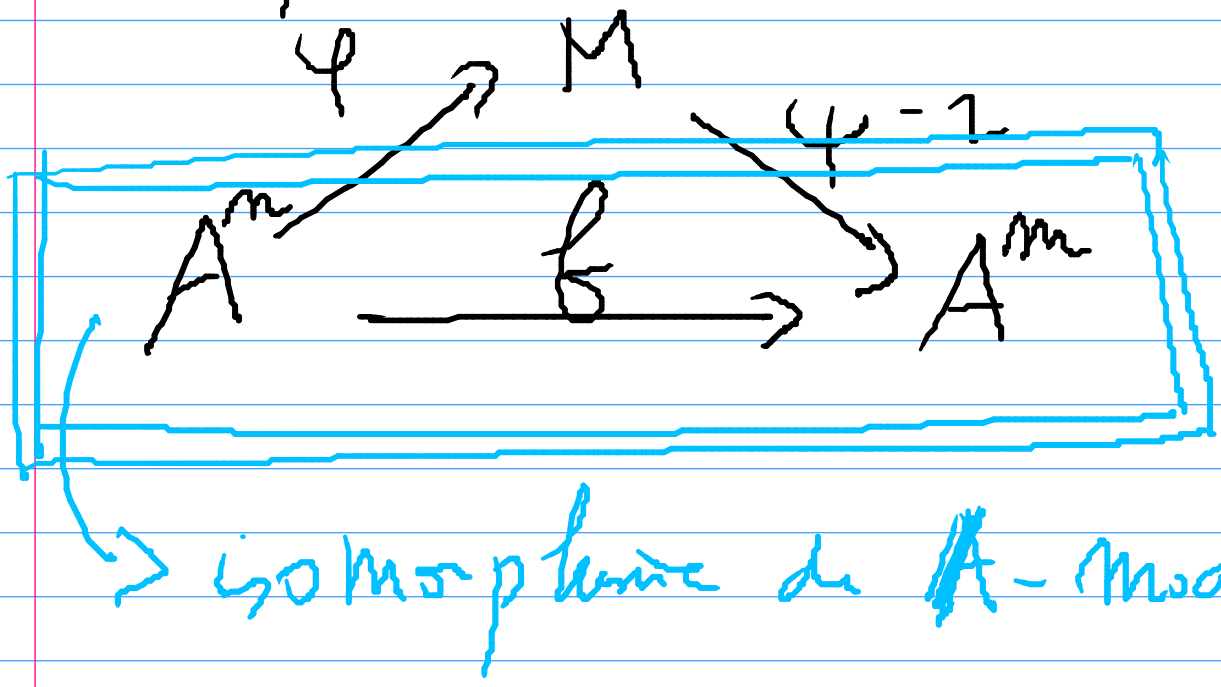
$$\varphi : A^n \longrightarrow M, \quad (a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i \cdot e_i$$

isomorphisme de A-modules

$$\psi : A^m \longrightarrow M, \quad (b_1, \dots, b_m) \longmapsto \sum_{j=1}^{m} b_j \cdot e'_j$$

$\hookrightarrow$ isomorphisme

On pose $f = \psi^{-1} \circ \varphi$



→ isomorphisme de A-module

Si $A = \mathbb{F}$ est un corps $\quad \mathbb{F}^n \simeq \mathbb{F}^m$

si et seulement si $n = m$

On se ramène au cas précédent :

soit I un idéal maximal de A

$M = A^n$ est un A-module

on considère le sous module

$$IM = I(A^n) = I^n$$

$$M/IM = A^n/I^n = (A/I)^n$$

est un A/I — module

espace vectoriel sur $\mathbb{F} = A/I$

$$f : A^m \longrightarrow A^m$$

$$f^{-1} : A^m \longrightarrow A^m$$

$$f(I^n) \subset I^m$$

$a_1, \dots, a_n \in I$

$$f(a_1, \dots, a_n) = \sum_{i=1}^{n} \boxed{a_i f(e_i)}$$

$\in I^m$

Morphisme quotient

$$\alpha = \boxed{\begin{array}{l} \bar{f} : \underbrace{A^n / I^n}_{\mathbb{F}^n} \longrightarrow A^m / I^m \\ v + I^n \longmapsto f(v) + I^m \end{array}}$$

$$\beta = \boxed{\bar{f}^{-1} : A^m / I^m \longrightarrow A^n / I^n}$$

Récapitulons :

$\alpha : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ linéaire

$\beta : \mathbb{F}^m \longrightarrow \mathbb{F}^n$ ——

$$f \circ f^{-1} = Id_{A^m} \Rightarrow \alpha \circ \beta = Id_{F^m}$$

$$f^{-1} \circ f = Id_{A^n} \Rightarrow \beta \circ \alpha = Id_{F^n}$$

Donc α et β sont des

isomorphismes entre l'espace vectoriel

$\Rightarrow$ $M = M$

A-Module libre de type fini

$\hookrightarrow$ $M \simeq A^n$ avec $n = \text{rang}(M)$

Différence entre "A-module" et "espace vectoriel"

un espace vectoriel est un A-module libre de type fini :

Pour les EV : une base c'est une famille libre maximale ou une famille génératrice minimale.

Cela n'est plus vrai pour les A-modules :

(i) $\{2\}$ famille libre dans $\mathbb{Z}$

(ii) $\{2, n\}$ n'est pas libre dans $\mathbb{Z}$

$n \cdot 2 + (-2) \cdot n = 0$

- $\{2\}$ est une famille libre maximale dans $\mathbb{Z}$

- $\{2,3\}$ est une famille génératrice minimale dans $\mathbb{Z}$.

Pour les EV : E ev de dim finie (ou F)

F sev de E

$$F = E \iff \dim F = \dim E$$

Cela ne marche plus avec les A-modules :

$$2\mathbb{Z} \subset \mathbb{Z}$$

$$\operatorname{rang}(2\mathbb{Z}) = \operatorname{rang}(\mathbb{Z}) = 1$$

Hypothèse A est un anneau principal

Ex
- $\mathbb{Z}$ – modules
- $\mathbb{K}[X]$ – modules

Théorème final A anneau principal

et M est un A-module de type fini : $\exists\, n, s \in \mathbb{N}$

- $\exists\, d_1 \mid \dots \mid d_n$ (dans $A - \{0\}$)

tel que $M \simeq A^s \times A/(d_1) \times \dots \times A/(d_n)$

---

les entiers n, s et les idéaux $(d_1) \subseteq \dots \subseteq (d_n)$ sont uniques.

Vernon Orange :

Th Soit G un groupe abélien de type fini : $\exists n, p \in \mathbb{N}$, $\exists d_1 | \dots | d_n$ $(d_i \geq 2)$ tel que $G \simeq \mathbb{Z}^p \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$

Sous module d'un module libre de rang fini.

Th Soit M un A-module libre de rang n, soit N un sous A-module de M

Alors N est un A-module libre et $\operatorname{rang}(N) \leq \operatorname{rang}(M) = n$

Preuve par récurrence sur $n \geq 1$:

$\boxed{n = 1}$ $M = Ae_1$ et

$$\varphi : A \longrightarrow M \text{ est}$$
$$a \longmapsto a \cdot e_1$$

un isomorphisme.

$\varphi^{-1}(N)$ est un sous A-module de A, c'est à dire un idéal de A.

A est principal

hyp $\exists\, a \in A$ tq $\varphi^{-1}(N) = aA$.

Alors $N = \varphi(\varphi^{-1}(N))$

$= A(ae_1)$

donc $\{ae_1\}$ est une base de N.

Remarque : $\boxed{\text{si } N = \{0\}, \text{ rang}(N) = 0}$

Supposons le résultat vrai pour

$\text{rang}(M) = n$

Soit M un module de rang $n+1$

et N un sous module de M

Soit $\{e_1, \dots, e_{n+1}\}$ une base de M

$\forall m \in M, \exists ! (a_1, \dots, a_{n+1}) \in A^{n+1}$

t.q. $m = \sum_1^{n+1} a_i \cdot e_i$

Not $a_i := e_i^*(m)$

$e_i^* : M \longrightarrow A$ linéaire

$$m = \sum_{i=1}^{n} e_i^*(m) \cdot e_i$$

Rmq $e_i^* \in \hom_A(M, A)$

Soit $e_{n+1}^* : M \longrightarrow A$

$$M = M' \oplus A e_{n+1}$$

où $M' = \langle e_1, \dots, e_n \rangle = \ker(e_{n+1}^*)$

M' est libre de rang n

$N \subset M$

$e^*_{n+1}(N)$ est un sous-A-module de A

$\boxed{1^{er} \text{ cas}}$ $e^*_{n+1}(N) = \{0\}$

$\Leftrightarrow$ $N \subseteq \underbrace{M'}_{\text{libre de rang } n}$

On peut appliquer l'hypothèse de récurrence :

Alors N est un sous-module libre, $\text{rang}(N) \leq n$

2ème cas

$e^*_{m+n}(N) = \alpha A$ avec $\alpha \neq 0$

Appliquer

$e^*_{m+n} : N \longrightarrow A$

Soit $r \in N$, $e^*_{m+n}(r) = \alpha$

Prop $N = N' \oplus Ar$

où $N' = M' \cap N$

$= \mathrm{Ker}(e^*_{m+n}) \cap N$

Preuve : $x \in N$

$$\varphi_{n-1}^{*}(x) \in \alpha A$$

donc $\exists\, a \in A$ tq

$$\varphi_{n-1}^{*}(x) = \alpha a$$

$$= \varphi_{n-1}^{*}(a \cdot v)$$

$\Leftrightarrow x - a \cdot v \in \ker(\varphi_{n-1}^{*})$

On a bien

$$x = \underbrace{(x - av)}_{\in N'} + \underbrace{av}_{\in Av}$$

On a bien

$$N = N' + Ar$$

$x \in N' \cap Ar$

$x = ar$ et $\ell_{m,n}^*(x) = 0$

$$\ell_{m,n}^*(ar) = nx$$

$\Rightarrow$ $n = 0$ donc $x = 0$

On a bien $\boxed{N = N' \oplus Ar}$

Récapitulons :

$$\boxed{\begin{aligned} M &= M' \oplus A e_{n+1} \\ N &= N' \oplus A v \end{aligned}}$$

M' est un module libre de rang n

et N' est un sous-module de M'. D'après l'HR : N' est libre de rang $\leq n$

$$N = N' \oplus A v$$

N' a pour base $\{v_1, \dots, v_\ell\}$

avec $\ell \leq n$

Alors N a pour base

$$\{v_1, \dots, v_\ell, v\}$$

Conclusion : N est libre

rang $N \leq n+1$

FIN

$A = \mathbb{Z}[x]$

- A est un A-module libre de rang 1.
- $N = (2, x) = \{2P + xQ \mid P, Q \in \mathbb{Z}[x]\}$

Prop $\boxed{N \text{ n'est pas un } A\text{-module libre}}$

$\ell = r$

Preuve • $\boxed{N \text{ n'est pas un idéal principal}}$

• N a pour base

$\{n_1, \dots, n_\ell\}$ $\quad \ell \geq 2$

relation $0 = n_1 \cdot n_2 + (-n_2) \cdot n_1$

→ impossible