

Déf (module libre). Soit A un anneau, $n \geq 1$

$$A^{\oplus n} := \{ (a_1, \dots, a_n) \mid a_i \in A \ (1 \leq i \leq n) \}$$

muni de la structure naturelle de A -module
(en fait (A, A) -bimodule)

- Un A -module libre de rang n
est un A -module isomorphe à $A^{\oplus n}$, comme A -module.

Rq: Soit M un A -module libre de rg n
alors M admet une A -base $\{m_1, \dots, m_n\}$

- $$\left\{ \begin{array}{l} \text{(i)} \quad M \text{ est engendré par } m_1, \dots, m_n \\ \quad \left(\text{i.e. } \forall m \in M, \exists a_1, \dots, a_n \in A \text{ tq } \right. \\ \quad \quad \quad \left. m = a_1 m_1 + \dots + a_n m_n \right) \\ \text{(ii)} \quad m_1, \dots, m_n \text{ sont } A\text{-lin. indep.} \\ \quad \left(\text{i.e. Si } a_1 m_1 + \dots + a_n m_n = 0 \Rightarrow a_1 = \dots = a_n = 0 \right) \end{array} \right.$$



Il n'est pas vrai que tout A -module
admet une base!

(e.g. $\mathbb{Z}$ -module $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$ -module $\mathbb{Q}$)

Variante / Généralisation (rg ∞)

Soit I un ensemble (eventuellement $|I| = \infty$)

$$A^{(I)} := \bigoplus_{i \in I} A$$

$$:= \left\{ \varphi: I \rightarrow A \mid \left\{ i \in I \mid \varphi(i) \neq 0 \right\} < \infty \right\}$$

(fonctions à support fini
à valeurs dans A)

muni de la str. naturelle de A -module
(en fait un $A\text{-Mod}_A$)

$$(a \cdot f)(i) := a \cdot f(i) \quad \forall i \in I$$

Déf Un A -module libre est un A -module
isomorphe à $A^{(I)}$ pour certain ensemble I .

Rq Un A -module libre admet une base.

Exemple $I = \{1, \dots, n\}$

$$A^{(I)} = \{ f: \{1, \dots, n\} \rightarrow A \} \xrightarrow{\cong} A^{\oplus n}$$
$$f \longmapsto (f(1), \dots, f(n))$$

est un isom. de A -modules.

Déf ^(produit direct)
 $A^I = \{ f: I \rightarrow A \} \in A\text{Mod.}$
attention : - si $|I| < \infty$, $A^I = A^{(I)}$
- si $|I| = \infty$, $A^I \supsetneq A^{(I)}$.
et dans ce cas, A^I n'est pas libre !

Supposons A est un anneau principal.

But: Classifier tous les A -modules finiment engendrés

Thm Soit A un anneau principal

Soit M un A -module finiment engendré (de type fini)

[Version 1] Alors $\exists r \geq 0$, $\exists a_1 | a_2 | \dots | a_m$ éléments de A
(i.e. $(a_1) \supset (a_2) \supset \dots \supset (a_m)$)

tg $M \cong A^{\oplus r} \oplus A/(a_1) \oplus \dots \oplus A/(a_m)$ comme A -module

[Version 2] $\exists r \geq 0$, $\exists$ éléments irréductibles $p_1, \dots, p_n$
(pas forcément distingués)
 $\exists$ entiers positifs $v_1, \dots, v_n$

tg $M \cong A^{\oplus r} \oplus \bigoplus_{i=1}^n A/(p_i^{v_i})$

Rq (Unicité)

Dans [Version 1], r, m , ainsi que les a_i sont
uniquement déterminés par M .

(a_i sont uniques à $A^\times$ -près)

Dans [Version 2], $r, n, \{v_i\}, \{p_i\}$ sont uniques
(p_i est à $A^\times$ -près,

les v_i pour un même ϕ , sont à permutation près).

§ Démonstration du Thm

Soient $m, n \geq 0$
Prop Soit $A \neq 0$ un anneau commutatif unitaire.

Si $A^{\oplus m} \cong A^{\oplus n}$ comme A -modules

alors $m = n$.

En particulier, le rang est une notion bien-définie pour un module libre de rang $< \infty$.

Preuve

(Rappel Un anneau $\neq 0$ comm. unit. admet toujours un idéal maximal.)

On choisit un idéal maximal $\mathfrak{m}$ de A .

En particulier $A/\mathfrak{m} =: k$ est un corps.

On considère le sous-module de $A^{\oplus m}$ engendré par

$$m A^{\oplus m} := \{ t(a_1, \dots, a_m) \mid \begin{matrix} t \in m \\ a_i \in A \end{matrix} \} \text{, en a un isom.}$$

$$(A^{\oplus m}) \otimes_A A/m = A^{\oplus m} / m A^{\oplus m} \xrightarrow{\cong} k^{\oplus m}$$

$$[(a_1, \dots, a_m)] \mapsto \left(\overset{k}{\underset{\vee}{[a_1]}}, \dots, \overset{k}{\underset{\vee}{[a_m]}} \right)$$

De plus. $A^{\oplus m} / m A^{\oplus m}$ est un $k = A/m$ -module
(i.e. k -e.v.)

• c'est un bon de k -e.v.

$$\Rightarrow m = \dim_k (A^{\oplus m} / m A^{\oplus m})$$

$$\text{Même argument } n = \dim_k (A^{\oplus n} / m A^{\oplus n})$$

$$\text{Or } A^{\oplus m} \cong A^{\oplus n} \Rightarrow A^{\oplus m} / m A^{\oplus m} \cong A^{\oplus n} / m A^{\oplus n}$$

$$\stackrel{(\star)}{\Rightarrow} m = n$$

($\star$) (Algèbre linéaire) : La dimension d'un e.v.
(de $\dim < \infty$) est bien-définie. $\square$

Rq Comme sous-module de $A^{\oplus m}$:
le sous-module engendré par $\{t \cdot (a_1, \dots, a_m)\}_{\substack{t \in m \\ a_i \in A}}$

= le sous-module (engendré par) $\{(t_1, \dots, t_m)\}_{t_i \in m}$

• " $\subseteq$ " est trivial :

• " $\supseteq$ " : $(t_1, \dots, t_m) = t_1 \cdot (1, 0, \dots, 0) + t_2 \cdot (0, 1, 0, \dots, 0) + \dots + t_m \cdot (0, 0, \dots, 1)$

Rq/! : la proposition n'est pas en général, pour un anneau non commutatif.

Prop Soit A un anneau principal.
Soit M un A -module libre de rg fini
alors tout sous- A -module de M est
libre (de rg fini $\leq \text{rg}(M)$)

Preuve : On peut supposer que $M = A^{\otimes n}$
pour $n = \text{rg}(M)$

On peut supposer que $n \geq 1$.

On fait par recurrence sur n :

Si $n=1$, $M=A$,

Un sous-module de A n'est rien autre qu'un idéal I

A principal $\Rightarrow \exists a \in A, I = (a)$

$$\left\{ \begin{array}{ll} \text{si } a=0, & I=0 \cong A^{\oplus 0} \\ \text{si } a \neq 0, & I=(a) \xleftarrow{\cong} A \end{array} \right.$$

(Rq: on voit ici que on ne peut pas enlever l'hypothèse "A principal")

Supposons n est pair $< n$.

Soit N un sous-module de $M = A^{\oplus n}$.

On considère $\pi = A^{\oplus n} \longrightarrow A$ un morph. de A -md

$$(a_1, \dots, a_n) \mapsto a_n$$

also $\ker(\pi) = A^{\oplus(n-1)}$

$\Rightarrow \pi(N)$ est un sous-module de A .

$$I_m(\pi|_N: N \rightarrow A)$$

$$\Rightarrow \exists a \in A \text{ tq } \pi(N) = (a).$$

si $a=0$: on a $N \subset \ker(\pi) = A^{\oplus(n-1)}$

on peut conclure par l'hypothèse de réc.

$$\text{rg}(N) \leq n-1 < \text{rg}(M).$$

si $a \neq 0$ on choisit une préimage de a dans N :

i.e. $x \in N$ tq $\pi(x) = a$

i.e. $x = (a_1, \dots, a_{n-1}, a)$

Affirmation

$$\perp \quad N = Ax \oplus (N \cap A^{\oplus(n-1)})$$

ii $\{ (a, b, \dots, a_{n-1}, b) \mid b \in A \}$

ii $\{ y \in N \mid \pi(y) = 0 \}$

Preuve: $Ax \cap (N \cap A^{\oplus(n-1)})$

$$= Ax \cap A^{\oplus(n-1)}$$

$$= \{ (a, b, \dots, a_{n-1}, b) \mid ab=0 \}$$

$$= \{ (0, \dots, 0) \}$$

$b \mapsto \text{caract}$

• $\forall z \in N, \pi(z) \in \text{Im}(\pi|_N) = (a)$

$$\Rightarrow \exists t \in A \quad t \cdot \pi(\beta) = t \cdot a \in A$$

$$\Rightarrow \pi \left(\underset{\substack{\uparrow \\ N}}{\beta} - \underset{\substack{\uparrow \\ A}}{t} \cdot \underset{\substack{\uparrow \\ N}}{x} \right) = t \cdot a - t \cdot \underbrace{\pi(x)}_a = 0$$

$$\Rightarrow \beta - t \cdot x \in N \cap A^{\oplus(n-1)}$$

$$\Rightarrow \beta \in A \cdot x + A^{\oplus(n-1)}$$

□
(Affirmation)

Par l'hyp. de réc.

$\Rightarrow N \cap A^{\oplus(n-1)}$ est un A -module libre de $\forall r' \leq n-1$

or $A \cdot x \hookleftarrow A$
 $t \cdot x \longleftarrow t$

$$\Rightarrow N = A \cdot x \oplus N \cap A^{\oplus(n-1)}$$

$$\simeq A \oplus A^{\oplus r'}$$

$$\simeq A^{\oplus(r'+1)}$$

$\Rightarrow N$ est A -module libre

$$\text{de } r = r' + 1 \leq n \quad \square$$

Cor Soit A un anneau principal
Soit M un A -mod. finiment engendré

$$\left[\begin{array}{l} \text{Alors } \exists n \geq m \geq 0 \\ \exists \phi : A^{\oplus m} \longrightarrow A^{\oplus n} \quad \begin{array}{l} \text{morphisme de } A\text{-mod} \\ \text{injectif} \end{array} \\ \text{tg } M \cong \text{Coker}(\phi) := A^{\oplus n} / \text{Im}(\phi) \end{array} \right.$$

Preuve: M est finiment engendré par $\{x_1, \dots, x_n\}$
 $\Rightarrow \exists n \geq 0$ et un morphisme surjectif de $A^{\oplus n}$

$$\begin{array}{ccc} A^{\oplus n} & \xrightarrow{\pi} & M \\ e_i & \longmapsto & x_i \end{array}$$

Prop $\ker(\pi) \subset A^{\oplus n}$ est un A -mod
libre de $r = m \leq n$.

On peut choisir un isom $\ker(\pi) \cong A^{\oplus m}$.

$$\phi : A^{\oplus m} \xrightarrow{\cong} \ker(\pi) \hookrightarrow A^{\oplus n}$$

$$\Rightarrow M \simeq \text{Im}(\pi) = A^{\oplus n} / \ker(\pi)$$

$$= A^{\oplus n} / \text{Im}(\phi) \simeq \text{coker}(\phi) \quad \square$$

$$\text{Rq} \quad \text{Hom}_A(A^{\oplus m}, A^{\oplus n}) \simeq A^{\oplus mn}$$

$\parallel$
 $\left\{ \text{matrice} \left(\underbrace{\quad}_m \right) \right\}_n \text{ à coeff dans } A$

$$\left(\phi : A^{\oplus m} \rightarrow A^{\oplus n} \right) \longmapsto \begin{cases} \phi(e_1) = \sum_{j=1}^n a_{1j} \varepsilon_j \\ \phi(e_2) = \sum_{j=1}^n a_{2j} \varepsilon_j \\ \vdots \\ \phi(e_m) = \sum_{j=1}^n a_{mj} \varepsilon_j \end{cases}$$

$\{e_1, \dots, e_m\}$ base de $A^{\oplus m}$

$\{\varepsilon_1, \dots, \varepsilon_n\} \longrightarrow A^{\oplus n}$

Donc

But : classifier les coker de matrices
 $\overline{\alpha}$ coeff. dans A .

Déf (équivalence élémentaires)

Deux matrices $n \times m$ à coeff A

M et M'

sont équivalentes si

$$\exists P \in GL_n(A), Q \in GL_m(A),$$

$$\text{tq } M' = P \cdot M \cdot Q$$

opération de lignes
élémentaires

opération
de colonnes
élémentaires

Lemme Si $M \sim M'$

alors $\text{oker}(M) \simeq \text{oker}(M')$

Pfenn

$$\begin{array}{ccc}
 A^{\oplus m} & \xrightarrow{M} & A^{\oplus n} \\
 \uparrow Q & \curvearrowright & \downarrow P \\
 A^{\oplus m} & \xrightarrow{M'} & A^{\oplus n}
 \end{array}$$

Commutative $\Leftarrow M' = P \cdot M \cdot Q$

$$\Rightarrow \begin{array}{ccc}
 A^{\oplus m} & \xrightarrow{M} & A^{\oplus n} \\
 \downarrow Q^{-1} & \curvearrowright & \downarrow P \\
 A^{\oplus m} & \xrightarrow{M'} & A^{\oplus n}
 \end{array}$$

$$\Rightarrow \text{ker}(M) \stackrel{P}{\simeq} \text{ker}(M')$$

(Ex)

□