Prérequis sur les A-modules

P. CALDERO
M1-Lyon1

Dans ce qui suit, $(A, +, .)$ désignera un anneau commutatif avec unité notée 1. On veut généraliser la notion d'espaces vectoriels dans le cas où les scalaires sont non plus dans un corps, mais dans l'anneau A. Au lieu de l'appeler A-espace vectoriel, on l'appellera A-module. Et on fait bien, puisque les propriétés n'ont plus rien à voir. En particulier, on n'a plus le théorème de la base incomplète. La cata !

.1 A-modules, généralités.

Définition .1.1. On appelle A-module un groupe abélien M pour une loi $+$ muni d'une opération de A sur M notée . telle que, pour a, b dans A, x, y, dans M, on ait

1. $a.(x + y) = a.x + a.y$
2. $(a + b).x = a.x + b.y$
3. $a.(b.x) = (a.b).x$
4. $1.x = x$.

Exemple .1.2. Un groupe abélien peut être vu comme un $\mathbb{Z}$-module. Effectivement, soit $(M, +)$ un groupe abélien, on peut définir pour tout n dans $\mathbb{Z}$ et x dans M :

$$n.x = \underbrace{x + \ldots + x}_{n \text{ fois}}, \text{ si } n \geq 0, \quad n.x = \underbrace{-x - \ldots - x}_{-n \text{ fois}} \text{ sinon.}$$

Exemple .1.3. L'anneau A peut être vu comme A-module sur lui-même. L'opération est définie par la multiplication interne.

Exemple .1.4. Soit E un espace vectoriel sur un corps $\mathbb{K}$ et u un endomorphisme de E. Alors, on peut munir E d'une structure de $\mathbb{K}[X]$-module par

$$P.x = P(u)(x),\ P \in \mathbb{K}[X],\ x \in E.$$

On définit comme d'habitude la notion de sous-module et de module quotient :

Définition .1.5. Un sous-module M' de M est un sous-groupe stable pour l'opération de A. On peut alors construire le quotient M/M' tel que

1. M/M', comme groupe, est le groupe quotient habituel,
2. Si $\bar{x} \in M/M'$, $a.\bar{x} = \overline{ax}$.

On vérifie que cette dernière égalité est bien définie.

On définit également la notion de morphisme de A-modules

Définition .1.6. Soient M et N deux A-modules. Un morphisme de A-modules de M dans N est un morphisme entre les groupes M et N qui de plus vérifie $f(a.x) = af(x)$ pour tout a dans A et x dans M. Un isomorphisme est un morphisme bijectif (sa réciproque étant alors automatiquement un morphisme).

Exemple .1.7. Si M' est un sous-module de M, alors l'injection naturelle de M' dans M définit un morphisme de A-modules. La surjection canonique de M sur M/M' définit un morphisme de A-modules.

Exemple .1.8. Si f est un morphisme de A-modules de M dans N, alors son noyau est un sous-module de M et son image est un sous-module de N. On peut alors construire un isomorphisme entre les sous-modules $A/\ker f$ et $\operatorname{Im} f$.

Exemple .1.9. L'ensemble $\hom_A(M, N)$ des morphismes du A-module M vers le A-module N est un A-module pour les opérations

$$(f + g)(x) = f(x) + g(x),\ (a.f)(x) = a.(f(x)),\ f, g \in \hom_A(M, N),\ a \in A,\ x \in M.$$

Exemple .1.10. Si on considère A comme module sur lui-même, alors tout idéal de A est un sous-module de A. On peut ainsi récupérer sur A/I une structure de A-module.

Définition .1.11. Si M est un A-module et I un idéal de A qui annule M ($a.x = 0$ pour tout a dans I et x dans M), alors on peut définir par passage au quotient une structure de A/I-module sur M.

Exemple .1.12. Soit E un espace vectoriel muni d'un endomorphisme u et donc d'une structure de $\mathbb{K}[X]$-module comme dans l'exemple .1.4. Alors, en notant P un polynôme annulateur de u, E est muni d'une structure de $\mathbb{K}[X]/(P)$-module.

Qu'est-ce que la somme directe $M \oplus N$ de deux modules M et N. Take a wild guess !

1. $M \oplus N = M \times N$ comme ensemble,
2. $(x, y) + (x', y') = (x + x', y + y')$, $x, x' \in M$, $y, y' \in N$,
3. $a.(x, y) = (a.x, a.y)$, $a \in A$, $x \in M$, $y \in N$.

.2 A-modules libre.

Même si la théorie des espaces vectoriels est éloignée de celle des A-modules, il existe de A-modules qui se comportent à peu près comme des espaces. Ce sont les modules libres :

Définition .2.1. Soit I un ensemble et $A^{(I)}$ l'ensemble des I-uplets d'éléments de A tels que toutes les coordonnées sont nulles à l'exception d'un nombre fini d'entre elles. Alors, l'addition coordonnées par coordonnées et la multiplication par $a \in A$ coordonnées par coordonnées fournissent une structure de A module sur $A^{(I)}$. Le module $A^{(I)}$ est appelé A-module libre. Par extension, tout module isomorphe à un module libre sera appelé module libre.

En fait, $A^{(I)}$ possède une partie libre et génératrice : si on appelle e_i, pour i dans I le I-uplet nul pour toutes les coordonnées sauf pour la i-ième qui vaut 1, alors la famille $(e_i)_{i \in I}$ est bien libre et génératrice dans un sens qu'il n'est pas difficile à deviner.

Un module M ne possède pas forcément de base, mais s'il en possède une, indexée par I, alors il est isomorphe à $A^{(I)}$. Donc, finalement, un module libre est juste un module possédant une base.

On peut alors se demander si le cardinal d'une base d'un module libre ne dépend pas de la base. Il est rassurant de voir que cela reste encore vrai.

Proposition .2.2. *Soit n et m deux entiers positifs. On suppose que les modules libres A^n et A^m sont isomorphes, alors $n = m$.*

Démonstration. Soit $\phi : A^n \to A^m$ un tel isomorphisme. Il est bien sûr déterminé de façon unique par l'image de la base canonique (e_j) de A^n dans la base canonique (f_i) de A^m. Il peut donc s'exprimer à l'aide d'une matrice de taille $m \times n$ à coefficients dans A. Soit $\Omega = (a_{ij})$ cette matrice.

Soit $\mathfrak{m}$ un idéal maximal de A (que l'on déduit de Zorn et donc de l'axiome du choix, avec toutes nos excuses aux non-axiomiens du choix). Alors $A/\mathfrak{m}$ est un corps que l'on note $\mathbb{K}$. La matrice $\overline{\Omega} = (\bar{a}_{ij})$, obtenue en prenant les classes modulo $\mathfrak{m}$, définit un morphisme $\bar{\phi}$ de $\mathbb{K}^n$ vers $\mathbb{K}^m$ de $\mathbb{K} - modules$ (donc de $\mathbb{K}$-espaces !) à l'aide des bases canoniques $(\bar{e}_j)$ de $\mathbb{K}^n$ et $(\bar{f}_i)$ de $\mathbb{K}^m$.

Montrons que ce morphisme est surjectif. Soit $\overline{Y}$ un vecteur colonne de $\mathbb{K}^m$, il se relève en un vecteur colonne Y de A^m et comme ϕ est surjectif, il existe un vecteur colonne X de A^n tel que $\Omega X = Y$. Ceci donne après passage au quotient $\overline{\Omega}.\overline{X} = \overline{Y}$. D'où la surjectivité annoncée.

Il existe donc un morphisme surjectif d'espaces vectoriels de $\mathbb{K}^n$ vers $\mathbb{K}^m$. Ceci implique que $m \leq n$. Et comme ϕ est un isomorphisme, on a aussi l'inégalité inverse.

Corollaire .2.3. *Deux bases du A-module libre L, si celles sont finies, ont même cardinal.*

Démonstration. Une base de cardinal n du module L fournit un isomorphisme de L vers A^n, qui à x dans L associe ses coordonnées dans la base. Ainsi, par composition, deux bases, l'une de cardinal n, l'autre de cardinal m, fournissent un isomorphisme de A^n vers A^m. Donc, $n = m$.

Remarque .2.4. Il n'est pas difficile de voir que si L possède une base infinie, alors toutes les bases de L sont aussi infinies.

On peut donc parler de dimension d'un module libre ! En bien, non, car le vocabulaire est parfois un excellent garde-fou : on parlera de rang.

Définition .2.5. Le cardinal d'une base d'un module libre L sera appelé rang de L. Il est bien défini par le corollaire qui précède.

Remarque .2.6. Attention ! Si L' est un sous-module libre du module libre L et si L et L' ont même rang, on peut avoir tout de même une stricte inclusion. Par exemple $2\mathbb{Z}$ est un $\mathbb{Z}$ module isomorphe à $\mathbb{Z}$, donc libre de rang 1. C'est aussi un sous-module strict de $\mathbb{Z}$ qui est aussi de rang 1 !

Comme dans le cadre des espaces vectoriels, on peut définir pour un A-module libre L, la matrice de passage d'une base (e_i) à une base (e'_i). Il s'agit de la matrice du morphisme identité Id_L où le module de départ est vu dans la base (e'_i) et ceux d'arrivée dans la base (e_i).

Proposition .2.7. *Si P est la matrice de passage de la base (e_i) à une base (e'_i) du module libre L de rang n et Q la matrice de passage d'une base (e'_i) à une base (e_i), alors $PQ = QP = \mathrm{I}_n$.*

On dira que P est inversible s'il existe une matrice Q à coefficients dans A telle que $PQ = QP = \mathrm{I}_n$.

Corollaire .2.8. *Soit L un module libre de rang n muni d'une base (e_i). Alors une famille (e'_i) de L est une base si et seulement si la matrice P qui la définit en colonnes dans la base (e_i) est inversible. Ce qui est équivalent à dire que le déterminant de P est dans le groupe des unité A^*.*

Démonstration. Le premier point est analogue au cas des espaces vectoriels.

Pour le dernier point, on note que

$$^t\mathrm{com}(P).P = \det(P)\mathrm{I}_n$$

est encore valable pour un anneau. Ceci implique que si $\det(P)$ est inversible, alors P l'est.

Inversement, si P est inversible, alors il existe Q telle que $PQ = \mathrm{I}_n$. En prenant le déterminant des deux côtés, on obtient alors que $\det(P)\det(Q) = 1$ et donc $\det(P)$ est inversible.

.3 Modules de type fini

Les modules de type fini vont généraliser les espaces vectoriels de dimension finie.

Définition .3.1. Un A-module M est dit de type fini s'il existe une famille génératrice finie de M, c'est-à-dire s'il existe un entier n et une famille $(g_i)_{1\leq i\leq n}$ telle que tout x de M peut s'écrire comme A-combinaison linéaire des g_i.

Par analogie avec la présentation d'un groupe par générateurs et relations (présentation qui, on le rappelle, demande la construction de groupes libres), on définit la notion de présentation d'un A-module M.

Proposition .3.2. *Soit M un A-module de type fini et $(g_i)_{1\leq i\leq n}$ une famille génératrice de M. L'application ϕ de A^n dans M définie par*

$$\phi(a_i) = \sum_{i=1}^{n} a_i g_i$$

est un morphisme surjectif de A-modules. Le module A^n et son sous-module $\ker\phi$ *constituent une présentation du A-module M.*