Modules

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

Référence : Objectif Agrégation, Chapitre 6.

AVERTISSEMENT La théorie des modules ne figure pas au programme de l'agrégation. Ainsi, je ne peux donc que vous conseiller de garder vos connaissances, si et seulement si elles s'avèrent nécessaires, pour les questions du jury (qui s'attendra alors à ces réponses).

1 Notion de module

Dans tout ce complément, on désigne par A un anneau commutatif unitaire.

1.1 Modules

Définition 1.1. Un A-module (à gauche) est un groupe abélien M muni d'une loi de composition externe $A \times M \to M$ vérifiant :

$$\forall a \in A, \forall m, m' \in M, \quad a(m+m') = am + am' \tag{1.2}$$
$$\forall a, a' \in A, \forall m \in M, \quad (a+a')m = am + a'm \tag{1.3}$$
$$(aa')m = a(a'm) \tag{1.4}$$
$$\forall m \in M, \quad 1_A m = m \tag{1.5}$$

Proposition 1.6. *Soit M un groupe abélien. La donnée d'une structure de A-module sur M est équivalente à la donnée d'un morphisme d'anneaux unitaires $A \to \mathrm{End}_{\mathrm{Gr}}(M)$.*

Démonstration. Si M est muni d'une structure de A-module, alors l'application $A \to \mathrm{End}_{\mathrm{Gr}}(M)$ donnée par $a \mapsto (\mu_a : m \mapsto am)$ est bien définie, est bien à valeurs dans $\mathrm{End}_{\mathrm{Gr}}(M)$ (par (1.2)) et est un morphisme d'anneaux (par (1.3) et (1.4)) unitaires (par (1.5)). Réciproquement, si $f : A \to \mathrm{End}_{\mathrm{Gr}}(M)$ est un morphisme d'anneaux unitaires, on vérifie de façon similaire que l'application $A \times M \to M$ donnée par $(a, m) \mapsto f(a)(m)$ définit une structure de A-module sur M. □

Exemple 1.7. On connait déjà quelques modules :

- Si $A = k$ est un corps, un k-module n'est rien d'autre qu'un k-espace vectoriel. Nous verrons dans la suite des points communs et des différences majeures entre ces deux théorie.
- Si $A = \mathbb{Z}$, un $\mathbb{Z}$-module n'est rien d'autre qu'un groupe abélien, autrement dit la Définition 1.1 n'apporte aucun renseignement supplémentaire sur la structure.
- L'anneau A est un A-module, et comme avant cela n'apporte aucune nouvelle information.
- D'après les deux derniers points, l'anneau $\mathbb{Z}/n\mathbb{Z}$ possède à la fois une structure de $\mathbb{Z}$-module et de $\mathbb{Z}/n\mathbb{Z}$-module. On va voir (voir notamment Exemple 3.4) que ces deux structures sont très différentes !

— Pour $n \in \mathbb{N}$, l'anneau A^n est un A-module.
— Pour $n, m \in \mathbb{N}^*$, le groupe $\mathrm{Mat}_{n,m}(A)$ des matrices $n \times m$ à coefficients dans A est un A-module.

Exemple 1.8. Soit k un corps et soit E un k-espace vectoriel. On a vu dans le complément sur les invariants de similitude que tout endomorphisme $u \in \mathrm{L}(E)$ munit E d'une structure de $k[X]$-module, où l'action de $k[X]$ est donnée par

$$P \cdot x \coloneqq P(u)(x),$$

pour tout $P \in k[X]$ et $x \in E$. On note E_u le $k[X]$-module ainsi obtenu.

Remarque 1.9. Soit G un groupe fini commutatif. On considère la représentation régulière de G, c'est-à-dire le $\mathbb{C}$-espace vectoriel $\mathbb{C}[G]$ de base $\{e_g\}_{g \in G}$. On peut munir $\mathbb{C}[G]$ d'une structure d'anneau commutatif unitaire en posant $e_g \cdot e_{g'} \coloneqq e_{gg'}$, l'unité étant e_{1_G}. (C'est même alors une $\mathbb{C}$-algèbre, appelée algèbre du groupe G.) On va montrer le fait suivant : la donnée d'une représentation linéaire de G est la donnée d'un $\mathbb{C}[G]$-module.
— Si V est une représentation de G, par définition on a

$$\begin{aligned} g(v + v') &= gv + gv', \\ (gg')v &= g(g'v), \\ 1_G v &= v, \end{aligned}$$

pour tout $g \in G$ et $v, v' \in V$. En posant $e_g \cdot v \coloneqq gv$ pour tout $g \in G$ et $v \in V$ et en étendant par linéarité à tout $\mathbb{C}[G]$, on obtient donc une structure de $\mathbb{C}[G]$-module sur V.
— Réciproquement, si V est un $\mathbb{C}[G]$-module, on pose $g \cdot v \coloneqq e_g \cdot v$ et les axiomes (1.2),(1.4),(1.5) garantissent que l'on a défini une action de groupe.

Ainsi, on peut naturellement faire de la théorie des représentations pour des anneaux (commutatifs) unitaires.

Une nouvelle notion par rapport à la théorie des espaces vectoriels est celle de *torsion*.

Définition 1.10. Soit M un A-module. Un élément $m \in M$ est dit de torsion s'il existe $a \in A \setminus \{0\}$ (non diviseur de zéro) tel que $am = 0$. On note $M_{\mathrm{tors}} \subseteq M$ le sous-ensemble des éléments de torsion.

Exemple 1.11. Si $A = k$ est un corps et si M est un k-espace vectoriel, seul 0_M est de torsion.

Exemple 1.12. Si G est un groupe abélien, un élément du $\mathbb{Z}$-module G est de torsion si et seulement si il est d'ordre fini.

Exemple 1.13. Soit k un corps, soient E un k-espace vectoriel et $u \in \mathrm{L}(E)$. Un élément $x \in E_u$ est de torsion si et seulement si il existe un polynôme $P \in k[X] \setminus \{0\}$ tel que $P(u)(x) = 0$. Ainsi, si E est de dimension finie alors $(E_u)_{\mathrm{tors}} = E_u$ (voir Proposition 6.3 pour plus de détails).

1.2 Sous-modules

Définition 1.14. Soit M un A-module. Un sous-groupe N de M est un sous-A-module si pour tout $a \in A$ et $n \in N$ on a $an \in N$.

En particulier, un sous-A-module est un A-module.

Remarque 1.15. On retrouve la notion de sous-espace vectoriel quand A est un corps.

Proposition 1.16. *Les sous-A-modules de A sont ses idéaux.*

Démonstration. Soit M un sous-groupe de A. C'est un sous-A-module si et seulement si $aM \subseteq M$ pour tout $a \in A$ si et seulement si c'est un idéal. □

Exemple 1.17. On suppose que A est intègre. Si M est un A-module alors M_{tors} est un sous-A-module de M.

Exemple 1.18. Soit k un corps, soient E un k-espace vectoriel et $u \in \mathrm{L}(E)$. On a vu dans le complément sur les invariants de similitudes que les sous-$k[X]$-modules de E_u sont exactement les sous-k-espaces vectoriels de E stables par u.

Propriété 1.19. *Soit M un A-module, soit E une partie de M et soit I un idéal de A. La partie de M*

$$\langle E \rangle_I = IE \coloneqq \left\{ \sum_{i=1}^{n} a_i e_i : n \in \mathbb{N}^*, a_i \in I, e_i \in E \right\},$$

est un sous-A-module de M.

1.3 Morphismes de modules

Définition 1.20. Soient M et N deux A-modules. Un morphisme de groupes $f : M \to N$ est un morphisme de A-modules (ou application A-linéaire) si

$$f(am) = af(m),$$

pour tout $a \in A$ et $m \in M$. On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules entre M et N et $\mathrm{End}_A(M) \coloneqq \mathrm{Hom}_A(M, M)$.

Le noyau et l'image d'un morphisme de A-modules sont définis comme le noyau et l'image en tant que morphisme de groupes.

Remarque 1.21. Soit k un corps, soient E un k-espace vectoriel et $u, v \in \mathrm{L}(E)$. On a vu dans le complément sur les invariants de similitudes que les $k[X]$-modules E_u et E_v sont isomorphes si et seulement si u et v sont semblables.

Propriété 1.22. *Soient M et N deux A-modules. L'ensemble* $\mathrm{Hom}_A(M, N)$ *est un A-module, et pour $f \in \mathrm{Hom}_A(M, N)$ l'ensemble* $\ker f$ *est un sous-A-module de M et* $\operatorname{im} f$ *est un sous-A-module de N.*

Démonstration. C'est comme pour les espaces vectoriels ; on fait seulement le cas de $\mathrm{Hom}_A(M, N)$. On sait déjà que c'est un groupe abélien, et la structure de A-module est donnée par $(af)(m) \coloneqq af(m)$. Remarquons que af est bien A-linéaire par commutativité de A. □

Exemple 1.23. Si M est un A-module, l'application $A \to \mathrm{End}_A(M)$ donnée par $a \mapsto \mu_a$ est un morphisme de A-modules.

Exemple 1.24. La projection sur la première coordonnée $A^n \to A$ est un morphisme de A-modules.

Remarque 1.25. À un élément $M \in \mathrm{Mat}_n(A)$ correspond canoniquement [1] un élément $f \in \mathrm{End}_A(A^n)$, et on peut alors définir le déterminant $\det f \in A$ de f. On a

$$f \text{ injective} \iff \ker f = \{0\},$$

et

$$f \text{ surjective} \overset{(\ddagger)}{\iff} f \text{ bijective} \overset{(\dagger)}{\iff} \det f \in A^\times.$$

On peut montrer (†) avec la formule de la comatrice, et (‡) en construisant un inverse à droite et en utilisant (†). En particulier, on n'a pas l'équivalence f injective $\iff$ f bijective : par exemple, le morphisme de $\mathbb{Z}$-modules $\mathbb{Z} \to \mathbb{Z}$ donné par $n \mapsto 2n$ est injectif mais pas bijectif.

1. Il faut attendre la Section 3 pour donner un vrai sens à ce « canoniquement ».

Les ressemblances avec la théorie des espaces vectoriels s'arrête (presque) là. Outre les définitions (produit et somme directe, module engendré, quotient, ...) et quelques théorèmes directs (propriétés universelles, théorèmes d'isomorphisme,...), il faut presque occulter tous les résultats non triviaux que vous connaissez sur les espaces vectoriels. Notamment, sur la dimension, appelée *rang* dans le cadre des modules.

2 Modules de type fini

Si $\mathcal{F}$ est un ensemble (possiblement infini), on rappelle qu'une famille $(a_m)_{m\in\mathcal{F}} \in A^{\mathcal{F}}$ est dite à support fini, et on note $(a_m)_{m\in\mathcal{F}} \in A^{(\mathcal{F})}$, si l'ensemble des $m \in \mathcal{F}$ tels que $a_m \neq 0$ est fini.

Définition 2.1. Soit M un A-module et soit $\mathcal{F}$ une famille (possiblement infinie) d'éléments de A. La famille $\mathcal{F}$ est génératrice si tout élément m' de M s'écrit sous la forme

$$m' = \sum_{m\in\mathcal{F}} a_m m,$$

pour $(a_m)_{m\in\mathcal{F}} \in A^{(\mathcal{F})}$.

Remarque 2.2. Si $A = k$ est un corps, la notion coïncide avec la notion de famille génératrice d'un k-espace vectoriel.

Définition 2.3. Un A-module M est de *type fini* s'il possède une famille génératrice finie.

Exemple 2.4. Le A-module A^n est de type fini puisque la « base canonique » est une famille génératrice à n éléments.

Exemple 2.5. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas de type fini. En effet, si $\mathbb{Q}$ est engendré par $q_1, \ldots, q_n$ sur $\mathbb{Z}$ alors on aurait que le dénominateur de tout élément de $\mathbb{Q}$ divise le produit des dénominateurs de $q_1, \ldots, q_n$ (ce qui est impossible puisqu'il existe une infinité de nombres premiers).

Exemple 2.6. Le $\mathbb{Z}$-module $\mathbb{Z}$ est de type fini car engendré par $\{1\}$. La famille $\{2, 3\}$ est également génératrice puisque $1 = 3 - 2$. De façon générale, pour $a, b \in \mathbb{Z} \setminus \{0\}$ alors $\{a, b\}$ est génératrice si et seulement si a et b sont premiers entre eux. De plus, si $a, b \neq \pm 1$ alors ni $\{a\}$ ni $\{b\}$ n'est génératrice. Ainsi, si $a, b \neq \pm 1$ et $\operatorname{pgcd}(a, b) = 1$ alors $\{a, b\}$ est une partie génératrice minimale. On obtient donc le premier avertissement suivant.

ATTENTION !
Les familles génératrices minimales n'ont pas nécessairement toutes le même cardinal.

Propriété 2.7. *Toute sur-famille d'une famille génératrice est génératrice.*

On a vu que A^n est un A-module de type fini. La proposition suivante montre que c'est l'archétype des modules de types finis.

Proposition 2.8. *Soit M un A-module de type fini. Alors il existe $n \in \mathbb{N}$ tel que M est un quotient de A^n.*

Démonstration. Par hypothèse, il existe une famille $\mathcal{G} = (m_1, \ldots, m_n) \in M^n$ telle que l'application $\Phi_{\mathcal{G}} : A^n \to M$ qui à $(a_1, \ldots, a_n)$ associe $\sum_{i=1}^n a_i m_i$ est surjective. L'application $\Phi_{\mathcal{G}}$ étant un morphisme de A-modules, on a donc $A^n / \ker \Phi_{\mathcal{G}} \simeq M$ en tant que A-modules. □

La proposition suivante rappelle un énoncé d'espaces vectoriels.

Proposition 2.9. *Soit M un A-module de type fini et soit $\mathcal{G}$ une famille génératrice. On peut extraire de $\mathcal{G}$ une famille génératrice finie.*

Démonstration. Par hypothèse, le A-module M possède une famille génératrice finie $\mathcal{F}$. Il suffit d'écrire chaque élément de $\mathcal{F}$ comme combinaison linéaire d'éléments de $\mathcal{G}$. Les éléments de $\mathcal{G}$ impliqués sont en nombre fini et forment une famille génératrice de M puisqu'on atteint tous les éléments de $\mathcal{F}$. □

Cependant, il ne faut pas trop en vouloir ! Lorsque $A = k$ est un corps, on sait bien qu'un k-module de type fini est de dimension finie et que tous ses sous-k-modules sont également de dimension finie donc de type fini. Cette propriété n'est plus vraie en générale pour les modules.

ATTENTION !
Il existe des modules de types finis avec des sous-modules qui ne sont pas de type fini.

On verra dans la Section 5 un cadre dans lequel cette situation n'arrive jamais.

Exemple 2.10. Soit k un corps et soit $A \coloneqq k[X_i : i \in \mathbb{N}]$ l'anneau de polynômes en une infinité de variables (la réunion croissante des $k[X_1, \dots, X_n]$). C'est un A-module de type fini, engendré par 1. Cependant, le sous-A-module $I \coloneqq \langle X_i : i \in \mathbb{N} \rangle$ (c'est bien un sous-A-module car c'est un idéal, voir Proposition 1.16) n'est pas de type fini. En effet, si $\langle f_1, \dots, f_k \rangle = I$ alors soit n tel que $f_i \in k[X_1, \dots, X_n]$ pour tout i. On a donc $X_{n+1} = \sum_{i=1}^{n} g_i f_i$ pour certains $g_i \in A$, et on trouve une contradiction en substituant 0 à $X_1, \dots, X_n$ (les éléments de I n'ont pas de coefficient constant).

Remarque 2.11. On parle de module *noethérien* quand tout sous-module d'un module de type fini est de type fini. Si l'anneau A est noethérien (donc tout idéal est de type fini, cf. Proposition 1.16), tout A-module de type fini est noethérien. On ne voit pas souvent le cas pathologique ci-dessus arriver puisque la majorité des anneaux que l'on rencontre sont noethériens, notamment : les anneaux principaux et $A[X]$ si A est noethérien (théorème de la base de Hilbert) donc $k[X_1, \dots, X_n]$ si k est un corps.

3 Modules libres

Définition 3.1. Soit M un A-module et soit $\mathcal{F}$ une famille (possiblement infinie) d'éléments de A. La famille $\mathcal{F}$ est libre si

$$\sum_{m \in \mathcal{F}} a_m m = 0 \implies a_m = 0 \text{ pour tout } m \in \mathcal{F},$$

pour toute famille à support fini $(a_m)_{m \in \mathcal{F}} \in A^{(\mathcal{F})}$ d'éléments de A.

Remarque 3.2. Si $A = k$ est un corps, la notion coïncide avec la notion de famille libre d'un k-espace vectoriel.

Propriété 3.3. *Une sous-famille d'une famille libre est libre.*

Exemple 3.4. Soit $n \in \mathbb{N}^*$ et soit $M \coloneqq \mathbb{Z}/n\mathbb{Z}$.
- La famille $\{1\}$ est une famille libre de M en tant que $\mathbb{Z}/n\mathbb{Z}$-module. En effet, si $m1 = 0$ pour $m \in \mathbb{Z}/n\mathbb{Z}$ alors $m = 0$.
- En revanche, seule la famille vide est une famille libre de M en tant que $\mathbb{Z}$-module. En effet, pour $m \in M \setminus \{0\}$ on a $nm = 0$ mais $n \in \mathbb{Z}$ n'est pas nul.

Exemple 3.5. Généralisant le deuxième point de l'exemple précédent, si G est un groupe abélien fini alors toute famille non triviale du $\mathbb{Z}$-module G n'est pas libre. En lien avec l'Exemple 1.12, une famille libre n'a aucun élément de torsion.

Exemple 3.6. On considère le $\mathbb{Z}$-module $\mathbb{Q}$. La famille $\{q\}$ est libre si et seulement si $q \in \mathbb{Q}^*$, et toute famille à deux éléments est liée.

Exemple 3.7. Dans le A-module A toute famille libre a au plus un seul élément : si $a, b \in A \setminus \{0\}$ on peut toujours écrire $b \cdot a - a \cdot b = 0$. Les familles libres sont exactement les $\{a\}$ pour $a \in A \setminus \{0\}$ non diviseur de 0_A.

Définition 3.8. Soit M un A-module. Une base de M est une famille à la fois libre et génératrice. On dit que M est *libre* si M possède une base.

Le vocabulaire est un peu trompeur ici : un module est libre (*free*) s'il possède une base, non pas seulement s'il possède une famille libre (*linearly independent family*).

Exemple 3.9. Par l'Exemple 3.4, la famille $\{1\}$ est une base du $\mathbb{Z}/n\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$.

Exemple 3.10. Plus généralement, le A-module A est libre et $\{1\}$ en est une base. Encore plus généralement, le A-module A^n est libre et la « base canonique » en est bien une base.

Exemple 3.11. La famille $\{X^i\}_{i \in \mathbb{N}}$ est une base du A-module $A[X]$.

Si A est un corps, tous les A-modules sont libres et être de type fini veut dire de dimension finie. En général, la terminologie laisse penser que certains modules ne sont pas libres...

ATTENTION !
Contrairement aux espaces vectoriels, il existe des modules qui n'ont pas de base, *i.e.* qui ne sont pas libres.

Exemple 3.12. Par l'Exemple 3.5, un groupe abélien non trivial ne possède pas de base en tant que $\mathbb{Z}$-module.

Exemple 3.13. Si I est un idéal propre non nul de A alors le A-module A/I n'est pas libre.

Exemple 3.14. Si A est intègre et si I est un idéal de A, le A-module I est libre si et seulement si I est principal. En effet, si $I = \langle a \rangle$ alors $\{a\}$ engendre I et est libre puisque A est intègre. Réciproquement, si I est libre soit $\mathcal{B}$ une base. Si $\mathcal{B} = \emptyset$ alors $I = \langle 0 \rangle$ est principal, si $\mathcal{B} = \{a\}$ alors $I = \langle a \rangle$, et si $a, b \in \mathcal{B}$ avec $a \neq b$ alors $\{a, b\}$ n'est pas libre (cf. Exemple 3.7) donc c'est absurde.

ATTENTION !
Pire encore, pour un module libre on ne peut pas nécessairement :
- **extraire de base d'une famille génératrice ;**
- **dire qu'une famille génératrice minimale est une base ;**
- **étendre une famille libre en une base ;**
- **dire qu'une famille libre maximale est une base.**

Exemple 3.15. Le $\mathbb{Z}$-module $\mathbb{Z}$ est libre de type fini et une base est $\{1\}$. En revanche, on a vu dans l'Exemple 2.6 que la famille $\{2, 3\}$ est une partie génératrice minimale de $\mathbb{Z}$. Cette famille n'étant pas libre (cf. Exemple 3.7), on en déduit qu'elle n'est pas une base (et qu'on ne peut pas non plus en extraire de base).

Exemple 3.16. On a vu dans l'Exemple 3.7 que les familles libres non vides du A-module A sont les $\{a\}$ pour $a \in A \setminus \{0\}$ non diviseur de 0. Les bases sont obtenues pour $a \in A^\times$ (on retrouve le cas de l'Exemple 3.10). En particulier, si $a \neq 0$ non diviseur de zéro n'est pas inversible alors la famille $\{a\}$ est une famille libre maximale mais n'est pas une base et on ne peut pas non plus la compléter en une base.

ATTENTION !
Un sous-module d'un module libre n'est pas nécessairement libre.

On verra dans la Section 5 un cadre dans lequel cette situation n'arrive jamais. On a déjà vu un tel cas dans l'Exemple 3.14 ; en voici un autre.

Exemple 3.17. Avec $A = \mathbb{Z}/4\mathbb{Z}$ alors A est un A-module libre, mais le sous-A-module $M := 2\mathbb{Z}/4\mathbb{Z}$ n'est pas libre, par exemple car son cardinal n'est pas une puissance de 4.

4 Rang d'un module libre de type fini

On veut maintenant définir la notion de rang, l'analogue de la dimension des espaces vectoriels. Rappelons que lorsque $A = k$ est un corps, on peut montrer que toutes les bases d'un k-espace vectoriel de type fini ont le même cardinal à l'aide du lemme suivant.

Lemme 4.1 (Lemme d'échange)**.** *Soit E un k-espace vectoriel engendré par une famille $(w_1, \dots, w_n)$. Si $(v_1, \dots, v_m)$ est une famille libre, alors $m \leq n$ et $(v_1, \dots, v_m, w_{m+1}, \dots, w_n)$ engendre E (après réindexation des w_i).*

Démonstration. Par récurrence sur m. Par exemple, pour $m = 1$ on a bien $1 \leq n$ (puisqu'alors E n'est pas réduit à $\{0\}$ car $\{v_1\}$ est une famille libre). Par hypothèse on peut écrire $v_1 = \sum_{i=1}^{n} \lambda_i w_i$. Puisque $v_1 \neq 0$ on sait qu'il existe i tel que $\lambda_i \neq 0$, en réorganisant on peut supposer que $i = 1$ et on a alors

$$w_1 = \frac{1}{\lambda_1}\left(v_1 - \sum_{i=2}^{n} \lambda_i w_i\right).$$

Ainsi, on a $w_1 \in \mathrm{vect}(v_1, w_2, \dots, w_n)$ et donc $(v_1, w_2, \dots, w_n)$ est génératrice (puisque le vect contient $w_1, \dots, w_n$). □

On peut voir le problème pour les modules : on a divisé par un scalaire, qui a priori peut ne pas être inversible dans l'anneau de base A. Et en effet, le lemme d'échange devient faux en général pour les modules.

Exemple 4.2. La famille $\{2, 3\}$ engendre le $\mathbb{Z}$-module $\mathbb{Z}$ (cf. Exemple 2.6) et la famille $\{6\}$ est libre (Exemple 3.7). On a $m = 1 \leq 2 = n$, mais ni $\{6, 2\}$ ni $\{6, 3\}$ n'engendre $\mathbb{Z}$ (on obtient $2\mathbb{Z}$ et $3\mathbb{Z}$ respectivement).

Proposition 4.3. *Soit M un A-module et supposons que $\mathcal{B} \subseteq M$ soit une base. Alors $\mathcal{B}' \subseteq \mathcal{B}$ est une base de M si et seulement si $\mathcal{B}' = \mathcal{B}$.*

Démonstration. Si $b \in \mathcal{B} \setminus \mathcal{B}'$ alors on peut écrire $b = \sum_{b' \in \mathcal{B}'} a_{b'} b'$ pour $a_{b'} \in A$. Mais alors $b + \sum_{b' \in \mathcal{B}'} (-a_{b'}) b' = 0$ et $1 \neq 0$ donc la famille $\mathcal{B}$ n'est pas libre. □

Proposition 4.4. *Soit M un A-module libre de type fini. Toutes les bases de M sont finies et ont le même cardinal, appelé* rang *de M.*

Démonstration. Soit $\mathcal{B}$ une base de M. Par la Proposition 2.9, on peut extraire une famille génératrice $\mathcal{B}' \subseteq \mathcal{B}$ finie. La famille $\mathcal{B}'$ est encore libre comme sous-famille d'une famille libre (Propriété 3.3), c'est donc une base de M. Finalement, par la Proposition 4.3 on a $\mathcal{B}' = \mathcal{B}$ donc $\mathcal{B}$ est finie.

On a donc montré que toute base de M est finie, reste à montrer qu'elles ont toutes le même cardinal. Si $\mathcal{B}$ est une base de M de cardinal n, l'application $\Phi_{\mathcal{B}} : A^n \to M$ de la Proposition 2.8 est une bijection donc $A^n \simeq M$ (en tant que A-modules). Ainsi, pour conclure il suffit de montrer que $A^n \simeq A^m$ (en tant que A-modules) implique $n = m$.

Pour cela, l'idée est de se ramener au cas des espaces vectoriels, via un quotient par un idéal maximal de A. Soit $\phi : A^n \to A^m$ un isomorphisme de A-modules. Par le théorème de Krull, l'anneau A possède un idéal maximal $\mathfrak{m}$, qui engendre des sous-A-modules $\mathfrak{m}A^n \subseteq A^n$ et $\mathfrak{m}A^m \subseteq A^m$ (cf. Propriété 1.19). Comme ϕ est A-linéaire, on a $\phi(\mathfrak{m}A^n) \subseteq \mathfrak{m}\phi(A^n) \subseteq \mathfrak{m}A^m$, on en déduit une application A-linéaire surjective

$$\overline{\phi} : A^n/\mathfrak{m}A^n \twoheadrightarrow A^m/\mathfrak{m}A^m.$$

Pour $k \in \{n, m\}$ on a $\mathfrak{m}^{\times k} = \mathfrak{m}A^k$: l'inclusion $\supseteq$ est claire, et on peut montrer $\subseteq$ via une somme coordonnée par coordonnée en utilisant la base canonique ($(m_1, \dots, m_k) = \sum_{i=1}^k m_i e_i$). On a $A^k/\mathfrak{m}^{\times k} \simeq (A/\mathfrak{m})^k$ (comme d'habitude, on regarde le noyau de l'application canonique $A^k \to (A/\mathfrak{m})^k$), l'application $\overline{\phi}$ devient donc

$$\overline{\phi} : (A/\mathfrak{m})^n \twoheadrightarrow (A/\mathfrak{m})^m.$$

On se convainc que cette application A-linéaire est $A/\mathfrak{m}$-linéaire. L'idéal $\mathfrak{m}$ étant un idéal maximal de A, l'anneau $k \coloneqq A/\mathfrak{m}$ est un corps. On a donc construit une surjection k-linéaire entre k^n et k^m, donc par la théorie des espaces vectoriels on a $n \geq m$. On obtient l'inégalité inverse en raisonnant avec ϕ^{-1}, et finalement $n = m$. □

Remarque 4.5. Si $A = k$ est un corps, fatalement le rang d'un k-module de libre de type fini est sa dimension en tant que k-espace vectoriel (c'est le cardinal d'une base).

ATTENTION !
Il n'y a pas de raisonnement du type « par égalité des rangs »

Exemple 4.6. Le sous-$\mathbb{Z}$-module $2\mathbb{Z}$ est un sous-$\mathbb{Z}$-module libre strict du $\mathbb{Z}$-module libre $\mathbb{Z}$, mais les deux sont de rang 1, une $\mathbb{Z}$-base de $2\mathbb{Z}$ étant $\{2\}$. Ainsi :

- deux modules libres de même rang dont l'un contient l'autre ne coïncident pas nécessairement ;
- en particulier, si M est un A-module libre de rang n alors une famille libre à n éléments de M n'est pas nécessairement une base de M.

5 Modules de types finis sur un anneau principal

On suppose dans cette section que l'anneau A est principal, c'est-à-dire que A est intègre et que tous ses idéaux sont principaux. On va voir que certain contre-exemples désagréables de la Section 3 (notamment Exemples 3.14 et 3.17) ne peuvent plus se produire.

Commençons tout d'abord par le résultat de réduction suivant, qui généralise la décomposition donnant le rang d'une matrice. Rappelons que deux matrices $M, N \in \mathrm{Mat}_{m,n}(A)$ sont équivalentes s'il existe $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que $M = PNQ$.

Théorème 5.1 (Forme normale de Smith)**.** *Soit $M \in \mathrm{Mat}_{m,n}(A)$. Il existe un unique entier $s \in \{0, \dots, \min(m, n)\}$ et des scalaires $d_1 \mid \cdots \mid d_s$ de $A \setminus \{0\}$, uniques à multiplication par un inversible près, tels que M soit équivalente à la matrice* $\mathrm{diag}(d_1, \dots, d_s, 0, \dots, 0) \in \mathrm{Mat}_{m,n}(A)$.

Démonstration. On a vu la preuve dans le cas particulier $A = k[X]$ dans le complément sur les invariants de similitude. L'idée est la même dans le cas A euclidien : on choisit un élément de plus petit stathme, que l'on place en haut à gauche et par qui on fait la division euclidienne de tous les autres coefficients via des opérations sur les lignes et les colonnes (en rechoisissant un élément de stathme strictement plus petit à chaque étape s'il existe). On arrive alors à une matrice

de la forme $\left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & M' \end{array}\right)$ où $M' \in \mathrm{Mat}_{m-1,n-1}(A)$ a tous ses coefficients multiples de d_1, et on recommence la procédure pour M'. L'unicité découle du fait suivant : l'élément $d_1 \cdots d_i \in A$ est associé au pgcd des mineurs de M de taille i. En effet, ces quantités sont invariantes par opération sur les lignes et les colonnes, de façon équivalente par multiplication à gauche et à droite par des matrices inversibles.

Le cas A principal suit le même principe, mais on remplace les divisions euclidiennes entre $a, b \in A \setminus \{0\}$ par une opération qui donne une relation de Bézout ($ua + vb = d$ où d est un pgcd de a et b, c'est-à-dire $\langle d \rangle = \langle a \rangle + \langle b \rangle$). Dans ce cas ce n'est plus le stathme qui diminue strictement mais le nombre de facteurs irréductibles (A est factoriel car principal). □

Lemme 5.2. *Soit M un A-module libre de rang r et N un sous-A-module de M. Alors N est un A-module libre de rang $\leq r$.*

Démonstration. On raisonne par récurrence sur r. Pour $r = 1$ on a $M \simeq A$ et c'est l'Exemple 3.14. Si $r \geq 2$, soit $(e_1, \ldots, e_r)$ une base de M et soit $\gamma : M \to A$ l'application r-ième coordonnée. C'est un morphisme surjectif de A-modules et $\ker \gamma = \oplus_{i=1}^{r-1} A e_i$. Ainsi le A-module $\ker \gamma$ est libre de rang $r-1$ et $M = \ker \gamma \oplus A e_r$. Si maintenant $N \subseteq \ker \gamma$ alors on applique l'hypothèse de récurrence, et sinon le sous-A-module $\gamma(N)$ de A est un idéal, donc principal, donc égal à $\langle a \rangle$ pour $a \in A \setminus \{0\}$. Soit $x \in N$ tel que $a = \gamma(x)$. On montre que $N = (N \cap \ker \gamma) \oplus Ax$, et on conclut par hypothèse de récurrence puisque $N \cap \ker \gamma$ est un sous-module du module libre $\ker \gamma$ de rang $r - 1$. □

On peut améliorer ce lemme avec le théorème fondamental suivant.

Théorème 5.3 (Théorème de la base adaptée)**.** *Soit M un A-module libre de type fini de rang r et soit N un sous-module de M. Il existe une base $(e_1, \ldots, e_r)$ de M, un entier $s \in \{0, \ldots, r\}$ et des scalaires $d_1, \ldots, d_s \in A \setminus \{0\}$ tels que :*
- *on a $d_1 \mid \cdots \mid d_s$;*
- *la famille $(d_1 e_1, \ldots, d_s e_s)$ est une base de N.*

Ainsi, le A-module N est libre de rang $s \leq r$, en particulier, l'entier s est unique. De plus, chaque d_i est déterminé à un inversible près.

Démonstration. Par le Lemme 5.2, le sous-module N est libre de rang $s \leq r$. On peut donc considérer la matrice de l'inclusion de N dans M relativement à deux bases, puis prendre sa forme normale de Smith (Théorème 5.1). Les matrices inversibles impliquées correspondent à des changements de bases, et la matrice diagonale obtenue est la matrice de l'inclusion dans ces bases. On en déduit le résultat. □

Remarque 5.4. À noter que l'on parle ici de base *adaptée* : on construit une base du petit à partir d'une base du grand, contrairement à la base *incomplète* pour les espaces vectoriels où l'on construit une base du grand à partir d'une base du petit.

Exemple 5.5. On prend $A = \mathbb{Z}$ et $M = \mathbb{Z}^2$. On considère le sous-module $N := \left\langle \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$. On a ici $r = s = 2, d_1 = 1, d_2 = 2$ et on peut prendre $e_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Remarquons quel la première base de N ne provient pas d'une base de M. En effet, si c'était le cas on aurait nécessairement $s = 2$ et $d_1 = d_2 = 1$ donc $M = N$, ce qui est absurde puisque $M \ni \begin{pmatrix} 0 \\ 1 \end{pmatrix} \notin N$.

Une conséquence toute aussi importante est la suivante.

Théorème 5.6 (Théorème de structure)**.** *Soit M un A-module de type fini. Il existe un unique couple $(r, s) \in \mathbb{N}^2$ d'entiers et une unique suite $\langle d_1 \rangle \supseteq \cdots \supseteq \langle d_s \rangle$ d'idéaux propres non nuls tels que*

$$M \simeq A^r \oplus \left(\bigoplus_{i=1}^{s} A/\langle d_i \rangle \right),$$

en tant que A-modules.

Les éléments d_i du théorème, déterminés à inversibles près [2], sont les *facteurs invariants* du A-module M.

Démonstration. Soit $\mathcal{G} = (m_1, \ldots, m_n)$ une famille génératrice de M. Le morphisme $\Phi_{\mathcal{G}}$ de A-modules (cf. preuve de la Proposition 2.8) est ainsi surjectif, le premier théorème d'isomorphisme donne donc $M \simeq A^n/\ker \Phi_{\mathcal{G}}$. Par le Théorème 5.3 de la base adaptée, puisque $\ker \Phi_{\mathcal{G}}$ est un sous-A-module de A^n on sait qu'il existe une base $(e_1, \ldots, e_n)$ de A^n et une unique suite $d_1 \mid \cdots \mid d_s$ d'éléments non nuls de A telles que $(d_1 e_1, \ldots, d_s e_s)$ est une base de $\ker \Phi_{\mathcal{G}}$. On a donc :

$$\begin{aligned} M &\simeq A^n/\ker \Phi_{\mathcal{G}} \\ &\simeq \left(\bigoplus_{i=1}^{n} Ae_i \right) / \left(\bigoplus_{i=1}^{s} Ad_i e_i \right) \\ &\simeq \left(\bigoplus_{i=1}^{s} Ae_i/Ad_i e_i \right) \oplus \bigoplus_{i=s+1}^{n} Ae_i \\ &\simeq \left(\bigoplus_{i=1}^{s} A/\langle d_i \rangle \right) \oplus A^{n-s}. \end{aligned}$$

Si $\langle d_i \rangle = A$ (*i.e.* $d_i \in A^\times$) il suffit d'enlever le terme correspondant puisqu'alors $A/\langle d_i \rangle \simeq \{0\}$. □

Remarque 5.7. Puisque A est intègre, la partie de torsion $M_{\text{tors}} \subseteq M$ est un sous-A-module (cf. Exemple 1.17). On a en fait $M_{\text{tors}} \simeq \oplus_{i=1}^{s} A/\langle d_i \rangle$ et $M/M_{\text{tors}} \simeq A^r$, autrement dit M/M_{tors} est libre de rang r. De plus, on a donc M sans torsion si et seulement si M est libre. Attention à ne pas oublier l'hypothèse M de type fini, comme le montre le contre-exemple de $\mathbb{Q}$ vu comme $\mathbb{Z}$-module (cf. Exemples 2.5 et 3.6).

Remarque 5.8. Si $A = k$ est un corps et M un k-espace vectoriel, on a vu qu'il n'y a pas de torsion (Exemple 1.11) donc on retrouve le fait qu'il existe un unique r tel que $M \simeq k^r$ en tant que k-espaces vectoriels. (On pouvait aussi dire que nécessairement $s = 0$ puisqu'il n'y a pas d'idéal propre non nul de k.)

6 Applications

On présente ici deux applications du Théorème 5.6 de structure.

2. On rappelle que dans un anneau commutatif unitaire intègre A, pour tous $a, b \in A$ on a $\langle a \rangle = \langle b \rangle \iff a$ et b sont associés, c'est-à-dire $a = ub$ pour $u \in A^\times$.

6.1 Théorèmes de structures pour les groupes abéliens

L'énoncé du Théorème 5.6 dans le cas $A = \mathbb{Z}$ se simplifie légèrement.

Théorème 6.1 (Théorème de structure des groupes abéliens de type fini)**.** *Soit G un groupe abélien de type fini. Il existe un unique couple $(r, s) \in \mathbb{N}^2$ d'entiers et une unique suite $d_1 \mid \cdots \mid d_s$ d'entiers ≥ 2 tels que*

$$G \simeq \mathbb{Z}^r \oplus \left(\bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \right),$$

en tant que groupes.

Corollaire 6.2 (Théorème de structure de groupes abéliens finis)**.** *Soit G un groupe abélien fini. Il existe un unique entier $s \in \mathbb{N}$ et une unique suite $d_1 \mid \cdots \mid d_s$ d'entiers ≥ 2 tels que*

$$G \simeq \bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z},$$

en tant que groupes.

Pour déterminer effectivement les d_i, on peut appliquer plusieurs fois le théorème chinois (dans les deux sens). Par exemple :

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} &\simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \\ &= \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \\ &= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \end{aligned}$$

et on s'arrête là car $2 \mid 12$.

6.2 Invariants de similitude

On retrouve la proposition qui était au centre du complément sur les invariants de similitude.

Proposition 6.3. *Soit k un corps, soit E un k-espace vectoriel de dimension finie et soit $u \in \mathrm{L}(E)$. On rappelle que E_u désigne le $k[X]$-module obtenu via l'action de u sur E (cf. Exemple 1.8). Il existe une unique famille de polynômes unitaires non constants $P_1 \mid \cdots \mid P_s$ de $k[X]$ tels que*

$$E_u \simeq \bigoplus_{i=1}^{s} k[X]/\langle P_i \rangle,$$

en tant que $k[X]$-modules.

Démonstration. Puisque E est finiment engendré sur k, il l'est également sur $k[X]$. Par le Théorème 5.6 de structure, on sait qu'il existe un unique couple $(r, s) \in \mathbb{N}^2$ et une unique suite $\langle P_1 \rangle \supseteq \cdots \supseteq \langle P_s \rangle$ d'idéaux propres non nuls tels que

$$E_u \simeq k[X]^r \oplus \left(\bigoplus_{i=1}^{s} k[X]/\langle P_i \rangle \right),$$

en tant que $k[X]$-modules. L'isomorphisme se restreignant en un isomorphisme de k-espaces vectoriels, on en déduit que $r = 0$ puisque E est de dimension finie. Les idéaux $\langle P_i \rangle$ sont propres et non nuls donc les P_i sont non constants. De plus, ils sont déterminés à un scalaire non nul près donc on peut les choisir unitaire. □