Part III

Modules

Chapter 1

Généralités sur les modules

Tous les anneaux sont supposés commutatifs, unitaires et non triviaux.

1.1 Modules, sous-modules

Définition 1.1.1 Soit A un anneau. Un *module (à gauche) sur A*, ou *A-module (à gauche)* est un groupe abélien $(M,+)$ muni en outre d'une loi de composition externe $A \times M \to M$, $(a,x) \mapsto ax$, telle que, quels que soient $a,b \in A$ et $x,y \in M$:

$$\begin{aligned}(a+b)x &= ax+bx,\\ a(x+y) &= ax+ay,\\ 1x &= x,\\ a(bx) &= (ab)x.\end{aligned}$$

Remarque 1.1.2 En développant $(1+1)(x+y)$ de deux façons, on voit que $x+y=y+x$; autrement dit, la commutativité du groupe $(M,+)$ est conséquence des autres axiomes.

Exercice 1.1.3 Vérifier que les quatre axiomes ci-dessus équivalent à la condition suivante: l'application $a \mapsto (x \mapsto ax)$ est un morphisme d'anneaux de A dans l'anneau des endomorphismes du groupe $(M,+)$.

On déduit très facilement des propriétés similaires à celles des espaces vectoriels. Cependant, l'une de ces propriétés est ici en défaut:

$$ax = 0_M \not\Longrightarrow (a = 0_A \text{ ou } x = 0_M).$$

Cherchez parmi les exemples ci-dessous lesquels ne la vérifient pas.

Exemples 1.1.4

1. Lorsque A est un corps, les A-modules sont les A-espaces vectoriels.
2. Tout groupe abélien est un $\mathbf{Z}$-module d'une unique manière: si $m \in \mathbf{N}$,on pose $mx := x + \cdots + x$ (somme de m termes), si $m \in -\mathbf{N}$, on pose $mx := -|m|x$.
3. Tout idéal de A est de façon naturelle un A-module.

4. Pour tout ensemble I, les groupes A^I (ensemble des familles d'éléments de A indexées par I) et $A^{(I)}$ (sous-ensemble de A^I formé des familles à support fini, *i.e.* des $(a_i)_{i\in I} \in A^I$ tels que presque tous les a_i sont nuls) sont des A-modules avec la définition évidente de la loi externe: $a(a_i)_{i\in I} := (aa_i)_{i\in I}$.

5. De manière générale, si l'on a une famille de A-modules M_i, le groupe produit $\prod M_i$ est un A-module avec la définition évidente de la loi externe: $a(x_i)_{i\in I} := (ax_i)_{i\in I}$. Il en est de même du sous-groupe somme-directe $\bigoplus M_i$ de $\prod M_i$ (formé des $(x_i)_{i\in I} \in \prod M_i$ tels que presque tous les x_i sont nuls).

6. Soit M un A-module et soit $f : A' \to A$ un morphisme d'anneaux. En posant $a'x := f(a')x$, on fait de M un A'-module. En particulier, si A' est un sous-anneau de A, la restriction à $A' \times M$ de la loi externe $A \times M \to M$ fait de M un A'-module (*restriction des scalaires*).

Un exemple particulièrement important. Cet exemple constitue (avec l'exemple ci-dessus des $\mathbf{Z}$-modules) une application essentielle de ce chapitre. Pour bien le comprendre, il est souhaitable de réviser le cours d'algèbre linéaire de L2 sur la réduction des endomorphismes, en particulier tout ce qui concerne les polynômes d'endomorphismes. Soient K un corps commutatif arbitraire et $A := K[X]$.

- Soit M un A-module. Par restriction des scalaires $K \subset A$, on en fait un K-espace vectoriel que nous noterons V (pour bien clarifier ce qui va suivre). L'application $\phi : x \mapsto Xx$ de V dans lui-même est un endomorphisme du K-espace vectoriel V.

- Réciproquement, soient V un espace vectoriel sur K et ϕ un endomorphisme de V. On définit une loi externe $A \times V \to V$ en posant $Px := (P(\phi))(x)$. On obtient ainsi un A-module que nous noterons M (pour le distinguer de l'espace vectoriel V). Le moins trivial à vérifier des quatre axiomes est le dernier; il découle de la règle bien connue $(P(\phi)) \circ (Q(\phi)) = PQ(\phi)$.

Remarque 1.1.5 En un certain sens, un $\mathbf{Z}$-module "est la même chose" qu'un groupe abélien et un $K[X]$-module "est la même chose" qu'un K-espace vectoriel muni d'un endomorphisme. On peut donc prévoir que la théorie des modules sur les anneaux principaux (ici $\mathbf{Z}$ et $K[X]$) aura des applications à l'étude des groupes abéliens et des endomorphismes.

Définition 1.1.6 Un *sous-module* d'un A-module M est un sous-groupe M' de $(M,+)$ qui est de plus stable pour la loi externe: $\forall a \in A$, $\forall x \in M'$, $ax \in M'$.

La loi externe de M induit donc une loi externe sur M' qui en fait un A-module. Noter qu'il suffit de vérifier que M' est non vide et stable pour l'addition et pour la loi externe. Noter aussi qu'un sous-module M' est *stable par combinaisons linéaires*, autrement dit, pour toute famille $(x_i)_{i\in I}$ d'éléments de M', toutes les *combinaisons linéaires* $\sum_{i\in I} a_i x_i$ sont des éléments de M'; comme toujours en algèbre, on suppose que presque tous les coefficients a_i (*i.e.* tous sauf un nombre fini) sont nuls: $(a_i)_{i\in I} \in A^{(I)}$.

Exemples 1.1.7

1. Si A est un corps, un sous-module est un sous-espace vectoriel (et réciproquement).

2. Si $A = \mathbf{Z}$, un sous-module est un sous-groupe (et réciproquement).

3. Les sous-modules du A-module A sont ses idéaux.

4. Si $x \in M$, le sous-ensemble $Ax := \{ax \mid a \in A\}$ est un sous-module de M. Plus généralement, si $(x_i)_{i\in I}$ est une famille d'éléments de M, l'ensemble des combinaisons linéaires $\sum_{i\in I} a_i x_i$ forme un sous-module de M, noté $\sum_{i\in I} Ax_i$.

5. $A^{(I)}$ est un sous-module de A^I.

6. $\bigoplus M_i$ est un sous-module de $\prod M_i$.

7. Si le $K[X]$-module M correspond au couple (V,ϕ) par la correspondance décrite plus haut, les sous-modules de M correspondent aux couples (V',ϕ'), où V' est un sous-espace vectoriel de V stable par ϕ et où $\phi' = \phi_{|V}$.

Soient M un A-module et $x \in M$. On pose:

$$\mathrm{Ann}_A(x) := \{a \in A \mid ax = 0\}.$$

C'est un idéal de A, appelé *annulateur* de x. On définit de même, pour tout sous-ensemble E de M:

$$\mathrm{Ann}_A(E) := \{a \in A \mid \forall x \in E\ ,\ ax = 0\} = \bigcap_{x\in E} \mathrm{Ann}_A(x).$$

C'est encore un idéal de A, appelé *annulateur* de E.

Un élément $x \in M$ est dit *de torsion* si l'idéal $\mathrm{Ann}_A(x)$ n'est pas trivial, *i.e.* s'il existe $a \neq 0$ tel que $ax = 0$. L'ensemble des éléments de torsion de M est noté $\mathrm{Tor}_A(M)$. Il est évidemment stable pour la loi externe, et il contient 0; mais il n'est pas nécessairement stable pour l'addition. Par exemple, lorsque $M = A$, les éléments de torsion sont les diviseurs de 0, et ils ne forment pas nécéssairement un idéal.

Exemple 1.1.8 On prend $A = M = \mathbf{Z}/6\mathbf{Z}$. Alors $\overline{2}$ et $\overline{3}$ sont des diviseurs de 0 dans A et donc des éléments de torsion de M, mais leur somme $\overline{5}$ n'est pas un élément de torsion de M.

Proposition 1.1.9 *Si A est intègre, $\mathrm{Tor}_A(M)$ est un sous-module de M, appelé* sous-module de torsion de M.

Preuve. - Si $ax = 0$ et $by = 0$ avec $a, b \neq 0$, on a $(ab)(x+y) = 0$ avec $ab \neq 0$. □

Dans le cas d'un espace vectoriel, le module de torsion est évidemment trivial.

Module quotient. Pour tout sous-module M' du A-module M, la relation de congruence modulo M' est une relation d'équivalence compatible avec l'addition, ce qui permet de munir l'ensemble quotient d'une loi de composition interne telle que l'addition des classes vérifie:

$$\forall x, y \in M\ ,\ \overline{x} + \overline{y} = \overline{x+y}.$$

On obtient ainsi un groupe, appelé groupe quotient et noté M/M'. En fait, des implications:

$$\forall a \in A\ ,\ \forall x, y \in M\ ,\ x \equiv y \pmod{M'} \Longleftrightarrow x - y \in M' \Longrightarrow ax - ay = a(x-y) \in M' \Longleftrightarrow ax \equiv ay \pmod{M'},$$

on déduit que la relation de congruence modulo M' est une relation d'équivalence compatible avec la loi externe, ce qui permet de munir le groupe quotient M/M' d'une loi de composition interne telle que:

$$\forall a \in A\ ,\ \forall x \in M\ ,\ a\overline{x} = \overline{ax}.$$

On vérifie immédiatement que l'on obtient ainsi un module, encore noté M/M' et appelé *module quotient de M par M'*. Dans le cas où A est un corps, resp. où $A = \mathbf{Z}$, on retrouve la notion d'espace vectoriel quotient, resp. de groupe quotient. Dans le cas où $M = A$ et où M' est un idéal I de A, on obtient une structure de A-module sur A/I (et non sa structure d'anneau quotient). Dans le cas où $A = K[X]$ et où M, M' correspondent respectivement à (V, ϕ) et à (V', ϕ'), on obtient le $K[X]$-module correspondant à (V'', ϕ''), où $V'' = V/V'$ (espace vectoriel quotient) et où ϕ'' est induit par ϕ par passage au quotient.

1.2 Morphismes

Définition 1.2.1 Soient M et N deux A-modules. On dit qu'un morphisme de groupes $f : M \to N$ est *A-linéaire*, ou que c'est un *morphisme de A-modules* si:

$$\forall a \in A\ ,\ \forall x \in M\ ,\ f(ax) = af(x).$$

On dit que f est un *isomorphisme* s'il est bijectif, que c'est un *endomorphisme* si $M = N$ et que c'est un *automorphisme* si c'est un endomorphisme bijectif. De même, f est un *monomorphisme*, resp. un *épimorphisme* s'il est injectif, resp. surjectif.

Le composé de deux morphismes est un morphisme et Id_M est un endomorphisme de M, ce qui justifie[1] la terminologie "morphisme". De même, l'application réciproque d'un morphisme bijectif est elle-même un morphisme, ce qui justifie la terminologie "isomorphisme".

Exemples 1.2.2

1. Si A est un corps, les morphismes sont les applications linéaires au sens des espaces vectoriels.
2. Si $A = \mathbf{Z}$, tous les morphismes de groupes sont des $\mathbf{Z}$-linéaires, donc des morphismes de modules.
3. L'inclusion canonique d'un sous-module $M' \to M$ est un morphisme, ainsi que la projection canonique $M \to M/M'$.
4. Les projections canoniques $\prod M_i \to M_{i_0}$ et les injections canoniques $M_{i_0} \to \bigoplus M_i$ sont des morphismes. (Ce sont des cas particuliers de l'exemple précédent: le vérifier !)

Exercice 1.2.3 Si les $K[X]$-modules M et N correspondent respectivement aux couples (V, ϕ) et (W, ψ), alors les morphismes de modules $f : M \to N$ sont les applications K-linéaires $f : V \to W$ telles que $f \circ \phi = \psi \circ f$. (Indication: cette dernière égalité signifie exactement que $f(Xx) = Xf(x)$.)

[1] Dans la présentation "catégorique" d'une théorie mathématique, il y a des objets et des morphismes et ces derniers doivent satisfaire des propriétés formelles analogues à celles que nous énonçons; dans ce cadre, un isomorphisme se définit comme un morphisme $f : M \to N$ inversible, *i.e.* tel qu'il existe $g : N \to M$ tel que $g \circ f = \mathrm{Id}_M$ et $f \circ g = \mathrm{Id}_N$.

Proposition 1.2.4 *Soit $f : M \to N$ un morphisme de A-modules.*
(i) Pour tout sous-module $M' \subset M$, l'image $f(M')$ est un sous-module de N. En particulier, $\mathrm{Im}f$ est un sous-module de N.
(ii) Pour tout sous-module $N' \subset N$, l'image réciproque $f^{-1}(N')$ est un sous-module de M. En particulier, $\mathrm{Ker}f$ est un sous-module de M.

Preuve. - C'est exactement la même que dans le cas des espaces vectoriels. □

Théorème 1.2.5 (Premier théorème d'isomorphisme) *Soit $f : M \to N$ un morphisme de A-modules. L'application induite $\overline{f} : M/\mathrm{Ker}f \to \mathrm{Im}f$ est un isomorphisme.*

Preuve. - Rappelons simplement la construction de $\overline{f}$. Si $x, y \in M$ ont même classe dans $M/\mathrm{Ker}f$, alors $x - y \in \mathrm{Ker}f \Rightarrow f(x) = f(y)$. Ainsi, $f(x)$ ne dépend que de $\overline{x} := x \pmod{\mathrm{Ker}f} \in M/\mathrm{Ker}f$, et l'on peut poser:

$$\overline{f}(\overline{x}) := f(x).$$

Pour le reste, la preuve est exactement la même que dans le cas des espaces vectoriels. □

Exemple 1.2.6 (Modules monogènes) On dit que le module M est *monogène* s'il existe $x \in M$ tel que $M = Ax$. Dans ce cas, l'application $a \mapsto ax$ est un épimorphisme de A sur M de noyau $\mathrm{Ann}_A(x)$, et donc $A/\mathrm{Ann}_A(x) \simeq M$.
Réciproquement, tout module A/I est monogène engendré par $\overline{1_A}$. Les modules monogènes sont donc, à isomorphisme près, les modules A/I.

Théorème 1.2.7 (Deuxième théorème d'isomorphisme) *Soient $M'' \subset M'$ des sous-modules du A-module M. Alors M'/M'' est un sous-module de M/M'' et le quotient est canoniquement isomorphe à M/M'.*

Preuve. - C'est la même que dans le cas des espaces vectoriels: l'application $x \pmod{M''} \mapsto x \pmod{M'}$ de M/M'' dans M/M' est bien définie, elle est linéaire surjective et son noyau est M'/M''; on peut donc appliquer le premier théorème d'isomorphisme. □

Remarque 1.2.8 Il est facile de vérifier que tous les sous-modules de M/M'' s'obtiennent de cette manière, et que l'on a donc une bijection $M' \mapsto M'/M''$ de l'ensemble des sous-modules de M qui contiennent M'' sur l'ensemble des sous-modules de M/M''.

Exercice 1.2.9 Décrire tous les sous-modules d'un module monogène.

Avant de formuler le troisième théorème d'isomorphisme, quelques constructions élémentaires. Il est clair que l'intersection $\bigcap M_i$ d'une famille de sous-modules $M_i \subset M$ est un sous-module de M. Par exemple l'intersection de tous les sous-modules de M contenant un sous-ensemble arbitraire $E \subset M$ est le plus petit sous-module contenant E, on dit que c'est le *sous-module engendré par E*.

Prenons $E := M_1 \cup M_2$, où M_1 et M_2 sont des sous-modules de M. Tout sous-module contenant E contient également toutes les sommes $x_1 + x_2$, $x_1 \in M_1$, $x_2 \in M_2$. Mais l'ensemble de ces sommes est un sous-module de M (prouvez-le !). On note donc:

$$M_1 + M_2 := \{x_1 + x_2 \mid x_1 \in M_1, x_2 \in M_2\}.$$

C'est le sous-module engendré par $M_1 \cup M_2$ et on l'appelle *somme de M_1 et M_2*.

Exercice 1.2.10 Décrire de manière analogue le sous-module $\sum M_i$ engendré par la réunion $\bigcup M_i$ d'une famille de sous-modules de M.

Théorème 1.2.11 (Troisième théorème d'isomorphisme) *Soient M_1 et M_2 des sous-modules de M. On a un isomorphisme naturel de $M_1/(M_1 \cap M_2)$ sur $(M_1 + M_2)/M_2$.*

Preuve. - Comme dans le cas des espaces vectoriels, on vérifie que le morphisme composé $M_1 \to M_1 + M_2 \to (M_1 + M_2)/M_2$ est surjectif et a pour noyau $M_1 \cap M_2$, ce qui permet d'appliquer le premier théorème d'isomorphisme. □

1.3 Familles

Pour toute famille $(x_i)_{i \in I}$ d'éléments de M, l'intersection de tous les sous-modules de M qui contiennent tous les x_i est un sous-module de M: c'est le plus petit-sous-module de M contenant tous les x_i, on dit qu'il est *engendré par les x_i*. Concrètement c'est le sous-module $\sum\limits_{i \in I} Ax_i$ de toutes les combinaisons linéaires des x_i. De manière équivalente, c'est l'image du morphisme:

$$\begin{cases} (a_i)_{i \in I} \mapsto \sum\limits_{i \in I} a_i x_i, \\ A^{(I)} \to M. \end{cases}$$

Définition 1.3.1 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *famille génératrice* (ou encore que les x_i *engendrent* M) si $M = \sum\limits_{i \in I} Ax_i$, autrement dit, si le morphisme ci-dessus est surjectif.

Les *relations* entre les x_i sont les familles de coefficients $(a_i)_{i \in I} \in A^{(I)}$ telles que $\sum\limits_{i \in I} a_i x_i = 0$, autrement dit, les éléments du noyau du morphisme ci-dessus.

Définition 1.3.2 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *famille libre* (ou encore que les x_i sont *linéairement indépendants*) si toute relation entre les x_i est triviale:

$$\forall (a_i)_{i \in I} \in A^{(I)} \ , \ \left(\sum_{i \in I} a_i x_i = 0 \right) \Longrightarrow (\forall i \in I \ , \ a_i = 0).$$

autrement dit, si le morphisme ci-dessus est injectif.

Définition 1.3.3 On dit que la famille $(x_i)_{i \in I}$ d'éléments de M est une *base* si elle est libre et génératrice:

$$\forall x \in M \ , \ \exists ! (a_i)_{i \in I} \in A^{(I)} \ : \ x = \sum_{i \in I} a_i x_i,$$

autrement dit, si le morphisme ci-dessus est bijectif.

Si $\mathcal{B} := (x_i)_{i\in I}$ est une base de M et si $x \in M$ s'écrit $x = \sum_{i\in I} a_i x_i$, on dira que les a_i sont les *coordonnées* de x dans la base $\mathcal{B}$.

Exercice 1.3.4 Montrer que les bases du A-module A sont les familles à un élément (x) telles que $x \in A^*$.

Naturellement, dans le cas où A est un corps, le vocabulaire ci-dessus est cohérent avec le vocabulaire usuel des espaces vectoriels. Cependant, il faut prendre garde que, lorsque A n'est pas un corps, de nombreuses propriétés usuelles tombent en défaut[2]. Voici les principales "anomalies".

1. Un A-module n'admet pas nécessairement une base. Soit par exemple I un idéal de A qui n'est égal ni à $\{0\}$ ni à A (par hypothèse il en existe puisque A n'est pas un corps). Alors deux éléments quelconques de I sont liés, il n'y a donc pas de famille libre ayant strictement plus d'un élément, de sorte que I ne peut être un A-module libre que si c'est un idéal principal; et même cela ne suffit pas si A n'est pas intègre (vérifiez-le). D'autre part, tout élément de A/I est de torsion, il n'y a donc aucune famille libre non vide dans A/I, donc aucune base.

2. Si le module M admet une base, un sous-module de M n'admet pas nécessairement une base: voir l'exemple ci-dessus.

3. Une famille libre maximale n'est pas nécessairement une base. Par exemple, dans le $\mathbf{Z}$-module $\mathbf{Z}$, la famille à un élément (2) est libre maximale, mais ce n'est pas une base; et elle n'est strictement contenue dans aucune famille libre.

4. Une famille génératrice minimale n'est pas nécessairement une base. Par exemple, dans le $\mathbf{Z}$-module $\mathbf{Z}$, la famille à deux éléments $(2,3)$ est génératrice, mais ce n'est pas une base; et elle ne contient strictement aucune famille génératrice.

Définition 1.3.5 On dit qu'un module est *libre* s'il admet une base.

Il existe une théorie générale des modules libres, mais, comme pour les espaces vectoriels, on s'intéressera surtout (en algèbre) au cas des modules admettant une base finie.

Calcul matriciel avec les familles

On ne manipulera ici que des familles finies (bien que le cas général puisse être traité de façon semblable) et on les écrira systématiquement sous forme de suites finies $\mathcal{X} := (x_1,\dots,x_n) \in M^n$, $\mathcal{Y} := (y_1,\dots,y_p) \in M^p$, etc.

Soit $x := a_1x_1 + \cdots + a_nx_n$ une combinaison linéaire des x_i. Notant $C := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in A^n$ le vecteur colonne des coefficients a_i, on adoptera l'écriture matricielle:

$$x = \mathcal{X}C.$$

[2]Cependant certaines d'entre elles seront rétablies dans le cas d'un anneau A principal: cela vaudra donc la peine de revenir ici après lecture complète de ce chapitre.

Noter qu'elle comporte un certain abus, puisque, en calcul matriciel usuel, on devrait avoir $\mathcal{X}C = x_1a_1 + \cdots + x_na_n$, ce qui n'a pas de sens (scalaires à droite des "vecteurs"). Il est possible de justifier cet abus mais on se contentera d'observer que les calculs qui en résultent sont cohérents.

Supposons que les y_j soient tous combinaisons linéaires des x_i:

$$y_j = \sum_{i=1}^{n} a_{i,j}x_i,\ j = 1,\ldots,p.$$

Alors on a une écriture matricielle:

$$\mathcal{Y} = \mathcal{X}P,\ \text{où}\ P := \begin{pmatrix} a_{1,1} & \ldots & a_{1,p} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \ldots & a_{n,p} \end{pmatrix} \in \mathrm{Mat}_{n,p}(A).$$

Soit maintenant $\mathcal{Z} := (z_1,\ldots,z_q) \in M^q$ une famille d'éléments qui sont combinaisons linéaires des y_j:

$$z_k = \sum_{j=1}^{p} b_{j,k}y_j,\ k = 1,\ldots,q.$$

On a donc $\mathcal{Z} = \mathcal{Y}Q$, où $Q \in \mathrm{Mat}_{p,q}(A)$ a pour coefficients les $b_{j,k}$. L'associativité du produit matriciel permet de prévoir les égalités:

$$\mathcal{Z} = \mathcal{Y}Q = (\mathcal{X}P)Q = \mathcal{X}(PQ) = \mathcal{X}R,\ \text{où}\ R := PQ \in \mathrm{Mat}_{n,q}(A).$$

Et l'on vérifie en effet sans peine les relations $z_k = \sum_{i=1}^{n} c_{i,k}y_j,\ k = 1,\ldots,q$, les coefficients $c_{i,k}$ de R étant donnés par la formule habituelle $c_{i,k} := \sum_{j=1}^{p} a_{i,j}b_{j,k},\ i = 1,\ldots,n,\ k = 1,\ldots,q$.

Exercice 1.3.6 Expliquer et prouver les relations:

$$\mathcal{X}(P+P') = \mathcal{X}P + \mathcal{X}P',\ (\mathcal{X}+\mathcal{X}')P = \mathcal{X}P + \mathcal{X}'P,\ \mathcal{X}I_n = \mathcal{X},\ \mathcal{X}P = \mathcal{Y} \Leftrightarrow \mathcal{X} = \mathcal{Y}P^{-1}.$$

On traduit simplement les notions de familles libres et génératrices dans ce langage:

- La famille $\mathcal{X}$ est libre si, chaque fois que l'on a $\mathcal{X}P = 0$ (famille triviale), on peut en déduire $P = 0$ (matrice nulle). Plus généralement, si $\mathcal{X}P = \mathcal{X}P'$, alors $P = P'$.
- La famille $\mathcal{X}$ est génératrice si toute famille $\mathcal{Y}$ peut s'écrire $\mathcal{Y} = \mathcal{X}P$ (la matrice P ayant le bon format).

À titre d'exemple (parmi beaucoup: inventez-en !) d'utilisation de ce formalisme, voici un résultat important.

Théorème 1.3.7 *Si M admet une base de n éléments $\mathcal{X} := (x_1,\ldots,x_n)$, alors toutes les bases de M ont n éléments.*

Preuve. - Soit $\mathcal{Y} = (y_1, \ldots, y_p)$ une autre base de M. Puisque ces deux familles sont génératrices, on peut écrire $\mathcal{Y} = \mathcal{X}P$ et $\mathcal{X} = \mathcal{Y}Q$ pour certaines matrices P, Q. On en déduit $\mathcal{X} = \mathcal{X}(PQ)$ et $\mathcal{Y} = \mathcal{Y}(QP)$. Mais puisque $\mathcal{X} = \mathcal{X}I_n$ et $\mathcal{Y} = \mathcal{Y}I_p$ et que ces familles sont libres, on en tire $PQ = I_n$ et $QP = I_p$. On applique alors le lemme ci-dessous. □

Lemme 1.3.8 *Soit A un anneau non trivial et soient $P \in Mat_{n,p}(A)$ et $Q \in Mat_{p,n}(A)$ telles que $PQ = I_n$, $QP = I_p$. Alors $n = p$.*

Preuve. - On choisit un idéal maximal quelconque $\mathfrak{M}$ de A (théorème de Krull) et l'on note $K := A/\mathfrak{M}$ l'anneau quotient, qui est un corps (le "corps résiduel"). En réduisant modulo $\mathfrak{M}$ les relations précédentes, on obtient des égalités entre matrices à coefficients dans K:

$$\overline{P}\,\overline{Q} = I_n \text{ et } \overline{Q}\,\overline{P} = I_p;$$

mais l'algèbre linéaire usuelle (sur un corps) nous dit alors que $n = p$. □

La démonstration ci-dessus est incomplète car elle ne prouve pas qu'il n'existe pas de base infinie. On peut le prouver de deux manières différentes, dont une compliquée (qui sera donc donnée en petits caractères). Voici un lemme, que l'on complétera avec l'exercice 1.4.7.

Lemme 1.3.9 *Soit M un A-module admettant un système générateur fini. Alors tout système générateur de M contient un système générateur fini.*

Preuve. - Soit $y_1, \ldots, y_n$ un système générateur fini de M et soit $(x_i)_{i\in I}$ un système générateur arbitraire (*i.e.* d'ensemble d'indices I non nécessairement fini). Pour chaque $j = 1, \ldots, n$, y_j est une combinaison linéaire des x_i, donc une combinaison linéaire d'un nombre fini d'entre eux, soient les x_i d'indices $i \in I_j$ où $I_j \subset I$ est un sous-ensemble fini. Soit $I' := I_1 \cup \cdots \cup I_n$, donc un sous-ensemble fini de I. D'après ce qui précède, chaque y_j est une combinaison linéaire des x_i, $i \in I_j$, donc, puisque $I_j \subset I'$, des x_i, $i \in I'$. Ces derniers engendrent donc M et forment bien un système générateur fini contenu dans le système générateur de départ $(x_i)_{i\in I}$. □

Voici maintenant la méthode plus compliquée. On la donne tout de même car la technique utilisée (formes multilinéaires alternées) est intéressante.

Proposition 1.3.10 *Si M admet une base de n éléments $\mathcal{X} := (x_1, \ldots, x_n)$, alors toute famille infinie dans M est liée.*

Preuve. - Soit A l'anneau (commutatif unitaire) concerné. On peut en fait démontrer l'énoncé suivant, qui est clairement plus fort: *toute famille de $(n+1)$ éléments de A^n est liée.* Si l'on note les $(n+1)$ éléments en question comme des vecteurs colonnes C_i, $i = 1, \ldots, n+1$, on peut déduire des formules de Cramer (c'est un exercice ...) l'identité suivante:

$$\sum_{i=1}^{n+1} (-1)^i \det(C_1, \ldots, \hat{C}_i, \ldots, C_{n+1}) C_i = 0.$$

(On rappelle la convention selon laquelle l'élément chapeauté est omis.) Si l'un au moins des déterminants $\det(C_1, \ldots, \hat{C}_i, \ldots, C_{n+1})$ est non nul, cela achève la preuve. Cependant, si tous sont nuls, la relation ci-dessus est triviale et ça devient plus compliqué (on peut le faire, par exemple en invoquant le "développement de Laplace", *cf.* Bourbaki, Algèbre, chapitre 3, §8).

Il est probablement plus simple et plus clair[3] d'utiliser les *formes multilinéaires alternées*. Celles-ci se définissent exactement comme en algèbre linéaire "classique" (*i.e.* sur un espace vectoriel): une forme p-linéaire alternée sur un A-module M est une application $f : M^p \to A$ qui est linéaire en chacun de ses arguments et telle que $f(x_1,\dots,x_p) = 0$ si $x_i = x_j$ avec $i \neq j$. On démontre comme dans le cas des espaces vectoriels sur les corps que la forme f est alors *antisymétrique*, *i.e.* pour toute permutation σ de $\{1,\dots,p\}$: $f(x_{\sigma(1)},\dots,x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1,\dots,x_p)$, où $\varepsilon(\sigma)$ désigne la signature de σ.

Reprenons les notations M et $\mathcal{X} := (x_1,\dots,x_n)$ de l'énoncé (donc $\mathcal{X}$ est une base du A-module libre M). Soit $\mathcal{Y} := (y_1,\dots,y_{n+1})$ une famille de $(n+1)$ éléments de M. Nous allons montrer que cette famille est liée.
Soit f une forme p-linéaire alternée sur M. Soient $z_1,\dots,z_p$ des éléments de M. En écrivant $z_j = \sum_{i=1}^{n} a_{i,j} x_i$, $j = 1,\dots,p$, puis en développant par multilinéarité, on voit que $f(z_1,\dots,z_p)$ est une combinaison linéaire (à coefficients dans A) des $f(x_{i_1},\dots,x_{i_p})$, où $i_1,\dots,i_p \in \{1,\dots,n\}$. Tenant compte du caractère alterné, on peut même se restreindre aux indices tels que $1 \leq i_1 < \cdots < i_p \leq n$. En particulier, si $p > n$, toute forme p-linéaire alternée sur M est identiquement nulle.
On considère maintenant le plus grand entier p tel qu'il existe une forme p-linéaire alternée f sur M et des indices $i_1,\dots,i_p$ avec $1 \leq i_1 < \cdots < i_p \leq n+1$ tels que $f(y_{i_1},\dots,y_{i_p})$ soit non nul. D'après ce que l'on vient de dire, $p \leq n$. Quitte à réindexer la famille $\mathcal{Y}$, on peut supposer que $f(y_1,\dots,y_p) \neq 0$. On va montrer que la famille $(y_1,\dots,y_p,y_{p+1})$ est liée, d'où il s'ensuivra immédiatement que $\mathcal{Y}$ est liée. (Puisque $p \leq n$, y_{p+1} désigne bien un membre de la famille $\mathcal{Y}$.)
On fixe une forme linéaire arbitraire λ sur L et l'on définit:

$$F(z_1,\dots,z_{p+1}) := \sum_{j=1}^{p+1} (-1)^j f(z_1,\dots,\hat{z_j},\dots,z_{p+1}) \lambda(z_j).$$

Il est clair que F est une forme $(p+1)$-linéaire. De plus, elle est alternée: si $z_{j_1} = z_{j_2}$ avec $j_1 \neq j_2$, tous les termes d'indices $j \notin \{j_1, j_2\}$ sont nuls et les deux termes d'indices $j = j_1$ et $j = j_2$ sont opposés. Par maximalité de p, on a donc:

$$\sum_{j=1}^{p+1} (-1)^j f(y_1,\dots,\hat{y_j},\dots,y_{p+1}) \lambda(y_j) = 0.$$

Le membre gauche est égal à $\lambda(Y)$, où l'on a posé:

$$Y := \sum_{j=1}^{p+1} (-1)^j f(y_1,\dots,\hat{y_j},\dots,y_{p+1}) y_j.$$

On a donc $\lambda(Y) = 0$. Comme cette relation a été démontrée pour toute forme linéaire λ, on peut en particulier l'appliquer aux n formes linéaires coordonnées (dans la base $\mathcal{X}$), ce qui entraîne que $Y = 0$. On a donc la relation linéaire:

$$\sum_{j=1}^{p+1} (-1)^j f(y_1,\dots,\hat{y_j},\dots,y_{p+1}) y_j = 0.$$

Le dernier terme de cette relation a pour coefficient $f(y_1,\dots,y_p)$, qui est non nul par hypothèse. C'est donc une relation linéaire non triviale entre $y_1,\dots,y_p,y_{p+1}$, autrement dit, la famille $(y_1,\dots,y_p,y_{p+1})$ est bien liée. □

Définition 1.3.11 Un module admettant une base de n éléments est dit *libre de rang n*. Son *rang* (qui est bien défini d'après le théorème précédent) est n.

[3]Une autre approche encore plus claire est l'*algèbre extérieure*, *cf.* Bourbaki, Algèbre, chapitre 3, §7.

Corollaire 1.3.12 *Soit M un module libre de rang n et soit $\mathcal{X}$ une base de M. Alors l'application $P \mapsto \mathcal{X}P$ est une bijection du groupe $GL_n(A)$ des matrices inversibles à coefficients dans A sur l'ensemble des bases de M.*

□

Rappelons que les éléments de $\mathrm{GL}_n(A)$ sont les matrices $P \in \mathrm{Mat}_n(A)$ telles que $\det P \in A^*$. En effet:

- Si $PQ = I_n$, alors $(\det P)(\det Q) = 1$, d'où $\det P \in A^*$.
- Si $\det P \in A^*$, notant $\tilde{A}$ la transposée de la matrice des cofacteurs de A, on a, d'après les formules de Cramer, $A\tilde{A} = \tilde{A}A = (\det A)I_n$ et $(\det A)^{-1}\tilde{A}$ est inverse de A.

Exercice 1.3.13 Soient M un A-module libre de rang n et $\mathcal{X}$ une base de M. Donner une condition sur $P \in \mathrm{Mat}_{n,p}(A)$ pour que la famille $\mathcal{X}P$ soit libre, resp. génératrice, resp. une base.

Écriture matricielle des morphismes. Soient $\mathcal{B} := (e_1, \ldots, e_n)$ une base du module M (qui est donc libre de rang n) et $\mathcal{C} := (f_1, \ldots, f_p)$ une base du module N (qui est donc libre de rang p). On en déduit des isomorphismes $A^n \to M$ et $A^p \to N$, respectivement définis (dans l'écriture classique en vecteurs colonnes) par $X \mapsto \mathcal{B}X$ et $\mathcal{Y} \mapsto \mathcal{C}Y$. Si $x = \mathcal{B}X \in M$, resp. $y = \mathcal{C}Y \in N$, les composantes $(x_1, \ldots, x_n)$ de X, resp. les composantes $(y_1, \ldots, y_p)$ de Y, sont les coordonnées de x dans la base $\mathcal{B}$, resp. les coordonnées de y dans la base $\mathcal{C}$.
Soit $f : M \to N$ un morphisme. Il existe une unique matrice $P \in \mathrm{Mat}_{p,n}(A)$ telle que $f(\mathcal{B}) = \mathcal{C}P$. c'est *la matrice de l'application linéaire f relative aux bases $\mathcal{B}$ et $\mathcal{C}$*. On a:

$$f(x) = y \Longleftrightarrow f(\mathcal{B}X) = \mathcal{C}Y \Longleftrightarrow f(\mathcal{B})X = \mathcal{C}Y \Longleftrightarrow \mathcal{C}PX = \mathcal{C}Y \Longleftrightarrow Y = PX.$$

La matrice $P = (a_{j,i})_{\substack{1 \le j \le p \\ 1 \le i \le n}}$ relie donc les coordonnées de x et de $y = f(x)$ par les formules:

$$y_j = \sum_{i=1}^{n} a_{j,i} x_i, \ j = 1, \ldots, p.$$

Le résultat suivant sera invoqué au début du chapitre 1 de la partie IV.

Proposition 1.3.14 *Soient R un anneau commutatif et $S \in Mat_{p,n}(R)$, que l'on considère comme une application linéaire $S : R^n \to R^p$.*
(i) Cette application est surjective (resp. injective) si, et seulement si, la famille des colonnes de S est génératrice (resp. libre) dans R^p.
(ii) On suppose de plus R intègre et $n = p$. L'application S est surjective (resp. injective) si, et seulement si, $\det S \in R^*$ *(resp.* $\det S \neq 0$*)*

Preuve. - (i) L'application $S : R^n \to R^p$ est définie comme $X \mapsto SX$, où $X \in R^n$ est considéré comme un vecteur colonne. Notant $C_1, \ldots, C_n$ les colonnes de S et $x_1, \ldots, x_n$ les composantes de X, on a $SX = x_1C_1 + \cdots + x_nC_n$. Par conséquent:

- $\mathrm{Ker}S = \{X \in R^n \mid x_1C_1 + \cdots + x_nC_n = 0\}$ est le module des relations entre les colonnes; sa nullité équivaut d'une part à l'injectivité de S, d'autre part à la liberté de la famille des colonnes de S.

- $\mathrm{Im}S = \{x_1C_1 + \cdots + x_nC_n \mid x_1, \ldots, x_n \in R\}$ est le module engendré par les colonnes; il est égal à S^p si, et seulement si S est surjective et aussi si, et seulement si la famille des colonnes de S est génératrice.

(ii) Puisque R est intègre, on peut introduire son corps des fractions K et l'application linéaire $\tilde{S} : K^n \to K^n$ encore définie comme $X \mapsto SX$. On vérifie alors que $\tilde{S}$ est injective si, et seulement si S l'est. En effet, on a immédiatement $\mathrm{Ker}S \subset \mathrm{Ker}\tilde{S}$, d'où l'implication directe. Réciproquement, supposons S injective et soit $X \in K^n$ tel que $SX = 0$. On peut écrire $X = \frac{1}{a}X_0$, avec $a \in R \setminus \{0\}$ et $X_0 \in R^n$. On a alors les implications: $SX = 0 \Rightarrow SX_0 = 0 \Rightarrow X_0 = 0$ puisque $S : R^n \to R^n$ est supposée injective; et l'égalité $X_0 = 0$ entraîne $X = 0$, ce qui montre que $\tilde{S}$ est injective. Or, d'après le cours d'algèbre linéaire "normale" (sur un corps), $\tilde{S}$ est injective si, et seulement si, $\det S \neq 0$.
Pour que l'application S soit surjective, il faut, et il suffit, qu'il existe $X_1, \ldots, X_n \in R^n$ tels que $SX_1, \ldots, SX_n$ soit la base canonique de R^n: en effet, la surjectivité requiert que les éléments de cette base aient des antécédents; et si réciproquement les SX_i forment cette base, a fortiori ils engendrent R^n et S est surjective. Notant T la matrice dont les colonnes sont $X_1, \ldots, X_n$, on voit que la condition ci-dessus équivaut à $ST = I_n$. Ceci entraîne $(\det S)(\det T) = 1$, d'où $\det S \in R^*$; réciproquement, si $\det S \in R^*$, on a bien $ST = I_n$ en prenant pour T la matrice $(\det S)^{-1}\, {}^t\mathrm{com}(S)$. □

1.4 Exercices sur le chapitre "Généralités"

Première série

Exercice 1.4.1 (i) Soit I un idéal de l'anneau A. Décrire tous les sous-modules M' du module $M := A/I$ et les quotients M/M' correspondants.
(ii) Soit $\mathfrak{M}$ un idéal maximal de l'anneau A. Montrer que le module $M := A/\mathfrak{M}$ est *simple*, autrement dit, il est non trivial et ses seuls sous-modules sont $\{0\}$ et lui-même. Réciproque ?

Exercice 1.4.2 Soit $f : M \to N$ un morphisme surjectif de modules et soit $g : N \to P$ une application de N dans un module P. Montrer que, si $g \circ f$ est linéaire, alors g est linéaire.

Exercice 1.4.3 Soient A un anneau intègre et M un A-module. Montrer que $M/\mathrm{Tor}_A(M)$ est sans torsion (*i.e.* que *son* sous-module de torsion est nul).

Exercice 1.4.4 1) Soient A un anneau intègre et K son corps des fractions, qui est de manière évidente un A-module. Montrer que tout sous-module de type fini de A admet un dénominateur commun, *i.e.* qu'il existe $a \in A \setminus \{0\}$ tel que ce sous-module soit inclus dans Aa^{-1}.
2) En déduire que, si K est de type fini, alors A est un corps.

Exercice 1.4.5 Soient $\mathcal{X} := (x_1, \ldots, x_n) \in M^n$ et $P \in M_n(A)$. Notons $\mathcal{Y} := (y_1, \ldots, y_n) := \mathcal{X}P$. Montrer que les sous-modules $M' := \mathcal{X}A^n$ et $M'' := \mathcal{Y}A^n$ respectivement engendrés par $\mathcal{X}$ et $\mathcal{Y}$ vérifient:

$$(\det P)M' \subset M'' \subset M'.$$

(Utiliser les formules de Cramer sous forme matricielle.)

Exercice 1.4.6 Déduire de l'exercice 1.4.5 le théorème de Cayley-Hamilton.

Exercice 1.4.7 Déduire du lemme 1.3.9 que, si un module admet une base finie, alors toutes ses bases sont finies.

Exercice 1.4.8 (i) On suppose que $M = M_1 \oplus M_2$, c'est-à-dire que $M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$. Montrer que l'application $(x_1, x_2) \mapsto x_1 + x_2$ est un isomorphisme de $M_1 \times M_2$ sur M.
(ii) Définir des endomorphismes p, q de M tels que $p^2 = p$, $q^2 = q$, $pq = qp = 0$, $p + q = \mathrm{Id}_M$, $\mathrm{Im}p = M_1$ et $\mathrm{Im}q = M_2$.
(iii) Soient p un endomorphisme idempotent de M et $q := \mathrm{Id}_M - p$. Montrer que $q^2 = q$, $pq = qp = 0$, $\mathrm{Im}p = \mathrm{Ker}q$ et $\mathrm{Im}q = \mathrm{Ker}p$. Notant M_1 et M_2 ces derniers, montrer que $M = M_1 \oplus M_2$.

Exercice 1.4.9 1) Soit A un anneau n'ayant qu'un idéal maximal $\mathfrak{M}$ (donc un anneau *local*). Démontrer que $A^* = A \setminus \mathfrak{M}$.
2) Soit M un module "de type fini", c'est-à-dire engendré par un nombre fini d'éléments. On suppose que $\mathfrak{M}M = M$. Démontrer que $M = \{0\}$. (Utiliser l'exercice 1.4.5.)
3) Soit M un module de type fini et soit N un sous-module tel que $M = \mathfrak{M}M + N$. Démontrer que $M = N$ ("Lemme de Nakayama").

Exercice 1.4.10 1) Soient A un anneau intègre, K son corps des fractions et M le module quotient K/A. Décrire le sous-module $\mathrm{Tor}_A(M)$, les idéaux $\mathrm{Ann}_A(x)$ pour $x \in M$ et l'idéal $\mathrm{Ann}_A(M)$.
2) Mêmes questions pour $M := A/I$ où A est quelconque et I un idéal de A.

Deuxième série

Exercice 1.4.11 Dans un A-module libre de rang n, peut-on majorer le nombre d'éléments d'une famille libre, resp. minorer le nombre d'éléments d'une famille génératrice ?

Exercice 1.4.12 Cet exercice sert au suivant, mais sera également invoqué dans l'appendice A.
1) Soient M' un sous-module du A-module M et $p : M \to M/M'$ l'épimorphisme canonique. Soient $N_1 \subset N_2$ deux sous-modules de M tels que $N_1 \cap M' = N_2 \cap M'$ et $p(N_1) = p(N_2)$. Démontrer que $N_1 = N_2$.
2) On prend pour A un corps K, puis $M := K^2$, $M' := K \times \{0\}$ et $N_\lambda := \{(x,y) \in K^2 \mid y = \lambda x\}$. Montrer que, pour tout $\lambda \neq 0$, on a $N_\lambda \cap M' = \{(0,0)\}$ et $p(N_\lambda) = M/M'$. So what ? (Miles)

Exercice 1.4.13 1) Soit M un A-module. On appelle *longueur de M* et l'on note $\ell(M)$ la borne supérieure des entiers n tels qu'il existe une suite strictement croissante $M_0 \subset \cdots \subset M_n$ de sous-modules. Donc $\ell(M) \in \mathbf{N} \cup \{+\infty\}$. Quels sont les modules de longueur 0, de longueur 1 ? Que vaut la longueur dans le cas où A est un corps ?
2) Que dire d'une suite strictement croissante $M_0 \subset \cdots \subset M_n$ lorsque $n = \ell(A)$?
3) Soit M' un sous-module de M. Démontrer l'égalité $\ell(M) = \ell(M') + \ell(M/M')$ (avec les règles usuelles sur $+\infty$ et l'addition). (Pour l'une des deux majorations, utiliser l'exercice précédent.)
4) Démontrer que, s'il existe une suite strictement croissante maximale $M_0 \subset \cdots \subset M_n$, alors $n = \ell(A)$. On définira le terme "maximale".

Exercice 1.4.14 Soient A un anneau et I un idéal fixé de A. Pour tout A-module M, on note IM le sous-module de M engendré par les im, $i \in I$, $m \in M$ et $\overline{M}$ le quotient M/IM.
1) Définir, pour tout morphisme $f : M \to N$, un morphisme $\overline{f} : \overline{M} \to \overline{N}$.
2) Montrer que $\overline{g \circ f} = \overline{g} \circ \overline{f}$ et que $\overline{\mathrm{Id}_M} = \mathrm{Id}_{\overline{M}}$. On dit que les opérations $M \rightsquigarrow \overline{M}$, $f \rightsquigarrow \overline{f}$ définissent un "foncteur".
3) En déduire que, si M et N sont isomorphes, alors $\overline{M}$ et $\overline{N}$ le sont, puis une nouvelle preuve de l'unicité du rang d'un module libre.
4) Montrer que, si f est surjectif, $\overline{f}$ l'est aussi. Donner un contre-exemple à la propriété analogue pour l'injectivité.

Exercice 1.4.15 Soit A un anneau intègre local d'idéal maximal $\mathfrak{M}$. Soient $K := S^{-1}A$, où $S := A \setminus \{0\}$, son corps des fractions et $k := A/\mathfrak{M}$ son *corps résiduel*. Soient enfin M un A-module de type fini, $V := S^{-1}M$, resp. $W := M/\mathfrak{M}M$ les espaces vectoriels sur K et k déduits par extension des scalaires. À l'aide du lemme de Nakayama, démontrer que $\dim_K(V) \leq \dim_k(W)$.