Chapitre 2

Modules et produit tensoriel

Version du 14 octobre 2004

2.1 Modules : définitions

Dans ce paragraphe, A désigne un anneau, pas nécessairement commutatif.

Définition 2.1.1 *Un A-module à gauche est un groupe abélien M muni d'une application $A \times M \to M$ notée $(a, m) \mapsto am$ ou $(a, m) \mapsto a \cdot m$, vérifiant, pour tout $a, b \in A$, $m, m' \in M$:*

1) (bi-additivité) $a(m + m') = am + am'$, $\quad (a + a')m = am + a'm$;

2) $a(bm) = (ab)m$;

3) $1 \cdot m = m$.

Un sous-A-module de M est un sous-groupe N tel que $AN = N$, c.-à-d., tel que $an \in N$ pour tout $a \in A$, $n \in N$.

On définit de même la notion de module à droite :

Définition 2.1.2 *Un A-module à droite est un groupe abélien M muni d'une application $M \times A \to M$ notée $(m, a) \mapsto ma$ ou $(m, a) \mapsto m \cdot a$, vérifiant, pour tout $a, b \in A$, $m, m' \in M$:*

1) (bi-additivité) $(m + m')a = ma + m'a$, $\quad m(a + a') = ma + ma'$;

2) $(mb)a = m(ba)$;

3) $m \cdot 1 = m$.

Un sous-A-module de M est un sous-groupe N tel que $NA = N$, c.-à-d., tel que $na \in N$ pour tout $a \in A$, $n \in N$.

Lemme 2.1.1 *Si A est commutatif, alors tout A-module à droite est aussi un A-module à gauche, et réciproquement.*

Démonstration. Soit M un A-module à droite ; c.-à-d., on suppose donnée une action $M \times A \to M$, $(m, a) \mapsto ma$. Pour tout $a \in A$, $m \in M$, posons

$$(*) \qquad a \cdot m = ma.$$

Montrons que ceci définit une structure de A-module à gauche sur M. Les axiomes 1) et 3) sont immédiats à vérifier. Le point crucial, qui utilise la commutativité de A, est la vérification de l'axiome 2). Soient $a, b \in A$ et $m \in M$. Alors,

$$a \cdot (b \cdot m) = a \cdot (mb) = (mb)a = m(ba) = (ba) \cdot m.$$

Or, $ba = ab$ puisque A est commutatif, et donc l'on obtient

$$a \cdot (b \cdot m) = (ab) \cdot m.$$

Ceci prouve que $(*)$ fait de M un A-module à gauche. La réciproque se démontre de façon analogue. $\square$

Exemples de modules 1) Supposons A commutatif. Alors, d'après le lemme, les notions de module à gauche ou à droite sont identiques, et l'on parlera simplement de A-modules dans ce cas.

Par exemple, si $A = \mathbb{Z}$, un $\mathbb{Z}$-module n'est autre qu'un groupe abélien. Et si A est un corps k, un k-module n'est rien d'autre qu'un k-espace vectoriel.

2) Soient k un corps et V un k-espace vectoriel. Soit A l'anneau des k-endomorphismes de V, c.-à-d.,

$$A = \mathrm{End}_k(V) = \{\text{applications } k\text{-linéaires } V \to V\};$$

c'est un anneau non-commutatif si $\dim V > 1$. Alors, V est un A-module à gauche , via l'application

$$\mathrm{End}_k(V) \times V \to V, \quad (\phi, v) \mapsto \phi(v).$$

D'autre part, soit V^* le dual de V, c.-à-d., l'espace des formes linéaires $f : V \to k$. C'est un A-module à droite, via l'application

$$V^* \times A \to V^*, (f, \phi) \mapsto f \circ \phi = {}^t\phi(f).$$

3) A est à la fois un A-module à gauche et à droite : si $x, a \in A$, l'action à gauche (resp. à droite) est définie par

$$a \cdot x = ax, \qquad \text{resp. } x \cdot a = xa.$$

Ces deux actions coïncident ssi A est commutatif ; dans ce cas, un sous-A-module de A n'est rien d'autre qu'un idéal de A.

Revenons au cas où A est arbitraire. Alors un sous-module à gauche de A est un sous-groupe I tel que $AI = A$, c.-à-d., un idéal à gauche de A. De même, un sous-module à droite de A est un idéal à droite. Un sous-groupe qui est à la fois un idéal à gauche et à droite s'appelle un idéal bilatère (*cf.* la remarque 1.3.2).

Exercices 2.1.1 1) Soient k un corps, V un k-espace vectoriel, U un sous-espace de V, et $A = \mathrm{End}_k(V)$. Montrer que :

a) $R_U = \{\phi \in A \mid \mathrm{Im}(\phi) \subseteq U\}$ est un idéal à droite de A ;

b) $L_U = \{\phi \in A \mid \ker \phi \supseteq U\}$ est un idéal à gauche de A.

2) Soit $A = M_n(k)$ et soit I un idéal bilatère $\neq 0$. Montrer que $I = A$. (Utiliser les matrices élémentaires E_{ij}.)

Définition 2.1.3 *Un morphisme de A-modules à gauche $f : M \to N$ est un morphisme de groupes abéliens tel que $f(am) = af(m)$ pour tout $a \in A, m \in M$.*

La notion d'isomorphisme est définie de la façon usuelle : $f : M \to N$ est un isomorphisme s'il existe un morphisme $g : N \to M$ tel que $gf = \mathrm{id}_M$ et $fg = \mathrm{id}_N$.

Proposition 2.1.2 *Soit $f : M \to N$ un morphisme de A-modules à gauche. Si f est bijectif, son inverse g est un morphisme. Par conséquent, f est un isomorphisme ssi f est bijectif.*

Démonstration. Il suffit de montrer la première assertion. Supposons f bijectif et soit g l'application inverse. Soient $n, n' \in N$ et $m = g(n)$, $m' = g(n')$. Alors,

$$f(am + a'm') = af(m) + a'f(m') = an + a'n'.$$

Appliquant g, on obtient

$$g(an + a'n') = am + a'm' = ag(n) + a'g(n').$$

Ceci prouve que g est un morphisme de A-modules à gauche. La proposition est démontrée. □

Bien sûr, tout ce qui précède a son analogue pour les A-modules à droite.

2.2 Modules quotients

Soient A un anneau, M un A-module à gauche, N un sous-A-module. On peut former le groupe abélien quotient M/N ; soit $\pi : M \to M/N$ la projection.

Proposition 2.2.1 1) *Il existe une unique structure de A-module à gauche sur M/N telle que la projection $\pi : M \to M/N$ soit un morphisme de A-modules.*

2) *De plus, pour tout sous-A-module L de M/N, son image inverse $\pi^{-1}(L)$ est un sous-A-module M' de M, et l'application $L \mapsto \pi^{-1}(L)$ est une bijection de l'ensemble des sous-A-modules de M/N sur l'ensemble des sous-A-modules M' de M contenant N ; la bijection réciproque est $M' \mapsto M'/N$.*

Démonstration. On veut que $\pi(am) = a\pi(m)$, donc on doit définir $a\pi(m)$ par la formule

$$a(m+N) = am + N.$$

À nouveau, il faut vérifier que c'est bien défini. C'est bien le cas, car si $m' = m + n$, avec $n \in N$, alors $am' = am + an \in am + N$. Ceci montre que la formule ci-dessus fait sens. On vérifie alors facilement qu'elle définit bien une structure de A-module à gauche sur M/N, telle que π soit un morphisme de A-modules. Ceci prouve la 1ère assertion. La 2ème est facile et laissée au lecteur. □

Théorème 2.2.2 [Théorème fondamental d'isomorphisme (pour les A-modules)]

Soit $f : M \to N$ un morphisme de A-modules à gauche.

1) $\mathrm{Im}(f)$, *resp.* $\ker f$, *est un sous-module de N, resp. de M.*

2) *Soit M' un sous-module de M contenu dans* $\ker f$. *Alors f se factorise à travers M/M', c.-à-d., il existe un morphisme de A-modules $\bar{f} : M/M' \to N$ tel que $\bar{f} \circ \pi = f$, où π désigne la projection $M \to M/M'$.*

3) *f induit un isomorphisme de A-modules*

$$\bar{f} : M/\ker f \xrightarrow{\cong} \mathrm{Im}(f).$$

Démonstration. 1) On voit facilement que $\mathrm{Im}(f)$ et $\ker f$ sont des sous-modules. En effet, soit $a \in A$; si $n = f(m)$ et $m' = f(m')$ alors $n + an' = f(m+am')$. De même, si $m, m' \in \ker f$ alors $f(m+am') = f(m)+af(m') = 0$.

Pour 2), on remarque que f prend la même valeur sur tout élément d'une classe $m + M'$, car si $m' = m + x$ avec $x \in M'$ alors $f(m') = f(m)$. On peut donc définir $\bar{f} : M/M' \to \mathrm{Im}(f) \subseteq N$ par la formule

$$\bar{f}(m + M') = f(m).$$

Alors, par définition, l'on a $\bar{f} \circ \pi = f$. De plus, $\bar{f}$ est un morphisme de A-modules. En effet, soient $\bar{x}, \bar{y} \in \overline{M} := M/M'$ et soient $x, y \in M$ tels que $\pi(x) = \bar{x}$ et $\pi(y) = \bar{y}$. Alors, d'après la définition de la structure de groupe abélien et de A-module de $\overline{M}$, et la définition de $\bar{f}$, l'on a

$$\bar{f}(\bar{x} + a\bar{y}) = \bar{f}(\pi(x + ay)) = f(x + ay) = f(x) + af(y) = \bar{f}(\bar{x}) + a\bar{f}(\bar{y}).$$

Ceci prouve que $\bar{f}$ est un morphisme de A-modules.

3) On peut appliquer ce qui précède au cas où $M' = \ker f$; on obtient alors un morphisme surjectif

$$\bar{f} : M/\ker f \longrightarrow \mathrm{Im}(f).$$

Rappelons maintenant que si $\phi : P \to Q$ est un morphisme de A-modules, alors :

1) ϕ est un isomorphisme $\Leftrightarrow$ ϕ est bijectif $\Leftrightarrow$ ϕ est surjectif et bijectif ;

2) ϕ est injectif $\Leftrightarrow \ker \phi = (0)$.

Ici, $\bar{f} : M/\ker f \to \mathrm{Im}(f)$ est un morphisme surjectif. Reste à voir qu'il est injectif. Soit $\overline{m} = m + \ker f \in \ker \bar{f}$. Alors

$$0 = \bar{f}(\overline{m}) = f(m)$$

donc $m \in \ker f$ et $\overline{m} = 0$. Ceci prouve le théorème. $\square$

2.3 Modules de type fini

Soient A un anneau et M un A-module à gauche. Comme dans le cas des idéaux, on voit qu'une intersection arbitraire de sous-modules de M est encore un sous-module de M. Ceci fournit le premier point de la proposition suivante.

Proposition 2.3.1 *Soit S un sous-ensemble de M. L'intersection de tous les sous-modules de M contenant S est le plus petit sous-module de M contenant S. On l'appelle* **le sous-module engendré par** *S et on le note (S) ; il est égal à l'ensemble des sommes finies*

$$\sum_{s \in S} a_s s, \quad \text{où } a_s \in A \text{ et } a_s = 0 \text{ sauf pour un nombre fini d'indices.}$$

Démonstration. Analogue à celle pour les idéaux, et laissée au lecteur. □

Définition 2.3.1 *On dit que M est un A-module de type fini s'il est engendré par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \ldots, x_n \in M$ tels que tout élément $m \in M$ s'écrive*

$$m = a_1 x_1 + \cdots + a_n x_n,$$

avec $a_i \in A$.

Exemples 2.3.1 Le A-module A est de type fini : il est engendré par l'élément 1 puisque $a = a \cdot 1$ pour tout $a \in A$.

Plus généralement, pour tout $n \geq 1$, notons

$$A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\};$$

c'est un A-module à gauche, où l'addition est définie coordonnée par coordonnée, et où l'action de A est définie par

$$b \cdot (a_1, \ldots, a_n) = (ba_1, \ldots, ba_n).$$

Ce module est de type fini. En effet, introduisons les éléments

$$e_1 = (1, 0, \ldots, 0), \quad \cdots \quad , e_n = (0, \ldots, 0, 1).$$

(Si $A = k$ est un corps, alors les e_i sont simplement les vecteurs de la base canonique de k^n.) Alors, tout élément $\underline{a} = (a_1, \ldots, a_n)$ de A^n s'écrit

$$\underline{a} = a_1 e_1 + \cdots + a_n e_n.$$

Proposition 2.3.2 *Soit M un A-module à gauche de type fini, et N un sous-module de M. Alors le module quotient M/N est de type fini.*

Démonstration. Notons π la projection $M \to M/N$. Par hypothèse, M est engendré par des éléments $x_1, \ldots, x_n$ donc tout $m \in M$ est de la forme

$$m = a_1 x_1 + \cdots + a_n x_n.$$

Alors $\pi(m) = a_1 \pi(x_1) + \cdots + a_n \pi(x_n)$. Ceci montre que M/N est engendré par $\pi(x_1), \ldots, \pi(x_n)$, donc de type fini. □

Remarque 2.3.1 Attention, un sous-module d'un module de type fini n'est pas nécessairement de type fini. Cette "pathologie" ne se produit pas pour les anneaux et modules noethériens, que l'on étudiera au Chapitre 3.

Exercice 2.3.1 On suppose que $A = k$ est un corps. Soit V un k-espace vectoriel. Montrer que V est un k-module de type fini ssi $\dim_k V < \infty$.

2.4 Modules quotients associés à un idéal bilatère

Soient A un anneau et I un idéal bilatère de A. On rappelle que, d'après la proposition 1.3.3, A/I est un anneau.

Soit M un A-module à gauche.

Définition 2.4.1 *On note IM le sous-module de M engendré par les éléments xm, pour $x \in I$, $m \in M$, c.-à-d.,*

$$IM = \{x_1m_1 + \cdots + x_nm_n \mid n \geq 1, x_i \in I, m_i \in M\}.$$

On veut étudier le A-module M/IM. Pour cela, le lemme ci-dessous sera utile.

Lemme 2.4.1 *Soit V un A-module à gauche tel que $IV = 0$, c.-à-d., $av = 0$ pour tout $a \in I$, $v \in V$.*
1) L'action $A \times V \xrightarrow{\phi} V$ se factorise en une action

$$(A/I) \times V \xrightarrow{\bar{\phi}} V,$$

qui fait de V un (A/I)-module à gauche.
2) Soit W un autre A-module à gauche tel que $IW = 0$ et soit $\gamma : V \to W$ un morphisme de A-modules. Alors γ est aussi un morphisme de (A/I)-modules.

Démonstration. 1) On définit $\bar{\phi}$ par la formule

$$(*) \qquad \bar{\phi}(a + I, v) = av.$$

Ceci est bien défini, car si $a' = a + x$, avec $x \in I$, alors $a'v = av$ puisque $Iv = 0$. Ayant ainsi vu que $(*)$ est bien définie, on voit facilement que ceci fait de M/IM un (A/I)-module. À titre d'exemple, montrons que, pour tout $a, b \in A$, $v \in V$, on a

$$\pi(a)(\pi(b)v) = (\pi(a)\pi(b))v,$$

où π désigne la projection $A \to A/I$. En utilisant $(*)$ et le fait que π est un morphisme d'anneaux, on obtient :

$$\pi(a)(\pi(b)v) = \pi(a)(bv) = a(bv) = (ab)v = \pi(ab)v = (\pi(a)\pi(b))v.$$

Ceci prouve l'égalité voulue, et les autres se démontrent de façon analogue. Ceci prouve le point 1).

Comme $\pi(a)v = av$ et $\pi(a)w = aw$ pour tout $a \in A$, $v \in V$, $w \in W$, on obtient :

$$\gamma(\pi(a)v) = \gamma(av) = a\gamma(v) = \pi(a)\gamma(v).$$

Ceci prouve le point 2). $\square$

On peut maintenant démontrer le théorème suivant.

Théorème 2.4.2 1) *Soit M un A-module à gauche. Alors M/IM est un (A/I)-module à gauche.*

2) *Tout morphisme de A-modules $f : M \to N$ induit un morphisme de (A/I)-modules*

$$\bar{f} : M/IM \to N/IN.$$

De plus, si f est un isomorphisme, il en est de même de $\bar{f}$.

Démonstration. Comme M/IM est annulé par I, le point 1) résulte du lemme précédent.

2) Notons π_N la projection $N \to N/IN$; c'est un morphisme de A-modules. Alors $\pi_N \circ f : M \to N/IN$ est un morphisme de A-modules et, comme $f(IM) \subseteq IN$, l'on a $IM \subseteq \ker(\pi_N \circ f)$. Par conséquent, $\pi_N \circ f$ se factorise en un morphisme de A-modules

$$\bar{f} : M/IM \longrightarrow N/IN,$$

tel que $\bar{f}(m + IM) = f(m) + IN$, pour tout $m \in M$.

D'après le lemme précédent, $\bar{f}$ est aussi un morphisme de (A/I)-modules. Ceci prouve la 1ère assertion de 2). Supposons maintenant que f soit un isomorphisme et soit $g : N \to M$ son inverse. Comme précédemment, on obtient que g induit un morphisme de (A/I)-modules

$$\bar{g} : N/IN \longrightarrow M/IM,$$

tel que $\bar{g}(n + IN) = g(n) + IM$, pour tout $n \in N$. Alors, pour tout $m \in M$, l'on a

$$(\bar{g} \circ \bar{f})(m + IM) = \bar{g}(f(m) + IN) = (g \circ f)(m) + IM = m + IM.$$

Ceci montre que $\bar{g} \circ \bar{f} = \mathrm{id}_{M/IM}$. On montre de même que $\bar{f} \circ \bar{g} = \mathrm{id}_{N/IN}$. Ceci prouve le théorème. $\square$

Remarque 2.4.1 La démonstration ci-dessus montre que $f(IM) = IN$ et $g(IN) = IM$ (s'en convaincre !). Ceci découle aussi directement des inclusions $f(IM) \subseteq IN$ et $g(IN) \subseteq IM$.

Définition 2.4.2 *La transformation $M \mapsto M/IM$ est un exemple de* **foncteur** *de la catégorie des A-modules vers celle des (A/I)-modules. Sans entrer ici dans la définition précise de* **catégories et foncteurs**, *disons que ceci signifie les trois choses suivantes :*

1) à tout A-module M on associe le (A/I)-module M/IM, qu'on pourra noter $F(M)$;

2) à tout morphisme de A-modules $f : M \to N$ on associe le morphisme de (A/I)-modules

$$\bar{f} : M/IM \longrightarrow N/IN;$$

on peut le noter aussi $F(f) : F(M) \to F(N)$;

3) la correspondance $f \mapsto \bar{f}$ est compatible avec la composition des morphismes, au sens que $\overline{\mathrm{id}_M} = \mathrm{id}_{M/IM}$ et, si l'on a des morphismes

$$M \xrightarrow{f} N \xrightarrow{g} P$$

alors $\overline{g \circ f} = \bar{g} \circ \bar{f}$.

Exercice 2.4.1 Dans le cas du théorème, montrer que la propriété 3) cidessus est bien vérifiée.

Remarque 2.4.2 La dernière assertion du théorème, c.-à-d., le fait que $\bar{f}$ est un isomorphisme si f en est un, est une proriété générale des foncteurs. En effet, soit F un foncteur et soit $f : M \to N$ un isomorphisme, d'inverse $g : N \to M$. Alors,

$$F(g) \circ F(f) = F(g \circ f) = F(\mathrm{id}_M) = \mathrm{id}_{F(M)},$$

et de même $F(f) \circ F(g) = \mathrm{id}_{F(N)}$.

2.5 Groupes ou modules d'homomorphismes

Notation Pour commencer, introduisons la notation suivante. Si X, Y sont deux ensembles, notons

$$\mathrm{Hom}_{\mathrm{Ens}}(X, Y)$$

l'ensemble des applications $X \to Y$.

2.5.1 Applications à valeurs dans un A-module

Lemme 2.5.1 *Soient N un A-module à gauche et S un ensemble. Alors* $\mathrm{Hom}_{Ens}(S, N)$ *est muni d'une structure de A-module à gauche.*

Démonstration. L'addition et l'action de A sont définies comme suit. Pour $\phi, \phi' : S \to N$ et $a \in A$, on définit $a\phi + \phi'$ par

$$(a\phi + \phi')(s) = a\phi(s) + \phi'(s),$$

pour tout $s \in S$. On vérifie facilement que ceci fait de $\mathrm{Hom}_{\mathrm{Ens}}(S, N)$ un A-module à gauche. □

2.5.2 Morphismes de A-modules

Soient M et N deux A-modules à gauche. On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-module de M vers N.

Proposition 2.5.2 1) $\mathrm{Hom}_A(M, N)$ *est un sous-groupe de* $\mathrm{Hom}_{Ens}(S, N)$.
2) *De plus, si A est commutatif,* $\mathrm{Hom}_A(M, N)$ *est un sous-A-module de* $\mathrm{Hom}_{Ens}(S, N)$.

Démonstration. 1) Il faut montrer que si $f, g \in \mathrm{Hom}_A(M, N)$, alors $f-g \in \mathrm{Hom}_A(M, N)$. On a défini l'application $f - g : M \to N$ par la formule

$$(f - g)(m) = f(m) - g(m),$$

pour tout $m \in M$. Vérifions que $f - g$ est un morphisme de A-modules. Soient $m, m' \in M$ et $b \in A$. Alors

$$\begin{aligned}(f-g)(bm+m') = f(bm+m') - g(bm+m') &= bf(m) + f(m') - bg(m) - g(m') \\ &= b(f-g)(m) + (f-g)(m').\end{aligned}$$

Ceci prouve le point 1).

2) Supposons de plus que A soit commutatif et montrons alors que $\mathrm{Hom}_A(M, N)$ est stable par l'action de A. Pour tout $f \in \mathrm{Hom}_A(M, N)$ et $a \in A$, on a défini l'application $af : M \to N$ par :

$$(af)(m) = af(m),$$

pour tout $m \in M$. Montrons que c'est un morphisme de A-modules. Il est clair que

$$(af)(m + m') = af(m + m') = af(m) + af(m') = (af)(m) + (af)(m');$$

d'autre part, pour tout $b \in A$,

$$(af)(bm) = af(bm) = abf(m) \mathbf{=} baf(m) = b(af)(m).$$

On observera qu'on a utilisé dans la 3ème égalité ci-dessus (en gras), le fait que A est commutatif. Ainsi, af est bien un élément de $\mathrm{Hom}_A(M, N)$. Ceci prouve que $\mathrm{Hom}_A(M, N)$ est un sous-A-module de $\mathrm{Hom}_{\mathrm{Ens}}(M, N)$. La proposition est démontrée. □

2.6 Produits et sommes directes

Soit A un anneau et soit I un ensemble quelconque. On suppose donné un A-module à gauche M_i, pour tout $i \in I$.

Définition 2.6.1 *Le <u>produit</u> des M_i est le A-module, noté $\prod_{i\in I} M_i$, dont les éléments sont les familles $(m_i)_{i\in I}$ telles que $m_i \in M_i$ pour tout $i \in I$. La structure de groupe abélien et de A-module à gauche est définie composante par composante, c.-à-d.,*

$$(m_i)_{i\in I} + a(m'_i)_{i\in I} = (m_i + am'_i)_{i\in I}.$$

Définition 2.6.2 *La <u>somme directe</u> des M_i, notée $\bigoplus_{i\in I} M_i$, est le sous-A-module de $\prod_{i\in I} M_i$ formé des familles qui sont nulles presque partout, c.-à-d., les familles $(m_i)_{i\in I}$ telles que $m_i = 0$ sauf pour un nombre fini d'indices. Il est clair que ceci est bien un sous-A-module.*

Remarque 2.6.1 Si l'ensemble I est fini, on voit que

$$\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i \qquad (I \text{ fini}).$$

Si I a n éléments $i_1, \dots, i_n$ on écrira aussi

$$\bigoplus_{i\in I} M_i = M_{i_1} \oplus \cdots \oplus M_{i_n}.$$

Définition 2.6.3 *Si tous les M_i sont égaux à un même A-module M, leur produit est noté M^I et leur somme $M^{(I)}$. Noter l'usage des parenthèses, qui distingue la somme du produit pour un ensemble d'indices infini.*

Le module $M \oplus \cdots \oplus M$ (n copies) sera aussi désigné par M^n ou $M^{\oplus n}$.

Définition 2.6.4 *Pour tout i, soit*

$$\pi_i : \prod_{j \in I} M_j \longrightarrow M_i$$

la projection sur la i-ème composante et soit

$$\tau_i : M_i \longrightarrow \bigoplus_{j \in I} M_j$$

l'insertion à la i-ème place, c.-à-d., pour tout $m \in M_i$, $\tau_i(m)$ est la famille $(m_j)_{j \in J}$ telle que $m_i = m$ et $m_j = 0$ si $j \neq i$.

De plus, désignons par σ l'inclusion $\bigoplus_{j \in I} M_j \subseteq \prod_{j \in I} M_j$.

Proposition 2.6.1 *π_i et τ_i sont des morphismes de A-modules. De plus, on a*

$$\pi_j \circ \sigma \circ \tau_i = \begin{cases} \mathrm{id}_{M_i} & \text{si } j = i; \\ 0 & \text{sinon.} \end{cases}$$

En particulier, τ_i est injectif et $\pi_i \circ \sigma$ et π_i sont surjectifs.

Démonstration. C'est clair. □

Remarque 2.6.2 Posons $S = \bigoplus_{j \in I} M_j$. D'après la proposition ci-dessus, on peut identifier chaque M_i au sous-module $\tau_i(M_i)$ de S, c.-à-d., au sous-module formé des familles qui sont nulles hors de la i-ème coordonnée. Alors, tout élément de S s'écrit sous la forme

$$m_{i_1} + \cdots + m_{i_n},$$

pour certains indices $i_1, \ldots, i_n \in I$ et $m_{i_k} \in M_{i_k}$ pour $k = 1, \ldots, n$. De façon plus condensée, tout élément m de S s'écrit comme une somme finie

$$m = \sum_{i \in I} \tau_i \pi_i(m) = \sum_{i \in I} m_i;$$

les $m_i = \tau_i \pi_i(m)$ sont nuls sauf pour un nombre fini d'entre eux. Souvent, on identifiera m_i à $\pi_i(m)$ et l'on écrira

$$m = \sum_{i \in I} \pi_i(m).$$

Exercice 2.6.1 Soit I un ensemble et soit donné, pour tout $i \in I$, un A-module à gauche M_i <u>non nul</u>. On suppose que $M := \bigoplus_{i \in I} M_i$ est de type fini. Montrer alors que I est fini.

Exercice 2.6.2 Soit $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'ensemble des entiers ≥ 0. Montrer que, comme $\mathbb{C}$-espace vectoriel,

$$\mathbb{C}[X] \cong \mathbb{C}^{(\mathbb{N})},$$

tandis que

$$\mathbb{C}^{\mathbb{N}} \cong \mathbb{C}[[X]],$$

où le terme de droite désigne l'anneau des séries formelles

$$\mathbb{C}[[X]] = \left\{ \sum_{n=0}^{\infty} a_n X^n \mid a_n \in \mathbb{C} \right\}.$$

Théorème 2.6.2 (Propriété universelle de la somme directe, et du produit)
Soit N un A-module à gauche.
1) *Pour avoir un morphisme $\phi : \bigoplus_{i \in I} M_i \to N$, il suffit d'avoir un morphisme $\phi_i : M_i \to N$ pour tout i. De façon plus précise, l'application*

$$\alpha : \prod_{i \in I} \operatorname{Hom}_A(M_i, N) \longrightarrow \operatorname{Hom}_A\left(\bigoplus_{i \in I} M_i, N \right), \quad (\phi_i)_{i \in I} \mapsto \bigoplus_{i \in I} \phi_i$$

est une bijection, dont l'inverse β est donnée par $\beta(\phi) = (\phi \circ \tau_i)_{i \in I}$. De plus, si chaque ϕ_i est surjectif,
2) *Pour avoir un morphisme $\psi : N \to \prod_{i \in I} M_i$, il suffit d'avoir un morphisme $\psi_i : N \to M_i$ pour tout i. De façon plus précise, l'application*

$$\gamma : \prod_{i \in I} \operatorname{Hom}_A(N, M_i) \longrightarrow \operatorname{Hom}_A\left(N, \prod_{i \in I} M_i \right), \quad (\psi_i)_{i \in I} \mapsto \prod_{i \in I} \psi_i$$

est une bijection, dont l'inverse δ est donnée par $\delta(\psi) = (\pi_i \circ \phi)_{i \in I}$.

Démonstration. Il est clair que l'application $\beta : \phi \mapsto (\phi \circ \tau_i)_{i \in I}$ est bien définie. D'autre part, étant donné une famille $\underline{\phi} = (\phi_i)_{i \in I}$, on définit

$$\alpha(\underline{\phi}) = \bigoplus_{i \in I} \phi_i$$

par la formule suivante : pour tout $m = \sum_{i \in I} m_i$,

$$(\bigoplus_{i \in I} \phi_i)(m) = \sum_{i \in I} \phi_i(m_i) = \sum_{i \in I} \phi_i \pi_i(m).$$

Ceci fait sens, car seul un nombre fini de m_i sont $\neq 0$ et donc on peut former dans N la somme finie $\sum_{i\in I} \phi_i(m_i)$. Ayant ainsi vu que α est bien définie, on obtient pour tout ϕ et tout m :

$$(\alpha \circ \beta)(\phi)(m) = \alpha\left((\phi\tau_i)_{i\in I}\right)(m) = \sum_{i\in I} \phi\tau_i\pi_i(m) = \sum_{i\in I} \phi(m_i) = \phi(m).$$

Ceci prouve que $\alpha \circ \beta(\phi) = \phi$ pour tout ϕ.

Réciproquement, si $\underline{\phi} = (\phi_j)_{j\in J}$ alors, pour tout $i \in I$, la i-ème composante de la famille $(\beta \circ \alpha)(\underline{\phi})$ est l'application de M_i vers N qui à tout $m \in M_i$ associe :

$$(*) \qquad (\alpha(\underline{\phi}) \circ \tau_i)(m) = \sum_{j\in I} \phi_j\pi_j(\tau_i(m)) = \phi_i(m),$$

où dans la dernière égalité l'on a utilisé la proposition précédente. Alors, $(*)$ montre que $(\beta \circ \alpha)(\underline{\phi}) = \underline{\phi}$ pour toute famille $\underline{\phi} = (\phi_j)_{j\in J}$. Ceci prouve l'assertion (1).

La preuve de l'assertion (2) est analogue (en fait, plus facile), et est laissée au lecteur. □

Le théorème précédent est extrêmement utile et important. D'abord, on peut le renforcer un peu de la façon suivante. Considérons, pour tout $i \in I$, un morphisme de A-modules

$$f_i : M_i \to M'_i,$$

et définissons $\tau'_i : M'_i \to \bigoplus_{j\in I} M'_j$ comme précédemment.

Théorème 2.6.3 (Propriétés fonctorielles des sommes et produits)
1) *Les morphismes* $\tau'_i \circ f_i$ *induisent un morphisme*

$$\bigoplus_{i\in I} M_i \longrightarrow \bigoplus_{i\in I} M'_i,$$

noté $\bigoplus_{i\in I} f_i$*. De plus, ce morphisme est surjectif (resp. injectif) si chacun des* f_i *l'est.*

2) *Les morphismes* $f_i \circ \pi_i$ *induisent un morphisme*

$$\prod_{i\in I} M_i \longrightarrow \prod_{i\in I} M'_i,$$

noté $\prod_{i\in I} f_i$*. De plus, ce morphisme est injectif (resp. surjectif) si chacun des* f_i *l'est.*

Démonstration. Dans les deux cas, l'existence du morphisme résulte du théorème précédent.

Supposons que chaque f_i soit injectif, et soit $\underline{m} = (m_i)_{i\in I}$ un élément de $\ker \prod_{i\in I} f_i$. Alors

$$0 = \left(\prod_{i\in I} f_i\right)(\underline{m}) = (f_i(m_i))_{i\in I}.$$

Comme chaque f_i est supposé injectif, on obtient $m_i = 0$ pour tout i, et donc $\underline{m} = 0$. Ceci montre que $\prod_{i\in I} f_i$ est injectif, et l'on obtient de même que $\bigoplus_{i\in I} f_i$ l'est aussi.

Supposons maintenant chaque f_i surjectif. Comme $\bigoplus_{i\in I} M_i$ est engendré par ses sous-modules M_i, pour montrer que $\bigoplus_{i\in I} f_i$ est surjectif il suffit de voir que chaque M_i est contenu dans l'image de $\bigoplus_{i\in I} f_i$. Or ceci est clair puisque chaque f_i est surjectif.

Montrons que $f := \prod_{i\in I} f_i$ est surjectif. Soit $\underline{m'} = (m'_i)_{i\in I}$ un élément du produit des M'_i. Comme chaque f_i est surjectif, il existe pour chaque i un élément $m_i \in M_i$ tel que $f_i(m_i) = m'_i$. (Ici, on a utilisé l'axiome du choix.) Alors $(m_i)_{i\in I}$ est un élément du produit des M_i qui s'envoie par f sur $\underline{m'}$. Ceci prouve que f est surjective. Le théorème est démontré. $\square$

Grâce au théorème précédent on peut démontrer, par exemple, le corollaire suivant. Le premier point du corollaire est déjà contenu dans le théorème précédent, mais on le répète en raison de son importance.

Corollaire 2.6.4 *Pour tout $i \in I$, soit N_i un sous-module de M_i. Alors,*

1) *$\bigoplus_{i\in I} N_i$ est un sous-module de $\bigoplus_{i\in I} M_i$, et*

2)
$$\frac{\bigoplus_{i\in I} M_i}{\bigoplus_{i\in I} N_i} \cong \bigoplus_{i\in I} \frac{M_i}{N_i}.$$

Démonstration. 1) D'après le théorème précédent, les inclusions $N_i \subseteq M_i$ induisent un morphisme injectif

$$\eta : \bigoplus_{i\in I} N_i \hookrightarrow \bigoplus_{i\in I} M_i,$$

qui permet d'identifier $\bigoplus_{i\in I} N_i$ au sous-module :

$$\{(m_i)_{i\in I} \in \bigoplus_{i\in I} M_i \mid \forall i \in I, \quad m_i \in N_i\}.$$

2) Pour tout $i \in I$, notons π_i la projection $\pi_i : M_i \to M_i/N_i$. D'après le théorème précédent, les π_i induisent un morphisme surjectif

$$\pi : \bigoplus_{i\in I} M_i \longrightarrow \bigoplus_{i\in I} M_i/N_i.$$

Le noyau de π est formé des familles presque partout nulles $\underline{m} = (m_i)_{i\in I}$ telles que

$$0 = \pi(\underline{m}) = (\pi_i(m_i))_{i\in I}.$$

Par conséquent, $\ker \pi = \bigoplus_{i\in I} N_i$. Le corollaire découle alors du Théorème fondamental d'isomorphisme. □

2.7 A-modules libres et A-modules sans torsion

Définition 2.7.1 *Soit M un A-module à gauche. On dit que M est un A-module libre s'il est isomorphe à une somme directe $A^{(I)}$, pour un certain ensemble I.*

Remarque 2.7.1 Considérons le module $A^{(I)}$. Pour tout $i \in I$, on note e_i la famille $(a_j)_{j\in J}$ telle que $a_i = 1$ et $a_j = 0$ si $j \neq i$. Alors, d'après la définition de $A^{(I)}$ (2.6.2 et 2.6.3), tout élément $\underline{a}$ de $A^{(I)}$ s'écrit de façon unique sous la forme

$$\underline{a} = \sum_{i\in I} a_i e_i,$$

où $a_i \in A$ et $a_i = 0$ sauf pour un nombre fini d'indices.

Exemple 2.7.1 Pour tout $n \geq 1$, le module $A^n = A \oplus \cdots \oplus A$ (n copies) est un A-module libre.

Une autre formulation est la suivante.

Définition 2.7.2 *Soit X un ensemble. Le A-module libre engendré par X, noté AX, est l'ensemble des sommes formelles finies*

$$\sum_{x\in X} a_x x,$$

où $a_x \in A$ et $a_x = 0$ sauf pour un nombre fini d'indices. L'addition, et la multiplication par un élément $b \in A$, sont définies par la formule :

$$\sum_{x\in X} a_x x + b \cdot \sum_{x\in X} a'_x x = \sum_{x\in X} (a_x + b a'_x) x.$$

Bien sûr, ce module est isomorphe à $A^{(X)}$. Pour distinguer l'élément $x \in X$ de l'élément $1 \cdot x$ de AX qui lui est associé, il est commode d'introduire la notation suivante. Pour tout $x \in X$, on pose

$$e_x = 1 \cdot x \in AX.$$

Alors, AX est l'ensemble des sommes formelles finies

$$\sum_{x \in X} a_x e_x,$$

où $a_x \in A$ et $a_x = 0$ sauf pour un nombre fini d'indices.

Avant d'énoncer la proposition ci-dessous, rappelons que si X, Y sont deux ensembles,

$$\mathrm{Hom}_{\mathrm{Ens}}(X, Y)$$

désigne l'ensemble des applications $X \to Y$.

Proposition 2.7.1 [Propriété universelle du A-module AX]

Soit M un A-module à gauche arbitraire. Pour avoir un morphisme de A-modules $\phi : AX \to M$, il suffit d'avoir une application d'ensembles $\psi : X \to M$. De façon plus précise, l'application

$$\mathrm{Hom}_A(AX, M) \longrightarrow \mathrm{Hom}_{Ens}(X, M), \quad \phi \mapsto \phi|_X,$$

où $\phi|_X$ désigne l'application $x \mapsto \phi(e_x)$, est une bijection. Son inverse est l'application $\psi \mapsto \widetilde{\psi}$, où $\widetilde{\psi}$ est définie, pour tout $\underline{a} = \sum_{x \in X} a_x e_x$, par

$$(*) \qquad \widetilde{\psi}\left(\sum_{x \in X} a_x e_x\right) = \sum_{x \in X} a_x \psi(x).$$

Démonstration. Observons d'abord que la formule $(*)$ qui définit $\widetilde{\psi}$ fait sens. En effet, pour chaque $\underline{a} = \sum_{x \in X} a_x e_x$, il n'y a qu'un nombre fini de coefficients a_x qui sont $\neq 0$ et donc la somme de droite dans $(*)$ est une honnête somme finie d'éléments de M. Ceci étant vu, il est clair que

$$\widetilde{\phi|_X} = \phi, \quad \text{et} \quad \widetilde{\psi}|_X = \psi.$$

Ceci montre que les applications $\phi \mapsto \phi|_X$ et $\psi \mapsto \widetilde{\psi}$ sont inverses l'une de l'autre. La proposition est démontrée. □

Définition 2.7.3 *Soient M un A-module à gauche et B une partie de M. Il résulte de la propriété universelle du A-module libre $A^{(B)} \cong AB$, qu'il existe un unique morphisme de A-modules*

$$\phi_B : A^{(B)} \longrightarrow M, \qquad (a_b)_{b\in B} \mapsto \sum_{b\in B} a_b b.$$

1) On dit que B est une famille libre si ce morphisme est injectif. Ceci équivaut à dire que pour tout $n \geq 1$, et tout $b_1, \ldots, b_n \in B$ et $a_1, \ldots, a_n \in A$, l'égalité

$$a_1 b_1 + \cdots + a_n b_n = 0$$

n'est possible que si $a_1 = \cdots = a_n = 0$.

2) On dit que B est une base de M si c'est une famille libre et génératrice, c.-à-d., si tout élément $m \in M$ s'écrit de façon unique comme combinaison linéaire des éléments de B. Ceci équivaut à dire que le morphisme ϕ_B est bijectif.

Proposition 2.7.2 *Soit M un A-module à gauche. Alors M possède une base B ssi M est un A-module libre.*

Démonstration. Si $M \cong A^{(I)}$, alors, d'après la remarque 2.7.1, les éléments e_i $(i \in I)$ forment une base de M. Réciproquement, supposons que B soit une base de M. Alors on a vu plus haut que l'application

$$A^{(B)} \longrightarrow M, \qquad (a_b)_{b\in B} \mapsto \sum_{b\in B} a_b b,$$

est un morphisme bijectif de A-modules, donc un isomorphisme. Ceci prouve la proposition. □

Remarque 2.7.2 Toute partie libre X de A est nécessairement réduite à un seul éléments. En effet, entre deux éléments distincts $a, b \in A$ on a toujours la relation de dépendance linéaire non triviale :

$$b \cdot a - a \cdot b = 0.$$

Remarque 2.7.3 Si k est un corps et V un k-espace vectoriel, on sait que les bases de V sont aussi caractérisées comme étant les parties libres maximales, ou les parties génératrices minimales. Dans le cas d'un anneau, ces deux propriétés sont strictement plus faibles que le fait d'être une base, comme le montrent les deux exemples suivants. Prenons $A = \mathbb{Z}$.

1) La partie $\{2\}$ est libre, car si $0 = n \cdot 2 = 2n$ alors $n = 0$. (Plus généralement, dans un anneau intègre A, tout singleton $\{a\}$ avec $a \neq 0$ est une partie libre). La partie $\{2\}$ est libre maximale, d'après la remarque précédente. Pourtant $\{2\}$ n'engendre pas $\mathbb{Z}$: le sous-module engendré est $2\mathbb{Z}$, l'idéal formé des entiers pairs.

2) La partie $\{2, 3\}$ est génératrice, car l'idéal engendré contient $1 = 3 - 2$ donc est égal à $\mathbb{Z}$. Comme aucune des sous-parties $\{2\}$ ou $\{3\}$ n'engendre $\mathbb{Z}$, alors $X = \{2, 3\}$ est une partie génératrice minimale. Mais ce n'est pas une base, car elle n'est pas libre, d'après la remarque précédente. (On a $3 \cdot 2 - 2 \cdot 3 = 0$).

Définition 2.7.4 Éléments et modules de torsion ; modules sans torsion

Soit M un A-module. On dit que $m \in M$ est un <u>élément de torsion</u> s'il existe $a \in A \setminus \{0\}$ tel que $am = 0$.

On dit que M est un <u>A-module de torsion</u> si tout élément $m \in M$ est de torsion. À l'opposé, on dit que M est (un A-module) <u>sans torsion</u> si M ne possède aucun élément de torsion autre que 0.

Lemme 2.7.3 *Supposons A intègre. Alors, tout A-module libre est sans torsion.*

Démonstration. Soient M un A-module libre, B une base de M, et m un élément non nul de M. Alors m s'écrit comme une combinaison linéaire finie

$$m = \sum_{b \in B} a_b b,$$

avec les $a_b \in A$, nuls sauf pour un nombre fini d'indices, mais non tous nuls (sinon, on aurait $m = 0$). Donc, il existe $b_0 \in B$ tel que $a_{b_0} \neq 0$. Soit $\alpha \in A \setminus \{0\}$. Alors,

$$\alpha m = \sum_{b \in B} (\alpha a_b) b.$$

Le coefficient de b_0 est αa_{b_0} ; il est non nul puisque A est supposé intègre. Par conséquent, $am \neq 0$. Ceci prouve que M est sans torsion. □

Corollaire 2.7.4 *Supposons A commutatif intègre et soit I un idéal non-nul de A. Alors, le A-module A/I est de torsion. En particulier, il n'est pas libre.*

Démonstration. Pour tout $y \in A/I$ et tout $x \in I$, on a $xy = 0$. Le corollaire en découle. □

Exercice 2.7.1 Soit A commutatif intègre et soit M un A-module. On pose

$$T(M) = \{m \in M \mid m \text{ est de torsion}\}.$$

Montrer que $T(M)$ est un sous-module de M. (On l'appelle le sous-module de torsion.)

Exercice 2.7.2 1) Soit A commutatif intègre. Pour tout $P, Q \in A[X] \setminus \{0\}$, montrer que

$$\deg(PQ) = \deg(P) + \deg(Q).$$

En déduire que $A[X]$ est intègre, et que ses seuls éléments inversibles sont les éléments inversibles de A.

2) Soit k un corps et soit

$$A = (k[X])[Y] = \left\{ \sum_{i=0} P_i(X) Y^i \mid n \geq 0, \quad P_i(X) \in k[X] \right\}.$$

Montrer que A est intègre. En déduire que l'idéal (X, Y) de A est un A-module sans torsion. Montrer que ce A-module n'est pas libre. (S'il était libre alors, d'après la remarque 2.7.2, il serait engendré par un unique élément $a \in A$. En considérant les degrés en Y et X, montrer que ceci est impossible.)

2.8 A-modules libres de type fini, invariance du rang

Proposition 2.8.1 *$A^{(I)}$ est un A-module de type fini $\Leftrightarrow$ I est un ensemble fini.*

Démonstration. On a déjà vu en 2.3 l'implication $\Leftarrow$. Réciproquement, supposons que $A^{(I)}$ soit engendré par un nombre fini d'éléments $m_1, \ldots, m_n$. Alors, il existe un sous-ensemble fini J de I tel que $m_1, \ldots, m_n$ aient tous des coordonnées nulles hors de J. Alors, il en est de même pour toute combinaison linéaire de $m_1, \ldots, m_n$, et ceci entraîne que $I = J$ (s'en convaincre !). Ceci prouve que I est fini. $\square$

Supposons A commutatif et soit M un A-module libre de type fini. D'après la proposition précédente, M est isomorphe à un module M^n, pour un certain $n \geq 1$. Il n'est pas a priori clair qu'un tel n soit unique. Ceci est le contenu du théorème suivant.

Théorème 2.8.2 [Invariance du rang d'un module libre de type fini]

Soit $A \neq 0$ un anneau commutatif et soit M un A-module libre de type fini. Il existe un unique entier $n \geq 1$ tel que

$$M \cong A^n.$$

Cet entier s'appelle le rang du A-module libre M.

Démonstration. Pour la démonstration, on aura besoin du lemme suivant.

Lemme 2.8.3 *Soient $N_1, \ldots, N_r$ des A-modules, I un idéal de A et $N = N_1 \oplus \cdots \oplus N_r$. Alors*

$$IN = \bigoplus_{i=1} IN_i.$$

Démonstration. D'après le corollaire 2.6.4, $\bigoplus_{i \in I} N_i$ s'identifie à un sous-module de N, et il est clair que ce sous-module est contenu dans IN. Ceci prouve l'inclusion $\supseteq$.

Réciproquement, pour tout $n = n_1 + \cdots + n_r$ dans N, et tout $x \in I$,

$$xn = xn_1 + \cdots + xn_r$$

appartient à $IN_1 + \cdots + IN_r$. L'autre inclusion en résulte, et le lemme est démontré. □

On peut maintenant démontrer le théorème. Supposons donné un isomorphisme de A-modules

$$f : A^m \xrightarrow{\sim} A^n,$$

pour deux entiers $m, n \geq 1$. Posons $M = A^m$ et $N = A^n$.

On admet pour le moment que A possède au moins un idéal maximal. Ceci sera démontré, modulo le lemme de Zorn, dans la section suivante. Soit donc $\mathfrak{m}$ un idéal maximal de A et soit $k = A/\mathfrak{m}$; c'est un corps. D'après le théorème 2.4.2, f induit un isomorphisme de k-espaces vectoriels

$$\bar{f} : M/\mathfrak{m}M \xrightarrow{\sim} N/\mathfrak{m}N.$$

De plus, d'après le lemme précédent et le corollaire 2.6.4, l'on a $M/\mathfrak{m}M \cong k^m$ et $N/\mathfrak{m}N \cong k^n$. On obtient donc un isomorphisme d'espaces vectoriels

$$k^m \cong k^n.$$

Ces deux k-espaces vectoriels ont donc même dimension, d'où $m = n$. □

Remarque 2.8.1 Dans le théorème, l'hypothèse que A soit commutatif est essentielle. En effet, on peut donner un exemple d'un anneau non-commutatif R tel que $R \cong R^2$ comme R-module à gauche.

Remarque 2.8.2 On peut aussi démontrer le théorème précédent en étudiant l'algèbre extérieure d'un A-module libre. Ceci sera peut-être traité dans un chapitre ultérieur ; voir aussi [BM, §IV.2].

2.9 Lemme de Zorn et existence de sous-modules maximaux

2.9.1 Le lemme de Zorn

Définition 2.9.1 *Soit E un ensemble. On rappelle qu'une relation $x \leq y$ sur E est une relation d'ordre si elle est :*

1) réflexive : $\forall x \in E, \quad x \leq x$;

2) antisymétrique : $\forall x, y \in E, \quad x \leq y$ et $y \leq x \Rightarrow x = y$;

3) transitive : $\forall x, y, z \in E, \quad x \leq y$ et $y \leq z \Rightarrow x = z$.

On dira alors que E est un ensemble ordonné. Dans ce cas, tout sous-ensemble F de E est muni de l'ordre induit.

On dit qu'un ensemble ordonné C est totalement ordonné si deux éléments quelconques de C sont comparables, c.-à-d., si pour tout $x, y \in C$ on a : $x \leq y$ ou $y \leq x$.

Définition 2.9.2 *Soit E un ensemble ordonné.*

1) On dit que $x \in E$ est un élément maximal s'il n'existe pas d'élément $y \in E$ tel que $y > x$.

2) Soit S un sous-ensemble de E et soit $x \in E$. On dit que $x \in E$ est un majorant de S si l'on a $s \leq x$ pour tout $s \in S$ (on ne demande pas que x appartienne à S).

Définition 2.9.3 *On dit qu'un ensemble ordonné est inductif s'ilest non-vide et vérifie la propriété suivante : tout sous-ensemble totalement ordonné F de E, admet un majorant dans E.*

On peut maintenant énoncer le

Théorème 2.9.1 [Lemme de Zorn]

Soit E un ensemble ordonné inductif. Alors E possède au moins un élément maximal.

Démonstration. Voir [Dou, Chap.1] ou [La, Appendix 2]. Dans ces deux références, il est montré que l'axiome du choix entraîne le lemme de Zorn, qui lui-même entraîne le théorème de Zermelo. □

Remarque 2.9.1 En fait, on peut aussi montrer que le théorème de Zermelo entraîne l'axiome du choix. Par conséquent, le lemme de Zorn ci-dessus est équivalent à l'axiome du choix.

Exercices 2.9.1 [Pour les lecteurs intéressés qui consulteront les références précédentes.] 1) Montrer que le théorème de Zermelo entraîne l'axiome du choix.

2) Comprendre où est caché l'usage de l'axiome du choix dans la démonstration du lemme de Zorn donnée dans [La].

2.9.2 Sous-modules maximaux des modules de type fini

Définition 2.9.4 *Soit M un A-module à gauche. On dit qu'un sous-module N est* <u>*propre*</u> *s'il est distinct de M. On dit qu'un sous-module N est* <u>*maximal*</u> *si c'est un élément maximal de l'ensemble des sous-modules propres de M (ordonné par inclusion).*

Définition 2.9.5 *On dit qu'un ensemble ordonné $(I, \leq)$ est* <u>*filtrant*</u> *s'il vérifie la propriété suivante : pour tout $i, j \in I$, il existe $k \in I$ tel que*

$$i \leq k \quad \text{et} \quad j \leq k.$$

De même, si $(M_i)_{i\in I}$ est une famille de sous-modules d'un A-module M, on dit que la famille est <u>*filtrante*</u> *si pour tout $i, j \in I$ il existe $k \in I$ tel que M_k contienne M_i et M_j.*

En général, une réunion de sous-modules de M n'est pas un sous-module. Toutefois, on a le lemme suivant.

Lemme 2.9.2 *Soit M un A-module à gauche et $(M_i)_{i\in I}$ une famille filtrante de sous-modules de M. Alors*

$$\bigcup_{i\in I} M_i$$

est un sous-module de M.

Démonstration. Soient $a \in A$ et $m, m' \in N := \bigcup_{i \in I} M_i$. Alors, existe $i, j \in I$ tels que $m \in M_i$ et $m' \in M_j$. Mais, comme la famille est filtrante, il existe $k \in I$ tel que
$$M_i + M_j \subseteq M_k.$$
Alors $m + am'$ appartient à M_k et donc à N. Ceci prouve le lemme. $\square$

Théorème 2.9.3 *Soit M un A-module à gauche de type fini et N un sous-module distinct de M. Alors il existe un sous-module maximal de M contenant N.*

Démonstration. En remplaçant M par le module quotient M/N, qui est encore de type fini, d'après la proposition 2.3.2, il suffit de démontrer que M possède un sous-module maximal. Pour cela, d'après le Lemme de Zorn, il suffit de montrer que l'ensemble des sous-modules propres de M est inductif.

Or, soit $(M_i)_{\in I}$ une famille totalement ordonnée de sous-modules propres de M. D'après le lemme précédent,
$$N = \bigcup_{i \in I} M_i$$
est un sous-module de M. De plus, c'est un sous-module propre.

En effet, M est engendré par un nombre fini d'éléments $m_1, \ldots, m_n$. Si on avait $N = M$, il existerait un indice $i \in I$ tel que $m_1, \ldots, m_n \in M_i$ et on aurait alors $M_i = M$, contrairement à l'hypothèse que les M_i sont des sous-modules propres. Donc $N \neq M$, et ceci montre que l'ensemble des sous-modules propres de M vérifie les hypothèses du Lemme de Zorn. Par conséquent, il possède un élément maximal M_0, qui est alors un sous-module (propre) maximal de M. Le théorème est démontré. $\square$

Corollaire 2.9.4 *Soient A un anneau commutatif et I un idéal de A. Alors I est contenu dans un idéal maximal $\mathfrak{m}$.*

Démonstration. Ceci résulte du théorème précédent, puisque A est un A-module de type fini ! $\square$

2.10 Produit tensoriel

Dans ce paragraphe, A est un anneau <u>commutatif</u>. Soient M, N deux A-modules. On veut définir un A-module $M \otimes_A N$ qui soit engendré par les "produits" d'un élément de M par un élément de N, c.-à-d., par des éléments notés $m \otimes n$.

2.10.0 Remarque préliminaire

À titre de motivation et de guide, considérons le cas où $A = \mathbb{C}$ est le corps des nombres complexes et où $M = \mathbb{C}[X]$ et $N = \mathbb{C}[Y]$ sont deux anneaux de polynômes. On veut définir le produit tensoriel $\otimes$ de sorte que l'on ait

$$\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y] = \mathbb{C}[X, Y],$$

le terme de droite désignant l'anneau des polynômes en deux variables, c.-à-d., l'ensemble des sommes finies

$$\sum_{i,j=0}^{n} a_{ij} X^i Y^j,$$

où $n \geq 0$ et $a_{ij} \in \mathbb{C}$. On voit ainsi que tout polynôme en X, Y est une **somme** de termes $P(X)Q(Y)$; de plus, d'après l'écriture ci-dessus on peut se limiter au cas où P et Q sont des monômes. On prendra garde au fait qu'un polynôme en X, Y arbitraire n'est pas, en général, égal à un produit de la forme $P(X)Q(Y)$. En effet, pour tout $R \in \mathbb{C}[X, Y]$, notons

$$V(R) = \{(x, y) \in \mathbb{C}^2 \mid R(x, y) = 0\}$$

Si R est de la forme $P(X)Q(Y)$, alors $V(R)$ est un ensemble fini, car P et Q n'ont chacun qu'un nombre fini de racines. Par contre, pour $R = XY - 1$, on a

$$V(R) = \{(z, z^{-1}) \mid z \in \mathbb{C}^\times\}$$

et cet ensemble est infini. Ceci montre que $XY - 1$ ne peut s'écrire comme un produit $P(X)Q(Y)$. Ceci illustre la nécessité de considérer non seulement ces produits, mais l'ensemble de toutes les sommes de tels produits.

2.10.1 Applications bilinéaires

Soient M, N, P trois A-modules.

Définition 2.10.1 *Soit ϕ une application d'ensembles $M \times N \to P$. On dit que ϕ est A-bilinéaire si elle est A-linéaire en chacune des variables, c.-à-d., si : $\forall a, a' \in A$, $m, m' \in M$, $n, n' \in N$,*

$$\phi(am + a'm', n) = a\phi(m, n) + a'\phi(m', n); \tag{1}$$

$$\phi(m, an + a'n') = a\phi(m, n) + a'\phi(m, n'). \tag{2}$$

On note $\mathrm{Bil}_A(M \times N, P)$ *l'ensemble de ces applications.*

Proposition 2.10.1
1) $\mathrm{Bil}_A(M \times N, P)$ *est un sous-A-module de* $\mathrm{Hom}_{Ens}(M \times N, P)$.
2) *On a des isomorphismes de A-modules*

$$\mathrm{Bil}_A(M \times N, P) \cong \begin{cases} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)); \\ \mathrm{Hom}_A(N, \mathrm{Hom}_A(M, P)). \end{cases}$$

Démonstration. 1) Il faut voir que, pour tout $\phi, \psi \in \mathrm{Bil}_A(M \times N, P)$ et $a \in A$, l'application $a\phi + \psi : M \times N \to P$ est A-bilinéaire. Pour tout $b \in A$, $m, m' \in M$ et $n \in N$, l'on a :

$$\begin{aligned}(a\phi + \psi)(m + bm', n) &= a\phi(m + bm', n) + \psi(m + bm', n) \\ &= a\phi(m, n) + ab\phi(m', n) + \psi(m, n) + b\psi(m', n) \\ &= (a\phi + \psi)(m) + b(a\phi + \psi)(m', n).\end{aligned}$$

(Noter qu'on a utilisé la commutativité de A dans la dernière égalité). Ceci montre la linéarité en la 1ère variable, et celle en la 2ème variable se montre de même. Ceci prouve le point 1).

2) Il suffit de montrer le 1er isomorphisme, le 2ème étant analogue. Notons

$$\beta : \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \longrightarrow \mathrm{Bil}_A(M \times N, P), \quad \theta \mapsto \beta(\theta)$$

l'application définie par

$$\beta(\theta)(m, n) = \theta(m)(n),$$

pour tout $m \in M$, $n \in N$. On voit facilement que $\beta(\theta)$ est A-bilinéaire.

De plus, β est un morphisme de A-modules. En effet, d'après les définitions, l'on a

$$\begin{aligned}\beta(a\theta + \theta')(m, n) &= (a\theta + \theta')(m)(n) = (a\theta(m) + \theta'(m))(n) \\ &= a\theta(m)(n) + \theta'(m)(n) = (a\beta(\theta) + \beta(\theta'))(m, n).\end{aligned}$$

Maintenant, pour montrer que β est un isomorphisme, il suffit d'exhiber une application inverse. Pour tout $\phi \in \mathrm{Bil}_A(M \times N, P)$ et tout $m \in M$, soit $\alpha(\phi)(m)$ l'application $n \mapsto \phi(m, n)$. Cette application appartient à $\mathrm{Hom}_A(N, P)$ puisque, pour m fixé, $\phi(m, -)$ est A-linéaire en la 2ème variable. Ainsi, on a obtenu une application

$$\alpha(\phi) : M \longrightarrow \mathrm{Hom}_A(N, P).$$

Montrons que cette application est A-linéaire, c.-à-d., que

$$\alpha(\phi)(m+am') = \alpha(\phi)(m) + a\alpha(\phi)(m')$$

(égalité d'applications de N vers P). Évaluant les deux membres en un élément $n \in N$ arbitraire, ceci revient à montrer que

$$\phi(m+am', n) = \phi(m,n) + a\phi(m', n).$$

Or cette égalité est bien vérifiée, puisque ϕ est A-linéaire en la 1ère variable. Ceci montre que $\alpha(\phi)$ est A-linéaire, et donc que α définit une application

$$\alpha : \mathrm{Bil}_A(M \times N, P) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

On vérifie alors facilement que $(\alpha \circ \beta)(\theta) = \theta$ et $(\beta \circ \alpha)(\phi) = \phi$ pour tout θ et ϕ. Ceci prouve la proposition. □

2.10.2 Définition du produit tensoriel

Soient M, N deux A-modules. On veut définir un A-module, noté $M \otimes_A N$ ou simplement $M \otimes N$, qui soit formé des sommes de "produits" $m \otimes n$ d'un élément de M par un élément de N. On veut de plus que ce "produit" $\otimes$ vérifie les deux propriétés suivantes.

1) bi-additivité : $\begin{cases} (m+m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n+n') = m \otimes n + m \otimes n'. \end{cases}$

2) "unicité de l'action de A" :

$$a \cdot (m \otimes n) = (am) \otimes n = m \otimes (an).$$

On forme donc le A-module libre $A(M \times N)$, qui est l'ensemble de toutes les sommes formelles finies

$$\sum_{(m,n) \in M \times N} a_{m,n} e_{m,n},$$

avec $a_{m,n} \in A$ et $a_{m,n} = 0$ sauf pour un nombre fini d'indices. Soit K le sous-A-module engendré par les éléments de l'un des types suivants :

$$\begin{array}{ll} (1) & e_{am+m',n} - ae_{m,n} - e_{m',n}, \\ (2) & e_{m,an+n'} - ae_{m,n} - e_{m,n'}, \end{array}$$

pour $a \in A$, $m, m' \in M$, $n, n' \in N$.

Définition 2.10.2 *On pose* $M \otimes_A N = A(M \times N)/K$ *et l'on note* $m \otimes n$ *l'image de* $e_{m,n}$ *dans* $M \otimes N$.

Remarque 2.10.1 Il résulte des relations (1) et (2) que le produit $m \otimes n$ vérifie la condition 1) (bi-additivité) et la condition 2) :

$$a \cdot (m \otimes n) = (am) \otimes n = m \otimes (an).$$

Théorème 2.10.2 [Propriété universelle de $M \otimes_A N$]
Pour tout A*-module* P*, on a une bijection*

$$\operatorname{Hom}_A(M \otimes_A N, P) \xrightarrow{\cong} \operatorname{Bil}_A(M \times N, P), \quad \phi \mapsto B(\phi),$$

où $B(\phi)$ *est l'application* $(m, n) \mapsto \phi(m \otimes n)$*. Son inverse est l'application* $\psi \mapsto T(\psi)$*, où* $T(\psi)$ *est l'unique* A*-morphisme*

$$T(\psi) : M \otimes_A N \longrightarrow P$$

tel que $T(\psi)(m \otimes n) = \psi(m, n)$ *pour tout* $m \in M$*,* $n \in N$*.*

En particulier, pour définir une application A*-linéaire* $M \otimes_A N \to P$*, il suffit d'avoir une application* A*-bilinéaire* $M \times N \to P$*.*

Démonstration. Montrons d'abord que l'application $\psi \mapsto T(\psi)$ est bien définie. Notons π la projection $A(M \times N) \to M \otimes_A N$.

Soit $\psi \in \operatorname{Bil}_A(M \times N, P)$. D'après la proposition 2.7.1, il existe un unique morphisme de A-modules

$$\widetilde{\psi} : A(M \times N) \longrightarrow P$$

tel que $\widetilde{\psi}(e_{m,n}) = \psi(m, n)$, pour tout $m \in M$, $n \in N$. Il faut voir que $\widetilde{\psi}$ passe au quotient, c.-à-d., s'annule sur le sous-module K. Comme celui-ci est engendré par les générateurs de type (1) ou (2), il suffit de voir que $\widetilde{\psi}$ s'annule sur ces générateurs. Pour ceux de type (1), l'on a :

$$\widetilde{\psi}(e_{am+m',n} - ae_{m,n} - e_{m',n}) = \phi(m + m', n) - a\psi(m, n) - \psi(m', n) = 0,$$

puisque ψ est A-linéaire en la 1ère variable. De même, la linéarité en la 2ème variable entraîne que $\widetilde{\psi}$ s'annule sur les générateurs de type (2). Par conséquent, il existe un unique morphisme de A-modules

$$T(\psi) : M \otimes_A N \longrightarrow P$$

tel que $T(\psi) \circ \pi = \widetilde{\psi}$. On a alors

$$T(\psi)(m \otimes n) = \widetilde{\psi}(e_{m,n}) = \psi(m, n),$$

pour tout $(m, n) \in M \times N$.

Alors, pour tout $\phi \in \mathrm{Hom}_A(M \otimes_A N, P)$, tout $\psi \in \mathrm{Bil}_A(M \times N, P)$ et tout $m \in M$, $n \in N$, l'on a

$$\begin{aligned} TB(\phi)(m \otimes n) &= B(\phi)(m, n) = \phi(m \otimes n) \\ \text{et} \quad BT(\psi)(m, n) &= T(\psi)(m \otimes n) = \psi(m, n). \end{aligned}$$

Ceci montre que $TB(\phi) = \phi$ et $BT(\psi) = \psi$, pour tout ϕ et ψ. Le théorème est démontré. □

On déduit du théorème, combiné avec la proposition 2.10.1, le corollaire suivant.

Corollaire 2.10.3 *Pour tout A-module P, on a une bijection*

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

2.10.3 Propriétés du produit tensoriel

Proposition 2.10.4 [Commutativité et associativité du produit tensoriel]

Soient M, N, P des A-modules. On a des isomorphismes de A-modules

$$M \otimes N \cong N \otimes M; \tag{1}$$
$$(M \otimes N) \otimes P \cong M \otimes (N \otimes P). \tag{2}$$

Démonstration. 1) L'application $M \times N \longrightarrow N \otimes M$, $(m, n) \mapsto n \otimes m$ est A-bilinéaire donc induit un A-morphisme

$$\sigma : M \otimes N \longrightarrow N \otimes M,$$

tel que $\sigma(m \otimes n) = n \otimes m$ pour tout m, n. On obtient de même un A-morphisme $\tau : N \otimes M \to M \otimes N$ tel que $\tau(n \otimes m) = m \otimes n$ pour tout m, n. Alors, il est clair que

$$\tau \circ \sigma = \mathrm{id}_{M \otimes N} \quad \text{et} \quad \sigma \circ \tau = \mathrm{id}_{N \otimes M}.$$

Ceci prouve le point 1).

2) Pour $p \in P$ fixé, l'application $(m,n) \mapsto m \otimes (n \otimes p)$ est A-bilinéaire, donc induit un A-morphisme

$$\theta_p : M \otimes N \longrightarrow M \otimes (N \otimes P),$$

tel que $\theta_p(m \otimes n) = m \otimes (n \otimes p)$ pour tout m, n. Alors, l'application

$$\begin{aligned} \theta : (M \otimes N) \times P &\longrightarrow M \otimes (N \otimes P), \\ &\qquad (m \otimes n, p) \mapsto \theta_p(m \otimes n) = m \otimes (n \otimes p), \end{aligned}$$

est A-bilinéaire, donc induit un morphisme de A-modules

$$\gamma : (M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P),$$

tel que $\gamma((m \otimes n) \otimes p) = m \otimes (n \otimes p)$ pour tout m, n, p. On obtient de façon analogue un morphisme de A-modules

$$\delta : M \otimes (N \otimes P) \longrightarrow (M \otimes N) \otimes P,$$

tel que $\gamma(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$ pour tout m, n, p. Il est alors clair que γ et δ sont inverses l'un de l'autre. Ceci prouve la proposition. $\square$

Théorème 2.10.5 [$\otimes_A$ est un bifoncteur]

Le produit tensoriel est un bifoncteur, au sens suivant. Tout morphisme de A-modules

$$f : M \to M', \quad \textit{resp.} \quad g : N \to N'$$

induit un morphisme de A-modules

$$\begin{aligned} f \otimes \mathrm{id}_N : M \otimes N &\longrightarrow M' \otimes N, \\ \textit{resp.} \quad \mathrm{id}_M \otimes g : M \otimes N &\longrightarrow M \otimes N' \end{aligned}$$

tel que

$$(f \otimes \mathrm{id}_N)(m \otimes n) = f(m) \otimes n, \quad \textit{resp.} \quad (\mathrm{id}_M \otimes g)(m \otimes n) = m \otimes g(n),$$

pour tout $m \in M, n \in N$.

Ces applications $f \mapsto f \otimes \mathrm{id}_N$ et $g \mapsto \mathrm{id}_M \otimes g$ sont fonctorielles, c.-à-d., préservent les morphismes identités et la composition. De plus, on a un diagramme commutatif

$$\begin{array}{ccc} M \otimes N & \xrightarrow{f \otimes \mathrm{id}_N} & M' \otimes N \\ {\scriptstyle \mathrm{id}_{M \otimes g}} \big\downarrow & & \big\downarrow {\scriptstyle \mathrm{id}_{M' \otimes g}} \\ M \otimes N' & \xrightarrow[f \otimes \mathrm{id}_{N'}]{} & M' \otimes N'. \end{array}$$

Démonstration. L'application $M \times N \longrightarrow M' \otimes N$, $(m,n) \mapsto f(m) \otimes n$ est A-bilinéaire donc induit une application A-linéaire

$$T_N(f) = f \otimes \mathrm{id}_N : M \otimes N \longrightarrow M' \otimes N,$$

telle que $T_N(f)(m \otimes n) = f(m) \otimes n$. Au vu de cette formule, il est clair que $T_N(\mathrm{id}_M) = \mathrm{id}_{M \otimes N}$ et que $T_N(f' \circ f) = T_N(f') \circ T_N(f)$, si f' est un morphisme de A-modules $M' \to M''$. Ceci montre que la correspondance

$$T_N : M \mapsto M \otimes N$$

est un foncteur. Par conséquent, le produit tensoriel est fonctoriel en la 1ère variable. L'assertion analogue pour la 2ème variable (*i.e.*, les morphismes $g : N \to N'$) se démontre de façon analogue.

Enfin, le diagramme indiqué est commutatif car la composée $(\mathrm{id}_{M'} \otimes g)(f \otimes \mathrm{id}_N)$ envoie chaque $m \otimes n$ sur $f(m) \otimes g(n)$, et il en est de même pour $(f \otimes \mathrm{id}_{N'})(\mathrm{id}_M \otimes g)$. Ceci prouve le théorème. $\square$

Corollaire 2.10.6 [$\otimes$ commute aux sommes directes]
Soient N et M_i, $i \in I$, des A-modules. On a un isomorphisme de A-modules :

$$\left(\bigoplus_{i \in I} M_i\right) \otimes N \cong \bigoplus_{i \in I} (M_i \otimes N)$$

Démonstration. Posons $S = \bigoplus_{i \in I} M_i$ et notons τ_i l'inclusion $M_i \to S$, pour tout i.

D'après le théorème précédent, chaque τ_i induit un A-morphisme

$$\tau_i \otimes \mathrm{id}_N : M_i \otimes N \longrightarrow S \otimes N,$$

qui envoie chaque $m_i \otimes n$ sur $\tau_i(m_i) \otimes n$. D'après la propriété universelle de la somme directe, ces morphismes induisent un morphisme de A-modules

$$\psi : \bigoplus_{i \in I} M_i \otimes N \longrightarrow S \otimes N,$$

tel que $\psi(\sum_{i \in I} m_i \otimes n) = (\sum_{i \in I} \tau_i(m_i)) \otimes n$.

D'autre part, tout élément de S s'écrit de façon unique comme une somme finie $\sum_{i \in I} \tau_i(m_i)$, avec $m_i \in M_i$ et $m_i = 0$ sauf pour un nombre fini d'indices, et l'application

$$S \times N \longrightarrow \bigoplus_{i \in I} M_i \otimes N, \qquad \left(\sum_{i \in I} \tau_i(m_i), n\right) \mapsto \sum_{i \in I} m_i \otimes n,$$

est bien définie et A-bilinéaire, donc induit un morphisme de A-modules

$$\phi : S \otimes N \longrightarrow \bigoplus_{i \in I} M_i \otimes N,$$

tel que $\phi((\sum_{i\in I} \tau_i(m_i)) \otimes n) = \sum_{i\in I} m_i \otimes n$. Il est alors clair que ϕ et ψ sont inverses l'un de l'autre. Ceci prouve le corollaire. □

Remarque 2.10.2 On peut aussi démontrer le corollaire précédent sans aucun calcul, grâce à un résultat sur les foncteurs connu sous le nom de Lemme (de représentabilité) de Yoneda. On verra cela dans une section ultérieure consacrée aux catégories et foncteurs.

Proposition 2.10.7 [Produit tensoriel par A/I]

Soient M un A-module et I un idéal de A. On a des isomorphismes de A-modules :

$$A \otimes M \cong M, \qquad (A/I) \otimes M \cong M/IM.$$

Démonstration. 1) On voit facilement que l'application $\tau : M \to A \otimes M$, $m \mapsto 1 \otimes m$, est un morphisme de A-modules. D'autre part, l'application

$$A \times M \longrightarrow M, \qquad (a, m) \mapsto am$$

est A-bilinéaire, donc induit un morphisme de A-modules $\sigma : A \otimes M \to M$ tel que $\sigma(a \otimes m) = am$ pour tout a, m. Alors, il est clair que σ et τ sont inverses l'un de l'autre.

2) Notons π, resp. π_M, la projection $A \to A/I$, resp. $M \to M/IM$. On rappelle que la structure de A-module de A/I est donnée par

$$a \cdot \pi(b) = \pi(a)\pi(b) = \pi(ab),$$

pour tout $a, b \in A$. Alors, l'application

$$(A/I) \times M \longrightarrow M/IM, \qquad (a + I, m) \mapsto am + IM,$$

est bien définie et A-bilinéaire. Elle induit donc un morphisme de A-modules

$$\sigma : (A/I) \otimes M \longrightarrow M/IM,$$

tel que $\sigma(\pi(a) \otimes m) = \pi_M(am)$.

D'autre part, l'application $\tau : M \to (A/I) \otimes M$, $m \mapsto \pi(1) \otimes m$, est un morphisme de A-modules. Son noyau contient le sous-module IM ; en effet, pour tout $m \in M$ et $x \in I$, on a

$$\tau(xm) = \pi(1) \otimes xm = x\pi(1) \otimes m = p(x) \otimes m = 0.$$

Par conséquent, τ se factorise en un A-morphisme

$$\overline{\tau} : M/IM \longrightarrow (A/I) \otimes M,$$

tel que $\overline{\tau}(m + IM) = \pi(1) \otimes m$. Alors, on voit facilement que σ et $\overline{\tau}$ sont inverses l'un de l'autre. La proposition est démontrée. $\square$

Table des matières

Bibliographie

[] Voici une bibliographie provisoire (elle aussi en évolution au fil du texte).

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, tome 1/Algèbre, Cedic Fernand Nathan, 1977.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

[La] S. Lang, Algebra, Addison-Wesley, 1965.

[Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.