Maîtrise de mathématiques
Cours d'Algèbre
(2011-2012)

Luis Paris

1 Rappels d'algèbre linéaire

Dans ce chapitre $\mathbb{K}$ désignera un corps commutatif.

1.1 Ensembles, espaces vectoriels et bases

Définition. Soit E un ensemble. Une *relation* $\mathcal{R}$ sur E est un sous-ensemble $\mathcal{R} \subset E \times E$. On utilise la notation $x\mathcal{R}y$ pour désigner une paire (x, y) appartenant à E. On dit que $\mathcal{R}$ est une *relation d'équivalence* si

(a) $\mathcal{R}$ est *réflexive*, c'est-à-dire $x\mathcal{R}x$ pour tout $x \in E$;

(b) $\mathcal{R}$ est *symétrique*, c'est-à-dire, si $x\mathcal{R}y$ alors $y\mathcal{R}x$, pour tous $x, y \in E$;

(c) $\mathcal{R}$ est *transitive*, c'est-à-dire, si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$ pour tous $x, y, z \in E$.

On dit qu'une relation $\mathcal{R}$ est une *relation d'ordre* si

(a) $\mathcal{R}$ est *réflexive* ;

(b) $\mathcal{R}$ est *anti-symétrique*, c'est-à-dire, si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$;

(c) $\mathcal{R}$ est *transitive.*

Une relation d'ordre $\mathcal{R}$ est un *ordre total* si, de plus,

(d) $x\mathcal{R}y$ ou $y\mathcal{R}x$ pour tous $x, y \in E$.

Définition. Soit E un ensemble non vide muni d'une relation d'ordre (partiel) notée $\leq$. Une partie $C \subset E$ est une *chaîne* de E si la restriction de $\leq$ à C est un ordre total. Soit $A \subset E$. Un *majorant* de A est un élément $x \in E$ tel que $a \leq x$ pour tout $a \in A$. Un *minorant* de A est un élément $x \in E$ tel que $x \leq a$ pour tout $a \in A$. Un élément $a_0 \in A$ est dit *maximal* (dans A) s'il n'existe pas de $a \in A$ tel que $a_0 \leq a$ et $a \neq a_0$. De même, un élément $a_0 \in A$ est dit *minimal* (dans A) s'il n'existe pas de $a \in A$ tel que $a \leq a_0$ et $a \neq a_0$.

Définition. Soit E un ensemble muni d'une relation d'ordre $\leq$. On dit que E est *inductif* si $E \neq \emptyset$ et si toute chaîne de E admet un majorant. Par ailleurs, un *bon ordre* sur E est un ordre total $\leq$ tel que toute partie non vide de E admet un élément minimal (qui est unique).

Axiome (Lemme de Zorn). *Soit E un ensemble inductif. Alors E admet un élément maximal.*

Lemme 1.1. *Soient E un ensemble inductif et $x \in E$. Alors il existe un élément maximal $m \in E$ tel que $x \leq m$.*

Démonstration. Soit $A = \{y \in E; x \leq y\}$. Soit $C \subset A$ une chaîne non vide. Alors C est aussi une chaîne non vide de E et, comme E est inductif, C a un majorant dans E. Un tel majorant doit être clairement dans A, donc C a un majorant dans A. Ceci montre que A est inductif. Par le lemme de Zorn, A un élément maximal, m. Cet élément est aussi maximal dans E et $x \leq m$. $\square$

Définition. Soient E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E. Un sous-ensemble $\mathcal{L}$ de $\mathcal{P}(E)$ est un *caractère fini* s'il vérifie la propriété suivante : si $Y \in \mathcal{P}(E)$, alors $Y \in \mathcal{L}$ si et seulement si $X \in \mathcal{L}$ pour toute partie finie X de Y.

Lemme 1.2. *Soit E un ensemble infini. Alors l'ensemble des parties finies de E n'est pas un caractère fini.*

Démonstration. Exercice. $\square$

Définition. Soit V un espace vectoriel sur $\mathbb{K}$. On dit qu'une partie L de V est *libre* si : pour tout $n \in \mathbb{N}$, tout n-uplet $(v_1, \ldots, v_n)$ d'éléments de L, et tout n-uplet $(t_1, \ldots, t_n)$ d'éléments de $\mathbb{K}$, l'égalité $t_1v_1 + \cdots + t_nv_n = 0$ implique $t_1 = t_2 = \cdots = t_n = 0$. On dit qu'une partie G de V est *génératrice* (ou *engendre* V) si, pour tout $v \in V$, il existe $n \in \mathbb{N}$, un n-uplet $(v_1, \ldots, v_n)$ d'éléments de G et un n-uplet $(t_1, \ldots, t_n)$ d'éléments de $\mathbb{K}$, tels que $v = t_1v_1 + \cdots + t_nv_n$ (on admet que, si $n = 0$, alors $v = \overrightarrow{0}$). On dit qu'une partie B de V est une *base* si elle est libre et génératrice.

Lemme 1.3. *Soit V un espace vectoriel sur $\mathbb{K}$. Une partie B de V est une base si et seulement si, pour tout $v \in V$, il existe un unique $n \in \mathbb{N}$, un unique n-uplet $(v_1, \ldots, v_n)$ d'éléments de B et un unique n-uplet $(t_1, \ldots, t_n)$ d'éléments de $\mathbb{K} \setminus \{0\}$ tels que $v = t_1v_1 + \cdots + t_nv_n$.*

Démonstration. Exercice. $\square$

Lemme 1.4. *Soit V un espace vectoriel sur $\mathbb{K}$. Alors l'ensemble des parties libres de V est un caractère fini.*

Démonstration. Exercice. $\square$

Lemme 1.5. *Soient E un ensemble et $\mathcal{L} \subset \mathcal{P}(E)$ un caractère fini non vide. Alors $\mathcal{L}$, ordonné par l'inclusion, est un ensemble inductif.*

Démonstration. Soit $\mathcal{C} \subset \mathcal{L}$ une chaîne non vide. Posons

$$X = \bigcup_{Y \in \mathcal{C}} Y\,.$$

Montrons que $X \in \mathcal{L}$ et X est un majorant de $\mathcal{C}$. Ceci démontrera le lemme. Soit $Z = \{x_1, \ldots, x_n\}$ un sous-ensemble fini de X. Pour tout $i \in \{1, \ldots, n\}$ il existe $Y_i \in \mathcal{C}$ tel que $x_i \in Y_i$. L'ensemble $\{Y_1, \ldots, Y_n\}$ est fini et totalement ordonné, dont admet un plus grand élément, Y_{i_0} (*i.e.* $Y_i \subset Y_{i_0}$ pour tout $i \in \{1, \ldots, n\}$). On a $Z \subset Y_{i_0}$, $Y_{i_0} \in \mathcal{L}$ et $\mathcal{L}$ est un caractère fini, donc $Z \in \mathcal{L}$. On a donc $Z \in \mathcal{L}$ pour toute partie finie Z de X donc $X \in \mathcal{L}$, car $\mathcal{L}$ est un caractère fini. Finalement, l'inclusion $Y \subset X$ pour tout $Y \in \mathcal{C}$ découle de la définition de X. $\square$

Corollaire 1.6. *Soient E un ensemble et $\mathcal{L} \subset \mathcal{P}(E)$ un caractère fini non vide. Alors $\mathcal{L}$ contient un élément maximal pour l'inclusion.* $\square$

Théorème 1.7. *Soit V un espace vectoriel sur $\mathbb{K}$.*

(1) *V admet une base.*

(2) *Soit $L \subset V$ une famille libre. Alors il existe une base de V contenant L.*

(3) *Soit W un sous-espace vectoriel de V. Alors W admet un supplémentaire (i.e. il existe un sous-espace vectoriel W' de V tel que $V = W \oplus W'$).*

Démonstration. On commence par démontrer (2). On se donne une famille libre $L \subset V$. On note $\mathcal{L}$ l'ensemble des familles libres de V qui contiennent L. l'ensemble $\mathcal{L}$ est un caractère fini non vide (il contient L), donc est un ensemble inductif, donc contient un élément maximal, B. On va montrer que B est une base. Comme $B \in \mathcal{L}$, B est une famille libre. On démontre qu'elle est génératrice par l'absurde. Supposons que B n'est pas une famille génératrice. Il existe un vecteur $v \in V$ qui n'est pas combinaison linéaires d'éléments de B. On a $v \notin B$ car, autrement, $v = 1 \cdot v$ serait combinaison linéaire de 1 vecteur de B. Posons $B' = B \cup \{v\}$. Soient $n \in \mathbb{N}$, $u_1, \ldots, u_n \in B'$ et $t_1, \ldots, t_n \in \mathbb{K}$, tels que $t_1 u_1 + \cdots + t_n u_n = \overrightarrow{0}$. Si $v \notin \{u_1, \ldots, u_n\}$, alors $t_1 = \cdots = t_n = 0$ car $u_1, \ldots, u_n \in B$ et B est libre. Supposons que $v \in \{u_1, \ldots, u_n\}$ (disons $v = u_1$). Si $t_1 \neq 0$, alors

$$v = -\frac{t_2}{t_1} u_2 - \cdots - \frac{t_n}{t_1} u_n\,,$$

donc v serait combinaison linéaire d'éléments de B : contradiction. Donc $t_1 = 0$. Alors $t_2 u_2 + \cdots t_n u_n = \overrightarrow{0}$, donc $t_2 = \cdots = t_n = 0$, car $u_2, \ldots, u_n \in B$ est B est libre. On a montré que B' est libre. Il contient strictement B (et donc aussi L), donc est un élément de $\mathcal{L}$ strictement plus grand que B : contradiction. On en conclue que B est génératrice.

Pour démontrer (1) il suffit d'appliquer (2) à $L = \emptyset$.

Maintenant on démontre (3). Soit W un sous-espace vectoriel de V. Par (1), W admet une base, B_W. Cet ensemble est libre dans V, donc il existe une base B de V contenant B_W. On pose $B_{W'} = B \setminus B_W$ et on note W' le sous-espace vectoriel de V engendré par $B_{W'}$. On va montrer que $V = W \oplus W'$.

Soit $v \in V$. Comme B est génératrice, il existe $n, m \in \mathbb{N}$, $u_1, \dots, u_n \in B_W$, $u'_1, \dots, u'_m \in B_{W'}$, $t_1, \dots, t_n, t'_1, \dots, t'_m \in \mathbb{K}$ tels que

$$v = t_1 u_1 + \cdots + t_n u_n + t'_1 u'_1 + \cdots + t'_m u'_m \,.$$

Posons

$$w = t_1 u_1 + \cdots + t_n u_n \in W \text{ et } w' = t'_1 u'_1 + \cdots + t'_m u'_m \in W' \,.$$

Alors $v = w + w'$. Ceci montre que $V = W + W'$.

Soit $v \in W \cap W'$. Comme $v \in W$, il existe $n \in \mathbb{N}$, $u_1, \dots u_n \in B_W$ et $t_1, \dots, t_n \in \mathbb{K}\setminus\{0\}$ tels que $v = t_1 u_1 + \cdots t_n u_n$. De même, comme comme $v \in W'$, il existe $m \in \mathbb{N}$, $u'_1, \dots u'_m \in B_{W'}$ et $t'_1, \dots, t'_m \in \mathbb{K} \setminus \{0\}$ tels que $v = t'_1 u'_1 + \cdots t'_m u'_m$. On a

$$t_1 u_1 + \cdots + t_n u_n + (-t'_1) u'_1 + \cdots + (-t'_m) u'_m = \overrightarrow{0} \,.$$

Ceci contredit le fait que B soit libre, à moins que $n = m = 0$. Dans ce cas $v = \overrightarrow{0}$. Ceci montre que $W \cap W' = \{\overrightarrow{0}\}$. $\square$

Soit I un ensemble. On note $\tilde{V}$ l'ensemble de toutes les fonctions de I dans $\mathbb{K}$. $\tilde{V}$ est muni d'opérations interne et externe $+$ et $\cdot$ définies par

$$(f + g)(i) = f(i) + g(i)$$

pout tous $f, g \in \tilde{V}$ et $i \in I$,

$$(t \cdot f)(i) = t \cdot (f(i))$$

pour tous $f \in \tilde{V}$, $t \in \mathbb{K}$ et $i \in I$. On dit que $f \in \tilde{V}$ est à *support fini* si l'ensemble $\{i \in I; f(i) \neq 0\}$ est fini. On note V l'ensemble des applications de I dans $\mathbb{K}$ à support fini. Pour tout $i \in I$ on définit l'application $\delta_i : I \to \mathbb{K}$ par

$$\delta_i(j) = \begin{cases} 1 & \text{si } j = i \\ 0 & \text{si } j \neq i \end{cases}$$

Proposition 1.8.

(1) *$\tilde{V}$ est un espace vectoriel sur $\mathbb{K}$ et V est un sous-espace vectoriel de $\tilde{V}$.*

(2) *L'application $I \to V$, $i \mapsto \delta_i$ est injective et $\{\delta_i; i \in I\}$ est une base de V.*

Démonstration. La partie (1) est laissée en exercice.

Soient $i, j \in I$ tels que $i \neq j$. Alors

$$\delta_i(j) = 0 \neq 1 = \delta_j(j)\,,$$

donc $\delta_i \neq \delta_j$. Ceci montre que l'application $I \to V$, $i \mapsto \delta_i$ est injective.

Soient $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$ et $t_1, \ldots, t_n \in \mathbb{K}$ tels que $t_1\delta_{i_1} + \cdots + t_n\delta_{i_n} = \overrightarrow{0}$ (où $\overrightarrow{0}$ désigne l'application $I \to \mathbb{K}$, $i \mapsto 0$.) Pour $j \in \{1, \ldots, n\}$ on a

$$0 = (t_1\delta_{i_1} + \cdots + t_n\delta_{i_n})(i_j) = t_j\,.$$

Ceci montre que $\{\delta_i; i \in I\}$ est libre.

Soit $f \in V$. Soit $\{i_1, \ldots, i_n\} = \{i \in I; f(i) \neq 0\}$ le support de f. Posons $t_j = f(i_j)$ pour tout $j \in \{1, \ldots, n\}$. Alors $f = t_1\delta_{i_1} + \cdots + t_n\delta_{i_n}$. Ceci montre que $\{\delta_i; i \in I\}$ engendre V. □

1.2 Espaces quotients

Soient V un espace vectoriel sur $\mathbb{K}$ et W un sous-espace vectoriel de V. Soit $\mathcal{R}$ la relation d'équivalence sur V définie par :

$$x\mathcal{R}y \iff x - y \in W\,.$$

Lemme 1.9. *La relation $\mathcal{R}$ est compatible avec les opérations de V. C'est-à-dire :*

(a) *Si $v_1\mathcal{R}v_1'$ et $v_2\mathcal{R}v_2'$, alors $(v_1+v_2)\mathcal{R}(v_1'+v_2')$, pour tous $v_1, v_2, v_1', v_2' \in V$;*

(b) *Si $v\mathcal{R}v'$, alors $(tv)\mathcal{R}(tv')$, pour tous $v, v' \in V$ et $t \in \mathbb{K}$.*

Démonstration. Exercice. □

Pour $v \in V$, on appelle *classe de v* et on note $\bar{v} = v + W = \{v + w; w \in W\}$ la classe d'équivalence de v par $\mathcal{R}$. On note V/W l'ensemble quotient, c'est-à-dire l'ensemble des classes d'équivalence.

Proposition 1.10.

(1) *Les opérations interne $+$ et externe $\cdot$ sur V/W données par*

$$\bar{x} + \bar{y} = \overline{x+y}\,, \quad t \cdot \bar{x} = \overline{tx}\,,$$

pour $x, y \in V$ et $t \in \mathbb{K}$, sont bien définies.

(2) *L'ensemble V/W muni des deux opérations $+$ et $\cdot$ est un espace vectoriel sur $\mathbb{K}$.*

(3) *L'application $\mu : V \to V/W$, $x \mapsto \bar{x}$, est une application linéaire surjective dont le noyau est W.*

Démonstration. Exercice. $\square$

Proposition 1.11. *Soient V, V' deux espaces vectoriels, W un sous-espace de V et $f : V \to V'$ une application linéaire. Si f s'annule sur W, alors il existe une unique application linéaire $\bar{f} : V/W \to V'$ telle que $f = \bar{f} \circ \mu$, c'est-à-dire le diagramme suivant commute.*

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\mu"'] & V' \\ V/W \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Démonstration. Pour $x \in V$ on pose $\bar{f}(\bar{x}) = f(x)$.

Montrons que $\bar{f} : V/W \to V'$ est bien définie. Soient $x, y \in V$ tels que $\bar{x} = \bar{y}$. On $x - y \in W$, donc

$$f(x) - f(y) = f(x-y) = \overrightarrow{0}\,,$$

donc $f(x) = f(y)$.

Montrons que $\bar{f}$ est linéaire. Soient $x_1, x_2 \in V$ et $t_1, t_2 \in \mathbb{K}$. Alors

$$\begin{aligned} \bar{f}(t_1\bar{x}_1 + t_2\bar{x}_2) = \bar{f}(\overline{t_1x_1 + t_2x_2}) = f(t_1x_1 + t_2x_2) = t_1f(x_1) + t_2f(x_2) \\ = t_1\bar{f}(\bar{x}_1) + t_2\bar{f}(\bar{x}_2)\,. \end{aligned}$$

On a $f = \bar{f} \circ \mu$ par définition de $\bar{f}$.

Soit $\overline{f'} : V/W \to V'$ une application linéaire telle que $f = \overline{f'} \circ \mu$. Pour tout $x \in V$ on a

$$\overline{f'}(\bar{x}) = \overline{f'} \circ \mu(x) = f(x) = \bar{f}(\bar{x})\,,$$

donc $\overline{f'} = \bar{f}$. $\square$

Proposition 1.12. *Soient V un espace vectoriel et W, W' deux sous-espaces de V tels que $V = W \oplus W'$. Alors $W' \simeq V/W$. En particulier, si V est de dimension finie, alors* $\dim(V/W) = \dim V - \dim W$.

Démonstration. Soit $f : V \to W'$ l'application définie comme suit. Soit $v \in V$. On écrit $v = w + w'$ où $w \in W$ et $w' \in W'$ et on pose $f(v) = w'$. On vérifie facilement que f est bien définie, est une application linéaire, et s'annule sur W. Il en résulte que f induit une application linéaire $\bar{f} : V/W \to W'$. Réciproquement, soit $\pi : V \to V/W$ l'application quotient et $g : W' \to V/W$ la restriction de π à W'. On vérifie facilement que $g \circ \bar{f} = \mathrm{Id}_{V/W}$ et $\bar{f} \circ g = \mathrm{Id}_{W'}$, donc $\bar{f}$ et g sont des isomorphismes. $\square$

1.3 Espaces duaux

Définition. Soit V un espace vectoriel sur $\mathbb{K}$. *L'espace dual* de V, noté V^*, est l'espace $\mathcal{L}(V, \mathbb{K})$ des formes linéaires $V \to \mathbb{K}$.

Supposons que V soit de dimension finie, n. Soit $B = \{e_1, \ldots, e_n\}$ une base de V. Pour tout $i \in \{1, \ldots, n\}$ on définit $e_i^* \in V^*$ par

$$e_i^*(e_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Proposition 1.13. *Soient V un espace vectoriel de dimension finie, n, $B = \{e_1, \ldots, e_n\}$ une base de V, et $B^* = \{e_1^*, \ldots, e_n^*\}$ défini comme avant. Alors B^* est une base de V^*. En particulier* $\dim V = \dim V^*$.

Démonstration. Soient $t_1, \ldots, t_n \in \mathbb{K}$ tels que $t_1 e_1^* + \cdots + t_n e_n^* = \overrightarrow{0}$. Pour $i \in \{1, \ldots, n\}$ on a

$$0 = (t_1 e_1^* + \cdots + t_n e_n^*)(e_i) = t_i \,.$$

Ceci montre que B^* est libre.

Soit $f \in V^*$. Pour tout $i \in \{1, \ldots, n\}$ on pose $t_i = f(e_i)$. Alors $f = t_1 e_1^* + \cdots + t_n e_n^*$. Ceci montre que B^* engendre V^*. □

Remarque.

(1) Si V est de dimension finie, alors V^* est isomorphe à V car a la même dimension. Par contre, il n'existe pas d'isomorphisme naturel de V dans V^* ou de V^* dans V.

(2) L'espace V^* n'est pas isomorphe à V si V est de dimension infinie.

Proposition 1.14. *Soit V un espace vectoriel de dimension finie. Soit $\varphi : V \to V^{**}$, $x \mapsto x^{**}$, où x^{**} est définie par*

$$x^{**}(f) = f(x) \,, \quad f \in V^* \,.$$

Alors φ est un isomorphisme. En particulier, il existe un isomorphisme naturel entre V et le bi-dual V^{**}.

Démonstration. Démontrons d'abord que, si $x \in V$, alors x^{**} est bien linéaire. Soient $f_1, f_2 \in V^*$ et $t_1, t_2 \in \mathbb{K}$. Alors

$$x^{**}(t_1 f_1 + t_2 f_2) = (t_1 f_1 + t_2 f_2)(x) = t_1 f_1(x) + t_2 f_2(x) = t_1 x^{**}(f_1) + t_2 x^{**}(f_2) \,.$$

Démontrons maintenant que φ est linéaire. Soient $x_1, x_2 \in V$ et $t_1, t_2 \in \mathbb{K}$. Pour tout $f \in V^*$ on a

$$(t_1 x_1 + t_2 x_2)^{**}(f) = f(t_1 x_1 + t_2 x_2) = t_1 f(x_1) + t_2 (x_2) = t_1 x_1^{**}(f) + t_2 x_2^{**}(f) \,,$$

donc $(t_1x_1+t_2x_2)^{**}=t_1x_1^{**}+t_2x_2^{**}$.

Finalement, montrons que φ est injectif. Comme $\dim V=\dim V^{**}$, ceci implique que φ est un isomorphisme. Soit $x\in V$ tel que $x^{**}=\overrightarrow{0}$. On a $f(x)=x^{**}(f)=0$ pour tout $f\in V^*$, donc $x=\overrightarrow{0}$. $\square$

1.4 Produits et sommes directes d'espaces vectoriels

Définition. Soit $\{V_i\}_{i\in I}$ une collection (infinie) d'espaces vectoriels sur $\mathbb{K}$. Le *produit directe* des V_i est l'espace vectoriel, noté $\prod_{i\in I}V_i$, dont les éléments sont les familles $(v_i)_{i\in I}$ telles que $v_i\in V_i$ pour tout $i\in I$. La structure d'espace vectoriel sur $\prod_{i\in I}V_i$ se fait composante par composante, c'est-à-dire,

$$(v_i)_{i\in I}+(v_i')_{i\in I}=(v_i+v_i')_{i\in I}\quad\text{et}\quad t\,(v_i)_{i\in I}=(tv_i)_{i\in I}\,,$$

pour tous $(v_i)_{i\in I},(v_i')_{i\in I}\in\prod_{i\in I}V_i$ et $t\in\mathbb{K}$. La *somme directe* des V_i, notée $\oplus_{i\in I}V_i$, est le sous-espace vectoriel de $\prod_{i\in I}V_i$ formé des familles qui sont nulles presque partout, c'est-à-dire des familles $(v_i)_{i\in I}$ telles que $v_i=\overrightarrow{0}$ sauf pour un nombre fini d'indices. Remarquez que $\prod_{i\in I}V_i=\oplus_{i\in I}V_i$ si et seulement si I est fini.

Notations. Pour tout $i\in I$ on note

$$\pi_i:\prod_{j\in I}V_j\to V_i$$

la projection sur la i-ème composante, et

$$\tau_i:V_i\to\bigoplus_{i\in I}V_i$$

l'*insertion* à la i-ème place. Pour $u\in V_i$, $\tau_i(u)$ est la famille $(v_j)_{j\in I}$ telle que $v_j=\overrightarrow{0}$ si $j\neq i$ et $v_i=u$. De plus, on notera $\sigma:\oplus_{j\in I}V_j\to\prod_{j\in I}V_j$ l'inclusion, et on posera

$$p_i=\pi_i\circ\sigma:\bigoplus_{j\in I}V_j\to V_i\,.$$

Lemme 1.15. *π_i et τ_i sont des applications linéaires. De plus,*

$$\pi_j\circ\sigma\circ\tau_i=p_j\circ\tau_i=\begin{cases}\mathrm{Id}_{V_i} & \text{si } i=j\\ 0 & \text{si } i\neq j\end{cases}$$

En particulier, τ_i est injectif, et π_i et p_i sont surjectifs.

Démonstration. Exercice. $\square$

Rappelons que, si V, W sont deux espaces vectoriels, $\mathcal{L}(V; W)$ désigne l'espace des applications linéaires de V dans W.

Théorème 1.16 (Propriétés universelles). *Soient $(V_i)_{i\in I}$ une collection d'espaces vectoriels et W un espace vectoriel.*

(1) *Soit $(f_i : V_i \to W)_{i\in I}$ une collection d'applications linéaires. Alors il existe une unique application linéaire $f : \oplus_{i\in I} V_i \to V$ telle que $f_i = f \circ \tau_i$ pour tout $i \in I$. De façon plus précise, on a un isomorphisme*

$$\alpha : \prod_{i\in I} \mathcal{L}(V_i; W) \longleftrightarrow \mathcal{L}\left(\bigoplus_{i\in I} V_i; W\right).$$

(2) *Soient $(g_i : W \to V_i)_{i\in I}$ une collection d'applications linéaires. Il existe une unique application linéaire $g : W \to \prod_{i\in I} V_i$ telle que $g_i = \pi_i \circ g$ pour tout $i \in I$. De façon plus précise, on a un isomorphisme*

$$\gamma : \prod_{i\in I} \mathcal{L}(W; V_i) \longleftrightarrow \mathcal{L}\left(W; \prod_{i\in I} V_i\right).$$

Démonstration. Soit $\tilde{f} = (f_i)_{i\in I} \in \prod_{i\in I} \mathcal{L}(V_i; W)$. On définit $f = \alpha(\tilde{f}) \in \mathcal{L}(\oplus_{i\in I} V_i; W)$ comme suit. Soit $v = (v_i)_{i\in I} \in (\oplus_{i\in I} V_i)$. Alors

$$f(v) = \sum_{i\in I} f_i(v_i).$$

Cette somme est finie car $f_i(v_i) = f_i(\overrightarrow{0}) = \overrightarrow{0}$ pour presque tous i, donc $\alpha(\tilde{f})$ est bien définie. Montrons qu'elle est linéaire. Soient $v = (v_i)_{i\in I}, v' = (v'_i)_{i\in I} \in (\oplus_{i\in I} V_i)$ et $t, t' \in \mathbb{K}$. Alors

$$\begin{aligned} f(t\,v + t'\,v') &= \sum_{i\in I} f_i(t\,v_i + t'\,v'_i) = \sum_{i\in I} t\,f_i(v_i) + t'\,f(v'_i) \\ &= t\sum_{i\in I} f_i(v_i) + t'\sum_{i\in I} f_i(v'_i) = t\,f(v) + t'\,f(v'). \end{aligned}$$

Montrons que l'application $\alpha : \prod_{i\in I} \mathcal{L}(V_i; W) \to \mathcal{L}(\oplus_{i\in I} V_i; W)$ est linéaire. Soient $\tilde{f} = (f_i)_{i\in I}, \tilde{f}' = (f'_i)_{i\in I} \in (\prod_{i\in I} \mathcal{L}(V_i, W))$ et $t, t' \in \mathbb{K}$. Soit $v = (v_i)_{i\in I} \in (\oplus_{i\in I} V_i)$. Alors

$$\begin{aligned} \alpha(t\,\tilde{f} + t'\,\tilde{f}')(v) &= \sum_{i\in I} (t\,f_i + t'\,f'_i)(v_i) = t\sum_{i\in I} f_i(v_i) + t'\sum_{i\in I} f'(v_i) \\ &= t\,\alpha(\tilde{f})(v) + t'\,\alpha(\tilde{f}')(v) = (t\,\alpha(\tilde{f}) + t'\,\alpha(\tilde{f}'))(v), \end{aligned}$$

donc
$$\alpha(t\,\tilde{f} + t'\,\tilde{f}') = t\,\alpha(f) + t'\,\alpha(\tilde{f}')\,.$$

Soit $\alpha' : \mathcal{L}(\oplus_{i\in I}V_i; W) \to \prod_{i\in I}\mathcal{L}(V_i, W)$ l'application définie par
$$\alpha'(f) = (f\circ\tau_i)_{i\in I}\,.$$

On vérifie facilement que $\alpha\circ\alpha' = \mathrm{Id}$ et $\alpha'\circ\alpha = \mathrm{Id}$, donc α est une bijection.

Soit $\tilde{g} = (g_i)_{i\in I} \in (\prod_{i\in I}\mathcal{L}(W; V_i))$. On définit $g = \gamma(\tilde{g}) \in \mathcal{L}(W; \prod_{i\in I} V_i)$ comme suit. Soit $w\in W$. Alors
$$g(w) = (g_i(w))_{i\in I}\,.$$
On montre facilement que g est linéaire. On montre aussi facilement que l'application $\gamma : \prod_{i\in I}\mathcal{L}(W; V_i) \to \mathcal{L}(W; \prod_{i\in I} V_i)$ est linéaire. Soit $\gamma' : \mathcal{L}(W; \prod_{i\in I} V_i) \to \prod_{i\in I}\mathcal{L}(W; V_i)$ l'application définie par
$$\gamma'(g) = (\pi_i\circ g)_{i\in I}\,.$$
On vérifie facilement que $\gamma\circ\gamma' = \mathrm{Id}$ et $\gamma'\circ\gamma = \mathrm{Id}$, donc γ est une bijection. $\square$

Proposition 1.17. *Soient $(V_i)_{i\in I}$ une collection d'espaces vectoriels et, pour tout $i\in I$, B_i une base de V_i. Alors $\sqcup_{i\in I}\tau_i(B_i)$ est une base de $\oplus_{i\in I}V_i$.*

Démonstration. Il est évident que $\tau_i(B_i)\cap\tau_j(B_j) = \emptyset$ si $i\neq j$. Soit $v = (v_i)_{i\in I} \in \oplus_{i\in I}V_i$. Il existe $n\in\mathbb{N}$ et $i_1,\dots,i_n\in I$ tels que $v_i = \overrightarrow{0}$ si $i\notin\{i_1,\dots,i_n\}$. Pour tout $j\in\{1,\dots,n\}$, il existe $m_j\in\mathbb{N}$, $e_{1,j},\dots,e_{m_j,j}\in B_{i_j}$ et $t_{1,j},\dots,t_{m_j,j}\in\mathbb{K}$ tels que
$$v_{i_j} = t_{1,j}e_{1,j} + \cdots + t_{m_j,j}e_{m_j,j}\,.$$
Il s'en suit que
$$v = \sum_{j=1}^{n}\tau_{i_j}(v_{i_j}) = \sum_{j=1}^{n}\sum_{k=1}^{m_j} t_{k,j}\tau_{i_j}(e_{k,j})\,.$$
Ceci montre que $\sqcup_{i\in I}\tau_i(B_i)$ engendre $\oplus_{i\in I}V_i$.

On suppose donnés $n\in\mathbb{N}$, $i_1,\dots,i_n\in I$, $m_j\in\mathbb{N}$, $e_{1,j},\dots,e_{m_j,j}\in B_{i_j}$ et $t_{1,j},\dots,t_{m_j,j}\in\mathbb{K}$ pour tout $j\in\{1,\dots,n\}$, et on suppose que
$$\sum_{j=1}^{n}\sum_{k=1}^{m_j} t_{k,j}\tau_{i_j}(e_{k,j}) = \overrightarrow{0}\,.$$

Pour $j\in\{1,\dots,n\}$ on pose
$$v_{i_j} = t_{1,j}e_{1,j} + \cdots + t_{m_j,j}e_{m_j,j} \in V_{i_j}\,,$$

et on pose $v_i = \overrightarrow{0}$ si $i \notin \{i_1, \ldots, i_n\}$. Alors

$$(v_i)_{i\in I} = \sum_{j=1}^{n} \sum_{k=1}^{m_j} t_{k,j} \tau_{i_j}(e_{k,j}) = \overrightarrow{0}\,,$$

donc $v_i = \overrightarrow{0}$ pour tout $i \in I$, donc $t_{1,j} = \cdots = t_{m_j,j} = 0$ pour tout $j \in \{1, \ldots, n\}$. Ceci montre que $\sqcup_{i\in I} \tau_i(B_i)$ est libre. □

Proposition 1.18. *Soient $(V_i)_{i\in I}$, $(V_i')_{i\in I}$ deux collections d'espaces vectoriels.*

(1) *Toute collection d'applications linéaires $\tilde{f} = (f_i)_{i\in I} \in \prod_{i\in I} \mathcal{L}(V_i; V_i')$ induit une application linéaire $f \in \mathcal{L}(\oplus_{i\in I} V_i; \oplus_{i\in I} V_i')$. Plus précisément, on a une application linéaire*

$$\alpha : \prod_{i\in I} \mathcal{L}(V_i; V_i') \to \mathcal{L}(\oplus_{i\in I} V_i; \oplus_{i\in I} V_i')\,.$$

L'application linéaire α est injective. De plus, si f_i est injective (resp. surjective) pour tout $i \in I$, alors $\alpha(\tilde{f}) = f$ est injective (resp. surjective).

(2) *Toute collection d'applications linéaires $\tilde{f} = (f_i)_{i\in I} \in \prod_{i\in I} \mathcal{L}(V_i; V_i')$ induit une application linéaire $f \in \mathcal{L}(\prod_{i\in I} V_i; \prod_{i\in I} V_i')$. Plus précisément, on a une application linéaire*

$$\gamma : \prod_{i\in I} \mathcal{L}(V_i; V_i') \to \mathcal{L}(\prod_{i\in I} V_i; \prod_{i\in I} V_i')\,.$$

L'application linéaire γ est injective. De plus, si f_i est injective (resp. surjective) pour tout $i \in I$, alors $\gamma(\tilde{f}) = f$ est injective (resp. surjective).

Démonstration. On démontre (1). La partie (2) est laissée en exercice. Soit $\tilde{f} = (f_i)_{i\in I} \in \prod_{i\in I} \mathcal{L}(V_i; V_i')$. On définit $f = \alpha(\tilde{f}) \in \mathcal{L}(\oplus_{i\in I} V_i; \oplus_{i\in I} V_i')$ comme suit. Soit $v = (v_i)_{i\in I} \in (\oplus_{i\in I} V_i)$. Alors

$$f(v) = \alpha(\tilde{f})(v) = (f_i(v_i))_{i\in I}\,.$$

On démontre facilement que f est bien définie et est une application linéaire. On démontre aussi facilement que l'application $\alpha : \prod_{i\in I} \mathcal{L}(V_i; V_i') \to \mathcal{L}(\oplus_{i\in I} V_i; \oplus_{i\in I} V_i)$ est linéaire.

On remarque que, pour tout $i \in I$, on a $f_i = p_i \circ f \circ \tau_i$. En particulier, si $f = \alpha(\tilde{f}) = 0$, alors $f_i = 0$ pour tout $i \in I$, donc $\tilde{f} = 0$. Ceci montre que α est injective.

Supposons que f_i est injective pour tout $i \in I$. Soit $v = (v_i)_{i\in I} \in (\oplus_{i\in I} V_i)$.

$$\begin{aligned}
& f(v) = (f_i(v_i))_{i\in I} = \overrightarrow{0} \\
\Rightarrow\ & f_i(v_i) = \overrightarrow{0} \text{ pour tout } i \in I \\
\Rightarrow\ & v_i = \overrightarrow{0} \text{ pour tout } i \in I \\
\Rightarrow\ & v = (v_i)_{i\in I} = \overrightarrow{0}
\end{aligned}$$

D'où f est injective.

Supposons que f_i est surjective pour tout $i \in I$. Soit $v' = (v'_i)_{i\in I} \in (\oplus_{i\in I} V'_i)$. On pose $v_i = \overrightarrow{0} \in V_i$ si $v'_i = \overrightarrow{0}$. Si $v'_i \neq \overrightarrow{0}$, on choisit $v_i \in V_i$ tel que $f_i(v_i) = v'_i$. On pose $v = (v_i)_{i\in I}$. Alors $v \in \oplus_{i\in I} V_i$ et $f(v) = v'$. D'où f est surjective. $\square$

Corollaire 1.19. *Soient $(V_i)_{i\in I}$ une collection d'espaces vectoriels et, pour tout $i \in I$, U_i un sous-espace vectoriel de V_i. Alors $\oplus_{i\in I} U_i$ est un sous-espace vectoriel de $\oplus_{i\in I} V_i$, et on a*

$$\frac{\oplus_{i\in I} V_i}{\oplus_{i\in I} U_i} = \bigoplus_{i\in I} \frac{V_i}{U_i}\,.$$

Démonstration. Pour $i \in I$ on note $\iota_i : U_i \to V_i$ l'inclusion. Alors les ι_i induisent une application linéaire injective $\iota : \oplus_{i\in I} U_i \to \oplus_{i\in I} V_i$. Pour $i \in I$ on note $\pi_i : V_i \to \frac{V_i}{U_i}$ l'application quotient. Alors les π_i induisent une application linéaire surjective $\pi : \oplus_{i\in I} V_i \to \oplus_{i\in I} \frac{V_i}{U_i}$. Reste à montrer que $\operatorname{Ker} \pi = \oplus_{i\in I} U_i$. Soit $v = (v_i)_{i\in I} \in (\oplus_{i\in I} V_i)$.

$$\begin{array}{rl} & \pi(v) = (\pi_i(v_i))_{i\in I} = \overrightarrow{0} \\ \Leftrightarrow & \pi_i(v_i) = \overrightarrow{0} \text{ pour tout } i \in I \\ \Leftrightarrow & v_i \in U_i \text{ pour tout } i \in I \\ \Leftrightarrow & v = (v_i)_{i\in I} \in (\oplus_{i\in I} U_i) \end{array}$$

$\square$

2 Produit tensoriel d'espaces vectoriels

Dans ce chapitre $\mathbb{K}$ désignera un corps commutatif.

2.1 Définitions et propriétés

Définition. Soient $V_1, \ldots, V_p, W$ des espaces vectoriels sur $\mathbb{K}$ et $f : V_1 \times \cdots \times V_p \to W$ une application. On dit que f est *p-linéaire* si, pour tous $i \in \{1, \ldots, p\}$, $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_i, v'_i \in V_i, v_{i+1} \in V_{i+1}, \ldots, v_p \in V_p$ et $t, t' \in \mathbb{K}$, on a

$$\begin{aligned} f(v_i, \ldots, v_{i-1}, tv_i + t'v'_i, v_{i+1}, \ldots, v_p) = t\, f(v_i, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p) \\ + t'\, f(v_i, \ldots, v_{i-1}, v'_i, v_{i+1}, \ldots, v_p)\,. \end{aligned}$$

Une *application linéaire* est une application 1-linéaire et une *application bilinéaire* est une application 2-linéaire. On note $\mathcal{L}_p(V_1, \ldots, V_p; W)$ l'espace des applications p-linaires de $V_1 \times \cdots \times V_p$ dans W.

Théorème 2.1. *Soient $V_1, \ldots, V_p$ des espaces vectoriels sur $\mathbb{K}$. Il existe un espace vectoriel $V_1 \otimes V_2 \otimes \cdots \otimes V_p$ et une application p-linéaire $\iota : V_1 \times \cdots \times V_p \to V_1 \otimes \cdots \otimes V_p$ vérifiant les propriétés suivantes.*

(a) *L'espace* $V_1 \otimes \cdots \otimes V_p$ *est engendré par l'ensemble* $\{\iota(v_1, \ldots, v_p); (v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p\}$ *;*

(b) *pour tout espace vectoriel* W *et tout application* p*-linéaire* $f \in \mathcal{L}_p(V_1, \ldots, V_p; W)$*, il existe une application linéaire* $\tilde{f} : V_1 \otimes \cdots \otimes V_p \to W$ *telle que* $f = \tilde{f} \circ \iota$ *, c'est-à-dire le diagramme suivant commute.*

$$\begin{tikzcd}
V_1 \times \cdots \times V_p \arrow[r, "f"] \arrow[d, "\iota"'] & W \\
V_1 \otimes \cdots \otimes V_p \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

De plus, le couple $(V_1 \otimes \cdots \otimes V_p, \iota)$ *est unique.*

Définition. L'espace $V_1 \otimes \cdots \otimes V_p$ s'appelle le *produit tensoriel* de $V_1, \ldots, V_p$. On note $\iota(v_1, \ldots, v_p) = v_1 \otimes \cdots \otimes v_p$ et on l'appelle *tenseur élémentaire.* Les éléments de $V_1 \otimes \cdots \otimes V_p$ sont appelés *tenseurs.*

Démonstration. On commence par construire $V_1 \otimes \cdots \otimes V_p$ et ι. On considère $E = V_1 \times \cdots \times V_p$ comme un ensemble et on note H l'espace vectoriel sur $\mathbb{K}$ ayant E comme base. On note N le sous-espace vectoriel de H engendré par

$$\begin{gathered}
\{(v_1, \ldots, v_{i-1}, tv_i + t'v'_i, v_{i+1}, \ldots, v_p) - t\,(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p) \\
-t'\,(v_1, \ldots, v_{i-1}, v'_i, v_{i+1}, \ldots, v_p) \mid i \in \{1, \ldots, p\}\,,\ v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_i, v'_i \in V_i, \\
v_{i+1} \in V_{i+1}, \ldots, v_p \in V_p\,,\ t, t' \in \mathbb{K}\}\,.
\end{gathered}$$

On pose $V_1 \otimes \cdots \otimes V_p = H/N$ et on note $\iota : V_1 \times \cdots \times V_p \to V_1 \otimes \cdots \otimes V_p$ l'application qui à $(v_1, \ldots v_p)$ associe sa classe dans le quotient H/N.

Soient $i \in \{1, \ldots, p\}$, $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_i, v'_i \in V_i, v_{i+1} \in V_{i+1}, \ldots, v_p \in V_p$ et $t, t' \in \mathbb{K}$. Comme

$$\begin{aligned}
(v_1, \ldots, v_{i-1}, tv_i + t'v'_i, v_{i+1}, \ldots, v_p) - t\,(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p)& \\
- t'\,(v_1, \ldots, v_{i-1}, v'_i, v_{i+1}, \ldots, v_p) \in N\,,&
\end{aligned}$$

on a

$$\begin{aligned}
\iota(v_1, \ldots, v_{i-1}, tv_i + t'v'_i, v_{i+1}, \ldots, v_p) - t\,\iota(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p)& \\
- t'\,\iota(v_1, \ldots, v_{i-1}, v'_i, v_{i+1}, \ldots, v_p) = \overrightarrow{0}\,.&
\end{aligned}$$

Ceci montre que ι est p-linéaire.

Comme H est engendré par l'ensemble $\{(v_1, \ldots, v_p); v_1 \in V_1, \ldots, v_p \in V_p\}$, $H/N = V_1 \otimes \cdots \otimes V_p$ est engendré par $\{\iota(v_1, \ldots, v_p); v_1 \in V_1, \ldots, v_p \in V_p\}$.

Soient W un espace vectoriel sur $\mathbb{K}$ et $f \in \mathcal{L}_p(V_1, \ldots, V_p; W)$. On considère $f : V_1 \times \cdots \times V_p \to W$ comme une application ensembliste et on note $F : H \to W$ l'application linéaire qu'elle définie. Pour $i \in \{1, \ldots, p\}$, $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_i, v_i' \in V_i, v_{i+1} \in V_{i+1}, \ldots, v_p \in V_p$ et $t, t' \in \mathbb{K}$ on a

$$\begin{aligned}
&F\big((v_1, \ldots, v_{i-1}, tv_i + t'v_i', v_{i+1}, \ldots, v_p) - t\,(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p) \\
&\qquad - t'\,(v_1, \ldots, v_{i-1}, v_i', v_{i+1}, \ldots, v_p)\big) \\
=&f(v_1, \ldots, v_{i-1}, tv_i + t'v_i', v_{i+1}, \ldots, v_p) - t\,f(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_p) \\
&\qquad - t'\,f(v_1, \ldots, v_{i-1}, v_i', v_{i+1}, \ldots, v_p) \\
=&\overrightarrow{0}\,.
\end{aligned}$$

Ceci montre que F s'annule sur les générateurs de N, donc s'annule sur N tout entier. On en déduit que F induit une application linéaire $\tilde{f} : H/N = V_1 \otimes \cdots \otimes V_p \to W$. Il est clair que, par définition, $\tilde{f} \circ \iota = f$. Par ailleurs, $\tilde{f}$ est unique car est entièrement déterminée par les images des générateurs de $V_1 \otimes \cdots \otimes V_p$.

Il reste à montrer l'unicité du couple $(V_1 \otimes \cdots \otimes V_p, \iota)$. Soit $(\tilde{V}, \tilde{\iota})$, où $\tilde{V}$ est un espace vectoriel sur $\mathbb{K}$ et $\tilde{\iota} : V_1 \times \cdots \times V_p \to \tilde{V}$ est une application p-linéaire, vérifiant :

(a) L'espace $\tilde{V}$ est engendré par l'ensemble $\{\tilde{\iota}(v_1, \ldots, v_p); (v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p\}$;

(b) pour tout espace vectoriel W et tout application p-linéaire $f \in \mathcal{L}_p(V_1, \ldots, V_p; W)$, il existe une application linéaire $\tilde{f} : \tilde{V} \to W$ telle que $f = \tilde{f} \circ \tilde{\iota}$, c'est-à-dire le diagramme suivant commute.

$$\begin{tikzcd}
V_1 \times \cdots \times V_p \arrow[r, "f"] \arrow[d, "\tilde{\iota}"'] & W \\
\tilde{V} \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Comme $\iota : V_1 \times \cdots \times V_p \to V_1 \otimes \cdots \otimes V_p$ est p-linéaire, il existe une application linéaire $\varphi : \tilde{V} \to V_1 \otimes \cdots \otimes V_p$ telle que $\iota = \varphi \circ \tilde{\iota}$. De même, comme $\tilde{\iota} : V_1 \times \cdots \times V_p \to \tilde{V}$ est p-linéaire, il existe une application linéaire $\psi : V_1 \otimes \cdots \otimes V_p \to \tilde{V}$ telle que $\tilde{\iota} = \psi \circ \iota$. L'application $\varphi \circ \psi$ est l'identité sur l'ensemble $\{\iota(v_1, \ldots, v_p); v_1 \in V_1, \ldots, v_p \in V_p\}$ qui engendre $V_1 \otimes \cdots \otimes V_p$, donc $\varphi \circ \psi = \mathrm{Id}$. De même, $\psi \circ \varphi$ est l'indentité sur $\{\tilde{\iota}(v_1, \ldots, v_p); v_1 \in V_1, \ldots, v_p \in V_p\}$ qui engendre $\tilde{V}$, donc $\psi \circ \varphi = \mathrm{Id}$. □

Lemme 2.2. *Soient $V_1, \ldots, V_p$ des espaces vectoriels sur $\mathbb{K}$.*

(1) *Soient $i \in \{1, \ldots, p\}$, $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_i, v_i' \in V_i, v_{i+1} \in V_{i+1}, \ldots, v_p \in V_p$ et $t, t' \in \mathbb{K}$. Alors*

$$\begin{aligned}
&v_1 \otimes \cdots \otimes v_{i-1} \otimes (tv_i + t'v_i') \otimes v_{i+1} \otimes \cdots \otimes v_p = \\
&t\,(v_1 \otimes \cdots \otimes v_{i-1} \otimes v_i \otimes v_{i+1} \otimes \cdots \otimes v_p) + t'\,(v_1 \otimes \cdots \otimes v_{i-1} \otimes v_i' \otimes v_{i+1} \otimes \cdots \otimes v_p)\,.
\end{aligned}$$

(2) *Soit* $(v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p$*. Si* $v_i = \overrightarrow{0}$ *pour un* $i \in \{1, \ldots, p\}$*, alors* $v_1 \otimes \cdots \otimes v_p = \overrightarrow{0}$*.*

Démonstration. Exercice. $\square$

Théorème 2.3. *Soient* $V_1, \ldots, V_p$ *des espaces vectoriels sur* $\mathbb{K}$ *et, pour tout* $i \in \{1, \ldots, p\}$*,* B_i *une base de* V_i*. Alors*

$$\{e_1 \otimes \cdots \otimes e_p \ ; \ (e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p\}$$

est une base de $V_1 \otimes \cdots \otimes V_p$*.*

Corollaire 2.4. *Soient* $V_1, \ldots, V_p$ *des espaces vectoriels de dimension finie. Alors* $V_1 \otimes \cdots \otimes V_p$ *est de dimension finie, et*

$$\dim(V_1 \otimes V_2 \otimes \cdots \otimes V_p) = \dim V_1 \cdot \dim V_2 \cdots \dim V_p \, .$$

Le lemme suivant est un résultat préliminaire à la démonstration du théorème 2.3.

Lemme 2.5. *Soient* $V_1, \ldots, V_p$ *des espaces vectoriels sur* $\mathbb{K}$ *et, pour tout* $i \in \{1, \ldots, p\}$*,* B_i *une base de* V_i*. Pour tout* $i \in \{1, \ldots, p\}$ *on se fixe un vecteur* $u_i \in B_i$*. Alors il existe une forme* p*-linéaire* $f : V_1 \times \cdots \times V_p \to \mathbb{K}$ *telle que*

$$f(e_1, \ldots, e_p) = \begin{cases} 1 & \textit{si } (e_1, \ldots, e_p) = (u_1, \ldots, u_p) \\ 0 & \textit{si } (e_1, \ldots, e_p) \neq (u_1, \ldots, u_p) \end{cases}$$

pour tout $(e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p$*.*

Démonstration. Pour tout $i \in \{1, \ldots, p\}$ il existe une forme linéaire $h_i : V_i \to \mathbb{K}$ vérifiant

$$h_i(e_i) = \begin{cases} 1 & \text{si } e_i = u_i \\ 0 & \text{si } e_i \neq u_i \end{cases}$$

pour tout $e_i \in B_i$. On définit $f : V_1 \times \cdots \times V_p \to \mathbb{K}$ par

$$f(v_1, v_2, \ldots, v_p) = h_1(v_1) \cdot h_2(v_2) \cdots h_p(v_p) \, .$$

On vérifie facilement que f est p-linéaire et que

$$f(e_1, \ldots, e_p) = \begin{cases} 1 & \text{si } (e_1, \ldots, e_p) = (u_1, \ldots, u_p) \\ 0 & \text{si } (e_1, \ldots, e_p) \neq (u_1, \ldots, u_p) \end{cases}$$

pour tout $(e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p$. $\square$

Démonstration du théorème 2.3. On pose $B = \{e_1 \otimes \cdots \otimes e_p; (e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p\}$. Soit $G = \{v_1 \otimes \cdots \otimes v_p; (v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p\}$. Soit $v_1 \otimes \cdots \otimes v_p \in G$. Pour tout $i \in \{1, \ldots, p\}$ il existe $m_i \in \mathbb{N}$, $e_{i,1}, \ldots, e_{i,m_i} \in B_i$ et $t_{i,1}, \ldots, t_{i,m_i} \in \mathbb{K}$ tels que

$$v_i = t_{i,1}e_{i,1} + \cdots + t_{i,m_i}e_{i,m_i} .$$

Alors

$$\begin{aligned} v_1 \otimes \cdots \otimes v_p &= \left(\sum_{j_1=1}^{m_1} t_{1,j_1} e_{1,j_1} \right) \otimes \cdots \otimes \left(\sum_{j_p=1}^{m_p} t_{p,j_p} e_{p,j_p} \right) \\ &= \sum_{j_1=1}^{m_1} \cdots \sum_{j_p=1}^{m_p} t_{1,j_1} \cdots t_{p,j_p} e_{1,j_1} \otimes \cdots \otimes e_{p,j_p} . \end{aligned}$$

En d'autres termes, tout élément de G est combinaison linéaire d'éléments de B. Comme G engendre $V_1 \otimes \cdots \otimes V_p$, on en déduit que B engendre aussi $V_1 \otimes \cdots \otimes V_p$.

On se donne $n \in \mathbb{N}$, $(e_{1,i} \otimes \cdots \otimes e_{p,i}) \in B$ et $t_i \in \mathbb{K}$ pour $i \in \{1, \ldots, n\}$, et on suppose que

$$\sum_{i=1}^{n} t_i(e_{1,i} \otimes \cdots \otimes e_{p,i}) = \overrightarrow{0} .$$

On se fixe $i \in \{1, \ldots, n\}$. Par le lemme 2.5 on sait qu'il existe une forme p-linéaire $f : V_1 \times \cdots \times V_p \to \mathbb{K}$ telle que

$$f(e'_1, \ldots, e'_p) = \begin{cases} 1 & \text{si } (e'_1, \ldots, e'_p) = (e_{1,i}, \ldots, e_{p,i}) \\ 0 & \text{si } (e'_1, \ldots, e'_p) \neq (e_{1,i}, \ldots, e_{p,i}) \end{cases}$$

pour tout $(e'_1, \ldots, e'_p) \in B_1 \times \cdots \times B_p$. Soit $\tilde{f} : V_1 \otimes \cdots \otimes V_p \to \mathbb{K}$ la forme linéaire induite par f. Alors

$$\tilde{f}(e'_1 \otimes \cdots \otimes e'_p) = \begin{cases} 1 & \text{si } (e'_1, \ldots, e'_p) = (e_{1,i}, \ldots, e_{p,i}) \\ 0 & \text{si } (e'_1, \ldots, e'_p) \neq (e_{1,i}, \ldots, e_{p,i}) \end{cases}$$

Il en résulte que

$$0 = \tilde{f}(\overrightarrow{0}) = \tilde{f}\left(\sum_{j=1}^{n} t_j(e_{1,j} \otimes \cdots \otimes e_{p,j}) \right) = t_i .$$

Ceci montre que B est libre. □

Corollaire 2.6. *Soient $V_1, \ldots, V_p$ des espaces vectoriels sur $\mathbb{K}$.*

(1) *Pour tout $i \in \{1, \ldots, p\}$ on se donne une famille libre $L_i \subset V_i$. Alors $\{e_1 \otimes \cdots \otimes e_p; (e_1, \ldots, e_p) \in L_1 \times \cdots \times L_p\}$ est une famille libre de $V_1 \otimes \cdots \otimes V_p$.*

(2) *Soit $(v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p$. On a $v_1 \otimes \cdots \otimes v_p = \overrightarrow{0}$ si et seulement s'il existe $i \in \{1, \ldots, p\}$ tel que $v_i = \overrightarrow{0}$.*

(3) *On a* $V_1 \otimes \cdots \otimes V_p = \{\overrightarrow{0}\}$ *si et seulement s'il existe* $i \in \{1, \dots, p\}$ *tel que* $V_i = \{\overrightarrow{0}\}$.

Démonstration. Pour tout $i \in \{1, \dots, p\}$ on se donne une famille libre $L_i \subset V_i$, et on pose $L = \{e_1 \otimes \cdots \otimes e_p; (e_1, \dots, e_p) \in L_1 \times \cdots \times L_p\}$. Pour tout $i \in \{1, \dots, p\}$ il existe une base B_i de V_i contenant L_i. Posons $B = \{e_1 \otimes \cdots \otimes e_p; (e_1, \dots, e_p) \in B_1 \times \cdots \times B_p\}$. Alors B est une base de $V_1 \otimes \cdots \otimes V_p$ et contient L, donc L est libre.

Soit $(v_1, \dots, v_p) \in V_1 \times \cdots \times V_p$. Si $v_i \neq \overrightarrow{0}$ pour tout $i \in \{1, \dots, p\}$, alors $L_i = \{v_i\}$ est libre pour tout $i \in \{1, \dots, p\}$, donc $L = \{e_1 \otimes \cdots \otimes e_p; (e_1, \dots, e_p) \in L_1 \times \cdots \times L_p\} = \{v_1 \otimes \cdots \otimes v_p\}$ est libre. En particulier, $v_1 \otimes \cdots \otimes v_p \neq \overrightarrow{0}$. Par ailleurs, si $v_i = \overrightarrow{0}$ pour un $i \in \{1, \dots, p\}$, alors $v_1 \otimes \cdots \otimes v_p = \overrightarrow{0}$ (voir Lemme 2.2 (2)).

Supposons qu'il existe $i \in \{1, \dots, p\}$ tel que $V_i = \{\overrightarrow{0}\}$. Alors, par (2), $v_1 \otimes \cdots \otimes v_p = \overrightarrow{0}$ pour tout $(v_1, \dots, v_p) \in V_1 \times \cdots \times V_p$, donc $V_1 \otimes \cdots \otimes V_p = \{\overrightarrow{0}\}$. Supposons que $V_i \neq \{\overrightarrow{0}\}$ pour tout $i \in \{1, \dots, p\}$. Pour tout i on choisit $v_i \in V_i$, $v_i \neq \overrightarrow{0}$. Alors, par (2), $v_1 \otimes \cdots \otimes v_p \neq \overrightarrow{0}$, donc $V_1 \otimes \cdots \otimes V_p \neq \{\overrightarrow{0}\}$. $\square$

Proposition 2.7.

(1) *Soit* V *un espace vectoriel sur* $\mathbb{K}$. *Alors* $\mathbb{K} \otimes V \simeq V \otimes \mathbb{K} \simeq V$.

(2) *Soient* V_1 *et* V_2 *deux espaces vectoriels sur* $\mathbb{K}$. *Alors* $V_1 \otimes V_2 \simeq V_2 \otimes V_1$.

(3) *Soient* V_1, V_2, V_3 *trois espaces vectoriels sur* $\mathbb{K}$. *Alors* $(V_1 \otimes V_2) \otimes V_3 \simeq V_1 \otimes (V_2 \otimes V_3) \simeq V_1 \otimes V_2 \otimes V_3$.

Démonstration. Soient V un espace vectoriel sur $\mathbb{K}$ et B une base de V. Par le théorème 2.3, $B' = \{1 \otimes e; e \in B\}$ est une base de $\mathbb{K} \otimes V$. L'application $B \to B'$, $e \mapsto 1 \otimes e$ est une bijection donc induit un isomorphisme $f : V \to \mathbb{K} \otimes V$. On observe que $f(v) = 1 \otimes v$ pour tout $v \in V$. On démontre de la même façon que $V \otimes \mathbb{K} \simeq V$.

Soient V_1, V_2 deux espaces vectoriels et B_1, B_2 des bases de V_1, V_2, respectivement. Posons $B = \{e_1 \otimes e_2; (e_1, e_2) \in B_1 \times B_2\}$ et $B' = \{e_2 \otimes e_1; (e_2, e_1) \in B_2 \times B_1\}$. L'application $f : B \to B'$, $e_1 \otimes e_2 \mapsto e_2 \otimes e_1$ est une bijection. Comme B est une base de $V_1 \otimes V_2$ et B' est une base de $V_2 \otimes V_1$, l'application f induit un isomorphisme $f : V_1 \otimes V_2 \to V_2 \otimes V_1$. Remarquez que $f(v_1 \otimes v_2) = v_2 \otimes v_1$ pour tout $(v_1, v_2) \in V_1 \times V_2$.

Soient V_1, V_2, V_3 des espaces vectoriels sur $\mathbb{K}$ et B_1, B_2, B_3 des bases de V_1, V_2, V_3, respectivement. Posons $B = \{(e_1 \otimes e_2) \otimes e_3; (e_1, e_2, e_3) \in B_1 \times B_2 \times B_3\}$ et $B' = \{e_1 \otimes e_2 \otimes e_3; (e_1, e_2, e_3) \in B_1 \times B_2 \times B_3\}$. L'application $f : B \to B'$, $(e_1 \otimes e_2) \otimes e_3 \mapsto e_1 \otimes e_2 \otimes e_3$ est une bijection. Par ailleurs, B est une base de $(V_1 \otimes V_2) \otimes V_3$ et B' est une base de $V_1 \otimes V_2 \otimes V_3$. On en déduit que f induit un isomorphisme $f : (V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes V_2 \otimes V_3$. Remarquez que $f((v_1 \otimes v_2) \otimes v_3) = v_1 \otimes v_2 \otimes v_3$ pour tout $(v_1, v_2, v_3) \in V_1 \times V_2 \times V_3$. On démontre de la même façon que $V_1 \otimes (V_2 \otimes V_3) \simeq V_1 \otimes V_2 \otimes V_3$. $\square$

Proposition 2.8. *Soient $(V_i)_{i\in I}$ une collection d'espaces vectoriels, et W un autre espace vectoriel sur $\mathbb{K}$. Alors*

$$\left(\bigoplus_{i\in I} V_i\right) \otimes W \simeq \bigoplus_{i\in I}(V_i \otimes W)\,.$$

Démonstration. Pour tout $i \in I$ on se donne une base B_i de V_i. De même, on se donne une base C de W. Notons $\tau_i : V_i \to \oplus_{j\in I} V_j$ et $\tau_i' : (V_i \otimes W) \to \oplus_{j\in I}(V_j \otimes W)$ les insertions. $\sqcup_{i\in I}\tau_i(B_i)$ est une base de $\oplus_{i\in I} V_i$ (voir la proposition 1.17), donc

$$\tilde{B} = \{e \otimes f\ ;\ (e,f) \in (\sqcup_{i\in i}\tau_i(B_i)) \times C\}$$

est une base de $(\oplus_{i\in I} V_i) \otimes W$. Par ailleurs, $\tilde{B}_i' = \{e \otimes f; (e,f) \in B_i \times C\}$ est une base de $V_i \otimes W$ pour tout $i \in I$, donc

$$\tilde{B}' = \sqcup_{i\in i}\tau_i'(\tilde{B}_i')$$

est une base de $\oplus_{i\in I}(V_i \otimes W)$. on a les bijections (naturelles)

$$\tilde{B} \simeq (\sqcup_{i\in I}\tau_i(B_i)) \times C \simeq (\sqcup_{i\in I} B_i) \times C \simeq \sqcup_{i\in I}(B_i \times C) \simeq \sqcup_{i\in I}\tilde{B}_i' \simeq \tilde{B}'$$

qui induisent un isomorphisme (naturel)

$$\left(\bigoplus_{i\in I} V_i\right) \otimes W \to \bigoplus_{i\in I}(V_i \otimes W)\,.$$

□

Proposition 2.9. *Soient $V_1, \ldots, V_p$ des espaces vectoriels sur $\mathbb{K}$ et, pour tout $i \in \{1, \ldots, p\}$, W_i un sous-espace vectoriel de V_i.*

(1) L'espace $W_1 \otimes \cdots \otimes W_p$ est un sous-espace vectoriel de $V_1 \otimes \cdots \otimes V_p$.

(2) Supposons que $V_i \neq \{\overrightarrow{0}\}$ pour tout $i \in \{1, \ldots, p\}$. On a $W_1 \otimes \cdots \otimes W_p = V_1 \otimes \cdots \otimes V_p$ si et seulement si $W_i = V_i$ pour tout $i \in \{1, \ldots, p\}$.

Démonstration. Pour $i \in \{1, \ldots, p\}$, on choisit une base L_i de W_i. Comme L_i est libre dans V_i, il existe une base B_i de V_i contenant L_i. Alors $B = \{e_1 \otimes \cdots \otimes e_p; (e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p\}$ est une base de $V_1 \otimes \cdots \otimes V_p$, $L = \{e_1 \otimes \cdots \otimes e_p; (e_1, \ldots, e_p) \in L_1 \times \cdots \times L_p\}$ est une base de $W_1 \otimes \cdots \otimes W_p$, et $L \subset B$, donc $W_1 \otimes \cdots \otimes W_p$ est un sous-espace vectoriel de $V_1 \otimes \cdots \otimes V_p$.

Supposons que $V_i \neq \{\overrightarrow{0}\}$, c'est-à-dire $B_i \neq \emptyset$, pour tout $i \in \{1, \ldots, p\}$. On a $W_1 \otimes \cdots \otimes W_p = V_1 \otimes \cdots \otimes V_p$ si et seulement si $L = B$. On a $L = B$ si et seulement si $L_i = B_i$ pour tout $i \in \{1, \ldots, p\}$. Finalement, on a $L_i = B_i$ pour tout $i \in \{1, \ldots, p\}$ si et seulement si $W_i = V_i$ pour tout $i \in \{1, \ldots, p\}$. □

Remarque. Si $V_1 = \{\overrightarrow{0}\}$, alors $V_1 \otimes W_2 = V_1 \otimes V_2 = \{\overrightarrow{0}\}$ pour tout sous-espace vectoriel W_2 de V_2.

2.2 Produit tensoriel d'applications linéaires

Définition. Soient V_1, V_2, W_1, W_2 des espaces vectoriels sur $\mathbb{K}$ et $f_1 : V_1 \to W_1$, $f_2 : V_2 \to W_2$ deux applications linéaires. Soit $F : V_1 \times V_2 \to W_1 \otimes W_2$ l'application définie par $F(v_1, v_2) = f_1(v_1) \otimes f_2(v_2)$. Il est clair que F est bi-linéaire, donc induit une application linéaire $f_1 \otimes f_2 : V_1 \otimes V_2 \to W_1 \otimes W_2$ appelée *produit tensoriel* de f_1 et f_2.

Proposition 2.10. *Soient $U_1, V_1, W_1, U_2, V_2, W_2$ des espaces vectoriels sur $\mathbb{K}$ et $f_1 : U_1 \to V_1$, $g_1 : V_1 \to W_1$, $f_2 : U_2 \to V_2$, $g_2 : V_2 \to W_2$ des applications linéaires. Alors*

$$(g_1 \circ f_1) \otimes (g_2 \circ f_2) = (g_1 \otimes g_2) \circ (f_1 \otimes f_2) : U_1 \otimes U_2 \to W_1 \otimes W_2 \,.$$

Démonstration. Soit $(u_1, u_2) \in U_1 \times U_2$. Alors

$$\begin{aligned}
&((g_1 \circ f_1) \otimes (g_2 \circ f_2))(u_1 \otimes u_2) \\
=&(g_1 \circ f_1)(u_1) \otimes (g_2 \circ f_2)(u_2) \\
=&(g_1 \otimes g_2)(f_1(u_1) \otimes f_2(u_2)) \\
=&(g_1 \otimes g_2) \circ (f_1 \otimes f_2)(u_1 \otimes u_2)
\end{aligned}$$

Comme l'ensemble $\{u_1 \otimes u_2; (u_1, u_2) \in U_1 \times U_2\}$ engendre $U_1 \otimes U_2$, ceci montre que $(g_1 \circ f_1) \otimes (g_2 \circ f_2) = (g_1 \otimes g_2) \circ (f_1 \otimes f_2)$. □

Proposition 2.11. *Soient V_1, V_2, W_1, W_2 des espaces vectoriels sur $\mathbb{K}$ et $f_1 : V_1 \to W_1$, $f_2 : V_2 \to W_2$ des applications linéaires.*

(1) $\mathrm{Im}(f_1 \otimes f_2) = \mathrm{Im}(f_1) \otimes \mathrm{Im}(f_2)$. *En particulier $f_1 \otimes f_2$ est surjective si f_1, f_2 sont surjectives. De plus, si f_1, f_2 sont de rang fini, alors $f_1 \otimes f_2$ est de rang fini et* $\mathrm{Rg}(f_1 \otimes f_2) = \mathrm{Rg}(f_1)\,\mathrm{Rg}(f_2)$.

(2) *$f_1 \otimes f_2$ est injective si f_1, f_2 sont injectives.*

(3) *$f_1 \otimes f_2$ est un isomorphisme si f_1, f_2 sont des isomorphismes.*

Démonstration. $V_1 \otimes V_2$ est engendré par $\{v_1 \otimes v_2; (v_1, v_2) \in V_1 \times V_2\}$, donc $\mathrm{Im}(f_1 \otimes f_2)$ est engendré par

$$\{(f_1 \otimes f_2)(v_1 \otimes v_2); (v_1, v_2) \in V_1 \times V_2\} = \{f_1(v_1) \otimes f_2(v_2); (v_1, v_2) \in V_1 \times V_2\}$$

qui clairement engendre $\mathrm{Im}(f_1) \otimes \mathrm{Im}(f_2)$.

Supposons que f_1 et f_2 sont injectives. Soit B_i une base de V_i pour $i \in \{1, 2\}$. Comme f_i est injective, $f_i(B_i)$ est libre, donc il existe une base C_i de W_i contenant $f(B_i)$. Posons

$B = \{e_1 \otimes e_2; (e_1, e_2) \in B_1 \times B_2\}$ et $C = \{e'_1 \otimes e'_2 : (e'_1, e'_2) \in C_1 \times C_2\}$. Alors B est une base de $V_1 \otimes V_2$ et C est une base de $W_1 \otimes W_2$. Pour $(e_1, e_2) \in B_1 \times B_2$ on a

$$(f_1 \otimes f_2)(e_1 \otimes e_2) = f_1(e_1) \otimes f_2(e_2) \in C\,,$$

donc $(f_1 \otimes f_2)$ evoie bijectivement B sur un sous-ensemble de C, donc sur une famille libre, donc $f_1 \otimes f_2$ est injective.

La partie (3) du lemme est une conséquence directe de (1) et (2). □

Proposition 2.12. *Soient V_1, W_1, V_2, W_2 des espaces vectoriels sur $\mathbb{K}$ et $f_1 : V_1 \to W_1$, $f_2 : V_2 \to W_2$ des applications linéaires. Posons $K_1 = \operatorname{Ker} f_1$ et $K_2 = \operatorname{Ker} f_2$. Pour $i \in \{1, 2\}$, on choisit un sous-espace V'_i de V_i tel que $V_i = K_i \oplus V'_i$. Alors*

$$\begin{aligned}\operatorname{Ker}(f_1 \otimes f_2) = (K_1 \otimes V_2) + (V_1 \otimes K_2) &= (K_1 \otimes V'_2) \oplus (V_1 \otimes K_2)\\ &= (K_1 \otimes V_2) \oplus (V'_1 \otimes K_2)\,.\end{aligned}$$

Les deux résultats suivants sont des préliminaires à la démonstration de la proposition 2.12.

Lemme 2.13. *Soient V, W deux espaces vectoriels sur $\mathbb{K}$ et U_1, U_2 deux sous-espaces vectoriels de V. Alors $(U_1 + U_2) \otimes W = (U_1 \otimes W) + (U_2 \otimes W)$.*

Démonstration. Exercice. □

Lemme 2.14. *Soit $f : V \to W$ une application linéaire.*

(1) *On pose $K = \operatorname{Ker} f$ et on choisit $V' \subset V$ tel que $V = K \oplus V'$. Alors $f|_{V'} : V' \to W$ est injective.*

(2) *Soient K, V' des sous-espaces vectoriels de V tels que $V = K \oplus V'$, $f|_K = 0$ et $f|_{V'}$ est injective. Alors $K = \operatorname{Ker} f$.*

Démonstration. Exercice. □

Démonstration de la proposition 2.12.

$$\begin{aligned}V_1 \otimes V_2 = (K_1 \oplus V'_1) \otimes V_2 = (K_1 \otimes V_2) \oplus (V'_1 \otimes V_2) &= (K_1 \otimes V_2) \oplus (V'_1 \otimes (K_2 \oplus V'_2))\\ &= (K_1 \otimes V_2) \oplus (V'_1 \otimes K_2) \oplus (V'_1 \otimes V'_2)\end{aligned}$$

Si $(u_1, u_2) \in K_1 \times V_2$, alors

$$(f_1 \otimes f_2)(u_1 \otimes u_2) = f_1(u_1) \otimes f_2(u_2) = \overrightarrow{0} \otimes f_2(u_2) = \overrightarrow{0}\,.$$

Comme $\{u_1 \otimes u_2; (u_1, u_2) \in K_1 \times V_2\}$ engendre $K_1 \otimes V_2$ on en déduit que la restriction de $f_1 \otimes f_2$ à $K_1 \otimes V_2$ est nulle. On démontre de la même façon que la restriction de $f_1 \otimes f_2$ à $V_1' \otimes K_2$ est nulle. Par ailleurs, par le lemme 2.14 (1), $f_1|_{V_1'}$ et $f_2|_{V_2'}$ sont injectives. Par la proposition 2.11 (2) il s'en suit que $(f_1 \otimes f_2)|_{V_1' \otimes V_2'}$ est injective. Par le lemme 2.14 (2), on en conclue que $\mathrm{Ker}(f_1 \otimes f_2) = (K_1 \otimes V_2) \oplus (V_1' \otimes K_2)$.

$$\begin{aligned}(K_1 \otimes V_2) \oplus (V_1' \oplus K_2) &= (K_1 \otimes (V_2 + K_2)) + (V_1' \oplus K_2)\\ &= (K_1 \otimes V_2) + (K_1 \otimes K_2) + (V_1' \oplus K_2)\\ &= (K_1 \otimes V_2) + ((K_1 + V_1') \otimes K_2) = (K_1 \otimes V_2) + (V_1 \otimes K_2)\end{aligned}$$

De même,

$$(K_1 \otimes V_2') \oplus (V_1 \oplus K_2) = (K_1 \otimes V_2) + (V_1 \otimes K_2)\,.$$

□

2.3 Isomorphismes canoniques

A partir de maintenant tous les espaces vectoriels considérés seront de dimension finie.

Rappelons que, si V, W sont des espaces vectoriels, $\mathcal{L}(V; W)$ désigne l'espace des applications linéaires de V dans W. Si $V_1, \ldots, V_p, W$ sont des espaces vectoriels, $\mathcal{L}_p(V_1, \ldots, V_p; W)$ désigne l'espace de applications p-linéaires de $V_1 \times \cdots \times V_p$ dans W.

Proposition 2.15. *Soient $V_1, \ldots, V_p, W$ des espaces vectoriels sur $\mathbb{K}$ (de dimension finie). Alors*

$$\mathcal{L}_p(V_1, \ldots, V_p; W) \simeq \mathcal{L}(V_1 \otimes \cdots \otimes V_p; W)\,.$$

Démonstration. Rappelons l'application $\iota : V_1 \times \cdots \times V_p \to V_1 \otimes \cdots \otimes V_p$ défini par

$$\iota(v_1, \ldots, v_p) = v_1 \otimes \cdots \otimes v_p\,.$$

Si $f : V_1 \otimes \cdots \otimes V_p \to W$ est une application linéaire, alors $\varphi(f) = f \circ \iota : V_1 \times \cdots \times V_p \to W$ est une application p-linéaire. L'application $\varphi : \mathcal{L}(V_1 \otimes \cdots \otimes V_p; W) \to \mathcal{L}_p(V_1, \ldots, V_p; W)$ ainsi définie est clairement linéaire.

Rappelons (voir Théorème 2.1) que, si $g : V_1 \times \cdots \times V_p \to W$ est une application p-linéaire, il existe une unique application linéaire $\tilde{g} : V_1 \otimes \cdots \otimes V_p \to W$ telle que $\tilde{g} \circ \iota = g$, c'est-à-dire $\varphi(\tilde{g}) = g$. Ceci montre que φ est une bijection. □

Corollaire 2.16. *Soient $V_1, \ldots, V_p$ des espaces vectoriels sur $\mathbb{K}$. Alors*

$$(V_1 \otimes \cdots \otimes V_p)^* \simeq \mathcal{L}_p(V_1, \ldots, V_p; \mathbb{K})\,.$$

Théorème 2.17. *Soient $V, V_1, \ldots, V_p, W$ des espaces vectoriels sur $\mathbb{K}$. Alors*

(1) $(V_1 \otimes \cdots \otimes V_p)^* \simeq V_1^* \otimes \cdots \otimes V_p^*$;

(2) $\mathcal{L}(V;W) \simeq V^* \otimes W$;

(3) $\mathcal{L}_p(V_1, \ldots, V_p; W) \simeq \mathcal{L}(V_1 \otimes \cdots \otimes V_p; W) \simeq V_1^* \otimes \cdots \otimes V_p^* \otimes W$.

Démonstration. On commence par démontrer (1). Soit $(f_1, \ldots, f_p) \in V_1^* \times \cdots \times V_p^*$. On définit $\Phi_1(f_1, \ldots, f_p) : V_1 \times \cdots \times V_p \to \mathbb{K}$ par

$$\Phi_1(f_1, f_2, \ldots, f_p)(v_1, v_2, \ldots, v_p) = f_1(v_1) \cdot f_2(v_2) \cdots f_p(v_p)\,,$$

pour tout $(v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p$. On observe que $\Phi_1(f_1, \ldots, f_p)$ est p-linéaire, donc induit une application linéaire $\Phi_2(f_1, \ldots, f_p) : V_1 \otimes \cdots \otimes V_p \to \mathbb{K}$.

Montrons que $\Phi_2 : V_1^* \times \cdots \times V_p^* \to (V_1 \otimes \cdots \otimes V_p)^*$ est p-linéaire. Soient $i \in \{1, \ldots, p\}$, $f_1 \in V_1^*, \ldots f_{i-1} \in V_{i-1}^*$, $f_i, f_i' \in V_i^*$, $f_{i+1} \in V_{i+1}^*, \ldots, f_p \in V_p^*$, et $t, t' \in \mathbb{K}$. Pour tout $(v_1, \ldots, v_p) \in V_1 \times \cdots \times V_p$ on a

$$\begin{aligned}
&\Phi_1(f_1, \ldots, f_{i-1}, tf_i + t'f_i', f_{i+1}, \ldots, f_p)(v_1, \ldots, v_{i-1}v_i, v_{i+1}, \ldots v_p)\\
&= f_1(v_1) \cdots f_{i-1}(v_{i-1})(tf_i + t'f_i')(v_i) f_{i+1}(v_{i+1}) \cdots f_p(v_p)\\
&= t\big(f_1(v_1) \cdots f_{i-1}(v_{i-1}) f_i(v_i) f_{i+1}(v_{i+1}) \cdots f_p(v_p)\big)\\
&\qquad + t'\big(f_1(v_1) \cdots f_{i-1}(v_{i-1}) f_i'(v_i) f_{i+1}(v_{i+1}) \cdots f_p(v_p)\big)\\
&= t\Phi_1(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p)(v_1, \ldots, v_{i-1}v_i, v_{i+1}, \ldots v_p)\\
&\qquad + t'\Phi_1(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)(v_1, \ldots, v_{i-1}v_i, v_{i+1}, \ldots v_p)\\
&= \big(t\Phi_1(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p) + t'\Phi_1(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)\big)\\
&\qquad (v_1, \ldots, v_{i-1}v_i, v_{i+1}, \ldots v_p)
\end{aligned}$$

donc

$$\begin{aligned}
\Phi_1(f_1, \ldots, f_{i-1}, tf_i + t'f_i', f_{i+1}, \ldots, f_p) = t\Phi_1(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p)&\\
+ t'\Phi_1(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)&\,.
\end{aligned}$$

On applique cette égalité à Φ_2 comme suit

$$\begin{aligned}
&\Phi_2(f_1, \ldots, f_{i-1}, tf_i + t'f_i', f_{i+1}, \ldots, f_p) \circ \iota\\
=&\Phi_1(f_1, \ldots, f_{i-1}, tf_i + t'f_i', f_{i+1}, \ldots, f_p)\\
=&t\Phi_1(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p) + t'\Phi_1(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)\\
=&t(\Phi_2(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p) \circ \iota) + t'(\Phi_2(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p) \circ \iota)\\
=&(t\Phi_2(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p) + t'\Phi_2(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)) \circ \iota
\end{aligned}$$

Par l'unicité du relèvement, on en conclue que

$$\begin{aligned}
\Phi_2(f_1, \ldots, f_{i-1}, tf_i + t'f_i', f_{i+1}, \ldots, f_p) = t\Phi_2(f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_p)&\\
+ t'\Phi_2(f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_p)&\,.
\end{aligned}$$

Donc, Φ_2 induit une application linéaire $\Phi : V_1^* \otimes \cdots \otimes V_p^* \to (V_1 \otimes \cdots \otimes V_p)^*$. Reste à montrer que Φ es bijective.

Pour tout $i \in \{1, \ldots, p\}$ on se donne une base B_i de V_i et on note B_i^* la base duale de B_i. Par le théorème 2.3, l'ensemble $\tilde{B} = \{e_1 \otimes \cdots \otimes e_p; (e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p\}$ est une base de $V_1 \otimes \cdots \otimes V_p$ et $\tilde{B}' = \{e_1^* \otimes \cdots \otimes e_p^*; (e_1^*, \ldots, e_p^*) \in B_1^* \times \cdots \times B_p^*\}$ est une base de $V_1^* \otimes \cdots \otimes V_p^*$. On note $\tilde{B}^*$ la base duale de $\tilde{B}$.

Soit $(e_1, \ldots, e_p) \in B_1 \times \cdots \times B_p$. Pour $i \in \{1, \ldots, p\}$, on note e_i^* l'élément de B_i^* tel que $e_i^*(e_i) = 1$ et $e_i^*(e_i') = 0$ pour $e_i' \in B_i$, $e_i' \neq e_i$. Pour $(e_1', \ldots, e_p') \in B_1 \times \cdots \times B_p$ on a

$$\Phi_1(e_1^*, \ldots, e_p^*)(e_1', \ldots, e_p') = e_1^*(e_1') \cdots e_p^*(e_p') = \begin{cases} 1 & \text{si } (e_1, \ldots, e_p) = (e_1', \ldots, e_p') \\ 0 & \text{si } (e_1, \ldots, e_p) \neq (e_1', \ldots, e_p') \end{cases}$$

$$\Rightarrow \Phi_2(e_1^*, \ldots, e_p^*)(e_1' \otimes \cdots \otimes e_p') = \begin{cases} 1 & \text{si } (e_1, \ldots, e_p) = (e_1', \ldots, e_p') \\ 0 & \text{si } (e_1, \ldots, e_p) \neq (e_1', \ldots, e_p') \end{cases}$$

$$\Rightarrow \Phi(e_1^* \otimes \cdots \otimes e_p^*)(e_1' \otimes \cdots \otimes e_p') = \begin{cases} 1 & \text{si } (e_1, \ldots, e_p) = (e_1', \ldots, e_p') \\ 0 & \text{si } (e_1, \ldots, e_p) \neq (e_1', \ldots, e_p') \end{cases}$$

D'où

$$\Phi(e_1^* \otimes \cdots \otimes e_p^*) = (e_1 \otimes \cdots \otimes e_p)^* .$$

Ceci montre que Φ envoie bijectivement $\tilde{B}'$ sur $\tilde{B}^*$, donc que Φ est un isomorphisme linéaire.

Maintenant on démontre (2). Soit $\Phi_1 : V^* \times W \to \mathcal{L}(V; W)$ l'application définie par

$$\Phi_1(f, w) : \begin{array}{ccc} V & \to & W \\ v & \mapsto & f(v)w \end{array}$$

pour $(f, w) \in V^* \times W$. On vérifie facilement que Φ_1 est bilinéaire, donc induit une application linéaire $\Phi : V^* \otimes W \to \mathcal{L}(V; W)$. On va montrer que Φ est un isomorphisme.

Soient B_V une base de V et B_W une base de W. On note B_V^* la base duale de B_V. Alors $\tilde{B} = \{e^* \otimes f; (e^*, f) \in B_V^* \times B_W\}$ est une base de $V^* \otimes W$. Par ailleurs, pour tout $(e, f) \in B_V \times B_W$ il existe une unique application linéaire $\varphi_{e,f} : V \to W$ telle que

$$\varphi_{e,f}(e') = \begin{cases} f & \text{si } e' = e \\ \vec{0} & \text{si } e' \neq e \end{cases}$$

pour tout $e' \in B_V$. Il est bien connu que l'ensemble $\tilde{B}' = \{\varphi_{e,f}; (e, f) \in B_V \times B_W\}$ est une base de $\mathcal{L}(V, W)$.

Soit $(e, f) \in B_V \times B_W$. Pour tout $e' \in B_V$ on a

$$\Phi(e^* \otimes f)(e') = e^*(e')f = \begin{cases} f & \text{si } e' = e \\ \vec{0} & \text{si } e' \neq e \end{cases}$$

D'où $\Phi(e^*, f) = \varphi_{e,f}$. Ceci montre que Φ envoie bijectivement $\tilde{B}$ sur $\tilde{B}'$, donc est un isomorphisme linéaire.

(3) est une conséquence directe de (1) et (2). En effet,

$$\begin{aligned}\mathcal{L}_p(V_1, \ldots, V_p; W) \simeq \mathcal{L}(V_1 \otimes \cdots \otimes V_p; W) \simeq (V_1 \otimes \cdots \otimes V_p)^* \otimes W \\ \simeq V_1^* \otimes \cdots \otimes V_p^* \otimes W\,.\end{aligned}$$

□

Proposition 2.18. *Soit V un espace vectoriel sur $\mathbb{K}$.*

(1) *L'application* $\mathrm{Tr} : \mathcal{L}(V) = V^* \otimes V \to \mathbb{K}$ *définie par*

$$\mathrm{Tr}(\alpha \otimes v) = \alpha(v)$$

est une forme linéaire sur $\mathcal{L}(V)$.

(2) *Soient $f, g \in \mathcal{L}(V)$. Alors*

$$\mathrm{Tr}(f \circ g) = \mathrm{Tr}(g \circ f)\,.$$

(3) *Soient $B = \{e_1, \ldots, e_n\}$ une base de V, $f \in \mathcal{L}(V)$ et $M = (m_{i,j})_{1 \le i,j \le n}$ la matrice de f dans la base B. Alors*

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} m_{i,i}\,.$$

Définition. Soit V un espace vectoriel sur $\mathbb{K}$. La forme linéaire $\mathrm{Tr} : \mathcal{L}(V) \to \mathbb{K}$ de la proposition 2.18 s'appelle la *trace* sur V.

Démonstration. L'application $\varphi : V^* \times V \to \mathbb{K}$ définie par

$$\varphi(\alpha, v) = \alpha(v)$$

est une application bilinéaire. Elle induit donc une application linéaire $\mathrm{Tr} : V^* \otimes V \to \mathbb{K}$.

Soient $B = \{e_1, \ldots, e_n\}$ une base de V et $B^* = \{e_1^*, \ldots, e_n^*\}$ la base duale de B. Pour tous $i, j \in \{1, \ldots, n\}$ on définie l'endomorphisme $\varphi_{i,j} : V \to V$ par

$$\varphi_{i,j}(e_k) = \begin{cases} \vec{e_j} & \text{si } k = i \\ 0 & \text{si } k \neq i \end{cases}$$

Rappelons que $\varphi_{i,j}$ s'identifie à $e_i^* \otimes e_j$ par l'isomorphisme $\mathcal{L}(V) \simeq V^* \otimes V$. En particulier,

$$\mathrm{Tr}(\varphi_{i,j}) = e_i^*(e_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Soient $i, j, k, l \in \{1, \ldots, n\}$. Pour tout $r \in \{1, \ldots, n\}$ on a

$$(\varphi_{i,j} \circ \varphi_{k,l})(e_r) = \begin{cases} \vec{e_j} & \text{si } r = k \text{ et } l = i \\ \vec{0} & \text{sinon} \end{cases}$$

donc

$$\varphi_{i,j} \circ \varphi_{k,l} = \begin{cases} \varphi_{k,j} & \text{si } l = i \\ 0 & \text{si } l \neq i \end{cases}$$

On en déduit que

$$\mathrm{Tr}(\varphi_{i,j} \circ \varphi_{k,l}) = \mathrm{Tr}(\varphi_{k,l} \circ \varphi_{i,j}) = \begin{cases} 1 & \text{si } l = i \text{ et } k = j \\ 0 & \text{sinon} \end{cases}$$

Soient $f \in \mathcal{L}(V)$ et $M = (m_{i,j})_{1 \leq i,j \leq n}$ la matrice de f dans la base B. On a

$$f = \sum_{i=1}^{n} \sum_{j=1}^{n} m_{i,j} \varphi_{i,j} \,,$$

donc

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} \sum_{j=1}^{n} m_{i,j} \mathrm{Tr}(\varphi_{i,j}) = \sum_{i=1}^{n} m_{i,i} \,.$$

Soient $f, g \in \mathcal{L}(V)$. Soient $M = (m_{i,j})_{1 \leq i,j \leq n}$ et $M' = (m'_{i,j})_{1 \leq i,j \leq n}$ les matrices de f, g dans la base B, respectivement. Alors

$$\begin{aligned} \mathrm{Tr}(f \circ g) &= \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} \sum_{l=1}^{n} m_{i,j} m'_{k,l} \mathrm{Tr}(\varphi_{i,j} \circ \varphi_{k,l}) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{n} m'_{k,l} m_{i,j} \mathrm{Tr}(\varphi_{k,l} \circ \varphi_{i,j}) \\ &= \mathrm{Tr}(g \circ f) \,. \end{aligned}$$

□

3 Algèbres

3.1 Définitions et rappels

Définition. Un ensemble A muni de deux opérations internes $+, \cdot$ et d'une opération externe $\mathbb{K} \times A \to A$, $(t, a) \mapsto t\,a$ est une *algèbre* sur $\mathbb{K}$ si :

(a) $(A, +, \cdot)$ est un anneau unitaire (l'unité sera notée 1_A) ;

(b) $(A, +,)$ est un espace vectoriel sur $\mathbb{K}$;

(c) $(ta) \cdot b = a \cdot (tb) = t(a \cdot b)$ pour tous $a, b \in A$ et $t \in \mathbb{K}$.

Définition. Soient A, B deux algèbres sur $\mathbb{K}$. Une application $f : A \to B$ est un *homomorphisme d'algèbres* si :

(a) f est un homomorphisme d'anneaux (en particulier, on a $f(1_A) = 1_B$) ;

(b) f est une application linéaire ;

Un homomorphisme bijectif est un *isomorphisme*. Dans ce cas la réciproque $f^{-1} : B \to A$ est un homomorphisme d'algèbres.

Définition. Soit A une algèbre sur $\mathbb{K}$. Un *idéal à gauche* de A est une partie $I \subset A$ telle que :

(a) $(I, +)$ est un sous-groupe de $(A, +)$;

(b) $a \cdot b \in I$ pour tous $a \in A$ et $b \in I$.

De même, un *idéal à droite* est une partie $I \subset A$ telle que

(a) $(I, +)$ est un sous-groupe de $(A, +)$;

(b) $a \cdot b \in I$ pour tous $a \in I$ et $b \in A$.

Un *idéal bilatère* est un idéal à gauche et à droite.

Lemme 3.1. *Soient A une algèbre sur $\mathbb{K}$ et I un idéal à gauche de A. Alors I est un sous-espace vectoriel de A.*

Démonstration. Exercice. □

Lemme 3.2. *Soit $f : A \to B$ un homomorphisme d'algèbres.*

(1) *Le noyau de f est un idéal bilatère de A.*

(2) *f est injectif si et seulement si* $\operatorname{Ker} f = \{0_A\}$.

Démonstration. Exercice. □

Soient A une algèbre sur $\mathbb{K}$ et I un idéal bilatère de A. On définit sur A/I des opérations internes $+, \cdot$ et une opération externe $\mathbb{K} \times A/I \to A/I$, $(t, \bar{a}) \mapsto t\bar{a}$ par :

$$\bar{a} + \bar{b} = \overline{a + b}\,,\ \bar{a} \cdot \bar{b} = \overline{a \cdot b}\,,\ t\bar{a} = \overline{ta}\,.$$

Lemme 3.3. *Soient A une algèbre sur $\mathbb{K}$ et I un idéal bilatère. Les opérations $+, \cdot$ et la multiplication externe sur A/I sont bien définies. A/I muni de ces opérations est une algèbre sur $\mathbb{K}$. L'application quotient $\mu : A \to A/I$ est un homomorphisme surjectif.*

Démonstration. Exercice. □

Théorème 3.4. *Soient A, B deux algèbres, I un idéal bilatère de A et $f : A \to B$ un homomorphisme tels que $I \subset \operatorname{Ker} f$.*

(1) *Il existe un unique homomorphisme $\bar{f} : A/I \to B$ tel que $f = \bar{f} \circ \mu$, c'est-à-dire le diagramme suivant commute,*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\mu"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

où $\mu : A \to A/I$ désigne l'homomorphisme quotient.

(2) $\operatorname{Im} f$ *est une sous-algèbre de B, et $\bar{f} : A/I \to \operatorname{Im} f$ est un un homomorphisme surjectif. C'est un isomorphisme si et seulement si $I = \operatorname{Ker} f$.*

Démonstration. Exercice. □

Remarque. Soit A une algèbre sur $\mathbb{K}$. On pose

$$\begin{array}{rccc} m : & A \times A & \to & A \\ & (a, b) & \mapsto & a \cdot b \end{array}$$

Alors m est une application bilinéaire. En effet, si $a_1, a_2, b \in A$ et $t_1, t_2 \in \mathbb{K}$, alors

$$m(t_1 a_1 + t_2 a_2, b) = (t_1 a_1 + t_2 a_2) \cdot b = t_1(a_1 \cdot b) + t_2(a_2 \cdot b) = t_1 m(a_1, b) + t_2 m(a_2, b)\,.$$

De même, si $a, b_1, b_2 \in A$ et $t_1, t_2 \in \mathbb{K}$, alors

$$m(a, t_1 b_1 + t_2 b_2) = t_1 m(a, b_1) + t_2 m(a, b_2)\,.$$

D'où m induit une application linéaire $\tilde{m} : A \otimes A \to A$.

Proposition 3.5. *Soit A un espace vectoriel et $\tilde{m} : A \otimes A \to A$ une application linéaire. On définit une multiplication $\cdot$ sur A par*

$$a \cdot b = \tilde{m}(a \otimes b)\,.$$

Alors A muni des opérations $+, \cdot$ et de la multiplication externe est une algèbre si et seulement si

(a)
$$\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_A) = \tilde{m} \circ (\mathrm{Id}_A \otimes \tilde{m}) \,.$$

(b) *Il existe* $1_A \in A$ *tel que*
$$\tilde{m}(1_A \otimes a) = \tilde{m}(a \otimes 1_A) = a$$
pour tout $a \in A$.

Démonstration. Soit A une algèbre sur $\mathbb{K}$. Soit $\tilde{m} : A \otimes A \to A$ définie comme avant. Si $a, b, c \in A$, alors
$$\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_A)(a \otimes b \otimes c) = (a \cdot b) \cdot c = a \cdot (b \cdot c) = \tilde{m} \circ (\mathrm{Id}_A \otimes \tilde{m})(a \otimes b \otimes c) \,,$$
donc
$$\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_A) = \tilde{m} \circ (\mathrm{Id}_A \otimes \tilde{m}) \,.$$
Par ailleurs, si $a \in A$, alors
$$\tilde{m}(1_A \otimes a) = (1_A \cdot a) = a \quad \text{et} \quad \tilde{m}(a \otimes 1_A) = (a \cdot 1_A) = a \,.$$

Maintenant on se donne un espace vectoriel A et $\tilde{m} : A \otimes A \to A$ une application linéaire vérifiant (a) et (b). Soit $\cdot$ l'opération interne définie comme avant. On sait déjà que A muni de $+$ et de la multiplication externe est un espace vectoriel. Montrons que $(A, +, \cdot)$ est un anneau.

Comme A est un espace vectoriel, $(A, +)$ est un groupe abélien.

Soient $a, b, c \in A$. Alors
$$(a \cdot b) \cdot c = \tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_A)(a \otimes b \otimes c) = \tilde{m} \circ (\mathrm{Id}_A \otimes \tilde{m})(a \otimes b \otimes c) = a \cdot (b \cdot c) \,.$$

Soit $a \in A$. Alors
$$(1_A \cdot a) = \tilde{m}(1_A \otimes a) = a \quad \text{et} \quad (a \cdot 1_A) = \tilde{m}(a \otimes 1_A) = a \,.$$

Soient $a, b, c \in A$. Alors
$$\begin{aligned}(a + b) \cdot c = \tilde{m}((a + b) \otimes c) = \tilde{m}((a \otimes c) + (b \otimes c)) = \tilde{m}(a \otimes c) + \tilde{m}(b \otimes c)& \\ = (a \cdot c) + (b \cdot c) \,.&\end{aligned}$$

De même, on a $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$.

Finalement, si $a, b \in A$ et $t \in \mathbb{K}$, alors
$$(ta) \cdot b = \tilde{m}((ta) \otimes b) = \tilde{m}(t(a \otimes b)) = t\,\tilde{m}(a \otimes b) = t(a \cdot b) \,.$$
De même, $a \cdot (tb) = t(a \cdot b)$. On en conclue que A est une algèbre sur $\mathbb{K}$. □

3.2 Exemples

Exemple 1 : On note $M_n(\mathbb{K})$ l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{K}$. Alors $M_n(\mathbb{K})$ est une algèbre sur $\mathbb{K}$. L'ensemble des éléments inversibles de $M_n(\mathbb{K})$ est le groupe linéaire $\mathrm{GL}_n(\mathbb{K})$. Remarquez qu'il existe un plongement naturel

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) & \to & \mathrm{GL}_{n+1}(\mathbb{K}) \\ A & \mapsto & \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \end{array}$$

Par contre, il n'existe pas d'homomorphisme injectif naturel $M_n(\mathbb{K}) \to M_{n+1}(\mathbb{K})$.

Exemple 2 : Soit G un groupe. On note $\mathbb{K}[G]$ l'espace vectoriel sur $\mathbb{K}$ ayant G comme base. On définit une application linéaire $\tilde{m} : \mathbb{K}[G] \otimes \mathbb{K}[G] \to \mathbb{K}[G]$ par

$$\tilde{m}(g_1 \otimes g_2) = g_1 g_2$$

pour tout $(g_1, g_2) \in G \times G$.

Lemme 3.6. *Soit $\cdot$ l'opération interne sur $\mathbb{K}[G]$ induite $\tilde{m}$. Alors $\mathbb{K}[G]$ muni des opérations internes $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$.*

Démonstration. Soient $g_1, g_2, g_3 \in G$. Alors

$$\tilde{m} \circ (\mathrm{Id} \otimes \tilde{m})(g_1 \otimes g_2 \otimes g_3) = g_1(g_2 g_3) = (g_1 g_2) g_3 = \tilde{m} \circ (\tilde{m} \otimes \mathrm{Id})(g_1 \otimes g_2 \otimes g_3)\,.$$

Comme $\{g_1 \otimes g_2 \otimes g_3; (g_1, g_2, g_3) \in G \times G \times G\}$ est une base de $\mathbb{K}[G] \otimes \mathbb{K}[G] \otimes \mathbb{K}[G]$, on en déduit que $\tilde{m} \circ (\mathrm{Id} \otimes \tilde{m}) = \tilde{m} \circ (\tilde{m} \otimes \mathrm{Id})$.

Notons 1_G l'élément neutre de G. Pour tout $g \in G$ on a

$$\tilde{m}(1_G \otimes g) = 1_G \cdot g = g\,.$$

Comme G est une base de $\mathbb{K}[G]$, on en déduit que $\tilde{m}(1_G \otimes a) = a$ pour tout $a \in \mathbb{K}[G]$. De même, $\tilde{m}(a \otimes 1_G) = a$ pour tout $a \in \mathbb{K}[G]$. □

Définition. Soit G un groupe. Alors $\mathbb{K}[G]$ s'appelle *l'algèbre de groupe* G.

Exemple 3 :

Définition. Un *monoïde* est un ensemble M muni d'une opération $\cdot$ vérifiant :

(a) La loi $\cdot$ est *associative*, c'est-à-dire : pour tous $m_1, m_2, m_3 \in M$ on a

$$(m_1 \cdot m_2) \cdot m_3 = m_1 \cdot (m_2 \cdot m_3)\,.$$

(b) M a un *élément neutre*, c'est à dire : il existe $1_M \in M$ tel que

$$1_M \cdot m = m \cdot 1_M = m$$

pour tout $m \in M$.

On dit que M est un *groupe* si, de plus,

(c) tout élément de M a un *inverse*, c'est-à-dire : pour tout $m \in M$ il existe $m' \in M$ tel que

$$m \cdot m' = m' \cdot m = 1_G\,.$$

Soit M un monoïde. On note $\mathbb{K}[M]$ l'espace vectoriel sur $\mathbb{K}$ ayant M comme base. On définit une application linéaire $\tilde{m} : \mathbb{K}[M] \otimes \mathbb{K}[M] \to \mathbb{K}[M]$ par

$$\tilde{m}(m_1 \otimes m_2) = m_1 m_2$$

pour tout $(m_1, m_2) \in M \times M$.

Lemme 3.7. *Soit $\cdot$ l'opération interne sur $\mathbb{K}[M]$ induite $\tilde{m}$. Alors $\mathbb{K}[M]$ muni des opérations internes $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$.*

Démonstration. Exercice. □

Définition. Soit M un monoïde. Alors $\mathbb{K}[M]$ s'appelle *l'algèbre de monoïde M*.

Exemple 4 : On note $\mathcal{N}_1$ la version "multiplicative" de $\mathbb{N}$. C'est-à-dire $\mathcal{N}_1$ est l'ensemble

$$\mathcal{N}_1 = \{1, X, X^2, X^3, \dots\}\,,$$

muni de l'opération $\cdot$ définie par

$$X^n \cdot X^m = X^{n+m}\,.$$

C'est clairement un monoïde, donc $\mathbb{K}[\mathcal{N}_1]$ est une algèbre. Elle s'appelle *l'algèbre des polynômes* à une variable, X, et elle se note $\mathbb{K}[X]$. Remarquez que $\mathcal{N}_1$ étant une base de $\mathbb{K}[X]$, tout élément $P \in \mathbb{K}[X]$ s'écrit de façon unique sous la forme

$$P = t_0 + t_1 X + \cdots + t_n X^n\,,$$

où $t_0, \cdots, t_n \in \mathbb{K}$ et $t_n \neq 0$.

Exemple 5 : On se donne un entier $m \geq 1$ et, à l'instar de $\mathbb{N}$, on écrit $\mathbb{N}^m$ multiplicativement. C'est-à-dire, on considère l'ensemble

$$\mathcal{N}_m = \{X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m} ; (a_1, \dots, a_m) \in \mathbb{N}^m\}$$

que l'on munit de l'opération $\cdot$ définie par

$$X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m} \cdot X_1^{b_1} X_2^{b_2} \cdots X_m^{b_m} = X_1^{a_1+b_1} X_2^{a_2+b_2} \cdots X_m^{a_m+b_m} .$$

C'est clairement un monoïde, donc $\mathbb{K}[\mathcal{N}_m]$ est une algèbre. Elle s'appelle *l'algèbre des polynômes* à m variables, $X_1, \ldots, X_m$, et elle se note $\mathbb{K}[X_1, \ldots, X_m]$. On utilisera les notations suivantes. Si $X = (X_1, \ldots, X_m)$ et $a = (a_1, \ldots, a_m) \in \mathbb{N}^m$, on pose

$$X^a = X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m} .$$

Comme $\mathcal{N}_m$ est une base de $\mathbb{K}[X_1, \ldots, X_m]$, si $P \in \mathbb{K}[X_1, \ldots, X_m]$, alors il existe un sous-ensemble fini $I \subset \mathbb{N}^m$ tel que

$$P = \sum_{a \in I} t_a X^a .$$

Cette écriture est unique si l'on impose $t_a \neq 0$ pour tout $a \in I$.

3.3 Produit tensoriel d'algèbres

Théorème 3.8. *Soient $\mathbb{K}$ un corps et A, B deux algèbres sur $\mathbb{K}$. Il existe une opération interne $\cdot$ sur $A \otimes B$ de sorte que :*

(a) *$A \otimes B$ muni des lois $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$;*

(b) *$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 \cdot a_2) \otimes (b_1 \cdot b_2)$ pour tous $a_1, a_2 \in A$ et $b_1, b_2 \in B$;*

(c) *L'élément neutre pour $\cdot$ dans $A \otimes B$ est $1_{A \otimes B} = 1_A \otimes 1_B$;*

(d) *Les applications*

$$\begin{array}{rccc} \iota_A : & A & \to & A \otimes B \\ & a & \mapsto & a \otimes 1_B \end{array} \qquad \begin{array}{rccc} \iota_B : & B & \to & A \otimes B \\ & b & \mapsto & 1_A \otimes b \end{array}$$

sont des homomorphismes injectifs.

Démonstration. Soit

$$\begin{array}{rccc} m : & A \times B \times A \times B & \to & A \otimes B \\ & (a_1, b_1, a_2, b_2) & \mapsto & (a_1 \cdot a_2) \otimes (b_1 \cdot b_2) \end{array}$$

On vérifie facilement que m est 4-linéaire. D'où m induit une application linéaire

$$\tilde{m} : (A \otimes B) \otimes (A \otimes B) \to A \otimes B .$$

On définit une opération $\cdot$ sur $A \otimes B$ par

$$u_1 \cdot u_2 = \tilde{m}(u_1 \otimes u_2) .$$

Par la proposition 3.5, pour démontrer que $A \otimes B$ muni des lois $+, \cdot$ et de la multiplication externe est une algèbre, il suffit de montrer :

(a)

$$\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_{A\otimes B}) = \tilde{m} \circ (\mathrm{Id}_{A\otimes B} \otimes \tilde{m}) .$$

(b) Il existe $1_{A\otimes B} \in A \otimes B$ tel que

$$\tilde{m}(1_{A\otimes B} \otimes u) = \tilde{m}(u \otimes 1_{A\otimes B}) = u$$

pour tout $u \in A \otimes B$.

Soient $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$. Alors

$$\begin{aligned} &\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_{A\otimes B})((a_1 \otimes b_1) \otimes (a_2 \otimes b_2) \otimes (a_3 \otimes b_3)) = ((a_1 \cdot a_2) \cdot a_3) \otimes ((b_1 \cdot b_2) \cdot b_3) \\ &= (a_1 \cdot (a_2 \cdot a_3)) \otimes (b_1 \cdot (b_2 \cdot b_3)) = \tilde{m} \circ (\mathrm{Id}_{A\otimes B} \otimes \tilde{m})((a_1 \otimes b_1) \otimes (a_2 \otimes b_2) \otimes (a_3 \otimes b_3)) \end{aligned}$$

Comme l'ensemble $\{(a_1 \otimes b_1) \otimes (a_2 \otimes b_2) \otimes (a_3 \otimes b_3); (a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B\}$ engendre $(A \otimes B) \otimes (A \otimes B) \otimes (A \otimes B)$, on en déduit que

$$\tilde{m} \circ (\tilde{m} \otimes \mathrm{Id}_{A\otimes B}) = \tilde{m} \circ (\mathrm{Id}_{A\otimes B} \otimes \tilde{m}) .$$

Posons $1_{A\otimes B} = 1_A \otimes 1_B$. pour $(a, b) \in A \times B$ on a

$$\tilde{m}(1_{A\otimes B} \otimes (a \otimes b)) = (1_A \cdot a) \otimes (1_B \cdot b) = a \otimes b .$$

Comme $\{a \otimes b; (a, b) \in A \times B\}$ engendre $A \otimes B$, on en déduit que

$$\tilde{m}(1_{A\otimes B} \otimes u) = u$$

pour tout $u \in A \otimes B$. De même, $\tilde{m}(u \otimes 1_{A\otimes B}) = u$ pour tout $u \in A \otimes B$.

Les parties (b) et (c) découlent immédiatement de la construction de la multiplication dans $A \otimes B$. Reste à démontrer (c).

On voit facilement que l'application

$$\begin{array}{rccc} \iota_A : & A & \to & A \otimes B \\ & a & \mapsto & a \otimes 1_B \end{array}$$

est un homomorphisme d'algèbres. De plus, comme $1_B \neq 0_B$, par le corollaire 2.6 (2), $\mathrm{Ker}\, \iota_A = \{0_A\}$, c'est-à-dire ι_A est injectif. $\square$

Définition. Soit E un ensemble fini. On note $F(E)$ l'espace des applications de E dans $\mathbb{K}$. Pour tout $x \in E$ on définit $\delta_x \in F(E)$ par

$$\delta_x(y) = \begin{cases} 1 & \text{si } y = x \\ 0 & \text{si } y \neq x \end{cases}$$

Rappelons que $F(E)$ est un espace vectoriel de dimension $\operatorname{card} E$, et $\{\delta_x ; x \in E\}$ est une base de $F(E)$. Par ailleurs, on définit sur $F(E)$ une multiplication interne $\cdot$ par

$$(f \cdot g)(x) = f(x) \cdot g(x)\,,$$

pour tout $x \in E$.

Lemme 3.9. *Soit E un ensemble fini. Alors $F(E)$ muni des opérations internes $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$. L'élément neutre pour la multiplication est l'application $1_{F(E)} : E \to \mathbb{K}$, $x \mapsto 1_{\mathbb{K}}$.*

Démonstration. Exercice. $\square$

Lemme 3.10. *Soient E et E' deux ensembles finis. Alors $F(E \times E') \simeq F(E) \otimes F(E')$.*

Démonstration. Soit $\varphi : F(E) \times F(E') \to F(E \times E')$ l'application définie par

$$\varphi(f, f')(x, x') = f(x) \cdot f'(x')\,.$$

Il est évident que φ est bilinéaire, donc induit une application linéaire $\Phi : F(E) \otimes F(E') \to F(E \times E')$. On va montrer que Φ est un isomorphisme.

Soient $(f_1, f_1'), (f_2, f_2') \in F(E) \times F(E')$. Pour tout $(x, x') \in E \times E'$ on a

$$\begin{aligned}
\Phi((f_1 \otimes f_1') \cdot (f_2 \otimes f_2'))(x, x') =& \Phi((f_1 \cdot f_2) \otimes (f_1' \cdot f_2'))(x, x') \\
=& f_1(x) f_2(x) f_1'(x') f_2'(x') \\
=& \Phi(f_1 \otimes f_1')(x, x') \cdot \Phi(f_2 \otimes f_2')(x, x') \\
=& (\Phi(f_1 \otimes f_1') \cdot \Phi(f_2 \otimes f_2'))(x, x')
\end{aligned}$$

donc

$$\Phi((f_1 \otimes f_1') \cdot (f_2 \otimes f_2')) = \Phi(f_1 \otimes f_1') \cdot \Phi(f_2 \otimes f_2')\,.$$

Soient $u, v \in F(E) \otimes F(E')$. Les éléments u et v s'écrivent sous la forme

$$u = \sum_{i=1}^{n} a_i (f_i \otimes f_i')\,, \quad v = \sum_{j=1}^{m} b_j (g_j \otimes g_j')\,,$$

où $a_i, b_j \in \mathbb{K}$ et $(f_i, f_i'), (g_j, g_j') \in F(E) \times F(E')$ pour tous $i \in \{1, \ldots, n\}$ et $j \in \{1, \ldots, m\}$.

Alors

$$\begin{aligned}
\Phi(u\cdot v) =&\Phi\left(\sum_{i=1}^{n}\sum_{j=1}^{m} a_ib_j(f_i\otimes f_i')\cdot(g_j\otimes g_j')\right)\\
=&\sum_{i=1}^{n}\sum_{j=1}^{m} a_ib_j\Phi((f_i\otimes f_i')\cdot(g_j\otimes g_j'))\\
=&\sum_{i=1}^{n}\sum_{j=1}^{m} a_ib_j\Phi(f_i\otimes f_i')\cdot\Phi(g_j\otimes g_j')\\
=&\left(\sum_{i=1}^{n} a_i\Phi(f_i\otimes f_i')\right)\cdot\left(\sum_{j=1}^{m} b_j\Phi(g_j\otimes g_j')\right)\\
=&\Phi(u)\cdot\Phi(v)\,.
\end{aligned}$$

Pour $(x,x')\in E\times E'$ on a

$$\Phi(1_{F(E)}\otimes 1_{F(E')})(x,x') = 1_{F(E)}(x)\cdot 1_{F(E')}(x') = 1_{\mathbb{K}} = 1_{F(E\times E')}(x,x')\,,$$

donc $\Phi(1_{F(E)}\otimes 1_{F(E')}) = 1_{F(E\times E')}$. On en conclue que Φ est un homomorphisme d'algèbres.

Il reste à démontrer que Φ est bijectif. Comme $\{\delta_x; x\in E\}$ est une base de $F(E)$ et $\{\delta_{x'}; x'\in E'\}$ est une base de $F(E')$, par la proposition 2.3, $B=\{\delta_x\otimes\delta_{x'}; (x,x')\in E\times E'\}$ est une base de $F(E)\otimes F(E')$. Par ailleurs, $\tilde{B}=\{\delta_{(x,x')}; (x,x')\in E\times E'\}$ est une base de $F(E\times E')$. On vérifie facilement que

$$\Phi(\delta_x\otimes\delta_{x'}) = \delta_{(x,x')}$$

pour tout $(x,x')\in E\times E'$, donc Φ est un isomorphisme (linéaire). $\square$

Proposition 3.11. *Soient M, M' deux monoïdes. Alors $\mathbb{K}[M]\otimes\mathbb{K}[M']\simeq\mathbb{K}[M\times M']$.*

Démonstration. Les applications

$$\begin{array}{rccc} \iota: & M & \to & M\times M' \\ & g & \mapsto & (g,1_{M'}) \end{array} \qquad \begin{array}{rccc} \iota': & M' & \to & M\times M' \\ & g' & \mapsto & (1_M,g') \end{array}$$

sont des homomorphismes injectifs (de monoïdes), et induisent des homomorphismes d'algèbres injectifs

$$\iota:\mathbb{K}[M]\to\mathbb{K}[M\times M'] \quad \text{et} \quad \iota':\mathbb{K}[M']\to\mathbb{K}[M\times M']\,.$$

Soit $\varphi: K[M]\times\mathbb{K}[M']$ l'application définie par

$$\varphi(u,u') = \iota(u)\cdot\iota'(u')\,.$$

On observe que φ est bilinéaire, donc induit une application linéaire $\Phi : \mathbb{K}[M] \otimes \mathbb{K}[M'] \to \mathbb{K}[M \times M']$. On va montrer que Φ est un isomorphisme.

Soient $(g_1, g_1'), (g_2, g_2') \in M \times M'$. Alors

$$\begin{aligned}\Phi((g_1 \otimes g_1') \cdot (g_2 \otimes g_2')) =&\Phi((g_1 g_2) \otimes (g_1' g_2')) \\ =&(g_1 g_2, g_1' g_2') \\ =&(g_1, g_1') \cdot (g_2, g_2') \\ =&\Phi(g_1 \otimes g_1') \cdot \Phi(g_2 \otimes g_2')\end{aligned}$$

Soient $u, v \in \mathbb{K}[M] \otimes \mathbb{K}[M']$. Comme $\{g \otimes g'; (g, g') \in M \times M'\}$ est une base de $\mathbb{K}[M] \otimes \mathbb{K}[M']$, u, v s'écrivent sous la forme

$$u = \sum_{i=1}^{m} a_i (f_i \otimes f_i') , \quad v = \sum_{j=1}^{m} b_j (g_j \otimes g_j') ,$$

où $a_i, b_j \in \mathbb{K}$ et $(f_i, f_i'), (g_j, g_j') \in M \times M'$ pour tous $i \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$. Alors

$$\begin{aligned}\Phi(u \cdot v) =&\Phi \left(\sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j (f_i \otimes f_i')(g_j \otimes g_j') \right) \\ =&\sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j \Phi((f_i \otimes f_i')(g_j \otimes g_j')) \\ =&\sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j \Phi(f_i \otimes f_i') \cdot \Phi(g_j \otimes g_j') \\ =&\left(\sum_{i=1}^{m} a_i \Phi(f_i \otimes f_i') \right) \cdot \left(\sum_{j=1}^{n} b_j \Phi(g_j \otimes g_j') \right) \\ =&\Phi(u) \cdot \Phi(v) .\end{aligned}$$

Comme, par ailleurs, $\Phi(1_M \otimes 1_{M'}) = (1_M, 1_{M'})$, ceci montre que Φ est un homomorphisme d'algèbres.

L'ensemble $\{g \otimes g'; (g, g') \in M \times M'\}$ est une base de $\mathbb{K}[M] \otimes \mathbb{K}[M']$, l'ensemble $M \times M'$ est une base de $\mathbb{K}[M \times M']$, et $\Phi(g \otimes g') = (g, g')$ pour tout $(g, g') \in M \times M'$, donc Φ est un isomorphisme (linéaire). $\square$

Corollaire 3.11. *Soit $m \in \mathbb{N}$. Alors*

$$\mathbb{K}[X_1, X_2, \ldots, X_m] \simeq \mathbb{K}[X_1] \otimes \mathbb{K}[X_2] \otimes \cdots \otimes \mathbb{K}[X_m] .$$

Démonstration. Rappelons que $\mathcal{N}_m$ désigne la version multiplicative de $\mathbb{N}^m$. Il est clair que $\mathcal{N}_m = \mathcal{N}_1 \times \mathcal{N}_1 \times \cdots \times \mathcal{N}_1$, donc

$$\begin{aligned}\mathbb{K}[X_1, X_2, \ldots, X_m] = \mathbb{K}[\mathcal{N}_m] = \mathbb{K}[\mathcal{N}_1 \times \mathcal{N}_1 \times \cdots \times \mathcal{N}_1] &\simeq \mathbb{K}[\mathcal{N}_1] \otimes \mathbb{K}[\mathcal{N}_1] \otimes \cdots \otimes \mathbb{K}[\mathcal{N}_1] \\ &= \mathbb{K}[X_1] \otimes \mathbb{K}[X_2] \otimes \cdots \otimes \mathbb{K}[X_m]\,.\end{aligned}$$

□

Rappelons que, si V est un espace vectoriel, alors $\mathcal{L}(V)$ muni des lois internes $+, \circ$ et de la multiplication externe est une algèbre sur $\mathbb{K}$.

Proposition 3.12. *Soient V et W deux espaces vectoriels sur $\mathbb{K}$. Alors on a l'isomorphisme d'algèbres $\mathcal{L}(V) \otimes \mathcal{L}(W) \simeq \mathcal{L}(V \otimes W)$.*

Démonstration. Soit $\Phi_1 : \mathcal{L}(V) \times \mathcal{L}(W) \to \mathcal{L}(V \otimes W)$ l'application définie par

$$\Phi_1(f, g) = f \otimes g\,.$$

On vérifie facilement que Φ_1 est bilinéaire, donc induit une application linéaire $\Phi : \mathcal{L}(V) \otimes \mathcal{L}(W) \to \mathcal{L}(V \otimes W)$. On va montrer que Φ est un isomorphisme d'algèbres.

Soient $(f, g), (f', g') \in \mathcal{L}(V) \times \mathcal{L}(W)$. Alors

$$\begin{aligned}\Phi(f \otimes g) \circ \Phi(f' \otimes g') = (f \otimes g) \circ (f' \otimes g') &= (f \circ f') \otimes (g \circ g') \\ &= \Phi((f \circ f') \otimes (g \circ g')) = \Phi((f \otimes g) \cdot (f' \otimes g'))\,.\end{aligned}$$

Soient $U, U' \in \mathcal{L}(V) \otimes \mathcal{L}(W)$. Il existe $(f_1, g_1), \ldots, (f_p, g_p) \in \mathcal{L}(V) \times \mathcal{L}(W)$ et $t_1, \ldots, t_p \in \mathbb{K}$ tels que

$$U = \sum_{i=1}^{p} t_i (f_i \otimes g_i)\,.$$

De même, il existe $(f'_1, g'_1), \ldots, (f'_q, g'_q) \in \mathcal{L}(V) \otimes \mathcal{L}(W)$ et $t'_1, \ldots, t'_q \in \mathbb{K}$ tels que

$$U' = \sum_{j=1}^{q} t'_j (f'_j \otimes g'_j)\,.$$

Alors

$$\begin{aligned}
\Phi(U)\circ\Phi(U') =& \Phi\left(\sum_{i=1}^{p} t_i(f_i\otimes g_i)\right)\circ\Phi\left(\sum_{j=1}^{q} t'_j(f'_j\otimes g'_j)\right)\\
=&\sum_{i=1}^{p}\sum_{j=1}^{q} t_it'_j(\Phi(f_i\otimes g_i)\circ\Phi(f'_j\otimes g'_j))\\
=&\sum_{i=1}^{p}\sum_{j=1}^{q} t_it'_j(\Phi((f_i\otimes g_i)\cdot(f'_j\otimes g'_j))\\
=&\Phi\left(\left(\sum_{i=1}^{p} t_i(f_i\otimes g_i)\right)\cdot\left(\sum_{j=1}^{q} t'_j(f'_j\otimes g'_j)\right)\right)\\
=&\Phi(U\cdot U')\,.
\end{aligned}$$

Ceci montre que Φ est un homomorphisme d'algèbres.

Soient $B=\{e_1,\dots,e_n\}$ une base de V et $B'=\{e'_1,\dots,e'_m\}$ une base de W. Pour tous $i,j\in\{1,\dots,n\}$ on note $\varphi_{i,j}:V\to V$ l'application linéaire définie par

$$\varphi_{i,j}(e_r)=\begin{cases} e_j & \text{si } i=r\\ \vec{0} & \text{si } r\neq i\end{cases}$$

De même, pour $k,l\in\{1,\dots,m\}$, on note $\psi_{k,l}:W\to W$ l'endomorphisme linéaire défini par

$$\psi_{k,l}(e'_s)=\begin{cases} e'_l & \text{si } s=k\\ \vec{0} & \text{si } s\neq k\end{cases}$$

L'ensemble $\{\varphi_{i,j};i,j\in\{1,\dots,n\}\}$ est une base de $\mathcal{L}(V)$ et $\{\psi_{k,l};k,l\in\{1,\dots,m\}\}$ est une base de $\mathcal{L}(W)$, donc $\tilde{B}=\{\varphi_{i,j}\otimes\psi_{k,j};i,j\in\{1,\dots,n\}$ et $k,l\in\{1,\dots m\}\}$ est une base de $\mathcal{L}(V)\otimes\mathcal{L}(W)$. Par ailleurs, l'ensemble $\{e_i\otimes e'_k;i\in\{1,\dots,n\}$ et $k\in\{1,\dots,m\}\}$ est une base de $V\otimes W$. Pour tous $i,j\in\{1,\dots,n\}$ et $k,l\in\{1,\dots,m\}$ on note $\rho_{i,j,k,l}:V\otimes W\to V\otimes W$ l'application linéaire définie par

$$\rho_{i,j,k,l}(e_r\otimes e'_s)=\begin{cases} e_j\otimes e'_l & \text{si } i=r \text{ et } k=s\\ \vec{0} & \text{sinon}\end{cases}$$

L'ensemble $\tilde{B}'=\{\rho_{i,j,k,l};i,j\in\{1,\dots,n\}$ et $k,l\in\{1,\dots,m\}\}$ est une base de $\mathcal{L}(V\otimes W)$. Soient $i,j\in\{1,\dots,n\}$ et $k,l\in\{1,\dots,m\}$. Pour $r\in\{1,\dots,n\}$ et $s\in\{1,\dots,m\}$ on a

$$\Phi(\varphi_{i,j}\otimes\psi_{k,l})(e_r\otimes e'_s)=(\varphi_{i,j}(e_r))\otimes(\psi_{k,l}(e'_s))=\begin{cases} e_j\otimes e'_l & \text{si } i=r \text{ et } k=s\\ \vec{0} & \text{sinon}\end{cases}$$

donc

$$\Phi(\varphi_{i,j}\otimes\psi_{k,l})=\rho_{i,j,k,l}\,.$$

On en conclue que Φ envoie bijectivement $\tilde{B}$ sur $\tilde{B}'$, donc est un isomorphisme. $\square$

4 Algèbres de polynômes

4.1 Généralités sur les algèbres de polynômes

Proposition 4.1. *Soient A une algèbre commutative sur $\mathbb{K}$ et $x_1, \ldots, x_m$ m éléments de A. Alors il existe un homomorphisme $\varphi : \mathbb{K}[X_1, \ldots, X_m] \to A$ qui envoie X_i sur x_i pour tout $i \in \{1, \ldots, m\}$.*

Démonstration. Soit $f : \mathcal{N}_m \to A$ l'application définie par

$$f(X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m}) = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} .$$

Comme $\mathcal{N}_m$ est une base de $\mathbb{K}[X_1, \ldots, X_m]$, l'application f induit une application linéaire $\varphi : \mathbb{K}[X_1, \ldots X_n] \to A$. Si $P = \sum_{a \in I} t_a X^a$, alors

$$\varphi(P) = \sum_{a \in I} t_a f(X^a) .$$

Si $a = (a_1, \ldots, a_m)$ et $b = (b_1, \ldots, b_m)$ sont dans $\mathbb{N}^m$, alors

$$f(X^a) \cdot f(X^b) = x_1^{a_1} \cdots x_m^{a_m} \cdot x_1^{b_1} \cdots x_m^{b_m} = x_1^{a_1+b_1} \cdots x_m^{a_m+b_m} = f(X^{a+b}) .$$

En utilisant cette égalité on démontre facilement que $\varphi(P_1) \cdot \varphi(P_2) = \varphi(P_1 \cdot P_2)$ pour tous $P_1, P_2 \in \mathbb{K}[X_1, \ldots, X_m]$. On en conclut que φ est un homomorphisme d'algèbres. $\square$

Définition. Soient A une algèbre et $x_1, \ldots, x_m \in A$. La sous-algèbre *engendrée* par $x_1, \ldots, x_m$ est la plus petite sous-algèbre de A contenant $x_1, \ldots, x_m$. On dit que A est *finiment engendrée* si elle est engendrée par un nombre fini d'éléments (i.e. il existe $m \in \mathbb{N}$ et $x_1, \ldots, x_m \in A$ tels que la sous-algèbre de A engendrée par $x_1, \ldots, x_m$ soit A elle-même).

Lemme 4.2. *Soient A une algèbre commutative et $x_1, \ldots, x_m \in A$. Soit $\varphi : \mathbb{K}[X_1, \ldots, X_m] \to A$ l'homomorphisme qui envoie X_i sur x_i pour tout $i \in \{1, \ldots, m\}$. Alors $\operatorname{Im} \varphi$ est la sous-algèbre de A engendrée par $x_1, \ldots, x_m$.*

Démonstration. Exercice. $\square$

Théorème 4.3. *Toute algèbre commutative finiment engendrée est isomorphe au quotient d'une algèbre de polynômes.*

Démonstration. Soit A une algèbre finiment engendrée. Soient $x_1, \ldots, x_m$ tels que A est engendrée par $x_1, \ldots, x_m$. Soit $\varphi : \mathbb{K}[X_1, \ldots, X_m] \to A$ l'homomorphisme qui envoie X_i sur x_i pour tout $i \in \{1, \ldots, m\}$. Posons $I = \operatorname{Ker} \varphi$. Alors φ induit un homomorphisme injectif $\bar{\varphi} : \mathbb{K}[X_1, \ldots, X_m]/I \to A$. Comme A est engendrée par $x_1, \ldots, x_m$, on a $\operatorname{Im} \varphi = \operatorname{Im} \bar{\varphi} = A$, donc $\bar{\varphi}$ est aussi surjectif, c'est-à-dire est un isomorphisme. $\square$

Définition. Pour $a = (a_1, \dots, a_m) \in \mathbb{N}^m$ on pose

$$|a| = a_1 + \cdots + a_m .$$

On dit qu'un polynôme $P \in \mathbb{K}[X_1, \dots, X_m]$ est *homogène de degré d* s'il s'écrit sous la forme

$$P = \sum_{a \in I} t_a X^a ,$$

où I est une partie finie de $\mathbb{N}^m$ telle que $|a| = d$ pour tout $a \in I$. Remarquons que le polynôme nul 0 est homogène de degré d pour tout $d \in \mathbb{N}$. Remarquons aussi que tout polynôme $P \in \mathbb{K}[X_1, \dots, X_m] \neq 0$ s'écrit de façon unique sous la forme

$$P = P_0 + P_1 + \cdots + P_d ,$$

où P_i est homogène de degré i pour tout $i \in \{1, \dots, d\}$ et $P_d \neq 0$. Le nombre d s'appelle le *degré* de P et se note deg P. On conviendra que le degré de 0 est $-\infty$.

Lemme 4.4. *Soient $P_1, P_2 \in \mathbb{K}[X_1, \dots, X_m]$ deux polynômes homogènes de degrés d_1, d_2, respectivement.*

(1) *Si $d_1 = d_2$, alors $t_1 P_1 + t_2 P_2$ est homogène de degré $d_1 = d_2$ pour tous $t_1, t_2 \in \mathbb{K}$.*

(2) *$P_1 \cdot P_2$ est homogène de degré $d_1 + d_2$.*

Démonstration. Exercice. □

Lemme 4.5. *Soient $P, P' \in \mathbb{K}[X_1, \dots, X_m]$ deux polynômes homogènes non nuls. Alors $P \cdot P' \neq 0$.*

Démonstration. On raisonne par récurrence sur m. Supposons d'abord que $m = 1$. Soient d, d' les degrés de P, P', respectivement. Alors P et P' sont de la forme $P = tX_1^d$ et $P' = t'X_1^{d'}$, où $t, t' \in \mathbb{K} \setminus \{0\}$. On a

$$P \cdot P' = (tt')X^{d+d'} \neq 0$$

car $tt' \neq 0$.

On suppose maintenant que $m \geq 2$ plus l'hypothèse de récurrence. On commence par faire l'observation suivante. Soit d le degré de P. Alors P s'écrit

$$P = P_0 + P_1 X_m + \cdots + P_k X_m^k ,$$

où $k \in \{0, \dots, d\}$, $P_i \in \mathbb{K}[X_1, \dots, X_{m-1}]$ est homogène de degré $d - i$ pour tout $i \in \{0, 1, \dots, k\}$ et $P_k \neq 0$. De même, si d' désigne le degré de P', on peut écrire P' sous la forme

$$P' = P'_0 + P'_1 X_m + \cdots + P'_{k'} X_m^{k'} ,$$

où $k' \in \{0,1,\ldots,d'\}$, $P'_i \in \mathbb{K}[X_1,\ldots,X_{m-1}]$ est homogène de degré $d'-i$ pour tout $i \in \{0,1,\ldots,k'\}$ et $P'_{k'} \neq 0$. On a

$$P \cdot P' = H_0 + H_1 X_m + \cdots + H_{k+k'} X_m^{k+k'}\,,$$

où

$$H_i = \sum_{j+j'=i} P_j P'_{j'}\,, \quad i \in \{0,\ldots,k+k'\}\,.$$

Par hypothèse de récurrence $H_{k+k'} = P_k P'_k$ est homogène de degré $d+d'-k-k'$ et est non nul, donc $P \cdot P' \neq 0$. □

Proposition 4.6. *Soient P, P' deux polynômes de degrés d, d', respectivement.*

(1) $\deg(P+P') \leq \max\{\deg P, \deg P'\}$.

(2) *Si P et P' son non nuls, alors $P \cdot P'$ est non nul et* $\deg(P \cdot P') = \deg P \cdot \deg P'$.

Démonstration. Posons $k = \max\{\deg P, \deg P'\}$. Alors P et P' s'écrivent sous la forme

$$P = P_0 + P_1 + \cdots + P_k \quad \text{et} \quad P' = P'_0 + P'_1 + \cdots + P'_k\,,$$

où P_i et P'_i sont homogènes de degré i pour tout $i \in \{0,1,\ldots,k\}$. On a

$$P + P' = (P_0 + P'_0) + (P_1 + P'_1) + \cdots + (P_k + P'_k)\,,$$

et $P_i + P'_i$ est homogène de degré i pour tout $i \in \{0,1,\ldots,k\}$. On en déduit que

$$\deg(P+P') \leq k = \max\{\deg P, \deg P'\}\,.$$

Supposons maintenant que P et P' son non nuls. Soient $d = \deg P$ et $d' = \deg P'$. On écrit

$$P = P_0 + P_1 + \cdots + P_d \quad \text{et} \quad P' = P'_0 + P'_1 + \cdots + P'_{d'}\,,$$

où P_i et P'_j son homogènes de degré i et j, respectivement, pour $i \in \{0,1,\ldots,d\}$ et $j \in \{0,1,\ldots,d'\}$, $P_d \neq 0$ et $P'_{d'} \neq 0$. On a

$$P \cdot P' = H_0 + H_1 \cdots + H_{d+d'}\,,$$

où

$$H_i = \sum_{j+j'=i} P_j P'_{j'}$$

est homogène de degré i pour tout $i \in \{0,1,\ldots,d+d'\}$. Par le lemme 4.5, $H_{d+d'} = P_d P'_{d'}$ est non nul, donc PP' est non nul et son degré est $d+d'$. □

Définition. On dit qu'une algèbre A est *intègre* si, pour tous $a, b \in A$, l'égalité $ab = 0$ implique $a = 0$ ou $b = 0$.

Corollaire 4.7. *L'algèbre* $\mathbb{K}[X_1, \ldots, X_m]$ *est intègre.* $\square$

Définition. Soit A une algèbre. On dit que $a \in A$ est une *unité* si $a \neq 0$ et s'il existe $b \in A$ tel que $ab = ba = 1_A$. L'ensemble des unités de A forme un groupe noté $\mathcal{U}(A)$.

Corollaire 4.8. *On a* $\mathcal{U}(\mathbb{K}[X_1, \ldots, X_m]) = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Démonstration. Il est clair que tout élément de $\mathbb{K}^*$ est inversible dans $\mathbb{K}[X_1, \ldots, X_m]$. Réciproquement, soit $P \in \mathcal{U}(\mathbb{K}[X_1, \ldots, X_m])$. Il existe $Q \in \mathbb{K}[X_1 \ldots, X_m]$ tel que $PQ = QP = 1$. Comme $PQ \neq 1$, on doit avoir $P \neq 0$ et $Q \neq 0$. Par ailleurs, par la proposition 4.6,

$$\deg P + \deg Q = \deg 1 = 0\,,$$

donc $\deg P = \deg Q = 0$, donc $P, Q \in \mathbb{K} \setminus \{0\}$. $\square$

4.2 Algèbres graduées

Définition. Soit A une algèbre sur $\mathbb{K}$. Une *graduation* de A est une décomposition de A comme somme directe

$$A = \bigoplus_{n=0}^{\infty} A_n\,,$$

où A_n est un sous-espace vectoriel de A pour tout $n \in \mathbb{N}$, et

$$A_p \cdot A_q \subset A_{p+q}$$

pour tous $p, q \in \mathbb{N}$. Une *algèbre graduée* est une algèbre munie d'une graduation.

Lemme 4.9. *Soit* $A = \oplus_{n=0}^{\infty} A_n$ *une algèbre graduée.*

(1) A_0 *est une sous-algèbre de* A.

(2) *Soit* $n \in \mathbb{N}$. *Alors le sous-espace* $I_n = \oplus_{k=n}^{\infty} A_k$ *est un idéal bilatère de* A.

Démonstration. Exercice. $\square$

Exemple 1. Soit $A = \mathbb{K}[X_1, \ldots, X_m]$ l'agèbre des polynômes en les variables $X_1, \ldots, X_m$. Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X_1, \ldots, X_m]$ l'espaces des polynômes homogènes de degré n. Alors

$$\mathbb{K}[X_1, \ldots, X_m] = \bigoplus_{n=0}^{\infty} \mathbb{K}_n[X_1, \ldots, X_m]$$

est une graduation de $\mathbb{K}[X_1, \ldots, X_m]$. Remarquez que $\mathbb{K}_0[X_1, \ldots X_m] = \mathbb{K}$.

Exemple 2. Soit V un espace vectoriel de dimension finie. On définit $V^{\otimes n}$ par récurrence sur n comme suit.

- $V^{\otimes 0} = \mathbb{K}$ et $V^{\otimes 1} = V$;
- si $n \geq 2$, alors $V^{\otimes n} = V^{\otimes(n-1)} \otimes V$.

Remarquons que, si $p, q \in \mathbb{N}^*$, $u \in V^{\otimes p}$ et $v \in V^{\otimes q}$, alors $u \otimes v \in V^{\otimes(p+q)}$. Si $p = 0$ on posera $u \otimes v = u \cdot v \in V^{\otimes q}$, et si $q = 0$, on posera $u \otimes v = v \cdot u \in V^{\otimes p}$. On pose

$$A = \bigoplus_{n=0}^{\infty} V^{\otimes n}$$

et on définit une opération $\cdot$ sur A comme suit. Soit $a, b \in A$. On écrit

$$a = u_0 + u_1 + \cdots + u_p \text{ et } b = v_0 + v_1 + \cdots + v_q \,,$$

où $p, q \in \mathbb{N}$, $u_i \in V^{\otimes i}$ pour tout $i \in \{1, \ldots, p\}$ et $v_j \in V^{\otimes j}$ pour tout $j \in \{1, \ldots, m\}$. Alors

$$a \cdot b = \sum_{k=0}^{p+q} \left(\sum_{i+j=k} u_i \otimes v_j \right) .$$

On peut vérifier que A muni des opérations internes $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$, et que $A = \oplus_{n=0}^{\infty} V^{\otimes n}$ est une graduation de A. Cette algèbre s'appelle *l'algèbre tensorielle de V*.

Proposition 4.10. *Soient $A = \oplus_{n=0}^{\infty} A_n$ et $B = \oplus_{n=0}^{\infty} B_n$ deux algèbres graduées. Alors $A \otimes B$ admet la graduation (naturelle) $A \otimes B = \oplus_{n=0}^{\infty} C_n$ où*

$$C_n = \bigoplus_{i+j=n} A_i \otimes B_j \,,$$

pour tout $n \in \mathbb{N}$.

Démonstration. On a

$$\begin{aligned} A \otimes B = \left(\bigoplus_{i=0}^{\infty} A_i \right) \otimes \left(\bigoplus_{j=0}^{\infty} B_j \right) &= \bigoplus_{i=0}^{\infty} \left(A_i \otimes \left(\bigoplus_{j=0}^{\infty} B_j \right) \right) \\ = \bigoplus_{i=0}^{\infty} \bigoplus_{j=0}^{\infty} A_i \otimes B_j &= \bigoplus_{k=0}^{\infty} \left(\bigoplus_{i+j=k} A_i \otimes B_j \right) = \bigoplus_{k=0}^{\infty} C_k \,. \end{aligned}$$

Soient $i, j, k, l \in \mathbb{N}$, $a_i \in A_i$, $a_j \in A_j$, $b_k \in B_k$, et $b_l \in B_l$. Alors

$$(a_i \otimes b_k) \cdot (a_j \otimes b_l) = (a_i \cdot a_j) \otimes (b_k \cdot b_l) \in A_{i+j} \otimes B_{k+l} \,.$$

Comme l'ensemble $\{a_i \otimes b_k; (a_i, b_k) \in A_i \times B_k\}$ engendre $A_i \otimes B_k$ et $\{a_j \otimes b_l; (a_j, b_l) \in A_j \times B_l\}$ engendre $A_j \otimes B_l$, on en déduit que

$$(A_i \otimes B_k) \cdot (A_j \otimes B_l) \subset (A_{i+j} \otimes B_{k+l}) \,.$$

On en conclue que $C_p \cdot C_q \subset C_{p+q}$ pour tous $p, q \in \mathbb{N}$. $\square$

Définition. Une *série formelle* à coefficients dans $\mathbb{K}$ est une somme (formelle) infinies

$$\sum_{k=0}^{\infty} a_k T^k ,$$

où $a_k \in \mathbb{K}$ pour tout $k \in \mathbb{N}$. On note $\mathbb{K}[\![T]\!]$ l'ensemble des séries formelles à coefficients dans $\mathbb{K}$. On définie une somme est un produit externe sur $\mathbb{K}[\![T]\!]$ par :

$$(\sum_{k=0}^{\infty} a_k T^k) + (\sum_{k=0}^{\infty} b_k T^k) = \sum_{k=0}^{\infty} (a_k + b_k) T^k$$
$$t(\sum_{k=0}^{\infty} a_k T^k) = \sum_{k=0}^{\infty} (t a_k) T^k$$

L'ensemble $\mathbb{K}[\![T]\!]$ muni de ces deux opérations est un espace vectoriel sur $\mathbb{K}$. On définit aussi une multiplication interne $\cdot$ dans $\mathbb{K}[\![T]\!]$ par

$$(\sum_{i=0}^{\infty} a_i T^i) \cdot (\sum_{j=0}^{\infty} b_j T^j) = \sum_{n=0}^{\infty} c_n T^n ,$$

où

$$c_n = \sum_{i+j=n} a_i b_j .$$

L'ensemble $\mathbb{K}[\![T]\!]$ muni des opérations $+, \cdot$ et de la multiplication externe est une algèbre sur $\mathbb{K}$.

Définition. Soit $A = \oplus_{n=0}^{\infty} A_n$ une algèbre graduée telle que A_n soit de dimension finie pour tout $n \in \mathbb{N}$. La *série de Hilbert-Poincaré* de A est la série formelle dans $\mathbb{R}[\![T]\!]$:

$$\mathrm{Hilb}(A) = \sum_{n=0}^{\infty} \dim(A_n) T^n .$$

Lemme 4.11. *Soient $A = \oplus_{n=0}^{\infty} A_n$ et $B = \oplus_{n=0}^{\infty} B_n$ deux algèbres graduées telles que A_n et B_n soient de dimension finie pour tout $n \in \mathbb{N}$. Alors*

$$\mathrm{Hilb}(A \otimes B) = \mathrm{Hilb}(A) \cdot \mathrm{Hilb}(B) .$$

Démonstration. Rappelons que la graduation de $A \otimes B$ est $A \otimes B = \oplus_{n=0}^{\infty} C_n$, où $C_n = \oplus_{i+j=n} A_i \otimes B_j$. Alors

$$\begin{aligned}
\mathrm{Hilb}(A \otimes B) =& \sum_{n=0}^{\infty} \dim(C_n) T^n \\
=& \sum_{n=0}^{\infty} \sum_{i+j=n} \dim(A_i \otimes B_j) T^n \\
=& \sum_{n=0}^{\infty} \sum_{i+j=n} \dim(A_i) \cdot \dim(B_j) T^n \\
=& \left(\sum_{i=0}^{\infty} \dim(A_i) T^i \right) \left(\sum_{j=0}^{\infty} \dim(B_j) T^j \right) \\
=& \mathrm{Hilb}(A) \cdot \mathrm{Hilb}(B) .
\end{aligned}$$

□

Corollaire 4.12.

$$\mathrm{Hilb}(\mathbb{K}[X_1, \ldots, X_m]) = \frac{1}{(1-T)^m} .$$

Démonstration. On a $\dim \mathbb{K}_d[X] = 1$ pour tout $d \in \mathbb{N}$, donc

$$\mathrm{Hilb}(\mathbb{K}[X]) = \sum_{d=0}^{\infty} T^d = \frac{1}{1-T} .$$

Il s'en suit que

$$\begin{aligned}
\mathrm{Hilb}(\mathbb{K}[X_1, \ldots, X_m]) = \mathrm{Hilb}(\mathbb{K}[X_1] \otimes \cdots \otimes \mathbb{K}[X_m]) = \mathrm{Hilb}(\mathbb{K}[X_1]) \cdots \mathrm{Hilb}(\mathbb{K}[X_m]) \\
= \frac{1}{(1-T)^m} .
\end{aligned}$$

□

Rappelons que, si $d, m \in \mathbb{N}$ sont tels que $d \leq m$, alors

$$C_m^d = \frac{m!}{d!(m-d)!} .$$

Lemme 4.13. *Soient $m, d \in \mathbb{N}$. Alors*

$$\sum_{k=0}^{d} C_{m+k}^{m} = C_{m+1+d}^{m+1} .$$

Démonstration. Rappelons que, si $1 \le d \le m$, alors

$$C_m^d + C_m^{d-1} = C_{m+1}^d .$$

Cette formule est facile à démontrer et est laissée en exercice.

Maintenant on démontre le lemme 4.13 par récurrence sur d. Si $d = 0$, alors

$$\sum_{k=0}^{d} C_{m+k}^m = C_m^m = 1 = C_{m+1}^{m+1} .$$

Supposons que $d \ge 1$ plus l'hypothèse de récurrence. Alors

$$\sum_{k=0}^{d} C_{m+k}^m = \sum_{k=0}^{d-1} C_{m+k}^m + C_{m+d}^m = C_{m+d}^{m+1} + C_{m+d}^m = C_{m+1+d}^{m+1} .$$

□

Proposition 4.14. *Pour tout $d \in \mathbb{N}$ on a*

$$\dim \mathbb{K}_d[X_1, \ldots, X_m] = C_{m-1+d}^{m-1} .$$

Démonstration. Par le corollaire 4.12 il suffit de montrer que

$$\frac{1}{(1-T)^m} = \sum_{d=0}^{\infty} C_{m-1+d}^{m-1} T^d .$$

On raisonne par récurrence sur m. Si $m = 1$, alors

$$\frac{1}{1-T} = \sum_{d=0}^{\infty} T^d = \sum_{d=0}^{\infty} C_d^0 T^d .$$

Supposons que $m \ge 1$ plus l'hypothèse de récurrence. Alors

$$\begin{aligned}\frac{1}{(1-T)^m} = \frac{1}{(1-T)^{m-1}} \cdot \frac{1}{1-T} &= \left(\sum_{k=0}^{\infty} C_{m-2+k}^{m-2} T^k \right) \left(\sum_{l=0}^{\infty} T^l \right) \\ &= \sum_{d=0}^{\infty} \left(\sum_{k=0}^{d} C_{m-2+k}^{m-2} \right) T^d = \sum_{d=0}^{\infty} C_{m-1+d}^{m-1} T^d .\end{aligned}$$

□

4.3 Fonctions polynomiales

On note $\mathcal{F}(\mathbb{K}^m;\mathbb{K})$ l'ensemble des applications de $\mathbb{K}^m$ dans $\mathbb{K}$. On munit $\mathcal{F}(\mathbb{K}^m;\mathbb{K})$ des opérations internes $+, \cdot$ et de la multiplication externe définies par :

$$(f+g)(u) = f(u) + g(u)\,, \quad (f\cdot g)(u) = f(u)\cdot g(u)\,, \quad (tf)(u) = t\cdot f(u)\,,$$

pour tous $f, g \in \mathcal{F}(\mathbb{K}^m;\mathbb{K})$, $t \in \mathbb{K}$ et $u \in \mathbb{K}^m$. Il est clair que $\mathcal{F}(\mathbb{K}^m;\mathbb{K})$ muni de ces opérations est une algèbre commutative sur $\mathbb{K}$.

On a un homomorphisme d'algèbres $\varphi : \mathbb{K}[X_1,\dots,X_m] \to \mathcal{F}(\mathbb{K}^m;\mathbb{K})$ défini comme suit. Si $u = (u_1,\dots,u_m) \in \mathbb{K}^m$ et $a = (a_1,\dots,a_m) \in \mathbb{N}^m$, on pose

$$u^a = u_1^{a_1} u_2^{a_2} \cdots u_m^{a_m}\,.$$

Si $P = \sum_{a\in I} t_a X^a \in \mathbb{K}[X_1,\dots,X_m]$, alors

$$\varphi(P)(u) = \sum_{a\in I} u^a\,,$$

pour tout $u \in \mathbb{K}^m$. Remarquons que l'on note souvent $P(u)$ à la place de $\varphi(P)(u)$.

Définition. L'algèbre $\operatorname{Im}\varphi$ s'appelle *l'algèbre des fonctions polynomiales* (sur $\mathbb{K}$ à m variables).

Lemme 4.15.

(1) *Soient $A \subset \mathbb{K}$ une partie infinie de $\mathbb{K}$ et $P \in \mathbb{K}[X_1,\dots,X_m]$. Si $\varphi(P)_{A^m} = 0$, alors $P = 0$.*

(2) *L'homomorphisme $\varphi : \mathbb{K}[X_1,\dots,X_m] \to \mathcal{F}(\mathbb{K}^m;\mathbb{K})$ est injectif si et seulement si $\mathbb{K}$ est infini.*

Démonstration. On démontre (1) par récurrence sur m. Supposons que $m = 1$. On a un ensemble infini $A \subset \mathbb{K}$ et un polynôme $P \in \mathbb{K}[X]$ tel que $P(u) = 0$ pour tout $u \in A$. Comme P a une infinité de racines, il en résulte immédiatement que $P = 0$.

On suppose maintenant que $m \geq 2$ plus l'hypothèse de récurrence. On se donne un ensemble infini $A \subset \mathbb{K}$ et un polynôme $P \in \mathbb{K}[X_1,\dots,X_m]$ tels que $P(u) = 0$ pour tout $u \in A^m$. On écrit

$$P = P_0 + P_1 X_m + \cdots + P_d X_m^d\,,$$

où $P_0, P_1, \dots, P_d \in \mathbb{K}[X_1,\dots,X_{m-1}]$. On se fixe $(u_1,\dots,u_{m-1}) \in A^{m-1}$ et on considère le polynôme

$$Q = P_0(u_1,\dots,u_{m-1}) + P_1(u_1,\dots,u_{m-1})X + \cdots + P_d(u_1,\dots,u_{m-1})X^d \in \mathbb{K}[X]\,.$$

On a $Q(v) = P(u_1, \ldots, u_{m-1}, v) = 0$ pour tout $v \in A$, donc $Q = 0$, donc

$$P_0(u_1, \ldots, u_{m-1}) = P_1(u_1, \ldots, u_{m-1}) = \cdots = P_d(u_1, \ldots, u_{m-1}) = 0\,.$$

Comme cette égalité est vraie quel que soit $(u_1, \ldots, u_{m-1}) \in A^{m-1}$, par hypothèse de récurrence, on en déduit que

$$P_0 = P_1 = \cdots = P_d = 0\,,$$

donc que $P = 0$.

Supposons que $\mathbb{K}$ est infini. Par (1), si $P \in \operatorname{Ker}\varphi$, alors $P = 0$. Ceci montre que φ est injectif. Montrons que φ n'est pas injectif si $\mathbb{K}$ est fini.

On commence par traiter le cas $m = 1$. Posons $k = |\mathbb{K}|$. L'ensemble $\mathbb{K}^*$ est un groupe d'ordre $k-1$, donc $u^{k-1} = 1$ pour tout $u \in \mathbb{K}^*$, donc $u^k - u = 0$ pour tout $u \in \mathbb{K}^*$. On a aussi de façon évidente $0^k - 0 = 0$, donc tous les éléments de $\mathbb{K}$ sont racine du polynôme $X^k - X$, donc $(X^k - X) \in \operatorname{Ker}\varphi$. Si $m \geq 2$ alors, pour la même raison, $(X_1^k - X_1) \in \operatorname{Ker}\varphi$. □

Lemme 4.16. *On suppose que $\mathbb{K}$ est infini. Soient $\mathcal{H}$ une famille non vide de polynômes dans $\mathbb{K}[X_1, \ldots, X_m]$ et $W = \{v \in V = \mathbb{K}^m ; P(v) = 0$ pour tout $P \in \mathcal{H}\}$. Supposons que $V \setminus W$ est non vide. Si $Q \in \mathbb{K}[X_1, \ldots, X_m]$ est tel que $Q(v) = 0$ pour tout $v \in V \setminus W$, alors $Q = 0$.*

Démonstration. Pour tout $P \in \mathcal{H}$ et tout $v \in V$ on a $(PQ)(v) = P(v)\,Q(v) = 0$. Par le lemme 4.15 il s'en suit que $PQ = 0$ pour tout $P \in \mathcal{H}$. Comme $W \neq V$ il existe $P_0 \in \mathcal{H}$ tel que $P_0 \neq 0$. Comme $\mathbb{K}[X_1, \ldots, X_m]$ est intègre et $P_0 Q = 0$, on conclue que $Q = 0$. □

4.4 Formule de Taylor

On suppose dans ce paragraphe que $\mathbb{K}$ est de caractéristique 0.

Définition. Une *dérivation* de $\mathbb{K}[X_1, \ldots, X_m]$ est une application linéaire $D : \mathbb{K}[X_1, \ldots, X_m] \to \mathbb{K}[X_1, \ldots, X_m]$ vérifiant

$$D(PQ) = D(P)\,Q + P\,D(Q)\,,$$

pour tous $P, Q \in \mathbb{K}[X_1, \ldots, X_m]$. On note $\operatorname{Der}(\mathbb{K}[X_1, \ldots, X_m])$ l'ensemble des dérivations de $\mathbb{K}[X_1, \ldots, X_m]$. C'est un sous-espace vectoriel de $\mathcal{L}(\mathbb{K}[X_1, \ldots, X_m])$.

Exemple 1. Soit $i \in \{1, \ldots, m\}$. Si $a = (a_1, \ldots, a_m) \in \mathbb{N}^m$, on pose

$$\frac{\partial}{\partial X_i}(X^a) = \begin{cases} a_i\, X_1^{a_1} \cdots X_{i-1}^{a_{i-1}} X_i^{a_i - 1} X_{i+1}^{a_{i+1}} \cdots X_m^{a_m} & \text{si } a_i \neq 0 \\ 0 & \text{si } a_i = 0 \end{cases}$$

Si $P = \sum_{a\in I} t_a X^a \in \mathbb{K}[X_1, \ldots, X_m]$, on pose

$$\frac{\partial}{\partial X_i}(P) = \sum_{a\in I} t_a \frac{\partial}{\partial X_i}(X^a)\,.$$

On vérifie facilement que l'application $\frac{\partial}{\partial X_i} : \mathbb{K}[X_1, \ldots, X_m] \to \mathbb{K}[X_1, \ldots, X_m]$ est une dérivation.

Exemple 2. Soient $Q_1, \ldots, Q_m \in \mathbb{K}[X_1, \ldots, X_m]$. Alors l'application

$$\begin{array}{rccc} Q_1\frac{\partial}{\partial X_1} + \cdots + Q_m\frac{\partial}{\partial X_m} : & \mathbb{K}[X_1, \ldots, X_m] & \to & \mathbb{K}[X_1, \ldots, X_m] \\ & P & \mapsto & Q_1\frac{\partial}{\partial X_1}(P) + \cdots + Q_m\frac{\partial}{\partial X_m}(P) \end{array}$$

est une dérivation.

Proposition 4.17. *On a*

$$\mathrm{Der}(\mathbb{K}[X_1, \ldots, X_m]) = \bigoplus_{i=1}^{m} \mathbb{K}[X_1, \ldots, X_m]\,\frac{\partial}{\partial X_i}\,.$$

Démonstration. Exercice. $\square$

Définition. Pour $v = (v_1, \ldots, v_m) \in \mathbb{K}^m$ on pose

$$\Delta_v = v_1\frac{\partial}{\partial X_1} + \cdots + v_m\frac{\partial}{\partial X_m}\,.$$

C'est un élément de $\mathrm{Der}(\mathbb{K}[X_1, \ldots, X_m])$.

Lemme 4.18. *Soient $P \in \mathbb{K}[X_1, \ldots, X_m]$ un polynôme de degré d et $v \in \mathbb{K}^m$. Alors $\Delta_v^{d+1}(P) = 0$.*

Démonstration. On raisonne par récurrence sur d. Si P est constant (i.e. $\deg P \leq 0$), alors $\frac{\partial}{\partial X_i}P = 0$ pour tout $i \in \{1, \ldots, m\}$, donc $\Delta_v(P) = 0$. Supposons que $d \geq 1$ plus l'hypothèse de récurrence. On observe que $\Delta_v(P)$ est de degré $\leq d-1$. Par hypothèse de récurrence, il s'en suit que $\Delta_v^d(\Delta_v(P)) = \Delta_v^{d+1}(P) = 0$. $\square$

Lemme 4.19. *Soient $P \in \mathbb{K}[X_1, \ldots, X_m]$ un polynôme homogène de degré d et $v \in \mathbb{K}^m$. Alors, pour tout $k \in \mathbb{N}$, on a*

$$\Delta_v^k(P)(\overrightarrow{0}) = \begin{cases} 0 & \text{si } k \neq d \\ d!\,P(v) & \text{si } k = d \end{cases}$$

Démonstration. On raisonne par récurrence sur d. Si P est constant, c'est-à-dire $P = u \in \mathbb{K}$, alors

$$\Delta_v^k(P) = \begin{cases} 0 & \text{si } k > 0 \\ P = u & \text{si } k = 0 \end{cases}$$

donc

$$\Delta_v^k(P)(\overrightarrow{0}) = \begin{cases} 0 & \text{si } k > 0 \\ u = 0!\, P(v) & \text{si } k = 0 \end{cases}$$

Supposons que $d \geq 1$ plus l'hypothèse de récurrence. Supposons d'abord que $P = X^a$, où $a = (a_1, \ldots, a_m) \in \mathbb{N}^m$. On a

$$\Delta_v(P) = \sum_{i=1}^{m} a_i v_i \, X_1^{a_1} \cdots X_{i-1}^{a_{i-1}} X_i^{a_i - 1} X_{i+1}^{a_{i+1}} \cdots X_m^{a_m} \,.$$

Par le lemme 4.18 on a $\Delta_v^k(P)(\overrightarrow{0}) = 0$ si $k \geq d+1$, et par hypothèse de récurrence, $\Delta_v^k(P)(\overrightarrow{0}) = \Delta_v^{k-1}(\Delta_v(P))(\overrightarrow{0}) = 0$ si $1 \leq k \leq d-1$. Il est évident que $\Delta^0(P)(\overrightarrow{0}) = P(\overrightarrow{0}) = 0$. Encore par hypothèse de récurrence, on a

$$\begin{aligned}\Delta_v^d(P)(\overrightarrow{0}) &= \Delta_v^{d-1}(\Delta_v(P))(\overrightarrow{0}) = (d-1)!\, \Delta_v(P)(v) \\ &= (d-1)! \sum_{i=1}^{m} a_i v_i \, v_1^{a_1} \cdots v_{i-1}^{a_{i-1}} v_i^{a_i - 1} v_{i+1}^{a_{i+1}} \cdots v_m^{a_m} = (d-1)!\, |a|\, v^a = d!\, P(v) \,.\end{aligned}$$

On suppose maintenant que P est un polynôme homogène de degré d quelconque. On écrit $P = \sum_{|a|=d} t_a X^a$. Si $k \neq d$, alors

$$\Delta_v^k(P)(\overrightarrow{0}) = \sum_{|a|=d} t_a \Delta_v^k(X^a)(\overrightarrow{0}) = 0 \,.$$

Par ailleurs,

$$\Delta_v^d(P)(\overrightarrow{0}) = \sum_{|a|=d} t_a \Delta_v^d(X^a)(\overrightarrow{0}) = \sum_{|a|=d} t_a \, d!\, v^a = d!\, P(v) \,.$$

□

Théorème 4.20 (Formule de Taylor). *Soient $P \in \mathbb{K}[X_1, \ldots, X_m]$ un polynôme de degré d et $v \in \mathbb{K}^m$. Alors*

$$\sum_{k=0}^{d} \frac{1}{k!} \Delta_v^k(P)(\overrightarrow{0}) = P(v) \,.$$

Démonstration. On écrit $P = P_0 + P_1 + \cdots + P_d$ où P_k est un polynôme homogène de degré k pour tout $k \in \{0, 1, \ldots, d\}$. Alors, par le lemme 4.19, on a

$$\begin{aligned}\sum_{k=0}^{d} \frac{1}{k!} \Delta_v^k(P)(\overrightarrow{0}) &= \sum_{k=0}^{d} \frac{1}{k!} \sum_{l=0}^{d} \Delta_v^k(P_l)(\overrightarrow{0}) \\ &= \sum_{k=0}^{d} \frac{1}{k!}\, k! P_k(v) = P(v)\,.\end{aligned}$$

□

4.5 p-formes symétriques

Dans ce paragraphe on garde l'hypothèse que $\mathbb{K}$ et de caractéristique 0. Par la suite $\mathfrak{S}_m$ désignera le groupe des permutations de $\{1, \ldots, m\}$ pour tout $m \in \mathbb{N}$, $m \geq 1$.

Définition. Soient G un groupe et E un ensemble. Une *action de G sur E* est une opération externe

$$\begin{array}{ccc} G \times E & \to & E \\ (g, x) & \mapsto & g \cdot x \end{array}$$

vérifiant :

(a) $1_G \cdot x = x$ pour tout $x \in E$;

(b) $g \cdot (g' \cdot x) = (gg') \cdot x$ pour tous $g, g' \in G$ et $x \in E$.

Définition. Soient G un groupe et V un espace vectoriel sur $\mathbb{K}$. Une *représentation linéaire* de G dans V est un homomorphisme $\rho : G \to \mathrm{GL}(V)$.

Remarque. D'une représentation linéaire $\rho : G \to \mathrm{GL}(V)$ on déduit une action de G sur V définie par

$$g \cdot v = \rho(g)(v)\,.$$

Une action de G dans V est de cette forme si et seulement si, pour tout $g \in G$, l'application

$$\begin{array}{ccc} V & \to & V \\ v & \mapsto & g \cdot v \end{array}$$

est linéaire. On parle alors d'*action linéaire*.

Définition. Soient V un espace vectoriel et $f : V \to V$ un endomorphisme linéaire. La *transposée* de f est l'application linéaire $f^t : V^* \to V^*$ définie par

$$f^t(\alpha)(v) = \alpha(f(v))$$

pour $\alpha \in V^*$ et $v \in V$. Rappelons que, si $f, g : V \to V$ sont deux endomorphismes linéaires de V, alors $(f \circ g)^t = g^t \circ f^t$.

Lemme 4.21. *Soient G un groupe, V un espace vectoriel sur $\mathbb{K}$ et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Alors l'application*

$$\begin{array}{rccc} \rho^* : & G & \to & \mathrm{GL}(V^*) \\ & g & \mapsto & \rho(g^{-1})^t \end{array}$$

est une représentation linéaire.

Démonstration. Exercice. □

Définition. Soient G un groupe, V un espace vectoriel et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Alors la représentation $\rho^* : G \to \mathrm{GL}(V^*)$ du lemme 4.21 s'appelle la *représentation duale* de ρ.

Notations. Pour la suite nous poserons $V = \mathbb{K}^m$, et nous noterons $\mathcal{F}$ l'algèbre des fonctions polynomiales sur $\mathbb{K}$ à m variables. Comme $\mathcal{F}$ est isomorphe à $\mathbb{K}[X_1, \dots, X_m]$, $\mathcal{F}$ est munie d'une graduation $\mathcal{F} = \oplus_{d=0}^{\infty} \mathcal{F}_d$, où $\mathcal{F}_d$ désigne l'espace (vectoriel) des fonctions polynomiales homogènes de degré d. Rappelons que, pour tout $d \in \mathbb{N}$, on définit $V^{\otimes d}$ par récurrence sur d comme suit :

- $V^{\otimes 0} = \mathbb{K}$ et $V^{\otimes 1} = V$;
- si $d \geq 2$, alors $V^{\otimes d} = (V^{\otimes (d-1)}) \otimes V$.

Observons que $V^* = \mathcal{F}_1$, et rappelons les égalités

$$(V^*)^{\otimes d} = (V^{\otimes d})^* = \mathcal{L}_d(V, \dots, V; \mathbb{K}) .$$

Lemme 4.22. *Soit $f \in \mathcal{L}_p(V, \dots, V; \mathbb{K})$. Soit $\tilde{f} : V \to \mathbb{K}$ l'application définie par $\tilde{f}(v) = f(v, \dots, v)$. Alors $\tilde{f} \in \mathcal{F}_p$.*

Démonstration. Soient $\alpha_1, \dots, \alpha_p \in V^* = \mathcal{F}_1$. Posons $f = \alpha_1 \otimes \cdots \otimes \alpha_p$. Pour tout $v \in V$ on a

$$(\tilde{f})(v) = \alpha_1(v)\, \alpha_2(v) \, \cdots \, \alpha_p(v) = (\alpha_1 \alpha_2 \cdots \alpha_p)(v)$$

donc $\tilde{f} = \alpha_1 \alpha_2 \cdots \alpha_p \in \mathcal{F}_p$.

Soit $f \in \mathcal{L}_p(V, \dots, V; \mathbb{K}) = (V^*)^{\otimes p}$. Alors f s'écrit sous la forme $f = \sum_{i=1}^n f_i$, où f_i est de la forme $f_i = \alpha_{i,1} \otimes \cdots \otimes \alpha_{i,p}$ avec $\alpha_{i,j} \in V^*$. On a $\tilde{f} = \sum_{i=1}^n \tilde{f}_i$ et, par ce qui précède, $\tilde{f}_i \in \mathcal{F}_p$ pour tout $i \in \{1, \dots, n\}$, donc $\tilde{f} \in \mathcal{F}_p$. □

Pour tout $\sigma \in \mathfrak{S}_p$ on définit $\varphi_\sigma : V^p \to V^{\otimes p}$ par

$$\varphi_\sigma(v_1, \dots, v_p) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(p)} .$$

Cette application est clairement p-linéaire, donc induit une application linéaire $\rho_\sigma : V^{\otimes p} \to V^{\otimes p}$.

Lemme 4.23. *Soit $p \in \mathbb{N}$, $p \geq 1$. On a $\rho_\sigma \in \mathrm{GL}(V^{\otimes p})$ pour tout $\sigma \in \mathfrak{S}_p$ et l'application*

$$\begin{array}{rccc} \rho : & \mathfrak{S}_p & \to & \mathrm{GL}(V^{\otimes p}) \\ & \sigma & \mapsto & \rho_\sigma \end{array}$$

est une représentation linéaire.

Démonstration. Exercice. □

Définition. Un tenseur $f \in V^{\otimes p}$ est *symétrique* si $\rho_\sigma(f) = f$ pour tout $\sigma \in \mathfrak{S}_p$. Un tenseur $f' \in (V^*)^{\otimes p} = (V^{\otimes p})^*$ est *symétrique* si $\rho^*(\sigma)(f') = f'$ pour tout $\sigma \in \mathfrak{S}_p$, où ρ^* est la représentation duale de ρ. On note $(V^{\otimes p})^{\mathfrak{S}}$ l'ensemble des tenseurs symétriques dans $V^{\otimes p}$. On montre facilement que c'est un sous-espace vectoriel de $V^{\otimes p}$. De même, on note $((V^*)^{\otimes p})^{\mathfrak{S}}$ l'ensemble des tenseurs symétriques dans $(V^*)^{\otimes p}$, et c'est un sous-espace vectoriel de $(V^*)^{\otimes p}$.

Remarque. Si $f \in (V^*)^{\otimes p} = \mathcal{L}_p(V, \ldots, V; \mathbb{K})$ est considérée comme une application p-linéaire, alors f est symétrique si et seulement si

$$f(v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(p)}) = f(v_1, \ldots, v_p)$$

pour tous $(v_1, \ldots, v_p) \in V^p$ et tout $\sigma \in \mathfrak{S}_p$.

Définition. On définit les applications linéaires $S : V^{\otimes p} \to V^{\otimes p}$ et $\check{S} : (V^*)^{\otimes p} \to (V^*)^{\otimes p}$ par

$$S(v) = \frac{1}{p!} \sum_{\sigma \in \mathfrak{S}_p} \rho(\sigma)(v)\,, \quad \check{S}(f) = \frac{1}{p!} \sum_{\sigma \in \mathfrak{S}_p} \rho^*(\sigma)(f)\,.$$

Proposition 4.24.

(1) *On a $\rho(\sigma) \circ S = S \circ \rho(\sigma) = S$ pour tout $\sigma \in \mathfrak{S}_p$. De même, $\rho^*(\sigma) \circ \check{S} = \check{S} \circ \rho^*(\sigma) = \check{S}$ pour tout $\sigma \in \mathfrak{S}_p$.*

(2) *S est une projection de $V^{\otimes p}$ sur $(V^{\otimes p})^{\mathfrak{S}}$. De même, $\check{S}$ est une projection de $(V^*)^{\otimes p}$ sur $((V^*)^{\otimes p})^{\mathfrak{S}}$.*

Démonstration. On démontre les égalités $\rho(\sigma) \circ S = S \circ \rho(\sigma) = S$. Les égalités $\rho^*(\sigma) \circ \check{S} = \check{S} \circ \rho^*(\sigma) = \check{S}$ se démontrent de la même façon.

Soient $v \in V^{\otimes p}$ et $\sigma \in \mathfrak{S}_p$. Alors

$$\begin{aligned}(\rho(\sigma)\circ S)(v) = \rho(\sigma)\left(\frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}\rho(\tau)(v)\right) &= \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}(\rho(\sigma)\circ\rho(\tau))(v)\\ &= \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}\rho(\sigma\tau)(v) = \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}\rho(\tau)(v) = S(v)\,.\end{aligned}$$

$$(S\circ\rho(\sigma))(v) = \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}(\rho(\tau)\circ\rho(\sigma))(v) = \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}\rho(\tau\sigma)(v) = \frac{1}{p!}\sum_{\tau\in\mathfrak{S}_p}\rho(\tau)(v) = S(v)\,.$$

Maintenant, on démontre que S est une projection de $V^{\otimes p}$ sur $(V^{\otimes p})^{\mathfrak{S}}$. Le fait que $\check{S}$ soit une projection de $(V^*)^{\otimes p}$ sur $((V^*)^{\otimes p})^{\mathfrak{S}}$ se démontre de la même façon. Soit $v \in V^{\otimes p}$. Par (1) on a $\rho(\sigma)(S(v)) = S(v)$ pour tout $\sigma \in \mathfrak{S}_p$, donc $S(v) \in (V^{\otimes p})^{\mathfrak{S}}$. Par ailleurs, si $v \in (V^{\otimes p})^{\mathfrak{S}}$, alors

$$S(v) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p}\rho(\sigma)(v) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p}v = \frac{1}{p!}\,p!\,v = v\,.$$

$\square$

Rappelons que, si $f \in \mathcal{L}_p(V,\ldots,V;\mathbb{K}) = (V^*)^{\otimes p}$, $\tilde{f} : V \to \mathbb{K}$ désigne l'application définie par $\tilde{f}(v) = f(v,\ldots,v)$. Rappelons aussi que $\tilde{f} \in \mathcal{F}_p$. On note $\nu_p : ((V^*)^{\otimes p})^{\mathfrak{S}} \to \mathcal{F}_p$ l'application qui à f associe $\tilde{f}$.

Proposition 4.25. *L'application $\nu_p : ((V^*)^{\otimes p})^{\mathfrak{S}} \to \mathcal{F}_d$ est un isomorphisme d'espaces vectoriels.*

Démonstration. On note $\{\omega_1,\ldots,\omega_m\}$ la base duale de la base canonique de $V = \mathbb{K}^m$. Remarquez que, si $M = X_{i_1}X_{i_2}\cdots X_{i_p}$ est un monôme de degré p, la fonction polynomiale associée à M est

$$\begin{array}{rccc}\omega_M : & V & \to & \mathbb{K}\\ & v & \mapsto & \omega_{i_1}(v)\omega_{i_2}(v)\cdots\omega_{i_p}(v)\end{array}$$

Remarquons encore que l'ensemble des ω_M, où M varie parmi les monômes de degré p, est une base de $\mathcal{F}_p$. Finalement l'élément

$$\tilde{\omega}_M = \check{S}(\omega_{i_1}\otimes\cdots\otimes\omega_{i_p}) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p}(\omega_{i_{\sigma^{-1}(1)}}\otimes\cdots\otimes\omega_{i_{\sigma^{-1}(p)}}) \in ((V^*)^{\otimes p})^{\mathfrak{S}}$$

ne dépend pas de l'ordre de $\{i_1,\ldots,i_p\}$ donc est bien défini (i.e. ne dépend que du monôme M). Par ce qui précède il existe une application linéaire $\mu_p : \mathcal{F}_p \to ((V^*)^{\otimes p})^{\mathfrak{S}}$ qui envoie ω_M sur $\tilde{\omega}_M$ pour tout monôme M de degré p.

Soit $M = X_{i_1} X_{i_2} \cdots X_{i_p}$ un monôme de degré p. Pour $v \in V$ on a

$$\begin{aligned}
(\nu_p \circ \mu_p)(\omega_M)(v) &= \nu_p \left(\frac{1}{p!} \sum_{\sigma \in \mathfrak{S}_p} (\omega_{i_{\sigma^{-1}(1)}} \otimes \cdots \otimes \omega_{i_{\sigma^{-1}(p)}}) \right)(v) \\
&= \frac{1}{p!} \sum_{\sigma \in \mathfrak{S}_p} (\omega_{i_{\sigma^{-1}(1)}} \otimes \cdots \otimes \omega_{i_{\sigma^{-1}(p)}})(v \otimes \cdots \otimes v) \\
&= \frac{1}{p!} \sum_{\sigma \in \mathfrak{S}_p} \omega_{i_{\sigma^{-1}(1)}}(v) \cdots \omega_{i_{\sigma^{-1}(p)}}(v) \\
&= \frac{1}{p!}\, p!\, \omega_{i_1}(v) \cdots \omega_{i_p}(v) = \omega_M(v)\,.
\end{aligned}$$

Ceci montre que $\nu_p \circ \mu_p = \mathrm{Id}$. En particulier, ν_p est surjective et μ_p est injective.

L'ensemble $\{\omega_{i_1} \otimes \cdots \otimes \omega_{i_p}; (i_1, \ldots, i_p) \in \{1, \ldots, m\}^p\}$ est une base de $(V^*)^{\otimes p}$. Il s'en suit que l'ensemble $\{\check{S}(\omega_{i_1} \otimes \cdots \otimes \omega_{i_p}); (i_1, \ldots, i_p) \in \{1, \ldots, m\}^p\}$ engendre $\mathrm{Im}\, \check{S} = ((V^*)^{\otimes p})^{\mathfrak{S}}$. Si $(i_1, \ldots, i_p) \in \{1, \ldots, m\}^p$, alors, par construction, $\check{S}(\omega_{i_1} \otimes \cdots \otimes \omega_{i_p})$ est l'image de ω_M par μ_p, où $M = X_{i_1} X_{i_2} \cdots X_{i_p}$. Ceci montre que μ_p est surjective, donc est un isomorphisme. □

5 Modules

Dans ce chapitre A désignera un anneau avec ses deux lois $+$ et $\cdot$.

5.1 Définitions et premières propriétés

Définition. Un *module* sur A est un groupe abélien M muni d'une opération externe $A \times M \to M$, $(a, m) \mapsto a \cdot m$ vérifiant :

(a) $(a_1 + a_2) \cdot m = (a_1 \cdot m) + (a_2 \cdot m)$ pour tous $a_1, a_2 \in A$ et $m \in M$;

(b) $a \cdot (m_1 + m_2) = (a \cdot m_1) + (a \cdot m_2)$ pour tous $a \in A$ et $m_1, m_2 \in M$;

(c) $a_1 \cdot (a_2 \cdot m) = (a_1 a_2) \cdot m$ pour tous $a_1, a_2 \in A$ et $m \in M$;

(d) $1_A \cdot m = m$ pour tout $m \in M$.

Lemme 5.1. *Soit M un module sur A. Alors*

(1) $0_A \cdot m = 0_M$ *pour tout* $m \in M$ *;*

(2) $a \cdot 0_M = 0_M$ *pour tout* $a \in A$ *;*

(3) $(-a) \cdot m = a \cdot (-m) = -(a \cdot m)$ *pour tous* $a \in A$ *et* $m \in M$.

Démonstration. Soit $m \in M$. Alors

$$0_A \cdot m = (0_A + 0_A) \cdot m = (0_A \cdot m) + (0_A \cdot m)\,,$$

donc $0_A \cdot m = 0_M$.

Soit $a \in A$. Alors

$$a \cdot 0_M = a \cdot (0_M + 0_M) = (a \cdot 0_M) + (a \cdot 0_M)\,,$$

donc $a \cdot 0_M = 0_M$.

Soient $a \in A$ et $m \in M$. Alors

$$(-a) \cdot m + a \cdot m = ((-a) + a) \cdot m = 0_A \cdot m = 0_M\,,$$

donc $(-a) \cdot m = -(a \cdot m)$. Par ailleurs,

$$a \cdot (-m) + a \cdot m = a \cdot ((-m) + m) = a \cdot 0_M = 0_M\,,$$

donc $a \cdot (-m) = -(a \cdot m)$. □

Exemple 1. Si $A = \mathbb{K}$ est un corps, alors être un espace vectoriel sur $\mathbb{K}$ est la même chose que d'être un module sur $\mathbb{K}$.

Exemple 2. Soit M un groupe abélien. On définit une opération $\mathbb{Z} \times M \to M$ comme suit. Pour $m \in M$ et $a \in \mathbb{Z}$, $a \geq 1$, on définit $a \cdot m$ par récurrence sur a en posant $1 \cdot m = m$, et $a \cdot m = (a-1) \cdot m + m$ si $a \geq 2$. On pose $0 \cdot m = 0_M$ et $a \cdot m = -((-a) \cdot m)$ si $a < 0$. Alors M muni de sa somme $+$ et de l'opération $\cdot$ ainsi définie est un module sur $\mathbb{Z}$.

Exemple 3. Posons $M = A^m$, que l'on considère comme groupe abélien, muni de l'opération $A \times M \to M$ définie par

$$a \cdot (b_1, \ldots, b_m) = (a \cdot b_1, \ldots, a \cdot b_m)$$

pour $a \in A$ et $(b_1, \ldots, b_m) \in M$. Alors M est un module sur A.

Exemple 4. Soient $\mathbb{K}$ un corps, V un espace vectoriel sur $\mathbb{K}$ et $A = \mathcal{L}(V)$. Alors V avec l'action naturelle de $A = \mathcal{L}(V)$ est un module sur A.

Définition. Soit M un module sur A. Une partie $N \subset M$ est un *sous-module* de M si $(N, +)$ est un sous-groupe de $(M, +)$, et $a \cdot n \in N$ pour tous $a \in A$ et $n \in N$.

Lemme 5.2. *Soient M un module sur A et N un sous-module de M. Alors N est un module sur A.*

Démonstration. Exercice. □

Lemme 5.3. *Soient M un module sur A et $N \subset M$ une partie. Alors N est un sous-module de M si et seulement si $N \neq \emptyset$, et on a $a_1n_1 + a_2n_2 \in N$ pour tous $a_1, a_2 \in A$ et $n_1, n_2 \in N$.*

Démonstration. Exercice. □

Exemple. Rappelons qu'un *idéal à gauche* de A est une partie $I \subset A$ telle que

(a) $(I, +)$ est un sous-groupe de $(A, +)$;

(b) $a \cdot b \in I$ pour tous $a \in A$ et $b \in I$.

On considère A comme un module sur A. alors $I \subset A$ est un sous-module si et seulement s'il est un idéal à gauche.

Lemme 5.4. *Soient M un module sur A et $\{N_i\}_{i\in I}$ une famille de sous-modules de M. Alors $\cap_{i\in I} N_i$ est un sous-module de M.*

Démonstration. Exercice. □

Définition. Soient M un module et $G \subset M$ une partie. Le sous-module de M *engendré* par G est le plus petit sous-module de M contenant G. C'est l'intersection de tous les sous-modules de M qui contiennent G. Remarquez que cette intersection est non vide car M contient G.

Remarque. Soit M un module sur A. Alors $\{0_M\}$ est le sous-module de M engendré par $\emptyset$.

Lemme 5.5. *Soient M un module sur A, $G \subset M$ une partie non vide, et N le sous-module de M engendré par G. Soit $m \in M$. Alors $m \in N$ si et seulement s'il existe $k \in \mathbb{N}$, $g_1, \dots, g_k \in G$ et $a_1, \dots, a_k \in A$ tels que $m = a_1g_1 + \cdots + a_kg_k$.*

Démonstration. Posons

$$N_0 = \{a_1g_1 + \cdots + a_kg_k \ ; \ k \in \mathbb{N}, \ g_1, \dots, g_k \in G \text{ et } a_1, \dots a_k \in A\} .$$

On va montrer que N_0 est un sous-module de M, puis que tout sous-module de M contenant G contient N_0.

On a $N_0 \neq \emptyset$ car $G \subset N_0$ et G est non vide. Soient $m, m' \in N_0$ et $b, b' \in A$. il existe $k \in \mathbb{N}$, $g_1, \dots, g_k \in G$ et $a_1, \dots, a_k \in A$ tels que $m = a_1g_1 + \cdots + a_kg_k$. De même, il existe $l \in \mathbb{N}$, $g'_1, \dots, g'_l \in G$ et $a'_1, \dots, a'_l \in A$ tels que $m' = a'_1g'_1 + \cdots + a'_lg'_l$. Alors

$$bm + b'm' = (ba_1)g_1 + \cdots + (b_ka_k)g_k + (b'a'_1)g'_1 + \cdots + (b'a'_l)g'_l ,$$

donc $bm + b'm' \in N_0$. Ceci montre que N_0 est un sous-module de M.

Soit N un sous-module de M contenant G. Soit $m \in N_0$. Il existe $k \in \mathbb{N}$, $g_1, \ldots, g_k \in G$ et $a_1, \ldots, a_k \in A$ tels que $m = a_1 g_1 + \cdots + a_k g_k$. Le fait que $g_1, \ldots, g_k$ soient dans N implique que $m \in N$. On a donc $N_0 \subset N$. $\square$

Définition. On dit qu'un module M sur A est de *type fini* s'il est engendré par un nombre fini d'éléments. On dit que M est *monogène* s'il est engendré par un unique élément.

Exemples.

(1) Un espace vectoriel sur $\mathbb{K}$ est de type fini si et seulement s'il est de dimension fini. il est monogène si et seulement s'il est de dimension 1 ou 0.

(2) Si $p \in \mathbb{N}$, $p \geq 1$, alors A^p est un module sur A de type fini. Il est engendré par $\{e_1, \ldots, e_p\}$, où
$$e_i = (0_A, \ldots, 0_A, 1_A, 0_A, \ldots, 0_A)$$
pour tout $i \in \{1, \ldots, p\}$. Il est monogène si et seulement si $p = 1$.

(3) Soient $\mathbb{K}$ un corps, V un espace vectoriel sur $\mathbb{K}$, et $A = \mathcal{L}(V)$. Alors V est un module monogène sur A. il est engendré par n'importe quel vecteur non nul.

Remarque. Un sous-module d'un module de type fini n'est pas forcément de type fini.

5.2 Morphismes et quotients

Définition. Soient M, M' deux modules sur A. Une application $f : M \to M'$ est un *morphisme* de modules (sur A) si :

(a) $f(m_1 + m_2) = f(m_1) + f(m_2)$ pour tous $m_1, m_2 \in M$;

(b) $f(a \cdot m) = a \cdot f(m)$ pour tous $a \in A$ et $m \in M$.

Un *isomorphisme* est un morphisme bijectif.

Lemme 5.6.

(1) *Soit $f : M \to M'$ un morphisme de modules sur A. Alors $f(0_M) = 0_{M'}$, et $f(-m) = -f(m)$ pour tout $m \in M$.*

(2) *Si $f : M \to M'$ est un isomorphisme de modules, alors $f^{-1} : M' \to M$ est un morphisme de modules.*

Démonstration. Exercice. $\square$

Lemme 5.7. *Soit $f : M \to M'$ un morphisme de modules.*

(1) *Soit* $N \subset M$ *un sous-module. Alors* $f(N)$ *est un sous-module de* M'*.*

(2) *Soit* $N' \subset M'$ *un sous-module. Alors* $f^{-1}(N')$ *est un sous-module de* M*.*

Démonstration. Exercice. □

Définition. Soit $f : M \to M'$ un morphisme de modules. Le *noyau* de f, noté $\operatorname{Ker} f$, est $\operatorname{Ker} f = f^{-1}(0_{M'})$. *L'image* de f, notée $\operatorname{Im} f$, est $\operatorname{Im} f = f(M)$. Par ce qui précède, $\operatorname{Ker} f$ est un sous-module de M et $\operatorname{Im} f$ est un sous-module de M'.

Lemme 5.8. *Soit* $f : M \to M'$ *un morphisme de modules.*

(1) f *est injectif si et seulement si* $\operatorname{Ker} f = \{0_M\}$*.*

(2) f *est surjectif si et seulement si* $\operatorname{Im} f = M'$*.*

(3) f *est un isomorphisme si et seulement si* $\operatorname{Ker} f = \{0_M\}$ *et* $\operatorname{Im} f = M'$*.*

Démonstration. Exercice. □

Soient M un module sur A et N un sous-module de M. Soit $\mathcal{R}$ la relation d'équivalence sur M définie par :

$$x\mathcal{R}y \iff x - y \in N\,.$$

Lemme 5.9. *La relation* $\mathcal{R}$ *est compatible avec les opérations de* M*. C'est-à-dire :*

(a) *si* $x_1\mathcal{R}x_1'$ *et* $x_2\mathcal{R}x_2'$*, alors* $(x_1 + x_2)\mathcal{R}(x_1' + x_2')$*, pour tous* $x_1, x_2, x_1', x_2' \in M$ *;*

(b) *si* $x\mathcal{R}x'$*, alors* $(ax)\mathcal{R}(ax')$*, pour tous* $x, x' \in M$ *et* $a \in A$*.*

Démonstration. Exercice. □

Définition. Pour $x \in M$, on appelle *classe de* x et on note $\bar{x} = x + N = \{x + y; y \in N\}$ la classe d'équivalence de x par $\mathcal{R}$. On note M/N l'ensemble quotient, c'est-à-dire l'ensemble des classes d'équivalence.

Proposition 5.10.

(1) *Les opérations interne* $+$ *et externe* $\cdot$ *sur* M/N *données par*

$$\bar{x} + \bar{y} = \overline{x + y}\,, \quad a \cdot \bar{x} = \overline{ax}\,,$$

où $x, y \in M$ *et* $a \in A$*, sont bien définies.*

(2) *L'ensemble* M/N *muni des deux opérations* $+$ *et* $\cdot$ *est un module sur* A*.*

(3) *L'application $\mu : M \to M/N$, $x \mapsto \bar{x}$, est un morphisme surjectif dont le noyau est N.*

Démonstration. Exercice. $\square$

Proposition 5.11. *Soient M, M' deux modules, N un sous-module de M et $f : M \to M'$ un morphisme. Si f s'annule sur N, alors il existe un unique morphisme $\bar{f} : M/N \to M'$ tel que $f = \bar{f} \circ \mu$, c'est-à-dire le diagramme suivant commute.*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\mu"'] & M' \\ M/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

De plus, si $N = \operatorname{Ker} f$, alors $\bar{f}$ est injectif.

Démonstration. Exercice. $\square$

Proposition 5.12. *Soient M un module et N un sous-module de M. Notons $\mathcal{M}(M, N)$ l'ensemble des sous-modules de M qui contiennent N et $\mathcal{M}(M/N)$ l'ensemble des sous-modules de M/N. Alors l'application*

$$\begin{array}{rccc} \varphi : & \mathcal{M}(M,N) & \to & \mathcal{M}(M/N) \\ & U & \mapsto & \mu(U) \end{array}$$

est une bijection.

Démonstration. Soit U' un sous-module de M'. Comme $0_{M/N} \in U'$, on a $N = \operatorname{Ker} \mu = \mu^{-1}(0_{M/N}) \subset \mu^{-1}(U')$, donc l'application

$$\begin{array}{rccc} \psi : & \mathcal{M}(M/N) & \to & \mathcal{M}(M,N) \\ & U' & \mapsto & \mu^{-1}(U') \end{array}$$

est bien définie. Soit $U' \in \mathcal{M}(M/N)$. Alors

$$(\varphi \circ \psi)(U') = \mu\big(\mu^{-1}(U')\big) = U' \,.$$

Ceci montre que $\varphi \circ \psi = \mathrm{Id}$. Soit $U \in \mathcal{M}(M, N)$. Posons $U' = \varphi(U) = \mu(U)$ et $V = \psi(U') = \mu^{-1}(U')$. Comme $U' = \mu(U)$, on a $U \subset \mu^{-1}(U') = V$. Réciproquement, soit $y \in V$. Posons $x' = \mu(y) \in U'$. il existe $x \in U$ tel que $x' = \mu(x)$. On a $\mu(y - x) = x' - x' = 0_{M/N}$, donc $y - x \in \operatorname{Ker} \mu = N \subset U$, donc $y = (y - x) + x \in U$. On en déduit que $V \subset U$, donc $(\psi \circ \varphi)(U) = U$. Ceci montre que $\psi \circ \varphi = \mathrm{Id}$. $\square$

Définition. Soient M un module et N_1, N_2 deux sous-modules de M. Alors la *somme* de N_1 et N_2 est :

$$N_1 + N_2 = \{n_1 + n_2 \ ; \ n_1 \in N_1 \text{ et } n_2 \in N_2\} \,.$$

Lemme 5.13. *Soient M un module et N_1, N_2 deux sous-modules de M. Alors $N_1 + N_2$ est une sous-module de M.*

Démonstration. Exercice. □

Théorème 5.14. *Soient M un module et N_1, N_2 deux sous-modules de M. Alors*

$$(N_1 + N_2)/N_2 \simeq N_1/(N_1 \cap N_2)\,.$$

Démonstration. On note $\iota : N_1 \to N_1 + N_2$ l'inclusion, $\pi : (N_1 + N_2) \to (N_1 + N_2)/N_2$ l'application quotient, et $\tilde{\varphi} = \pi \circ \iota : N_1 \to (N_1 + N_2)/N_2$. On a $\operatorname{Ker} \tilde{\varphi} = N_1 \cap N_2$, donc, par la proposition 5.11, $\tilde{\varphi}$ induit un homomorphisme injectif $\varphi : N_1/(N_1 \cap N_2) \to (N_1 + N_2)/N_2$. Cet homomorphisme est surjectif car, si $m = n_1 + n_2 \in N_1 + N_2$, alors $\bar{m} = \bar{n}_1$ dans $(N_1 + N_2)/N_2$, donc $\bar{m} = \varphi(\bar{n}_1)$. □

Définition. Soit M un module. Deux sous-modules N_1, N_2 de M sont *supplémentaires* si $N_1 \cap N_2 = 0_M$ et $N_1 + N_2 = M$. Dans ce cas on pose $N_1 + N_2 = N_1 \oplus N_2$ et on parle de la *somme directe* de N_1 et N_2.

Corollaire 5.15. *Soient M un module et N_1, N_2 deux sous-modules tels que $N_1 \cap N_2 = \{0\}$. Alors*

$$(N_1 \oplus N_2)/N_2 \simeq N_1\,, \quad (N_1 \oplus N_2)/N_1 \simeq N_2\,.$$

Définition. Deux idéaux à gauche I, J de A sont dits *étrangers* si $I + J = A$.

Théorème 5.16 (Théorème Chinois). *Soient I, J deux idéaux à gauche étrangers de A. Alors*

$$A/(I \cap J) \simeq A/I \times A/J\,.$$

Remarque. Les idéaux I et J ne sont pas forcément bilatères, donc les quotients A/I, A/J et $A/I \cap J$ n'ont pas forcément de structure d'algèbre. L'isomorphisme du théorème 5.16 est un isomorphisme de modules sur A.

Démonstration. On vérifie facilement que $I/(I \cap J) + J/(I \cap J) = A/(I \cap J)$ et $(I/(I \cap J)) \cap (J/(I \cap J)) = \{0\}$, donc $A/(I \cap J) = I/(I \cap J) \oplus J/(I \cap J)$, donc $A/(I \cap J) \simeq I/(I \cap J) \times J/(I \cap J)$. Par ailleurs,

$$A/I = (I + J)/I \simeq J/(I \cap J) \text{ et } A/J = (I + J)/J \simeq I/(I \cap J)\,,$$

donc $A/(I \cap J) \simeq A/I \times A/J$. □

5.3 Modules de type fini

Proposition 5.17. *Soit M un module sur A. Alors M est monogène si et seulement s'il existe un idéal à gauche $I \subset A$ tel que $M \simeq A/I$.*

Démonstration. Si $M = A/I$, où I est un idéal à gauche, alors $M = A \cdot \bar{1}_A$, donc M est monogène. Réciproquement, supposons que M soit monogène. Soit $m \in M$ un générateur. L'application $\varphi : A \to M$, $a \mapsto a \cdot m$ est un homomorphisme de modules surjectif. Par la proposition 5.11, on en déduit que φ induit un isomorphisme $\bar{\varphi} : A/I \to M$, où $I = \operatorname{Ker} \varphi$. □

Définition. Soient M un module et $m \in M$. L'*annulateur* de m, noté $\operatorname{Ann}(m)$, est $\{a \in A; a \cdot m = 0_M\}$.

Lemme 5.18.

(1) *Soit M un module et $m \in M$. Alors $\operatorname{Ann}(m)$ est un idéal à gauche de A.*

(2) *Soient M un module monogène et $m \in M$ un générateur. Alors $M \simeq A/\operatorname{Ann}(m)$.*

Démonstration. Soient M un module et $m \in M$. On a $\operatorname{Ann}(m) \neq \emptyset$ car $0_A \in \operatorname{Ann}(m)$. Soient $a_1, a_2 \in \operatorname{Ann}(m)$ et $b_1, b_2 \in A$. Alors

$$(b_1a_1 + b_2a_2) \cdot m = b_1 \cdot (a_1 \cdot m) + b_2 \cdot (a_2 \cdot m) = b_1 \cdot 0_M + b_2 \cdot 0_M = 0_M ,$$

donc $b_1a_1 + b_2a_2 \in \operatorname{Ann}(m)$. Ceci montre que $\operatorname{Ann}(m)$ est un idéal à gauche de A.

Soient M un module monogène et $m \in M$ un générateur. L'application $\varphi : A \to M$, $a \mapsto a \cdot m$ est un homomorphisme surjectif dont le noyau est $\operatorname{Ann}(m)$. Par la proposition 5.11, φ induit un isomorphisme $A/\operatorname{Ann}(m) \to M$. □

Proposition 5.19. *On suppose que A est un anneau commutatif.*

(1) *Soient M un module monogène et $m, m' \in M$ deux générateurs. Alors $\operatorname{Ann}(m) = \operatorname{Ann}(m')$.*

(2) *Soient M un module monogène, $m \in M$ un générateur, et $I \subset A$ un idéal à gauche tel que $M \simeq A/I$. Alors $I = \operatorname{Ann}(m)$.*

Démonstration. Soient M un module monogène et $m, m' \in M$ deux générateurs. Il existe $u \in A$ tel que $m' = u \cdot m$. Si $a \in \operatorname{Ann}(m)$, alors

$$a \cdot m' = a \cdot (u \cdot m) = (au) \cdot m = (ua) \cdot m = u \cdot (a \cdot m) = 0_M ,$$

donc $a \in \operatorname{Ann}(m')$. D'où $\operatorname{Ann}(m) \subset \operatorname{Ann}(m')$. De même, $\operatorname{Ann}(m') \subset \operatorname{Ann}(m)$.

Soient M un module monogène, $m \in M$ un générateur, et $I \subset A$ un idéal à gauche tel que $M \simeq A/I$. Soit $\psi : A/I \to M$ un isomorphisme, $\pi : A \to A/I$ l'application quotient, et $\varphi = \psi \circ \pi : A \to M$. On remarque que φ est un homomorphisme surjectif, $\operatorname{Ker}\varphi = I$, $m' = \varphi(1_A)$ est un générateur de M, et $\operatorname{Ker}\varphi = \operatorname{Ann}(m')$. Par la partie (1) on en conclue que $I = \operatorname{Ann}(m') = \operatorname{Ann}(m)$. $\square$

Remarques.

(1) Le résultat de la proposition 5.19 est faux si A n'est pas commutatif.

(2) Supposons que A soit commutatif. Il se peut que l'on ait deux idéaux bilatères $I, J \subset A$ tels que $A/I \simeq A/J$ comme anneau, mais $I \neq J$ (un exemple sera donné en exercice). Par contre, par la proposition 5.19, si I, J sont deux idéaux à gauche tels que $A/I \simeq A/J$ comme modules sur A, alors $I = J$.

Lemme 5.20. *Tout quotient d'un module de type fini est un module de type fini.*

Démonstration. Soient M un module de type fini, $G = \{g_1, \dots, g_n\}$ une famille finie qui engendre M, N un sous-module de M, et $M \to M/N$, $m \mapsto \bar{m}$, l'application quotient. Pour $m \in M$ il existe $a_1, \dots, a_n \in A$ tels que $m = a_1 g_1 + \cdots + a_n g_n$. On a alors $\bar{m} = a_1 \bar{g}_1 + \cdots + a_n \bar{g}_n$. Ceci montre que $\bar{G} = \{\bar{g}_1, \dots, \bar{g}_n\}$ engendre M/N. $\square$

Lemme 5.21. *Un module M est de type fini si et seulement s'il est le quotient d'un A^n avec $n \in \mathbb{N}$.*

Démonstration. Pour $n \in \mathbb{N}$, A^n est un module de type fini, donc tout quotient de A^n est un module de type fini. Réciproquement, soit M un module de type fini. Soit $G = \{g_1, \dots, g_n\}$ une famille finie génératrice de M. On définit $\mu : A^n \to M$ par

$$\mu(a_1, \dots, a_n) = a_1 g_1 + \cdots + a_n g_n \,.$$

Si $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in A^n$ et $x, y \in A$, alors

$$\begin{gathered} x\,\mu(a) + y\,\mu(b) = x(a_1 g_1 + \cdots + a_n g_n) + y(b_1 g_1 + \cdots + b_n g_n) \\ = (xa_1 + yb_1) g_1 + \cdots + (xa_n + yb_n) g_n = \mu((xa_1 + yb_1, \dots, xa_n + yb_n)) = \mu(xa + yb)\,, \end{gathered}$$

donc μ est un homomorphisme. Il est surjectif car G engendre M. On en conclue que $M \simeq A^n / \operatorname{Ker}\mu$. $\square$

5.4 Modules simples et semi-simples

Définition. Un module M sur A est *simple* si $M \neq \{0\}$ et si les seuls sous-modules de M sont $\{0\}$ et M.

Exemple. Si $A = \mathbb{K}$ est un corps, un module simple est un espace vectoriel de dimension 1.

Définition. Un idéal I de A est appelé *maximal* si I est propre (i.e. $I \neq A$) et I n'est strictement inclus dans aucun idéal propre de A.

Proposition 5.22. *Soit M un module sur A. Les conditions suivantes sont équivalentes :*

(a) *M est un module simple.*

(b) *M est monogène, et tout élément de $M \setminus \{0\}$ engendre M.*

(c) *$M \simeq A/I$, où I est un idéal maximal de A.*

Démonstration. (a) $\Rightarrow$ (b) : Supposons que M soit simple. Soit $m \in M \setminus \{0\}$. Alors $A \cdot m$ est un sous-module de M différent de $\{0\}$, donc $A \cdot m = M$.

(b) $\Rightarrow$ (a) : Supposons que $A \cdot m = M$ pour tout $m \in M \setminus \{0_M\}$. Soit $M' \subset M$ un sous-module différent de $\{0\}$. Soit $m \in M'$, $m \neq 0_M$. Alors $M = A \cdot m \subset M' \subset M$, donc $M' = M$.

(a) $\Leftrightarrow$ (c) : Rappelons que $\mathcal{M}(A, I)$ désigne l'ensemble des sous-modules (idéaux) $J \subset A$ tel que $I \subset J \subset A$, $\mathcal{M}(A/I)$ désigne l'ensemble des sous-modules de A/I, et il existe une bijection $\mu : \mathcal{M}(A, I) \to \mathcal{M}(A/I)$, $J \mapsto J/I$. Par ailleurs, I est maximal si et seulement si $|\mathcal{M}(A, I)| = 2$ et A/I est simple si et seulement si $|\mathcal{M}(A/I)| = 2$. On en conclue que A/I est simple si et seulement si I est maximal. $\square$

Théorème 5.23 (Krull). *Soient A un anneau non trivial (i.e. $A \neq \{0\}$) et I un idéal à gauche propre de A (i.e. $I \neq A$). Alors A contient un idéal maximal contenant I.*

Démonstration. Notons $\mathcal{I}$ l'ensemble des idéaux propres de A qui contiennent I. On a $\mathcal{I} \neq \emptyset$ car $I \in \mathcal{I}$. Soit $\mathcal{C}$ une chaîne dans $\mathcal{I}$. Posons

$$J_0 = \bigcup_{J \in \mathcal{C}} J\,.$$

On laisse en exercice la démonstration que J_0 est un idéal de A contenant I. Montrons par l'absurde que c'est un idéal propre. Supposons que $J_0 = A$, en particulier $1_A \in J_0$. Par définition, il existe $J \in \mathcal{C}$ tel que $1_A \in J$. Mais, si $1_A \in J$, alors $A = A \cdot 1_A \subset J$, ce qui contredit l'hypothèse que J est propre. D'où, $1_A \notin J_0$ et J_0 est propre. On a donc démontré que J_0 est un majorant de $\mathcal{C}$ dans $\mathcal{I}$.

Par le lemme de Zorn, $\mathcal{I}$ a un élément maximal, et cet élément est forcément un idéal maximal contenant I. $\square$

Corollaire 5.24. *Soit A un anneau non trivial. Alors A contient un idéal maximal.*

Démonstration. On applique la proposition 5.23 à $I = \{0_A\}$. $\square$

Corollaire 5.25. *Soit A un anneau non trivial. Il existe un module simple sur A.*

Démonstration. Soit $I \subset A$ un idéal maximal. Alors A/I est un module simple. $\square$

Définition. Soit M un module sur A. Un sous-module *maximal* de M est un sous-module propre $M' \subsetneq M$ tel que M' ne soit inclus dans aucun sous-module propre de M.

Lemme 5.26. *Soient M un module sur A et $M' \subset M$ un sous-module propre. Alors M/M' est simple si et seulement si M' est maximal.*

Démonstration. Rappelons que $\mathcal{M}(M, M')$ désigne l'ensemble des sous-modules $N \subset M$ tel que $M' \subset N \subset M$, $\mathcal{M}(M/M')$ désigne l'ensemble des sous-modules de M/M', et il existe une bijection $\mu : \mathcal{M}(M, M') \to \mathcal{M}(M/M')$, $N \mapsto N/M'$. Par ailleurs, M' est maximal si et seulement si $|\mathcal{M}(M, M')| = 2$ et M/M' est simple si et seulement si $|\mathcal{M}(M/M')| = 2$. On en conclue que M/M' est simple si et seulement si M' est maximal. $\square$

Définition. Soient M un module sur A et $\{N_i\}_{i\in I}$ une famille de sous-modules de M. La *somme* des N_i est le sous-module de M noté $\sum_{i\in I} N_i$ engendré par $\cup_{i\in I} N_i$. Un élément m appartient à $\sum_{i\in I} N_i$ si et seulement s'il existe $p \in \mathbb{N}$, $i_1, \ldots, i_p \in I$, et $n_{i_j} \in N_{i_j}$ pour tout $j \in \{1, \ldots, p\}$ tels que $m = n_{i_1} + \cdots + n_{i_p}$. On dit que la somme $\sum_{i\in I} N_i$ est une *somme directe* et on note $\sum_{i\in I} N_i = \oplus_{i\in I} N_i$ si pour tous $p \in \mathbb{N}$, $i_1, \ldots, i_p \in I$, $n_{i_1} \in N_{i_1}, \ldots, n_{i_p} \in N_{i_p}$, l'égalité $n_{i_1} + \cdots + n_{i_p} = 0_M$ implique $n_{i_j} = 0_M$ pour tout $j \in \{1, \ldots, p\}$.

Remarque. Soient M un module sur A et $\{N_i\}_{i\in I}$ une collection de sous-modules. Alors la condition "$N_i \cap N_j = \{0_M\}$ pour tous $i, j \in I$, $i \neq j$" n'implique pas que $\sum_{i\in I} N_i = \oplus_{i\in I} N_i$.

Exemple. On suppose $A = \mathbb{R}$ et $M = \mathbb{R}^2$. On pose $N_1 = \mathbb{R}\,(1,0)$, $N_2 = \mathbb{R}\,(0,1)$ et $N_3 = \mathbb{R}\,(-1,-1)$. On a $N_i \cap N_j = \{\overrightarrow{0}\}$ pour tous $i, j \in \{1,2,3\}$, $i \neq j$. Par ailleurs, $v_1 = (1,0) \in N_1$, $v_2 = (0,1) \in N_2$, $v_3 = (-1,-1) \in N_3$ et $v_1 + v_2 + v_3 = \overrightarrow{0}$.

Lemme 5.27. *Soient M un module sur A et $\{N_i\}_{i\in I}$ une collection de sous-modules. On a $\sum_{i\in I} N_i = \oplus_{i\in I} N_i$ si et seulement si, pour tout $m \in \sum_{i\in I} N_i$, il existe $p \in \mathbb{N}$ unique, des indices $i_1, \ldots, i_p \in I$ uniques, et des éléments $n_{i_1} \in N_{i_1} \setminus \{0\}, \ldots, n_{i_p} \in N_{i_p} \setminus \{0\}$ uniques, tels que $m = n_{i_1} + \cdots + n_{i_p}$.*

Démonstration. Exercice. $\square$

Définition. Un module M est *semi-simple* s'il existe une collection $\{S_i\}_{i\in I}$ de sous-modules simples telle que $M = \sum_{i\in I} S_i$. On admettra que $\{0\}$ est un module semi-simple (on admettra que c'est la somme sur 0 sous-modules simples).

Exemples.

(1) Si $A = \mathbb{K}$ est un corps, alors tout module (espace vectoriel) sur $\mathbb{K}$ est semi-simple.

(2) $\mathbb{Z}/4\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module semi-simple (à faire en exercice).

Lemme 5.28.

(1) *Soient M un module et N_1, N_2 deux sous-modules de M tels que $M = N_1 + N_2$. Alors $M = N_1 \oplus N_2$ si et seulement si $N_1 \cap N_2 = \{0_M\}$.*

(2) *Soient M un module et $\{N_i\}_{i\in I}$ et $\{N_j\}_{j\in J}$ deux collections de sous-modules (non triviaux) de M. Posons $M_1 = \sum_{i\in I} N_i$, $M_2 = \sum_{j\in J} N_j$ et $M' = \sum_{i\in I\cup J} N_i$. On a*

$$M_1 = \bigoplus_{i\in I} N_i\,,\ \ M_2 = \bigoplus_{j\in J} N_j \ \text{ et } M' = M_1 \oplus M_2$$

si et seulement si $I \cap J = \emptyset$ et

$$M' = \bigoplus_{i\in I\cup J} N_i\,.$$

Démonstration. Exercice. □

Proposition 5.29. *Soient M un module semi-simple, $\{S_i\}_{i\in I}$ une collection de sous-modules simples telle que $M = \sum_{i\in i} S_i$ et M' un sous-module de M. Alors il existe une partie $J_0 \subset I$ telle que*

$$M = M' \oplus \left(\bigoplus_{j\in J_0} S_j\right)\,.$$

Démonstration. Posons

$$\mathcal{J} = \left\{ J \subset I\ ;\ M' + \left(\sum_{j\in J} S_j\right) = M' \oplus \left(\bigoplus_{j\in J} S_j\right)\right\}\,.$$

On a $\mathcal{J} \neq \emptyset$ car $\emptyset \in \mathcal{J}$. On observe que $J \in \mathcal{J}$ si et seulement si toute partie finie X de J appartient à $\mathcal{J}$. En d'autres termes, $\mathcal{J}$ est un caractère fini, donc est inductif, donc admet un élément maximal, J_0. On va montrer que

$$M = M' \oplus \left(\bigoplus_{j\in J_0} S_j\right)\,.$$

Posons $M'' = M' + (\sum_{j\in J_0} S_j)$. Comme $J_0 \in \mathcal{J}$, on a $M'' = M' \oplus (\oplus_{j\in J_0} S_j)$. Reste à montrer que $M = M''$. Pour cela il suffit de montrer que $S_i \subset M''$ pour tout $i \in I$. Si $i \in J_0$ alors il est évident que $S_i \subset M''$. On peut donc supposer que $i \notin J_0$.

Supposons que $M'' \cap S_i \neq \{0\}$. Comme S_i est simple et $S_i \cap M'' \subset S_i$, on a $S_i \cap M'' = S_i$ c'est-à-dire $S_i \subset M''$. Supposons que $S_i \cap M'' = \{0\}$. Par le lemme 5.28 il en résulte que

$$M' + \sum_{j \in J_0 \cup \{i\}} S_j = M'' + S_i = M'' \oplus S_i = M' \oplus \left(\bigoplus_{j \in J_0 \cup \{i\}} S_j \right) ,$$

donc $J_0 \cup \{i\} \in \mathcal{J}$. Ceci contredisant la maximalité de J_0, on en conclue que l'on ne peut pas avoir $S_i \cap M'' = \{0\}$. $\square$

Corollaire 5.30. *Soient M un module semi-simple et $\{S_i\}_{i \in I}$ une collection de sous-modules simples telle que $M = \sum_{i \in i} S_i$. Alors il existe une partie $J_0 \subset I$ telle que*

$$M = \bigoplus_{j \in J_0} S_j .$$

Démonstration. On applique la proposition 5.29 à $M' = \{0_M\}$. $\square$

Corollaire 5.31. *Soit M un module semi-simple. Alors tout sous-module de M a un facteur direct. C'est-à-dire, si M' est un sous-module de M, il existe un sous-module M'' de M tel que $M = M' \oplus M''$.*

Démonstration. On choisit une famille $\{S_i\}_{i \in I}$ de sous-modules simples telle que $M = \sum_{i \in I} S_i$. D'après la proposition 5.29, il existe une partie $J_0 \subset I$ telle que $M = M' \oplus (\oplus_{j \in J_0} S_j)$. Posons $M'' = \oplus_{j \in J_0} S_j$. Alors $M = M' \oplus M''$. $\square$

Lemme 5.32. *Soit M un module. Si M est isomorphe à un module semi-simple, alors M est semi-simple.*

Démonstration. Exercice. $\square$

Corollaire 5.33. *Soit M un module semi-simple. Alors tout sous-module de M est semi-simple et tout quotient de M est semi-simple.*

Démonstration. Soit M' un sous-module de M. On choisit une famille $\{S_i\}_{i \in I}$ de sous-modules simples de M telle que $M = \sum_{i \in I} S_i$. Par la proposition 5.29, il existe une partie $J_0 \subset I$ telle que $M = M' \oplus (\oplus_{j \in J_0} S_j)$. Posons $M'' = \oplus_{j \in J_0} S_j$. Alors M'' est semi-simple et, comme $M = M' \oplus M''$, $M/M' \simeq M''$, donc M/M' est semi-simple.

Encore par la proposition 5.29, il existe une partie $K_0 \subset I$ telle que $M = M'' \oplus (\oplus_{k \in K_0} S_k)$. Alors $M' \simeq M/M'' \simeq \oplus_{k \in K_0} S_k$, donc M' est semi-simple. $\square$

Proposition 5.34. *Soit M un module sur A. Alors M est semi-simple si et seulement si tout sous-module de M admet un facteur direct.*

Démonstration. Par le corollaire 5.31, si M est semi-simple, alors tout sous-module de M admet un facteur direct.

Maintenant, on se donne un module M tel que tout sous-module de M admet un facteur direct et on montre que M est semi-simple. Ceci se fait en trois étapes.

Étape 1 : Soient N un sous-module de M et $N' \subset N$ un sous-module de N. Montrons que N' admet un facteur direct dans N. Soit N'' un facteur direct de N' dans M (i.e. $M = N' \oplus N''$). On a

$$N' \cap (N'' \cap N) = \{0_M\} \cap N = \{0_M\}\,.$$

Par ailleurs, soit $n \in N$. Comme $M = N' \oplus N''$, on peut écrire n sous la forme $n = n' + n''$, où $n' \in N'$ et $n'' \in N''$. Comme $n' \in N' \subset N$, on a $n'' = n - n' \in N$, donc $n'' \in N'' \cap N$. D'où $N = N' + (N'' \cap N)$, donc $N = N' \oplus (N'' \cap N)$.

Étape 2 : Soit N un sous-module de M non trivial. Montrons que N contient un sous-module simple. On choisit $n \in N$, $n \neq 0$. On a un morphisme de modules $\varphi : A \to N$, $a \mapsto a \cdot n$. Notons I le noyau de φ. C'est un idéal propre à gauche de A et φ induit un morphisme de modules injectif $\bar{\varphi} : A/I \to N$. Notons $N_1 = \operatorname{Im} \bar{\varphi} = \operatorname{Im} \varphi$. D'après le théorème 5.23, il existe un idéal maximal J de A contenant I. Posons $N_2 = \varphi(J) = \bar{\varphi}(J/I)$. D'après l'étape 1, il existe un sous-module N_3 de N_1 tel que $N_1 = N_2 \oplus N_3$. Alors

$$N_3 \simeq N_1/N_2 \simeq (A/I)/(J/I) \simeq A/J\,,$$

donc N_3 est simple.

Étape 3 : Posons $N = \sum_{S \subset M, S \text{ simple}} S$. Montrons que $N = M$ par l'absurde. Supposons que $M \neq N$. Par hypothèse, il existe un sous-module N' de M tel que $M = N \oplus N'$. Le sous-module N' est non trivial car $N \neq M$. Par l'étape 2, on en déduit que N' contient un sous-module simple, S_0. Ceci n'est pas possible car, par définition, N contient tous les sous-modules simples de M et $N \cap S_0 = \{0_M\}$. $\square$

Corollaire 5.35. *Soient M un module semi-simple, $\{S_i\}_{i \in I}$ une collection de sous-modules simples telle que $M = \oplus_{i \in I} S_i$ et S un sous-module simple de M. Il existe $i_0 \in I$ tel que $S \simeq S_{i_0}$.*

Démonstration. Par le corollaire 5.31, il existe un sous-module N' de M tel que $M = S \oplus N'$. Par la proposition 5.29, il existe une partie $J_0 \subset I$ telle que $M = N' \oplus (\oplus_{j \in J_0} S_j)$. On a

$$S \simeq M/N' \simeq \oplus_{j \in J_0} S_j\,,$$

donc $|J_0| = 1$ car S est simple. Soit $i_0 \in I$ tel que $J_0 = \{i_0\}$. Alors $S \simeq S_{i_0}$. $\square$

Définition. Un anneau A est appelé *semi-simple* si tout module sur A est semi-simple.

Exemple. Tout corps est un anneau semi-simple.

Proposition 5.36. *Un anneau A est semi-simple si et seulement si A est un module semi-simple sur A.*

Démonstration. Si A est semi-simple, il est évident que A, vu comme module sur A, est semi-simple. Supposons que A soit un module semi-simple sur A et montrons que A est semi-simple, c'est-à-dire que tout module sur A est semi-simple. Soit M un module sur A. Pour $m \in M$, soit $A \cdot m$ le sous-module de M engendré par m. On a un morphisme surjectif $A \to A \cdot m$, $a \mapsto a \cdot m$, donc $A \cdot m$ est un quotient de A (à isomorphisme près). Comme A est semi-simple, par le corollaire 5.33, $A \cdot m$ est aussi semi-simple, donc il existe une collection $\{S_i\}_{i \in I_m}$ de sous-modules simples telle que $A \cdot m = \sum_{i \in I_m} S_i$. Finalement

$$M = \sum_{m \in M} A \cdot m = \sum_{m \in M} \sum_{i \in I_m} S_i \,,$$

donc M est semi-simple. □

6 Représentations linéaires des groupes finis

6.1 Définitions et premières propriétés

Définition. Soient $\mathbb{K}$ un corps et V un espace vectoriel sur $\mathbb{K}$. On note $\mathrm{GL}(V)$ le groupe des isomorphismes linéaires de V sur lui-même. Un élément de $\mathrm{GL}(V)$ est, par définition, une application linéaire A de V dans V qui admet un inverse A^{-1}. Soit G un groupe. Une *représentation linéaire* de G dans V est un homomorphisme $\rho : G \to \mathrm{GL}(V)$. Lorsque ρ est donnée, on dit que V est un *espace de représentation* ou tout simplement une *représentation* de G. Si V est de dimension finie, alors sa dimension s'appelle le *degré* de la représentation ρ.

Définition. Soient $\mathbb{K}$ un corps, V, V' deux espaces vectoriels sur $\mathbb{K}$, G un groupe et $\rho : G \to \mathrm{GL}(V)$, $\rho' : G \to \mathrm{GL}(V')$ deux représentations linéaires de G. On dit que ρ et ρ' sont *isomorphes* s'il existe un isomorphisme linéaire $\tau : V \to V'$ tel que

$$\rho(g) = \tau \circ \rho'(g) \circ \tau^{-1}$$

pour tout $g \in G$.

Exemple 1. Une représentation de degré 1 est un homomorphisme de G dans $\mathbb{K}^*$. Si G est fini, alors $\rho(g)$ est forcément une racine de l'unité. La représentation $\mathbb{I}_G : G \to \mathbb{K}^*$, $g \mapsto 1_{\mathbb{K}}$ s'appelle la *représentation unité*.

Exemple 2. Soit G un groupe. Pour tout $g \in G$ on définit l'application linéaire $\rho(g) : \mathbb{K}[G] \to \mathbb{K}[G]$ par

$$\rho(g)(h) = gh \text{ pour tout } h \in G\,.$$

On vérifie facilement que l'application $\rho : G \to \mathrm{GL}(\mathbb{K}[G])$ est une représentation linéaire de G. Elle s'appelle la *représentation régulière*. Si G est fini, alors son degré est $|G|$.

Par ailleurs, si $\rho : G \to \mathrm{GL}(V)$ est une représentation linéaire et V contient un vecteur v_1 tel que l'ensemble $\{\rho(g)(v_1); g \in G\}$ soit une base de V, alors ρ est isomorphe à la représentation régulière (en exercice).

Exemple 3. Supposons que notre groupe G agit sur un ensemble X. Notons V l'espace vectoriel sur $\mathbb{K}$ ayant X pour base. Pour tout $g \in G$ on définit $\rho(g) \in \mathrm{GL}(V)$ par

$$\rho(g)(x) = g \cdot x \text{ pour tout } x \in X\,.$$

Alors $\rho : G \to \mathrm{GL}(V)$ est une représentation linéaire de G appelée *représentation de permutation* associée à l'action de G sur X.

Lemme 6.1. *Soient A une algèbre sur $\mathbb{K}$ et M un module sur A. On définit une loi $\mathbb{K} \times M \to M$ par*

$$t\,m = (t\,1_A) \cdot m\,,$$

pour tous $t \in \mathbb{K}$ et $m \in M$. Alors M muni de la loi $+$ est de cette multiplication est un espace vectoriel sur $\mathbb{K}$.

Démonstration. Exercice. □

Proposition 6.2. *Soit G un groupe.*

(1) *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. On définit une opération $\mathbb{K}[G] \times V \to V$, $(a, v) \mapsto a \cdot v$ comme suit. Soient $a \in \mathbb{K}[G]$ et $v \in V$. On écrit $a = \sum_{g \in I} t_g \cdot g$, où I est une partie finie de G et $t_g \in \mathbb{K}$ pour tout $g \in I$. Alors*

$$a \cdot v = \sum_{g \in I} t_g\, \rho(g)(v)\,.$$

Alors V muni de cette loi est un module sur $\mathbb{K}[G]$ que l'on note Mod_ρ.

(2) *Soit M un module sur $\mathbb{K}[G]$. Il existe une représentation linéaire $\rho : G \to \mathrm{GL}(V)$, unique à isomorphisme près, telle que $M \simeq \mathrm{Mod}_\rho$.*

Démonstration. On se donne une représentation linéaire $\rho : G \to \mathrm{GL}(V)$ et on considère la loi $\mathbb{K}[G] \times V \to V$ définie dans la proposition. On doit montrer que :

(a) $(a + a') \cdot v = (a \cdot v) + (a' \cdot v)$ pour tous $a, a' \in \mathbb{K}[G]$ et $v \in V$;

(b) $a \cdot (v + v') = (a \cdot v) + (a \cdot v')$ pour tous $a \in \mathbb{K}[G]$ et $v, v' \in V$;

(c) $a \cdot (a' \cdot v) = (aa') \cdot v$ pour tous $a, a' \in \mathbb{K}[G]$ et $v \in V$;

(d) $1_G \cdot v = v$ pour tout $v \in V$.

On se donne $a, a' \in \mathbb{K}[G]$ et $v, v' \in V$. On choisit une partie finie $I \subset G$ telle que a, a' puissent s'écrire sous la forme $a = \sum_{g\in I} t_g\, g$ et $a' = \sum_{g \in I} t'_g\, g$ avec $t_g, t'_g \in \mathbb{K}$ pour tout $g \in I$.

$$\begin{aligned}(a+a')\cdot v &= \left(\sum_{g\in I}(t_g+t'_g)g\right)\cdot v = \sum_{g\in I}(t_g+t'_g)\rho(g)(v)\\ &= \left(\sum_{g\in I} t_g\,\rho(g)(v)\right) + \left(\sum_{g\in I} t'_g\,\rho(g)(v)\right) = (a\cdot v) + (a'\cdot v)\,.\end{aligned}$$

$$\begin{aligned}a\cdot(v+v') &= \sum_{g\in I} t_g\,\rho(g)(v+v') = \sum_{g\in I} t_g(\rho(g)(v)+\rho(g)(v'))\\ &= \left(\sum_{g\in I} t_g\,\rho(g)(v)\right) + \left(\sum_{g\in I} t_g\,\rho(g)(v')\right) = (a\cdot v) + (a\cdot v')\,.\end{aligned}$$

$$(aa')\cdot v = \left(\sum_{g\in I}\sum_{g'\in I} t_g t'_{g'}\, gg'\right)\cdot v = \sum_{g\in I}\sum_{g'\in I} t_g t'_{g'}\,\rho(gg')(v)$$

$$= \sum_{g\in I}\sum_{g'\in I} t_g t'_{g'}\,(\rho(g)\circ\rho(g'))(v) = \sum_{g\in I} t_g\,\rho(g)\left(\sum_{g'\in I} t'_{g'}\,\rho(g')(v)\right) = a\cdot(a'\cdot v)\,.$$

$$1_G\cdot v = \rho(1_G)(v) = \mathrm{Id}(v) = v\,.$$

Maintenant, on se donne un module M sur $\mathbb{K}[G]$. Rappelons que M est un espace vectoriel sur $\mathbb{K}$ (voir Lemme 6.1). Pour tout $g \in G$ on définit $\rho(g) : M \to M$ par

$$\rho(g)(m) = g\cdot m\,.$$

Il est évident que $\rho(g)$ est une application linéaire. Si $g, g' \in G$, alors

$$(\rho(g)\circ\rho(g'))(m) = g\cdot(g'\cdot m) = (gg')\cdot m = \rho(gg')(m)\,,$$

pour tout $m \in M$, donc $\rho(g)\circ\rho(g') = \rho(gg')$. De plus

$$\rho(1_G)(m) = 1_G\cdot m = m$$

pour tout $m \in M$, donc $\rho(1_G) = \mathrm{Id}_M$. Ceci implique que, pour tout $g \in G$,

$$\mathrm{Id} = \rho(1_G) = \rho(gg^{-1}) = \rho(g)\circ\rho(g^{-1})\,,$$

donc $\rho(g)$ est inversible (i.e. $\rho(g) \in \mathrm{GL}(M)$) et ρ est un homomorphisme. En d'autres termes, ρ est une représentation linéaire de G. On démontre facilement que $M = \mathrm{Mod}_\rho$. $\square$

Définition. Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire d'un groupe G et W un sous-espace vectoriel de V. On dit que W est *stable* par ρ si $\rho(g)(W) = W$ pour tout $g \in G$. Dans ce cas on a une représentation linéaire $\rho^W : G \to \mathrm{GL}(W)$, $g \mapsto \rho(g)|_W$. On dit que ρ^W (ou W) est une *sous-représentation* de ρ (ou de V).

Exemple. Supposons que G soit fini et $\rho : G \to \mathrm{GL}(\mathbb{K}[G])$ est la représentation régulière. Posons $w_0 = \sum_{g\in G} g$. On a $\rho(g)(w_0) = w_0$ pour tout $g \in G$ donc la droite $W = \mathbb{K} \cdot w_0$ engendrée par w_0 est stable par ρ, et ρ^W est une sous-représentation isomorphe à la représentation unité.

Lemme 6.3. *Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire d'un groupe G et W un sous-espace vectoriel de V. Alors W est stable par ρ si et seulement si W est un sous-module de $\mathrm{Mod}_\rho = V$.*

Démonstration. Exercice. $\square$

A partir de maintenant nous supposerons que $\mathbb{K}$ est de caractéristique 0, G est un groupe fini et tous les espaces vectoriels considérés seront de dimension finie sauf mention du contraire.

Théorème 6.4. *Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de V et $W \subset V$ un sous-espace vectoriel stable par ρ. Il existe un sous-espace vectoriel $W' \subset V$ stable par ρ tel que $V = W \oplus W'$.*

Démonstration. On choisit W_0 un sous-espace supplémentaire de W (i.e. $V = W \oplus W_0$) et on note $\pi_0 : V \to V$ la projection de V sur W parallèlement à W_0. Rappelons que $\pi_0^2 = \pi_0$, $\operatorname{Ker} \pi_0 = W_0$ et $\operatorname{Im} \pi_0 = W$. Posons

$$\pi = \frac{1}{|G|} \sum_{g\in G} (\rho(g) \circ \pi_0 \circ \rho(g^{-1}))\,.$$

On va d'abord montrer que π est une projection d'image W, c'est-à-dire que $\pi^2 = \pi$ et $\operatorname{Im} \pi = W$. Si l'on pose $W' = \operatorname{Ker} \pi$ on aura alors $V = W \oplus W'$.

Soit $v \in V$. pour tous $g, h \in G$ on a $(\pi_0 \circ \rho(g^{-1}))(v) \in W$ car W est l'image de π_0, donc $(\rho(h^{-1}g) \circ \pi_0 \circ \rho(g))(v) \in W$, car W est stable par ρ, donc

$$\begin{aligned}
&(\pi_0 \circ \rho(h^{-1}g) \circ \pi_0 \circ \rho(g^{-1}))(v) = (\rho(h^{-1}g) \circ \pi_0 \circ \rho(g^{-1}))(v)\\
\Rightarrow\ &(\rho(h) \circ \pi_0 \circ \rho(h^{-1}g) \circ \pi_0 \circ \rho(g^{-1}))(v) = (\rho(hh^{-1}g) \circ \pi_0 \circ \rho(g^{-1}))(v)\\
&\qquad = (\rho(g) \circ \pi_0 \circ \rho(g^{-1}))(v)
\end{aligned}$$

d'où

$$\begin{aligned}
(\pi \circ \pi)(v) &= \frac{1}{|G|}\frac{1}{|G|}\sum_{h\in G}\sum_{g\in G}(\rho(h)\circ \pi_0 \circ \rho(h^{-1}g)\circ \pi_0 \circ \rho(g^{-1}))(v) \\
&= \frac{1}{|G|}\frac{1}{|G|}\sum_{h\in G}\sum_{g\in G}(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(v) \\
&= \pi(v)
\end{aligned}$$

Soit $w \in W$. Pour tout $g \in G$ on a $\rho(g^{-1})(w) \in W$ car W est stable par ρ, donc $(\pi_0 \circ \rho(g^{-1}))(w) = \rho(g^{-1})(w)$, donc

$$(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(w) = \rho(gg^{-1})(w) = \rho(1_G)(w) = w\,.$$

On en déduit que

$$\pi(w) = \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(w) = \frac{1}{|G|}\sum_{g\in G} w = w\,.$$

En particulier, $w \in \operatorname{Im}\pi$.

Soit $v \in V$. Pour tout $g \in G$ on a $(\pi_0 \circ \rho(g^{-1}))(v) \in W$ car W est l'image de π_0, donc $(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(v) \in W$ car W est stable par ρ. On en déduit que

$$\pi(v) = \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(v) \in W\,.$$

En conclusion : $W = \operatorname{Im}\pi$.

On pose $W' = \operatorname{Ker}\pi$. Comme π est une projection et $W = \operatorname{Im}\pi$, on a $V = W \oplus W'$. Reste à montrer que W' est stable par ρ.

Soit $w \in W'$. Pour tout $h \in G$ on a

$$\begin{aligned}
\pi(\rho(h)(w)) &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ \pi_0 \circ \rho(g^{-1}h))(w) \\
&= \rho(h)\left(\frac{1}{|G|}\sum_{g\in G}(\rho(h^{-1}g)\circ \pi_0 \circ \rho(g^{-1}h))(w)\right) \\
&= \rho(h)\left(\frac{1}{|G|}\sum_{g\in G}(\rho(g)\circ \pi_0 \circ \rho(g^{-1}))(w)\right) \\
&= \rho(h)(\pi(w)) = \rho(h)(\overrightarrow{0}) = \overrightarrow{0}
\end{aligned}$$

donc $\rho(h)(w) \in \operatorname{Ker}\pi = W'$. $\square$

Corollaire 6.5. *L'algèbre de groupe* $\mathbb{K}[G]$ *est semi-simple.*

Démonstration. Soient M un module sur $\mathbb{K}[G]$ et N un sous-module de M. Soit $\rho : G \to \mathrm{GL}(M)$ la représentation linéaire définie par $\rho(g)(m) = g \cdot m$ pour tous $g \in G$ et $m \in M$. Le sous-espace N de M est stable par ρ, donc il existe un sous-espace vectoriel N' stable par ρ tel que $M = N \oplus N'$. Alors N' est un sous-module de M et est un facteur direct de N. $\square$

Maintenant nous allons supposer pour un petit moment que $\mathbb{K} = \mathbb{R}$ est le corps des nombres réels.

Définition. Soient V un espace vectoriel sur $\mathbb{R}$ et $\langle \,|\, \rangle : V \times V \to \mathbb{R}$ une forme bilinéaire symétrique. On dit que $\langle \,|\, \rangle$ est un *produit scalaire* si $\langle u \mid u \rangle > 0$ pour tout $u \in V \setminus \{\vec{0}\}$. Dans ce cas le *groupe orthogonal* de $\langle \,|\, \rangle$, noté $O(V, \langle \,|\, \rangle)$, est formé des transformations linéaires $f : V \to V$ qui laissent invariante la forme, c'est-à-dire telles que $\langle f(u)|f(v)\rangle = \langle u|v\rangle$ pour tous $u, v \in V$.

Proposition 6.6. *Soient V un espace vectoriel réel et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Il existe un produit scalaire $\langle \,|\, \rangle$ sur V tel que l'image de ρ soit incluse dans $O(V, \langle \,|\, \rangle)$.*

Démonstration. Soit $\langle \,|\, \rangle_0 : V \times V \to \mathbb{R}$ un produit scalaire quelconque. Pour $u, v \in V$ on pose

$$\langle u|v\rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(u)|\rho(g)(v)\rangle_0 \,.$$

Il est clair que $\langle \,|\, \rangle$ est un produit scalaire. Par ailleurs, si $h \in G$, alors

$$\langle \rho(h)(u)|\rho(h)(v)\rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(hg)(u)|\rho(hg)(v)\rangle_0 = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(u)|\rho(g)(v)\rangle_0 = \langle u|v\rangle$$

pour tous $u, v \in V$, donc $\rho(h) \in O(V, \langle \,|\, \rangle)$. $\square$

Lemme 6.7. *Soient V un espace vectoriel réel, W un sous-espace vectoriel de V et $\langle \,|\, \rangle$ un produit scalaire sur V. Posons $W^\perp = \{v \in V ; \langle v|w\rangle = 0$ pour tout $w \in W\}$. Alors $V = W \oplus W^\perp$.*

Démonstration. Exercice. $\square$

Proposition 6.8. *Soient V un espace vectoriel réel, $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire, $\langle \,|\, \rangle$ un produit scalaire invariant par ρ (i.e. $\operatorname{Im} \rho \subset O(V, \langle \,|\, \rangle)$) et W un sous-espace vectoriel de V invariant par ρ. Alors $W^\perp$ est aussi invariant par ρ.*

Démonstration. Soient $g \in G$ et $v \in W^\perp$. Pour tout $w \in W$ on a $\rho(g^{-1})(w) \in W$, car W est stable par ρ, donc

$$\langle \rho(g)(v)|w\rangle = \langle \rho(g)(v)|(\rho(g) \circ \rho(g^{-1}))(w)\rangle = \langle v|\rho(g^{-1})(w)\rangle = 0 \,.$$

D'où $\rho(g)(v) \in W^{\perp}$. $\square$

On revient à la situation ou $\mathbb{K}$ est un corps de caractéristique 0, mais pas nécessairement $\mathbb{R}$.

Définition. Soient $\{\rho_i : G \to \mathrm{GL}(V_i)\}_{i=1}^n$ une famille finie de représentations linéaires. On pose

$$V_1 \oplus V_2 \oplus \cdots \oplus V_n = V_1 \times V_2 \times \cdots \times V_n \,,$$

et on définit une représentation linéaire

$$\rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_n : G \to \mathrm{GL}(V_1 \oplus V_2 \oplus \cdots \oplus V_n)$$

par

$$(\rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_n)(g)(v_1, v_2, \ldots, v_n) = (\rho_1(g)(v_1), \rho_2(g)(v_2), \ldots, \rho_n(g)(v_n))\,.$$

Cette représentation s'appelle la *somme directe* de $\rho_1, \rho_2, \ldots, \rho_n$.

Exemple. Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire et W_1, W_2 deux espaces supplémentaires invariants par ρ. Posons $\rho_1 = \rho^{W_1} : G \to \mathrm{GL}(W_1)$ et $\rho_2 = \rho^{W_2} : G \to \mathrm{GL}(W_2)$. Alors $\rho \simeq \rho_1 \oplus \rho_2$ (par abus on pose $\rho = \rho_1 \oplus \rho_2$).

Définition. Une représentation $\rho : G \to \mathrm{GL}(V)$ est *simple* si V ne contient pas de sous-espace vectoriel invariant par ρ autre que V ou $\{\vec{0}\}$.

Théorème 6.9. *Toute représentation linéaire de G se décompose comme somme directe d'un nombre fini de représentations simples.*

Démonstration. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. On montre que ρ se décompose comme somme directe de représentations simples par récurrence sur $\dim V$. Si $\dim V = 1$, alors ρ est forcément simple et il n'y a rien à démontrer. Supposons que $\dim V > 1$ plus l'hypothèse de récurrence. Si ρ est simple, il n'y a rien à démontrer. On peut donc supposer que ρ n'est pas simple, c'est-à-dire qu'il existe un sous-espace vectoriel $W_1 \subset V$ invariant par ρ tel que $W_1 \neq V$ et $W_1 \neq \{\vec{0}\}$. Par le théorème 6.4, il existe un sous-espace vectoriel W_2 invariant par ρ tel que $V = W_1 \oplus W_2$. Posons $\rho_1 = \rho^{W_1} : G \to \mathrm{GL}(W_1)$ et $\rho_2 = \rho^{W_2} : G \to \mathrm{GL}(W_2)$. Alors $\rho = \rho_1 \oplus \rho_2$. De plus, comme $W_1 \neq V$ et $W_1 \neq \{\vec{0}\}$, on a $\dim W_1 < \dim V$ et $\dim W_2 < \dim V$. Par hypothèse de récurence, il existe des collections finies de représentations simples $\{\mu_i : G \to \mathrm{GL}(U_i)\}_{i=1}^k$ et $\{\mu_i : G \to \mathrm{GL}(U_i)\}_{i=k+1}^m$ telles que

$$\rho_1 = \mu_1 \oplus \cdots \oplus \mu_k\,, \quad \rho_2 = \mu_{k+1} \oplus \cdots \oplus \mu_m\,.$$

Alors

$$\rho = \rho_1 \oplus \rho_2 = \mu_1 \oplus \cdots \oplus \mu_k \oplus \mu_{k+1} \oplus \cdots \oplus \mu_m\,.$$

$\square$

Proposition 6.10. *Soient $\rho_1 : G \to \mathrm{GL}(V_1)$ et $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations linéaires de G. Alors il existe une unique représentation linéaire $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2)$ telle que*

$$(\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$$

pour tous $v_1 \in V_1$, $v_2 \in V_2$ et $g \in G$.

Démonstration. Soit $g \in G$. L'application $\varphi(g) : V_1 \times V_2 \to V_1 \otimes V_2$, $(v_1, v_2) \mapsto \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$ est bilinéaire, donc induit une application linéaire $\rho(g) : V_1 \otimes V_2 \to V_1 \otimes V_2$. Soient $g, g' \in G$. L'application $\rho(g) \circ \rho(g')$ envoie $v_1 \otimes v_2$ sur $\rho(gg')(v_1) \otimes \rho(gg')(v_2)$ pour tout $(v_1, v_2) \in V_1 \times V_2$, donc $\rho(g) \circ \rho(g') = \rho(gg')$. Par ailleurs, l'application $\rho(1_G)$ envoie $v_1 \otimes v_2$ sur $\rho_1(1_G)(v_1) \otimes \rho_2(1_G)(v_2) = v_1 \otimes v_2$ pour tout $(v_1, v_2) \in V_1 \times V_2$, donc $\rho(1_G) = \mathrm{Id}_{V_1 \otimes V_2}$. Ceci montre d'abord que, si $g \in G$, alors $\rho(g) \circ \rho(g^{-1}) = \rho(gg^{-1}) = \rho(1_G) = \mathrm{Id}$, donc $\rho(g)$ est inversible. Ensuite $\rho : G \to \mathrm{GL}(V_1 \otimes V_2)$ est une représentation. On a $\rho(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$ pour tout $(v_1, v_2) \in V_1 \times V_2$ par définition. Finalement, ρ est unique car $\rho(g)$ est entièrement déterminée par les images de $v_1 \otimes v_2$ pour $(v_1, v_2) \in V_1 \times V_2$. □

Définition. La représentation $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2)$ de la proposition 6.10 s'appelle le *produit tensoriel* de ρ_1 et ρ_2.

Définition. Soit V un espace vectoriel sur $\mathbb{K}$. On définit $\tilde{\theta} : V \times V \to V \otimes V$ par $\tilde{\theta}(v_1, v_2) = v_2 \otimes v_1$. Il est clair que $\tilde{\theta}$ est bilinéaire, donc induit une application linéaire $\theta : V \otimes V \to V \otimes V$. L'application θ^2 envoie $v_1 \otimes v_2$ sur $v_1 \otimes v_2$ pour tout $(v_1, v_2) \in V \times V$, donc $\theta^2 = \mathrm{Id}$. On pose

$$\mathrm{Sym}^2(V) = \{u \in V \otimes V \ ; \ \theta(u) = u\}, \quad \mathrm{Alt}^2(V) = \{u \in V \otimes V \ ; \ \theta(u) = -u\}.$$

Lemme 6.11. *Soit V un espace vectoriel sur $\mathbb{K}$. Alors*

$$V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V).$$

De plus, si $n = \dim V$, alors

$$\dim \mathrm{Sym}^2(V) = \frac{n(n+1)}{2}, \quad \dim \mathrm{Alt}^2(V) = \frac{n(n-1)}{2}.$$

Démonstration. On se donne une base $B = \{e_1, \ldots, e_n\}$ (ordonnée) de V. Posons

$$\tilde{B}_S = \{e_i \otimes e_j + e_j \otimes e_i ; 1 \leq i \leq j \leq n\}, \ \tilde{B}_A = \{e_i \otimes e_j - e_j \otimes e_i ; 1 \leq i < j \leq n\},$$
$$\tilde{B} = \tilde{B}_S \cup \tilde{B}_A.$$

On remarque les 3 choses suivantes :

(a) $\tilde{B}_S \subset \mathrm{Sym}^2(V)$ et $|\tilde{B}_S| = \frac{n(n+1)}{2}$;

(b) $\tilde{B}_A \subset \mathrm{Alt}^2(V)$ et $|\tilde{B}_A| = \frac{n(n-1)}{2}$;

(c) $|\tilde{B}| = |\tilde{B}_S| + |\tilde{B}_S| = n^2 = \dim(V \otimes V)$.

Donc, pour démontrer le lemme 6.11, il suffit de démontrer que $\tilde{B}$ est linéairement indépendant.

Soient $a_{i,j} \in \mathbb{K}$, $1 \leq i \leq j \leq n$, et $b_{i,j} \in \mathbb{K}$, $1 \leq i < j \leq n$, tels que

$$\sum_{i \leq j} a_{i,j}(e_i \otimes e_j + e_j \otimes e_i) + \sum_{i<j} b_{i,j}(e_i \otimes e_j - e_j \otimes e_i) = \overrightarrow{0}\,.$$

Alors

$$\sum_{i=1}^{n} 2\, a_{i,i}(e_i \otimes e_i) + \sum_{i<j} \big((a_{i,j} + b_{i,j})(e_i \otimes e_j) + (a_{i,j} - b_{i,j})(e_j \otimes e_i)\big) = \overrightarrow{0}\,.$$

Ceci implique que $a_{i,j} = 0$ pour tous $i, j \in \{1, \ldots, n\}$, $i \leq j$, et $b_{i,j} = 0$ pour tous $i, j \in \{1, \ldots, n\}$, $i < j$. Donc, $\tilde{B}$ est libre. □

Lemme 6.12. *Soit* $\rho : G \to \mathrm{GL}(V)$ *une représentation linéaire. Alors* $\mathrm{Sym}^2(V)$ *et* $\mathrm{Alt}^2(V)$ *sont invariants par* $\rho \otimes \rho$.

Démonstration. On commence par démontrer que $\theta \circ (\rho \otimes \rho)(g) = (\rho \otimes \rho)(g) \circ \theta$ pour tout $g \in G$. Soit $(v_1, v_2) \in V \times V$. Alors

$$\begin{aligned} ((\rho \otimes \rho)(g) \circ \theta)(v_1 \otimes v_2) &= (\rho \otimes \rho)(g)(v_2 \otimes v_1) = \rho(g)(v_2) \otimes \rho(g)(v_1) \\ &= \theta(\rho(g)(v_1) \otimes \rho(g)(v_2)) = (\theta \circ (\rho \otimes \rho)(g))(v_1 \otimes v_2)\,. \end{aligned}$$

Pour $g \in G$ et $u \in \mathrm{Sym}^2(V)$ on a

$$(\theta \circ (\rho \otimes \rho)(g))(u) = ((\rho \otimes \rho)(g) \circ \theta)(u) = (\rho \otimes \rho)(g)(u)\,,$$

donc $(\rho \otimes \rho)(g)(u) \in \mathrm{Sym}^2(V)$. D'où $\mathrm{Sym}^2(V)$ est invariant par $\rho \otimes \rho$. De même, pour $g \in G$ et $u \in \mathrm{Alt}^2(V)$ on a

$$(\theta \circ (\rho \otimes \rho)(g))(u) = ((\rho \otimes \rho)(g) \circ \theta)(u) = (\rho \otimes \rho)(g)(-u) = -(\rho \otimes \rho)(g)(u)\,,$$

donc $(\rho \otimes \rho)(g)(u) \in \mathrm{Alt}^2(V)$. D'où $\mathrm{Alt}^2(V)$ est invariant par $\rho \otimes \rho$. □

Définition. Les sous-représentations $\rho_S^2 = (\rho \otimes \rho)^{\mathrm{Sym}^2(V)} : G \to \mathrm{GL}(\mathrm{Sym}^2(V))$ et $\rho_A^2 = (\rho \otimes \rho)^{\mathrm{Alt}^2(V)} : G \to \mathrm{GL}(\mathrm{Alt}^2(V))$ sont appelées *carré symétrique* et *carré alterné* de ρ, respectivement.

6.2 Théorie des caractères

A partir de maintenant nous supposerons que $\mathbb{K} = \mathbb{C}$ est le corps des nombres complexes. Rappelons que G désigne un groupe fini et tous les espaces vectoriels considérés sont de dimension finie, sauf mention du contraire.

Définition. Soit V un espace vectoriel complexe. Une *forme hermitienne* sur V est une application $\langle\,|\,\rangle : V \times V \to \mathbb{C}$ vérifiant :

(a) $\langle t_1 u_1 + t_2 u_2 | v\rangle = t_1\langle u_1|v\rangle + t_2\langle u_2|v\rangle$ pour tous $u_1, u_2, v \in V$ et $t_1, t_2 \in \mathbb{C}$;

(b) $\langle u | t_1 v_1 + t_2 v_2\rangle = \overline{t_1}\langle u|v_1\rangle + \overline{t_2}\langle u|v_2\rangle$ pour tous $u, v_1, v_2 \in V$ et $t_1, t_2 \in \mathbb{C}$;

(c) $\langle u|v\rangle = \langle v, u\rangle^*$ pour tous $u, v \in V$. (Si $z = x + iy$ est un nombre complexe, nous noterons indifféremment z^* ou $\bar{z}$ le conjugué de z, $x - iy$.)

On dit que $\langle\,|\,\rangle$ est une *forme hermitienne définie positive* (ou un *produit scalaire complexe*) si, de plus,

(d) $\langle u|u\rangle > 0$ pour tout $u \in V \setminus \{\overrightarrow{0}\}$.

Définition. Soit $\langle\,|\,\rangle$ une forme hermitienne définie positive sur un espace vectoriel complexe V. Le *groupe unitaire* de $\langle\,|\,\rangle$, noté $U(V, \langle\,|\,\rangle)$, est le groupe formé des transformations linéaires $f : V \to V$ vérifiant $\langle f(u)|f(v)\rangle = \langle u|v\rangle$ pour tous $u, v \in V$.

Proposition 6.14. *Soient V un espace vectoriel complexe et $\langle\,|\,\rangle$ une forme hermitienne sur V définie positive. Alors toute transformation $f \in U(V, \langle\,|\,\rangle)$ est diagonalisable, c'est-à-dire, pour tout $f \in U(V, \langle\,|\,\rangle)$ il existe une base $\{e_1, \ldots, e_n\}$ de V et des scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ tels que $f(e_i) = \lambda_i\, e_i$ pour tout $i \in \{1, \ldots, n\}$.*

Démonstration. Exercice. □

Le résultat suivant se démontre de la même façon que la proposition 6.6.

Proposition 6.15. *Soient V un espace vectoriel complexe et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Il existe un produit scalaire complexe $\langle\,|\,\rangle$ sur V tel que l'image de ρ soit incluse dans $U(V, \langle\,|\,\rangle)$.*

Démonstration. Exercice. □

Corollaire 6.16. *Soient V un espace vectoriel complexe et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Alors $\rho(g)$ est diagonalisable pour tout $g \in G$.*

Démonstration. Par la proposition 6.15, il existe un produit scalaire complexe $\langle\,|\,\rangle$ sur V tel que $\rho(g)$ soit inclus dans $U(V, \langle\,|\,\rangle)$. Par la proposition 6.14, on en conclue que $\rho(g)$ est diagonalisable. □

Définition. Soit $\rho : G \to GL(V)$ une représentation linéaire de G. Alors l'application

$$\begin{array}{rccc} \chi_\rho : & G & \to & \mathbb{C} \\ & g & \mapsto & \mathrm{Tr}(\rho(g)) \end{array}$$

s'appelle le *caractère* de la représentation ρ. Un *caractère* de G est un caractère d'une représentation linéaire de G.

Proposition 6.17. *Soit χ le caractère d'une représentation $\rho : G \to \mathrm{GL}(V)$ de rang n.*

(1) $\chi(1_G) = n$.

(2) $\chi(g^{-1}) = \chi(g)^*$ *pour tout* $g \in G$.

(3) $\chi(hgh^{-1}) = \chi(g)$ *pour tous* $h, g \in G$.

Démonstration. On a $\rho(1_G) = \mathrm{Id}_V$ et $\mathrm{Tr}(\mathrm{Id}_V) = n$ car V est de dimension n, donc $\chi(1_G) = n$.

Soit $g \in G$. Comme G est fini, g est d'ordre fini, donc il existe un entier positif p tel que $g^p = 1_G$. On a alors $\rho(g)^p = \mathrm{Id}_V$. Si λ est une valeur propre de $\rho(g)$, alors λ^p est une valeur propre de $\rho(g)^p = \mathrm{Id}$, donc $\lambda^p = 1$. Cette égalité implique que $|\lambda| = 1$, donc que $\lambda^{-1} = \lambda^*$. Par le corollaire 6.16, il existe une base $\{e_1, \ldots, e_n\}$ de V et des scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ tels que $\rho(g)(e_i) = \lambda_i\, e_i$ pour tout $i \in \{1, \ldots, n\}$. Alors

$$\chi(g)^* = \sum_{i=1}^{n} \lambda_i^* = \sum_{i=1}^{n} \lambda_i^{-1} = \chi(g^{-1})\,.$$

Soient $g, h \in G$. Alors

$$\chi(hgh^{-1}) = \mathrm{Tr}(\rho(h)\,\rho(g)\,\rho(h)^{-1}) = \mathrm{Tr}(\rho(g)\,\rho(h)^{-1}\,\rho(h)) = \mathrm{Tr}(\rho(g)) = \chi(g)\,.$$

□

Lemme 6.18. *Soient V_1, V_2 deux espaces vectoriels, $f_1 \in \mathcal{L}(V_1)$ et $f_2 \in \mathcal{L}(V_2)$. Alors* $\mathrm{Tr}(f_1 \oplus f_2) = \mathrm{Tr}(f_1) + \mathrm{Tr}(f_2)$ *et* $\mathrm{Tr}(f_1 \otimes f_2) = \mathrm{Tr}(f_1) \cdot \mathrm{Tr}(f_2)$.

Démonstration. Exercice. □

Corollaire 6.19. *Soient $\rho_1 : G \to \mathrm{GL}(V_1)$ et $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations linéaires de G et χ_1, χ_2 les caractères de ρ_1, ρ_2, respectivement.*

(1) *Le caractère de* $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$ *est* $\chi_1 + \chi_2$.

(2) *Le caractère de* $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2)$ *est* $\chi_1 \cdot \chi_2$.

Démonstration. Soit $g \in G$. Alors

$$\begin{aligned}\chi_{\rho_1 \oplus \rho_2}(g) &= \mathrm{Tr}((\rho_1 \oplus \rho_2)(g)) = \mathrm{Tr}(\rho_1(g) \oplus \rho_2(g)) \\ &= \mathrm{Tr}(\rho_1(g)) + \mathrm{Tr}(\rho_2(g)) = (\chi_1 + \chi_2)(g)\,. \\ \chi_{\rho_1 \otimes \rho_2}(g) &= \mathrm{Tr}((\rho_1 \otimes \rho_2)(g)) = \mathrm{Tr}(\rho_1(g) \otimes \rho_2(g)) \\ &= \mathrm{Tr}(\rho_1(g)) \cdot \mathrm{Tr}(\rho_2(g)) = (\chi_1 \cdot \chi_2)(g)\,.\end{aligned}$$

□

Proposition 6.20. *Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G et χ son caractère. Soient χ_S le caractère du carré symétrique et χ_A le caractère du carré alterné de ρ. Pour tout $g \in G$ on a*

$$\chi_S(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))\,, \quad \chi_A(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))\,.$$

Remarque. Selon ces formules on a bien

$$\chi_S + \chi_A = \chi^2 = \chi_{\rho \otimes \rho}\,.$$

Démonstration. Soit $g \in G$. Par le corollaire 6.16, il existe une base $\{e_1, \ldots, e_n\}$ de V et des scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ tels que $\rho(g)(e_i) = \lambda_i\, e_i$ pour tout $i \in \{1, \ldots, n\}$. On a vu dans la démonstration du lemme 6.11 que l'ensemble $\tilde{B}_S = \{e_i \otimes e_j + e_j \otimes e_i; 1 \leq i \leq j \leq n\}$ est une base de $\mathrm{Sym}^2(V)$. On a

$$\rho_S^2(g)(e_i \otimes e_j + e_j \otimes e_i) = (\rho \otimes \rho)(g)(e_i \otimes e_j + e_j \otimes e_i) = \lambda_i \lambda_j (e_i \otimes e_j + e_j \otimes e_i)$$

pour tous $i, j \in \{1, \ldots, n\}$, $i \leq j$, d'où

$$\begin{aligned}\chi_S(g) = \mathrm{Tr}(\rho_S^2(g)) &= \sum_{i \leq j} \lambda_i \lambda_j = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j + \frac{1}{2} \sum_{i=1}^{n} \lambda_i^2 \\ &= \frac{1}{2} \left(\sum_{i=1}^{n} \lambda_i \right) \left(\sum_{j=1}^{n} \lambda_j \right) + \frac{1}{2} \sum_{i=1}^{n} \lambda_i^2 = \frac{1}{2}\chi(g)^2 + \frac{1}{2}\chi(g^2)\,.\end{aligned}$$

On a vu aussi dans la démonstration du lemme 6.11 que l'ensemble $\tilde{B}_A = \{e_i \otimes e_j - e_j \otimes e_i; 1 \leq i < j \leq n\}$ est une base de $\mathrm{Alt}^2(V)$. On a

$$\rho_A^2(g)(e_i \otimes e_j - e_j \otimes e_i) = (\rho \otimes \rho)(g)(e_i \otimes e_j - e_j \otimes e_i) = \lambda_i \lambda_j (e_i \otimes e_j - e_j \otimes e_i)$$

pour tous $i, j \in \{1, \dots, n\}$, $i < j$, d'où

$$\chi_A(g) = \mathrm{Tr}(\rho_A^2(g)) = \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j - \frac{1}{2} \sum_{i=1}^{n} \lambda_i^2$$
$$= \frac{1}{2} \left(\sum_{i=1}^{n} \lambda_i \right) \left(\sum_{j=1}^{n} \lambda_j \right) - \frac{1}{2} \sum_{i=1}^{n} \lambda_i^2 = \frac{1}{2} \chi(g)^2 - \frac{1}{2} \chi(g^2) .$$

□

Proposition 6.21 (Lemme de Schur). *Soient $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations linéaires simples de G et $\varphi : V_1 \to V_2$ une application linéaire telle que $\varphi \circ \rho_1(g) = \rho_2(g) \circ \varphi$ pour tout $g \in G$.*

(1) *Si φ n'est pas un isomorphisme, alors $\varphi = 0$.*

(2) *Si $V_1 = V_2$ et $\rho_1 = \rho_2$, alors φ est une homothétie.*

Remarque. Si φ est un isomorphisme linéaire dans la proposition 6.21 (1), alors ρ_1 et ρ_2 sont isomorphes.

Démonstration. On commence par démontrer (1). On suppose que $\varphi \neq 0$ et on démontre que φ est un isomorphisme, c'est-à-dire que $\mathrm{Ker}\,\varphi = \{\overrightarrow{0}\}$ et $\mathrm{Im}\,\varphi = V_2$.

Soit $v \in \mathrm{Ker}\,\varphi$. Pour tout $g \in G$ on a

$$\varphi(\rho_1(g)(v)) = \rho_2(g)(\varphi(v)) = \rho_2(g)(\overrightarrow{0}) = \overrightarrow{0} ,$$

donc $\rho_1(g)(v) \in \mathrm{Ker}\,\varphi$. Ceci montre que $\mathrm{Ker}\,\varphi$ est invariant par ρ_1. Comme ρ_1 est simple et $\mathrm{Ker}\,\varphi \neq V_1$ (car $\varphi \neq 0$), on en déduit que $\mathrm{Ker}\,\varphi = \{\overrightarrow{0}\}$.

Soit $w \in \mathrm{Im}\,\varphi$. Il existe $v \in V_1$ tel que $w = \varphi(v)$. Pour tout $g \in G$ on a

$$\rho_2(g)(w) = \rho_2(g)(\varphi(v)) = \varphi(\rho_1(g)(v)) ,$$

donc $\rho_2(g)(w) \in \mathrm{Im}\,\varphi$. Ceci montre que $\mathrm{Im}\,\varphi$ est invariant par ρ_2. Comme ρ_2 est simple et $\mathrm{Im}\,\varphi \neq \{\overrightarrow{0}\}$ (car $\varphi \neq 0$), on en conclue que $\mathrm{Im}\,\varphi = V_2$.

Maintenant on suppose que $V_1 = V_2$ et $\rho_1 = \rho_2$. Soient λ une valeur propre de φ et $U \subset V_1$ l'espace des vecteurs porpres pour la valeur propre λ. Remarquons que $U \neq \{\overrightarrow{0}\}$. Si $u \in U$, alors, pour tout $g \in G$,

$$\varphi(\rho_1(g)(u)) = \rho_1(g)(\varphi(u)) = \rho_1(g)(\lambda\, u) = \lambda\, \rho_1(g)(u) ,$$

donc $\rho_1(g)(u) \in U$. Ceci montre que U est invariant par ρ_1. comme ρ_1 est simple et $U \neq \{\overrightarrow{0}\}$, on en conclut que $U = V_1$, donc que φ est l'homothétie de rapport λ. □

Corollaire 6.22. *Soient $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations linéaires simples de G et $\varphi : V_1 \to V_2$ une application linéaire. Posons*

$$\varphi_0 = \frac{1}{|G|} \sum_{g\in G} (\rho_2(g) \circ \varphi \circ \rho_1(g)^{-1}) \, .$$

(1) *Si ρ_1 et ρ_2 ne sont pas isomorphes, alors $\varphi_0 = 0$.*

(2) *Si $V_1 = V_2$ et $\rho_1 = \rho_2$ alors φ_0 est l'homothétie de rapport $\frac{1}{n}\mathrm{Tr}(\varphi)$, où $n = \dim V_1$.*

Démonstration. Pour tout $h \in G$ on a

$$\begin{aligned}\varphi_0 \circ \rho_1(h) &= \frac{1}{|G|} \sum_{g\in G} (\rho_2(g) \circ \varphi \circ \rho_1(g^{-1}h)) = \rho_2(h) \circ \left(\frac{1}{|G|} \sum_{g\in G} (\rho_2(h^{-1}g) \circ \varphi \circ \rho_1(g^{-1}h)) \right) \\ &= \rho_2(h) \circ \left(\frac{1}{|G|} \sum_{g\in G} (\rho_2(g) \circ \varphi \circ \rho_1(g^{-1})) \right) = \rho_2(h) \circ \varphi_0 \, .\end{aligned}$$

Si ρ_1 et ρ_2 ne sont pas isomorphes alors, par ce qui précède et la proposition 6.21, $\varphi_0 = 0$. Supposons que $V_1 = V_2$ et $\rho_1 = \rho_2$. De nouveau par ce qui précède et la proposition 6.21, φ_0 est une homothétie. De plus

$$\mathrm{Tr}(\varphi_0) = \frac{1}{|G|} \sum_{g\in G} \mathrm{Tr}(\rho_1(g) \circ \varphi \circ \rho_1(g)^{-1}) = \mathrm{Tr}(\varphi) \, ,$$

donc le rapport de φ_0 est

$$\frac{1}{n}\mathrm{Tr}(\varphi_0) = \frac{1}{n}\mathrm{Tr}(\varphi) \, .$$

□

On se donne deux représentations linéaires simples $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$. On choisit des bases $B = \{e_1, \ldots, e_n\}$ et $B' = \{e'_1, \ldots, e'_m\}$ de V et V', respectivement, et, pour tout $g \in G$, on note $A(g) = (a_{i,j}(g))_{1\le i,j\le n}$ la matrice de $\rho(g)$ par rapport à la base B et $A'(g) = (a'_{k,l}(g))_{1\le k,l\le m}$ la matrice de $\rho'(g)$ par rapport à B'.

Corollaire 6.23.

(1) *Si ρ et ρ' ne sont pas isomorphes, alors, pour tous $i, j \in \{1, \ldots, n\}$ et $k, l \in \{1, \ldots, m\}$,*

$$\sum_{g\in G} a_{i,j}(g^{-1}) \, a'_{k,l}(g) = 0 \, .$$

(2) *Supposons que $V = V'$, $\rho = \rho'$ et $B = B'$. Pour tous $i, j, k, l \in \{1, \ldots, n\}$,*

$$\frac{1}{|G|} \sum_{g\in G} a_{i,j}(g^{-1}) \, a_{k,l}(g) = \begin{cases} \frac{1}{n} & \textit{si } i = l \textit{ et } j = k \\ 0 & \textit{sinon} \end{cases}$$

Démonstration. Soit $\varphi : V \to V'$ une application linéaire quelconque. Notons $M = (x_{l,i})$ la matrice de φ par rapport aux bases B et B'. Pour $k \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$, le (k, j)-ème coefficient de la matrice de $\rho'(g) \circ \varphi \circ \rho(g^{-1})$ est

$$\sum_{l=1}^{m} \sum_{i=1}^{n} a'_{k,l}(g)\, x_{l,i}\, a_{i,j}(g^{-1})\,.$$

Supposons que ρ et ρ' ne sont pas isomorphes. Alors, par le corollaire 6.22, on a

$$\sum_{g \in G} \sum_{l=1}^{m} \sum_{i=1}^{n} a'_{k,l}(g)\, x_{l,i}\, a_{i,j}(g^{-1}) = 0\,.$$

Soient $i, j \in \{1, \ldots, n\}$ et $k, l \in \{1, \ldots, m\}$. On choisit $\varphi : V \to V'$ de sorte que $x_{l,i} = 1$ et $x_{l',i'} = 0$ si $(l', i') \neq (l, i)$. Alors l'égalité précédente devient

$$\sum_{g \in G} a'_{k,l}(g)\, a_{i,j}(g^{-1}) = 0\,.$$

Supposons que $V = V'$, $\rho = \rho'$ et $B = B'$. Alors, par le corollaire 6.22, on a

$$\frac{1}{|G|} \sum_{g \in G} \sum_{l=1}^{n} \sum_{i=1}^{n} a_{k,l}(g)\, x_{l,i}\, a_{i,j}(g^{-1}) = \begin{cases} \frac{1}{n} \sum_{i=1}^{n} x_{i,i} & \text{si } k = j \\ 0 & \text{sinon} \end{cases}$$

Soient $i, j, k, l \in \{1, \ldots, n\}$. On choisit $\varphi : V \to V$ de sorte que $x_{l,i} = 1$ et $x_{l',i'} = 0$ si $(l', i') \neq (l, i)$. Alors l'égalité précédente devient

$$\frac{1}{|G|} \sum_{g \in G} a_{k,l}(g)\, a_{i,j}(g^{-1}) \begin{cases} \frac{1}{n} & \text{si } k = j \text{ et } l = i \\ 0 & \text{sinon} \end{cases}$$

$\square$

Définition. Soit $\mathbb{C}^G$ l'espace des applications (ensemblistes) de G dans $\mathbb{C}$. Rappelons que $\mathbb{C}^G$ est muni d'une somme et d'une multiplication externe définis par

$$(\alpha + \beta)(g) = \alpha(g) + \beta(g)\,, \quad (t\,\alpha)(g) = t\,\alpha(g)\,,$$

pour tout $g \in G$. On observe que $\mathbb{C}^G$ muni de ces deux opérations est un espace vectoriel de dimension $|G|$. Soit $\langle\,|\,\rangle : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}$ l'application définie par

$$\langle \alpha | \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \beta(g)^*\,.$$

On vérifie facilement que $\langle\,|\,\rangle$ est une forme hermitienne définie positive.

Remarque. Pour tout $g \in G$ on définit $\delta_g : G \to \mathbb{C}$ par

$$\delta_g(h) = \begin{cases} |G| & \text{si } h = g \\ 0 & \text{si } h \neq g \end{cases}$$

Alors $\{\delta_g ; g \in G\}$ est une base orthonormée de $\mathbb{C}^G$.

Théorème 6.24.

(1) *Si χ est le caractère d'une représentation simple, alors $\langle \chi | \chi \rangle = 1$.*

(2) *Si χ et χ' sont les caractères de deux représentations simples non isomorphes, alors $\langle \chi | \chi' \rangle = 0$.*

Démonstration. Soient $\rho : G \to \mathrm{GL}(V)$ une représentation simple et χ son caractère. Soient $B = \{e_1, \dots, e_n\}$ une base de V et, pour tout $g \in G$, $A(g) = (a_{i,j}(g))_{1 \leq i,j \leq n}$ la matrice de $\rho(g)$ dans la base B. Alors

$$\begin{aligned}
\langle \chi | \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\, \chi(g)^* \\
&= \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi(g^{-1}) && \text{(par la proposition 6.17)} \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^{n} a_{i,i}(g) \right) \left(\sum_{j=1}^{n} a_{j,j}(g^{-1}) \right) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{|G|} \sum_{g \in G} a_{i,i}(g)\, a_{j,j}(g^{-1}) \\
&= n \cdot \frac{1}{n} = 1 && \text{(par le corollaire 6.23)}
\end{aligned}$$

Soient $\rho : G \to \mathrm{GL}(V)$, $\rho' : G \to \mathrm{GL}(V')$ deux représentations simples non isomorphes et χ, χ' leurs caractères respectifs. Soient $B = \{e_1, \dots, e_n\}$ une base de V, $B' = \{e'_1, \dots, e'_m\}$ une base de V' et, pour $g \in G$, $A(g) = (a_{i,j}(g))_{1 \leq i,j \leq n}$ la matrice de $\rho(g)$ dans la base B

et $A'(g) = (a'_{k,l}(g))_{1\leq k,l\leq m}$ la matrice de $\rho'(g)$ dans la base B'. Alors

$$\begin{aligned}
\langle \chi' | \chi \rangle &= \frac{1}{|G|} \sum_{g\in G} \chi'(g)\,\chi(g)^* \\
&= \frac{1}{|G|} \sum_{g\in G} \chi'(g)\,\chi(g^{-1}) && \text{(par la proposition 6.17)} \\
&= \frac{1}{|G|} \sum_{g\in G} \left(\sum_{k=1}^{m} a'_{k,k}(g) \right) \left(\sum_{i=1}^{n} a_{i,i}(g^{-1}) \right) \\
&= \sum_{i=1}^{n} \sum_{k=1}^{m} \frac{1}{|G|} \sum_{g\in G} a'_{k,k}(g)\, a_{i,i}(g^{-1}) \\
&= 0 && \text{(par le corollaire 6.23)}
\end{aligned}$$

□

Théorème 6.25. *Soient $\rho : G \to \mathrm{GL}(V)$ une représentation et ϕ son caractère. On écrit ρ comme somme directe de représentations simples :*

$$\rho = \mu_1 \oplus \cdots \oplus \mu_k\,,$$

et on note χ_i le caractère de μ_i pour tout $i \in \{1, \ldots, k\}$. Soient $\mu : G \to \mathrm{GL}(W)$ une représentation simple et χ son caractère. Alors $\langle \phi | \chi \rangle$ est le nombre de $i \in \{1, \ldots, k\}$ tels que $\mu_i \simeq \mu$.

Démonstration. Notons m le nombre de $i \in \{1, \ldots, k\}$ tels que $\mu \simeq \mu_i$. On a $\phi = \chi_1 + \cdots + \chi_k$ par le corollaire 6.19, donc $\langle \phi | \chi \rangle = m$ par Le théorème 6.24. □

Définition. Si $\rho : G \to \mathrm{GL}(V)$ est une représentation et $m \in \mathbb{N}$ est un entier positif ou nul, on définit $m \cdot \rho$ par récurrence sur m comme suit. $0 \cdot \rho$ est la représentation triviale $G \to \mathrm{GL}(\{0\})$. On pose $1 \cdot \rho = \rho$. Si $m \geq 2$, alors $m \cdot \rho = (m-1) \cdot \rho \oplus \rho$.

Corollaire 6.26. *Soient $\rho : G \to \mathrm{GL}(V)$ et $\rho' : G \to \mathrm{GL}(V')$ deux représentations linéaires de G. On a $\rho \simeq \rho'$ si et seulement si $\chi_\rho = \chi_{\rho'}$.*

Démonstration. Supposons que $\rho \simeq \rho'$. Soit $\varphi : V \to V'$ un isomorphisme linéaire tel que $\varphi \circ \rho(g) = \rho'(g) \circ \varphi$ pour tout $g \in G$. Alors, pour $g \in G$,

$$\chi_{\rho'}(g) = \mathrm{Tr}(\rho'(g)) = \mathrm{Tr}(\varphi \circ \rho(g) \circ \varphi^{-1}) = \mathrm{Tr}(\rho(g)) = \chi_\rho(g)\,.$$

Supposons que $\chi_\rho = \chi_{\rho'}$. On considère une décomposition $\rho \simeq m_1 \cdot \mu_1 \oplus \cdots \oplus m_k \cdot \mu_k$, où $\mu_1, \ldots, \mu_k$ sond des représentations simples deux à deux non isomorphes. Par le théorème 6.25 on a $\langle \chi_{\rho'} | \chi_{\mu_i} \rangle = \langle \chi_\rho | \chi_{\mu_i} \rangle = m_i$ pour tout $i \in \{1, \ldots, k\}$. De plus, si μ est une représentation isomorphe à aucun des μ_i, alors $\langle \chi_{\rho'} | \chi_\mu \rangle = \langle \chi_\rho | \chi_\mu \rangle = 0$. Encore par le théorème 6.25, on en conclue que

$$\rho' \simeq m_1 \cdot \mu_1 \oplus \cdots \oplus m_k \cdot \mu_k \simeq \rho \, .$$

$\square$

Corollaire 6.27. *Soient $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire non triviale et χ son caractère. Alors $\langle \chi | \chi \rangle > 0$. De plus, on a $\langle \chi | \chi \rangle = 1$ si et seulement si ρ est simple.*

Démonstration. On considère une décomposition $\rho \simeq m_1 \cdot \mu_1 \oplus \cdots \oplus m_k \cdot \mu_k$, où $\mu_1, \ldots, \mu_k$ sont des représentations simples deux à deux non isomorphes. Alors, par le théorème 6.24,

$$\langle \chi | \chi \rangle = \sum_{i=1}^{k} m_i^2 > 0 \, .$$

Il est clair que $\langle \chi | \chi \rangle = 1$ si et seulement si $k = 1$ et $m_1 = 1$, c'est-à-dire si et seulement si ρ est simple. $\square$

Définition. Un *caractère simple* de G est le caractère d'une représentation simple de G.

Corollaire 6.28. *Il n'existe qu'un nombre fini de caractères simples.*

Démonstration. Notons $\mathcal{S}$ l'ensemble des caractères simples de G. Par le théorème 6.24, $\mathcal{S}$ est une famille orthonormale de $\mathbb{C}^G$, donc est libre, donc est fini car $\mathbb{C}^G$ est de dimension finie. $\square$

Notation. A partir de maintenant les représentations simples seront notées $\mu_1, \ldots, \mu_h$, leurs caractères respectifs $\chi_1, \ldots, \chi_h$ et leurs degrés respectifs $n_1, \ldots, n_h$. Rappelons que, par la proposition 6.17, on a $n_i = \chi_i(1_G)$ pour tout $i \in \{1, \ldots, h\}$.

Notation. On note $R_G : G \to \mathrm{GL}(\mathbb{C}[G])$ la représentation régulière de G et $r_G : G \to \mathbb{C}$ son caractère.

Proposition 6.29. *Pour $g \in G$ on a*

$$r_G(g) = \begin{cases} |G| & si\ g = 1_G \\ 0 & si\ g \neq 1_G \end{cases}$$

Démonstration. Si $g = 1_G$ alors, par la proposition 6.17, $r_G(g) = \dim \mathbb{C}[G] = |G|$. Si $g \neq 1_G$, alors $R_G(g)(h) = gh \neq h$ pour tout $h \in G$, donc $r_G(g) = \mathrm{Tr}(R_G(g)) = 0$. $\square$

Corollaire 6.30.

(1) $R_G = n_1 \cdot \mu_1 \oplus \cdots \oplus n_h \cdot \mu_h$.

(2) $|G| = n_1^2 + \cdots + n_h^2$.

(3) *Si* $g \in G \setminus \{1_G\}$, *alors* $n_1\,\chi_1(g) + \cdots + n_h\,\chi_h(g) = 0$.

Démonstration. Pour $i \in \{1, \ldots, h\}$ on a

$$\langle r_G | \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} r_G(g)\,\chi_i(g)^* = \frac{1}{|G|} |G|\, n_i = n_i\,.$$

Par le théorème 6.25, on en déduit que

$$R_G = n_1 \cdot \mu_1 \oplus \cdots \oplus n_h \cdot \mu_h\,.$$

De cette égalité suit

$$|G| = \deg(R_G) = n_1 \deg(\mu_1) + \cdots + n_h \deg(\mu_h) = n_1^2 + \cdots + n_h^2\,.$$

On en déduit aussi que, pour $g \in G \setminus \{1_G\}$,

$$0 = r_G(g) = n_1\,\chi_1(g) + \cdots + n_h\,\chi_h(g)\,.$$

□

Définition. Une application $\alpha : G \to \mathbb{C}$ est dite *centrale* si $\alpha(hgh^{-1}) = \alpha(g)$ pour tous $g, h \in G$. Remarquez que tout caractère est une fonction centrale (voir la proposition 6.17).

Définition. Si $\alpha : G \to \mathbb{C}$ une fonction centrale et $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire, on définit $\varphi_{\alpha,\rho} : V \to V$ par

$$\varphi_{\alpha,\rho}(v) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\,\rho(g^{-1})(v)\,, \quad \text{pour } v \in V\,.$$

C'est une application linéaire.

Proposition 6.31. *Soient* $\alpha : G \to \mathbb{C}$ *une fonction centrale,* $\mu : G \to \mathrm{GL}(V)$ *une représentation simple, et* χ *le caractère de* μ*. Alors* $\varphi_{\alpha,\mu}$ *est une homothétie de rapport* $\frac{1}{n}\langle \alpha | \chi \rangle$*, où* n *est la dimension de* V*.*

Démonstration. Pour tout $g \in G$ on a

$$\begin{aligned}
\mu(g) \circ \varphi_{\alpha,\mu} \circ \mu(g)^{-1} &= \mu(g) \circ \left(\frac{1}{|G|} \sum_{h \in G} \alpha(h)\,\mu(h^{-1}) \right) \circ \mu(g)^{-1} \\
&= \frac{1}{|G|} \sum_{h \in G} \alpha(h)\,\mu(gh^{-1}g^{-1}) \\
&= \frac{1}{|G|} \sum_{h \in G} \alpha(ghg^{-1})\,\mu(gh^{-1}g^{-1}) \\
&= \frac{1}{|G|} \sum_{h \in G} \alpha(h)\,\mu(h^{-1}) \\
&= \varphi_{\alpha,\mu}
\end{aligned}$$

Par la proposition 6.21 (Lemme de Schur) il s'en suit que $\varphi_{\alpha,\mu}$ est une homothétie. De plus,

$$\mathrm{Tr}(\varphi_{\alpha,\mu}) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\mathrm{Tr}(\mu(g^{-1})) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\chi(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\chi(g)^* = \langle\alpha|\chi\rangle\,,$$

donc le rapport de $\varphi_{\alpha,\mu}$ est $\frac{1}{n}\langle\alpha|\chi\rangle$. □

Théorème 6.32. *Soit H l'espace vectoriel des fonctions centrales. Alors $\chi_1,\ldots,\chi_h$ est une base orthonormée de H.*

Démonstration. On sait déjà que $B = \{\chi_1,\ldots,\chi_h\}$ est une famille orthonormée de H. Donc, pour démontrer que c'est une base, il suffit de montrer que B engendre H. Pour cela, on se donne un $\alpha \in H$ orthogonal à χ_i pour tout $i \in \{1,\ldots,h\}$ et on montre que $\alpha = 0$.

L'application φ_{α,μ_i} est une homothétie de rapport 0 (Proposition 6.31) c'est-à-dire est nulle pour tout $i \in \{1,\ldots,h\}$. De l'égalité

$$R_G = n_1\cdot\mu_1 \oplus\cdots\oplus n_h\cdot\mu_h$$

on déduit

$$\varphi_{\alpha,R_G} = n_1\cdot\varphi_{\alpha,\mu_1}\oplus\cdots\oplus n_h\cdot\varphi_{\alpha,\mu_h} = 0\,.$$

On applique φ_{α,R_G} à $1_G \in \mathbb{C}[G]$:

$$\overrightarrow{0} = \varphi_{\alpha,R_G}(1_G) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)R_G(g^{-1})(1_G) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)g^{-1}\,.$$

Comme $\{g^{-1}; g\in G\}$ est une base de $\mathbb{C}[G]$ il s'en suit que $\alpha(g) = 0$ pour tout $g \in G$. □

Théorème 6.33. *le nombre de représentations simples de G est égal au nombre de classes de conjugaison de G.*

Démonstration. Soients $C_1,\ldots,C_k$ les classes de conjugaison de G. Pour tout $i \in \{1,\ldots,k\}$ on définit $\alpha_i : G \to \mathbb{C}$ par

$$\alpha_i(g) = \begin{cases} 1 & \text{si } g\in C_i \\ 0 & \text{si } g\notin C_i \end{cases}$$

On montre facilement que $\{\alpha_i; 1\le i\le k\}$ est une base de H, donc $h = \dim H = k$. □