

9 Produit tensoriel et applications

Version du 28 mai 2006

32 Produit tensoriel

Dans tout ce qui suit, A est un anneau commutatif. Soient M, N deux A -modules. On veut définir un A -module $M \otimes_A N$ qui soit engendré par les “produits” d’un élément de M par un élément de N , c.-à-d., par des éléments notés $m \otimes n$.

32.0 Remarque préliminaire

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

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

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

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

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

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

Si R est de la forme $P(X)Q(Y)$, soient $\alpha_1, \dots, \alpha_r$ et β_1, \dots, β_s les racines de P et Q , alors $V(R)$ est la réunion des droites verticales $x = \alpha_i$ et des droites horizontales $y = \beta_j$. Par contre, pour $R = XY - 1$, on a

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

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

32.1 Applications bilinéaires

Soient M, N, P trois A -modules.

Définition 32.1.1 Soit ϕ une application d'ensembles $M \times N \rightarrow P$. On dit que ϕ est **A -bilinéaire** si elle est A -linéaire en chacune des variables, c.-à-d., si : $\forall a, a' \in A, m, m' \in M, n, n' \in N$,

$$\phi(am + a'm', n) = a\phi(m, n) + a'\phi(m', n); \quad (1)$$

$$\phi(m, an + a'n') = a\phi(m, n) + a'\phi(m, n'). \quad (2)$$

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

Définition 32.1.2 (Applications à valeurs dans un A -module) Soit X un ensemble. Si f, g sont deux applications de X dans P , et $a \in A$, on définit les applications $f + g$ et af par :

$$(f + g)(x) = f(x) + g(x), \quad (af)(x) = af(x), \quad \forall x \in X.$$

Ceci munit l'ensemble des applications de X dans P , noté $\text{Hom}_{\text{Ens}}(X, P)$, d'une structure de A -module.

Lemme 32.1.3 1) L'ensemble $\text{Hom}_A(M, N)$ des morphismes de A -modules $M \rightarrow N$ est un sous- A -module de $\text{Hom}_{\text{Ens}}(M, N)$.

2) De même, $\text{Bil}_A(M \times N, P)$ est un sous- A -module de $\text{Hom}_{\text{Ens}}(M \times N, P)$.

Démonstration. 1) Soient $\phi, \psi \in \text{Hom}_A(M, N)$ et $a \in A$. Il faut montrer que l'application

$$a\phi + \psi : M \rightarrow N, \quad m \mapsto a\phi(m) + \psi(m),$$

est A -linéaire. Soient $m, m' \in M$ et $b \in A$. Alors,

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

(Noter qu'on a utilisé la commutativité de A dans la dernière égalité). Ceci montre que $a\phi + \psi$ est A -linéaire, c.-à-d., appartient à $\text{Hom}_A(M, N)$.

La démonstration du point 2) est tout-à-fait analogue (on vérifie la A -linéarité par rapport à chacune des variables), et est laissée au lecteur. \square

Proposition 32.1.4 *On a des isomorphismes de A -modules*

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

Démonstration. Il suffit de montrer le premier isomorphisme, le deuxième étant analogue. Notons

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

l'application définie par

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

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

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

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

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

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

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

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

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

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

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

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

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

32.2 Produit tensoriel : définition et propriété universelle

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

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

2) “unicité de l'action de A ” :

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

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

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

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

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

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

Définition 32.2.1 On pose $M \otimes_A N = A(M \times N)/K$ et l'on note $m \otimes n$ l'image de $e_{m,n}$ dans $M \otimes N$.

Remarque 32.2.2 Il résulte des relations (1) et (2) que le produit $m \otimes n$ vérifie la condition 1) (bi-additivité) et la condition 2) :

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

En particulier, tout élément de $M \otimes_A N$ est une somme finie d'éléments $m \otimes n$.

Proposition 32.2.3 Soit $(e_i)_{i \in I}$, resp. $(f_j)_{j \in J}$, un système de générateurs de M , resp. N , comme A -module. Alors $M \otimes_A N$ est engendré comme A -module par les éléments $e_i \otimes f_j$, pour $i \in I$, $j \in J$.

Démonstration. Soient $m \in M$ et $n \in N$. Par hypothèse, m et n s'écrivent comme des sommes finies

$$m = a_1 e_{i_1} + \cdots + a_r e_{i_r}, \quad n = b_1 f_{j_1} + \cdots + b_s f_{j_s},$$

avec les a_t et b_u dans A . D'après les relations (1) et (2), on a

$$m \otimes n = \sum_{t=1}^r \sum_{j=1}^s a_t b_u e_{i_t} \otimes f_{j_u}.$$

Puisque tout élément de $M \otimes_A N$ est une somme finie d'éléments $m \otimes n$, il en résulte que les $e_i \otimes f_j$ engendrent $M \otimes_A N$ comme A -module. \square

Théorème 32.2.4 (Propriété universelle de $M \otimes_A N$, I) Pour tout A -module P , on a une bijection

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

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

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

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

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

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

Soit $\psi \in \text{Bil}_A(M \times N, P)$. D'après la propriété universelle du module libre $A(M \times N)$, il existe un unique morphisme de A -modules

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

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

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

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

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

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

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

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

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

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

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

On déduit du théorème, combiné avec la proposition 32.1.4, le corollaire suivant.

Corollaire 32.2.5 (Propriété universelle de $M \otimes_A N$, II) *Pour tout A -module P , on a une bijection*

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

32.3 Premières propriétés du produit tensoriel

Proposition 32.3.1 (Commutativité et associativité) *Soient M, N, P des A -modules. On a des isomorphismes de A -modules*

$$M \otimes N \cong N \otimes M; \quad (1)$$

$$(M \otimes N) \otimes P \cong M \otimes (N \otimes P). \quad (2)$$

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

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

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

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

Ceci prouve le point 1).

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

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

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

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

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

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

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

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

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

Proposition 32.3.2 *On a $A \otimes_A M \cong M$, pour tout A -module M .*

Démonstration. D'abord, l'application $\phi : M \rightarrow A \otimes_A M$, $m \mapsto 1 \otimes m$ est A -linéaire. D'autre part, l'application

$$A \times M \rightarrow M, \quad (a, m) \mapsto am$$

est A -bilinéaire, donc induit une application A -linéaire $\phi : A \otimes_A M \rightarrow M$ telle que

$$\phi(a \otimes m) = am, \quad \forall a \in A, m \in M.$$

Alors $\phi \circ \psi = \text{id}_M$ et, pour tout $a \in A$, $m \in M$, l'on a

$$\psi(\phi(a \otimes m)) = 1 \otimes am = a \otimes m,$$

d'où $\psi \circ \phi = \text{id}_{A \otimes_A M}$. Ceci prouve la proposition. \square

Théorème 32.3.3 (\otimes_A est un bifoncteur) *Le produit tensoriel est un bifoncteur, au sens suivant. Tout morphisme de A -modules*

$$f : M \rightarrow M', \quad \text{resp.} \quad g : N \rightarrow N'$$

induit un morphisme de A -modules

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

tel que

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

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

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

$$\begin{array}{ccc} M \otimes N & \xrightarrow{f \otimes \text{id}_N} & M' \otimes N \\ \text{id}_M \otimes g \downarrow & & \downarrow \text{id}_{M'} \otimes g \\ M \otimes N' & \xrightarrow{f \otimes \text{id}_{N'}} & M' \otimes N'. \end{array}$$

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

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

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

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

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

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

Remarque 32.3.4 1) Si $f : M \rightarrow M'$ est surjective, il en est de même de $f \otimes \text{id}_N : M \otimes N \rightarrow M' \otimes N$. En effet, si $m' = f(m)$, alors $m' \otimes n = (f \otimes \text{id}_N)(m \otimes n)$, pour tout $n \in N$.

2) **Attention**, si $f : M \rightarrow M'$ est injective, $f \otimes \text{id}_N$ n'est pas nécessairement injective. Par exemple, soient $A = \mathbb{Z} = M' = M$, soit f le morphisme injectif $x \mapsto 2x$, et soit $N = \mathbb{Z}/2\mathbb{Z}$. Alors, $f \otimes \text{id}_N$ est l'application nulle, car pour tout $x \in \mathbb{Z}$ on a

$$(f \otimes \text{id}_N)(x \otimes \bar{1}) = 2x \otimes \bar{1} = x \otimes 2\bar{1} = 0.$$

D'autre part, d'après la proposition 32.3.2, $M' \otimes_A N$ s'identifie à N , donc est non nul. Ceci montre que $f \otimes \text{id}_N$ n'est pas injective.

32.4 Applications multilinéaires et produits tensoriels itérés

La notion d'application bilinéaire se généralise comme suit. Soit n un entier ≥ 2 et M_1, \dots, M_n et P des A -modules.

Définition 32.4.1 Soit ϕ une application d'ensembles

$$M_1 \times \cdots \times M_n \rightarrow P.$$

On dit que ϕ est **A -multilinéaire** si elle est A -linéaire en chacune des variables. On note $\text{Mult}_A(M_1 \times \cdots \times M_n, P)$ l'ensemble de ces applications.

Considérons le A -module libre $A(M_1 \times \cdots \times M_n)$, qui est l'ensemble de toutes les sommes formelles finies

$$\sum_{(m_1, \dots, m_n) \in M_1 \times \cdots \times M_n} a_{(m_1, \dots, m_n)} e_{(m_1, \dots, m_n)},$$

avec $a_{(m_1, \dots, m_n)} \in A$ et $a_{(m_1, \dots, m_n)} = 0$ sauf pour un nombre fini d'indices. Soit K le sous- A -module engendré par les éléments du type suivant, pour $i = 1, \dots, n$,

$$e_{(m_1, \dots, am_i + m'_i, \dots, m_n)} - ae_{(m_1, \dots, m_i, \dots, m_n)} - e_{(m_1, \dots, m'_i, \dots, m_n)}.$$

Définition 32.4.2 On pose

$$M_1 \otimes_A \cdots \otimes_A M_n = A(M_1 \times \cdots \times M_n)/K$$

et l'on note $m_1 \otimes \cdots \otimes m_n$ l'image de $e_{(m_1, \dots, m_n)}$ dans $M_1 \otimes_A \cdots \otimes_A M_n$.

On obtient alors, exactement comme au paragraphe 32.2, le théorème suivant.

Théorème 32.4.3 (Propriété universelle de $M_1 \otimes_A \cdots \otimes_A M_n$) Pour tout A -module P , on a une bijection

$$\text{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_n, P) \xrightarrow{\cong} \text{Mult}_A(M_1 \times \cdots \times M_n, P), \quad \phi \mapsto B(\phi),$$

où $B(\phi)$ est l'application $(m_1, \dots, m_n) \mapsto \phi(m_1 \otimes \cdots \otimes m_n)$. Son inverse est l'application $\psi \mapsto T(\psi)$, où $T(\psi)$ est l'unique A -morphisme

$$T(\psi) : M_1 \otimes_A \cdots \otimes_A M_n \longrightarrow P$$

tel que $T(\psi)(m_1 \otimes \cdots \otimes m_n) = \psi(m_1, \dots, m_n)$.

En particulier, pour définir une application A -linéaire $M_1 \otimes_A \cdots \otimes_A M_n \rightarrow P$, il suffit d'avoir une application A -multilinéaire $M_1 \times \cdots \times M_n \rightarrow P$.

D'autre part, on a le théorème suivant.

Théorème 32.4.4 Pour tout i , on a un isomorphisme

$$M_1 \otimes_A \cdots \otimes_A M_n \xrightarrow{\cong} (M_1 \otimes_A \cdots \otimes_A M_i) \otimes_A (M_{i+1} \otimes_A \cdots \otimes_A M_n).$$

Démonstration. Posons $M = M_1 \otimes_A \cdots \otimes_A M_n$. L'application

$$(m_1, \dots, m_n) \mapsto (m_1 \otimes \cdots \otimes m_i) \otimes (m_{i+1} \otimes \cdots \otimes m_n)$$

est A -multilinéaire, donc induit une application A -linéaire

$$\phi : M \rightarrow (M_1 \otimes_A \cdots \otimes_A M_i) \otimes_A (M_{i+1} \otimes_A \cdots \otimes_A M_n)$$

telle que

$$\phi(m_1 \otimes \cdots \otimes m_n) = (m_1 \otimes \cdots \otimes m_i) \otimes (m_{i+1} \otimes \cdots \otimes m_n).$$

Construisons l'application inverse. Pour m_1, \dots, m_i fixés, l'application

$$(m_{i+1}, \dots, m_n) \mapsto m_1 \otimes \cdots \otimes m_n$$

est A -multilinéaire donc induit

$$\tau(m_1, \dots, m_i) \in \text{Hom}_A(M_{i+1} \otimes_A \cdots \otimes_A M_n, M)$$

tel que

$$\tau(m_1, \dots, m_i)(m_{i+1} \otimes \cdots \otimes m_n) = m_1 \otimes \cdots \otimes m_n.$$

On voit de plus que l'application $(m_1, \dots, m_i) \mapsto \tau(m_1, \dots, m_i)$ est A -multilinéaire. Donc il existe

$$\tau \in \text{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_i, \text{Hom}_A(M_{i+1} \otimes_A \cdots \otimes_A M_n, M))$$

tel que $\tau(m_1 \otimes \cdots \otimes m_i)(m_{i+1} \otimes \cdots \otimes m_n) = m_1 \otimes \cdots \otimes m_n$. D'après la propriété universelle du produit tensoriel (Corollaire 32.2.4), τ correspond à l'application A -linéaire

$$\psi : (M_1 \otimes_A \cdots \otimes_A M_i) \otimes_A (M_{i+1} \otimes_A \cdots \otimes_A M_n) \rightarrow M$$

qui envoie $(m_1 \otimes \cdots \otimes m_i) \otimes (m_{i+1} \otimes \cdots \otimes m_n)$ sur $m_1 \otimes \cdots \otimes m_n$. Il est alors clair que ϕ et ψ sont inverses l'une de l'autre. Le théorème est démontré. \square

Corollaire et notation 32.4.5 Il résulte du théorème que tous les modules obtenus à partir de M_1, \dots, M_n en ajoutant des parenthèses pour former des produits tensoriels de deux modules, sont canoniquement isomorphes à $M_1 \otimes_A \cdots \otimes_A M_n$, par l'application qui consiste à "omettre les parenthèses". Par exemple, on a

$$(M_1 \otimes M_2) \otimes (M_3 \otimes M_4) \cong (M_1 \otimes M_2 \otimes M_3 \otimes M_4) \cong (M_1 \otimes (M_2 \otimes (M_3 \otimes M_4)))$$

via

$$(m_1 \otimes m_2) \otimes (m_3 \otimes m_4) = m_1 \otimes m_2 \otimes m_3 \otimes m_4 = (m_1 \otimes (m_2 \otimes (m_3 \otimes m_4))).$$

Par conséquent, dans la suite, on omettra les parenthèses dans les produits tensoriels de plus de deux modules.

Signalons enfin la proposition suivante, qui résulte de l'identification précédente et de la proposition 32.2.3, ou bien se démontre directement, comme la proposition 32.2.3.

Proposition 32.4.6 Pour $r = 1, \dots, n$, soit $(e_i)_{i \in I_r}$ un système de générateurs de M_r comme A -module. Alors $M_1 \otimes_A \cdots \otimes_A M_n$ est engendré comme A -module par les éléments $e_{i_1} \otimes \cdots \otimes e_{i_n}$, avec $i_r \in I_r$.

32.5 Produits tensoriels d'algèbres et produits de variétés

Soit k un corps. Commençons par montrer que le produit tensoriel \otimes_k a la propriété proposée comme motivation en 32.0, c.-à-d., que le produit tensoriel de deux algèbres de polynômes est une algèbre de polynômes. Soient m, n des entiers ≥ 1 et X_1, \dots, X_m et Y_1, \dots, Y_n des indéterminées. Pour abrégé, on note

$$\begin{aligned} k[X] &:= k[X_1, \dots, X_m], & k[Y] &:= k[Y_1, \dots, Y_n] \\ k[X, Y] &:= k[X_1, \dots, X_m, Y_1, \dots, Y_n] \end{aligned}$$

et l'on désignera par $P(X)$, resp. $Q(Y)$, un élément arbitraire de $k[X]$, resp. $k[Y]$. La multiplication définit une application k -bilineaire

$$k[X] \times k[Y] \rightarrow k[X, Y], \quad (P, Q) \mapsto P(X)Q(Y).$$

D'après la propriété universelle du produit tensoriel, ceci induit donc une application k -linéaire

$$\phi : k[X] \otimes_k k[Y] \rightarrow k[X, Y]$$

telle que $\phi(P \otimes Q) = P(X)Q(Y)$, pour tout $P \in k[X]$, $Q \in k[Y]$.

Pour $\mu = (\mu_1, \dots, \mu_m) \in \mathbb{N}^m$, on pose

$$X^\mu := X_1^{\mu_1} \dots X_m^{\mu_m},$$

et l'on définit de même Y^ν , pour $\nu \in \mathbb{N}^n$. Alors les monômes X^μ , resp. Y^ν , resp. $X^\mu Y^\nu$ forment une base de $k[X]$, resp. $k[Y]$, resp. $k[X, Y]$.

D'après la proposition 32.2.3, les éléments $X^\mu \otimes Y^\nu$ engendrent $k[X] \otimes k[Y]$ comme k -espace vectoriel. D'autre part, comme leurs images par ϕ sont les produits $X^\mu Y^\nu$, qui forment une base de $k[X, Y]$, on en déduit la proposition suivante :

Proposition 32.5.1 *Les $X^\mu \otimes Y^\nu$ forment une base de $k[X] \otimes k[Y]$, et ϕ est un isomorphisme d'espaces vectoriels*

$$k[X] \otimes k[Y] \xrightarrow{\sim} k[X, Y].$$

Définition et proposition 32.5.2 *Soit A un anneau et B, C deux A -algèbres. Il existe sur le A -module $B \otimes_A C$ une unique structure de A -algèbre telle que*

$$(*) \quad (b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'.$$

La A -algèbre $B \otimes_A C$ s'appelle le produit tensoriel des A -algèbres B et C .

Démonstration. L'application $B \times C \times B \times C \rightarrow B \otimes_A C$, $(b, c, b', c') \mapsto bb' \otimes cc'$ est A -multilinéaire donc induit une application A -linéaire

$$\begin{aligned} \tau : B \otimes_A C \otimes_A B \otimes_A C &\rightarrow B \otimes_A C \\ \text{telle que} & \\ \tau(b \otimes c \otimes b' \otimes c') &= bb' \otimes cc'. \end{aligned}$$

Comme $B \otimes_A C \otimes_A B \otimes_A C = (B \otimes_A C) \otimes_A (B \otimes_A C)$, τ correspond à une application de multiplication A -bilinéaire

$$(B \otimes_A C) \times (B \otimes_A C) \rightarrow B \otimes_A C$$

telle que $(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'$. La commutativité et l'associativité sont alors immédiates pour les éléments de la forme $b \otimes c$, et comme ces éléments engendrent $B \otimes_A C$ comme A -module, on obtient que la multiplication est commutative et associative, et qu'elle est uniquement déterminée par la formule (*). La proposition est démontrée. \square

Corollaire 32.5.3 *L'isomorphisme $k[X] \otimes k[Y] \xrightarrow{\sim} k[X, Y]$ de la proposition 32.5.1 est un isomorphisme d'algèbres.*

Démonstration. Laissée au lecteur! \square

Pour établir la proposition 32.5.1, on a montré que les $X^\mu \otimes Y^\nu$ forment une base de $k[X] \otimes k[Y]$, en montrant que leurs images dans $k[X, Y]$ sont linéairement indépendantes. Ceci est en fait un cas particulier du résultat général ci-dessous.

Théorème 32.5.4 *Soient A un anneau, I, J deux ensembles, et M resp. N le A -module libre de base $(e_i)_{i \in I}$, resp. $(f_j)_{j \in J}$. Alors $M \otimes_A N$ est un A -module libre de base $(e_i \otimes f_j)_{(i,j) \in I \times J}$.*

Démonstration. Ce théorème n'est pas facile à établir en partant directement de la définition du produit tensoriel, mais il découle facilement des propriétés universelles du produit tensoriel et des modules libres.

Soit $V = A(I \times J)$ un A -module libre de base $\{v(i, j)\}_{(i,j) \in I \times J}$. Il existe une unique application A -linéaire $\phi : V \rightarrow M \otimes_A N$ telle que

$$(1) \quad \phi(v(i, j)) = e_i \otimes f_j, \quad \forall i \in I, j \in J.$$

D'autre part, il existe une unique application A -bilinéaire $\theta : M \times N \rightarrow V$ telle que

$$\theta(e_i, f_j) = v(i, j), \quad \forall i \in I, j \in J;$$

explicitement, pour tout couple $x = \sum_i a_i e_i$, $y = \sum_j b_j f_j$, les deux sommes étant finies, on a

$$\theta(x, y) = \sum_{i,j} a_i b_j v(i, j).$$

Par conséquent, d'après la propriété universelle 32.2.4, il existe une unique application A -linéaire $\psi : M \otimes_A N \rightarrow V$ telle que

$$(2) \quad \psi(e_i \otimes f_j) = v(i, j), \quad \forall i \in I, j \in J.$$

Comme les $v(i, j)$, resp. $e_i \otimes f_j$, engendrent V , resp. $M \otimes_A N$, il résulte de (1) et (2) que $\psi \circ \phi = \text{id}$ et $\phi \circ \psi = \text{id}$. Donc ϕ et ψ sont des isomorphismes réciproques l'un de l'autre. Le théorème est démontré. \square

On va généraliser le corollaire 32.5.3 comme suit. Soit V , resp. W , une sous-variété algébrique fermée de k^m , resp. k^n , définie par des polynômes $P_1, \dots, P_r \in k[X]$, resp. $Q_1, \dots, Q_s \in k[Y]$.

Notons que $k[X]$ et $k[Y]$ sont de façon naturelle des sous-algèbres de $k[X, Y]$. Par exemple, si $P \in k[X]$ et si $z = (x, y)$ est un élément de k^{m+n} , alors $P(z) = P(x)$. On a alors le lemme suivant.

Lemme 32.5.5 $V \times W$ est une sous-variété algébrique fermée de k^{m+n} , définie par les polynômes $P_1, \dots, P_r, Q_1, \dots, Q_s$.

Démonstration. Il est clair que ces polynômes s'annulent sur $V \times W$. Réciproquement, soit $z = (x, y)$ un point de k^{m+n} sur lequel ces polynômes s'annulent. Alors $0 = P_i(z) = P_i(x)$, pour $i = 1, \dots, r$, et ceci entraîne $x \in V$. On obtient de même que $y \in W$. Ceci prouve le lemme. \square

Posons $I = \mathcal{I}(V)$, $J = \mathcal{I}(W)$, et $K = \mathcal{I}(V \times W)$. Alors $k[V \times W] = k[X, Y]/K$. Observons que $K \cap k[X] = I$; en effet, si $P \in k[X]$ s'annule sur $V \times W$, alors pour tout $x \in V, y \in W$, on a $0 = P(x, y) = P(x)$, et donc $P \in I$. Par conséquent, l'inclusion naturelle $k[X] \subset k[X, Y]$ permet d'identifier $k[V]$ à une sous-algèbre de $k[V \times W]$: si $f \in k[V]$ et $(v, w) \in V \times W$, alors $f(v, w) = f(v)$. De même, $k[W]$ s'identifie à une sous-algèbre de $k[V \times W]$.

Alors, la multiplication

$$k[V] \times k[W] \rightarrow k[V \times W], \quad (f, g) \mapsto fg,$$

est k -bilinéaire, donc induit une application k -linéaire

$$\phi : k[V] \otimes_k k[W] \rightarrow k[V \times W]$$

telle que $\phi(f \otimes g) = fg$, pour tout f, g . Alors,

$$\phi((f \otimes g) \cdot (f' \otimes g')) = \phi(ff' \otimes gg') = ff'gg' = fgf'g' = \phi(f \otimes g)\phi(f' \otimes g'),$$

et comme les tenseurs $f \otimes g$ engendrent $k[V] \otimes_k k[W]$ comme k -espace vectoriel, on en déduit que ϕ est un morphisme d'algèbres. De plus, ϕ est surjectif puisque $k[V \times W]$ est engendré par les images des monômes $X^\mu Y^\nu$.

Théorème 32.5.6 ϕ est un isomorphisme de k -algèbres

$$k[V] \otimes_k k[W] \xrightarrow{\sim} k[V \times W].$$

Démonstration. D'après ce qui a déjà été dit, il suffit de montrer que ϕ est injectif. Soit $\alpha \in \text{Ker } \phi$.

Soit $\{e_i\}_{i \in B}$, resp. $\{f_j\}_{j \in C}$ une base de $k[V]$, resp. $k[W]$. Comme les $e_i \otimes f_j$ forment une base de $k[V] \otimes k[W]$, alors α peut s'écrire comme une somme finie

$$\alpha = \sum_i e_i \otimes \psi_i, \quad \text{avec } \psi_i \in k[W].$$

(On écrit $x = \sum_{i,j} a_{ij} e_i \otimes f_j$ et $\psi_i = \sum_j a_{ij} f_j$). Fixons $w_0 \in W$. Pour tout $v \in V$, on a

$$0 = \alpha(v, w_0) = \sum_i e_i(v) \psi_i(w_0),$$

et donc l'élément $\sum_i \psi_i(w_0) e_i$ est identiquement nul sur V . Comme les e_i sont linéairement indépendants dans $k[V]$, ceci implique $\psi_i(w_0) = 0$. Comme w_0 était arbitraire dans W , ceci montre que $\psi_i = 0$ pour tout i , et donc $\alpha = 0$. Ceci montre que ϕ est injectif. Le théorème est démontré. \square

32.6 Produits et sommes directes

Le but de ce paragraphe est d'introduire la notion de somme directe arbitraire (c.-à-d., pour un ensemble d'indices infini) et de montrer que le produit tensoriel "commute aux sommes directes" (Théorème 32.6.9). Ce résultat n'est pas utilisé dans les Sections 33 et 34. Ce paragraphe peut donc être omis en première lecture. (Seul le corollaire 32.6.8 est utilisé à la fin du chapitre, lors de la construction des algèbres symétriques et extérieures.)

Soit A un anneau commutatif et soit I un ensemble quelconque. On suppose donné un A -module M_i , pour tout $i \in I$. On veut définir un A -module appelé la somme directe des M_i . Pour ceci, il est commode d'introduire d'abord le module produit des M_i .

Définition 32.6.1 Le produit des M_i est le A -module, noté $\prod_{i \in I} M_i$, dont les éléments sont les familles $(m_i)_{i \in I}$ telles que $m_i \in M_i$ pour tout $i \in I$. La structure de groupe abélien et de A -module est définie composante par composante, c.-à-d.,

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

Définition 32.6.2 La somme directe des M_i , notée $\bigoplus_{i \in I} M_i$, est le sous- A -module de $\prod_{i \in I} M_i$ formé des familles qui sont nulles presque partout, c.-à-d., les familles $(m_i)_{i \in I}$ telles que $m_i = 0$ sauf pour un nombre fini d'indices. Il est clair que ceci est bien un sous- A -module.

Remarque 32.6.3 Si l'ensemble I est fini, on voit que

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

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

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

Définition 32.6.4 Pour tout i , soit

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

la projection sur la i -ème composante et soit

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

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

De plus, désignons par σ l'inclusion $\bigoplus_{j \in I} M_j \subseteq \prod_{j \in I} M_j$ et posons $p_i = \pi_i \circ \sigma$: c'est la projection de $\bigoplus_{j \in I} M_j$ sur M_i .

Proposition 32.6.5 π_i et τ_i sont des morphismes de A -modules. De plus, on a

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

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

Démonstration. C'est clair. \square

Théorème 32.6.6 (Propriété universelle de la somme directe, et du produit)

Soit N un A -module.

1) Pour avoir un morphisme $\phi : \bigoplus_{i \in I} M_i \rightarrow N$, il suffit d'avoir un morphisme $\phi_i : M_i \rightarrow N$ pour tout i . De façon plus précise, l'application

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

est une bijection, dont l'inverse β est donnée par $\beta(\phi) = (\phi \circ \tau_i)_{i \in I}$. De plus, si chaque ϕ_i est surjectif,

2) Pour avoir un morphisme $\psi : N \rightarrow \prod_{i \in I} M_i$, il suffit d'avoir un morphisme $\psi_i : N \rightarrow M_i$ pour tout i . De façon plus précise, l'application

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

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

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

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

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

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

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

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

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

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

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

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

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

Le théorème ci-dessous et son corollaire seront utilisés à la fin de ce chapitre, dans la construction de l'algèbre symétrique ou extérieure d'un A -module.

Considérons, pour tout $i \in I$, un morphisme de A -modules

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

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

Théorème 32.6.7 1) *Les morphismes $\tau'_i \circ f_i$ induisent un morphisme*

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

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

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

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

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

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

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

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

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

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

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

Le point 1) du corollaire ci-dessous est déjà contenu dans le théorème précédent, mais on le répète en raison de son importance.

Corollaire 32.6.8 *Pour tout $i \in I$, soit N_i un sous-module de M_i . Alors,*

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

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

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

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

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

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

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

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

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

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

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

Théorème 32.6.9 (\otimes commute aux sommes directes) Soient N et M_i , $i \in I$, des A -modules. On a un isomorphisme de A -modules :

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

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

D'après le théorème 32.3.3, chaque τ_i induit un A -morphisme

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

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

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

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

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

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

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

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

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

Remarque 32.6.10 On retrouve ainsi le fait que le produit tensoriel de A -modules libres $A(I)$ et $A(J)$ est le A -module libre $A(I \times J)$. En effet,

$$A(I) = \bigoplus_{i \in I} M_i, \quad A(J) = \bigoplus_{j \in J} N_j,$$

où $M_i = A = N_j$ pour tout i, j . D'après le théorème précédent et le fait que $A \otimes_A A = A$, on obtient que

$$A(I) \otimes_A A(J) \cong \bigoplus_{I \times J} A = A(I \times J).$$

33 Extension des scalaires et changement de base

33.0 Complexifié d'un \mathbb{R} -espace vectoriel

L'exemple le plus simple de changement de (corps de) base est le procédé de complexification d'un espace vectoriel réel V , que le lecteur a certainement déjà rencontré, sous l'une des formes suivantes.

1ère méthode. Supposons V de dimension finie n . Choisissons une base (e_1, \dots, e_n) de V . Ceci permet d'identifier V à \mathbb{R}^n , via $\sum_i x_i e_i \mapsto (x_1, \dots, x_n)$. On définit alors le complexifié $V_{\mathbb{C}}$ comme étant \mathbb{C}^n , c.-à-d., l'ensemble des combinaisons linéaires $z_1 e_1 + \dots + z_n e_n$, avec $z_i \in \mathbb{C}$.

2ème méthode. Plutôt que de choisir une base de V , prenons $\{1, i\}$ comme base de la \mathbb{R} -algèbre \mathbb{C} . Ceci conduit à considérer l'espace vectoriel réel $V \oplus V$, qu'on écrit formellement comme

$$V \oplus iV,$$

la structure de \mathbb{R} -espace vectoriel étant donnée par $a \cdot (v, v') = (av, av')$, pour $a \in \mathbb{R}$, $v, v' \in V$.

Comme $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[X]/(X^2+1)$ comme \mathbb{R} -algèbre, pour définir l'action de \mathbb{C} sur cet espace, il suffit de définir une action de i telle $i \cdot i \cdot w = -w$, pour tout $w \in V \oplus iV$. Comme la notation le suggère, on pose

$$i \cdot (v, 0) = (0, v) \quad \text{c.-à-d.,} \quad i \cdot (v + 0) = 0 + iv,$$

d'où nécessairement $i \cdot (0, v) = (-v, 0)$. On obtient ainsi une structure de \mathbb{C} -espace vectoriel sur

$$V_{\mathbb{C}} = V \oplus iV.$$

Explicitement, si $z = a + ib$ et $w = u + iv$, il résulte de ce qui précède que

$$z \cdot w = (au - bv) + i(bu + av).$$

(Cette formule est parfois donnée comme définition de $V_{\mathbb{C}}$, sans explications...)

Remarque 33.0.1 C'est un exercice que de vérifier que les deux définitions précédentes coïncident, et donc qu'aucune d'elles ne dépend de la \mathbb{R} -base (de V ou de \mathbb{C}) choisie. (On aurait aussi pu prendre $\{1, j\}$ comme base de \mathbb{C} sur \mathbb{R} , où $j = \exp(2i\pi/3)$.)

En fait, le produit tensoriel permet de construire l'espace vectoriel complexifié $V_{\mathbb{C}}$ de façon *canonique*, c.-à-d., sans avoir besoin de choisir une base d'un côté ou de l'autre. Mieux, ceci se généralise de la façon suivante.

33.1 Extension et restriction des scalaires

Soit $\phi : A \rightarrow B$ un morphisme d'anneaux commutatifs ; c.-à-d., B est une A -algèbre.

Définition et proposition 33.1.1 (Extension des scalaires) *Soit M un A -module. Alors sur le A -module $B \otimes_A M$, il existe une unique structure de B -module telle que*

$$(*) \quad b \cdot (b' \otimes m) = bb' \otimes m, \quad \forall b, b' \in B, m \in M.$$

On l'appelle le module obtenu par extension des scalaires (ou changement de base) de A à B .

Démonstration. Par hypothèse, B, M sont des A -modules, et l'on peut former le A -module $B \otimes_A M$, où l'action de A est définie par :

$$a \cdot (b \otimes m) = \phi(a)b \otimes m = b \otimes am.$$

Il faut voir que l'action $(*)$ de B est bien définie. Or, on voit facilement que l'application

$$B \times B \times M \rightarrow B \otimes_A M, \quad (b, b', m) \mapsto bb' \otimes m$$

est A -trilinéaire. Elle induit donc une application A -linéaire

$$\gamma : B \otimes_A B \otimes_A M \rightarrow B \otimes_A M$$

telle que $\gamma(b \otimes b' \otimes m) = bb' \otimes m$, puis une application A -bilinéaire $B \times (B \otimes_A M) \rightarrow B \otimes_A M$, telle que

$$b \cdot (b' \otimes m) = bb' \otimes m.$$

Comme tout élément w de $B \otimes_A M$ est une somme de tenseurs $b' \otimes m$, on obtient facilement que $1 \cdot w = w$ et $b \cdot (c \cdot w) = bc \cdot w$, pour tout $w \in B \otimes_A M$, $b, c \in B$. Ceci montre que $B \otimes_A M$ est un B -module. \square

Définition 33.1.2 (Restriction des scalaires) *Soit N un B -module. On peut le considérer comme A -module via $\phi : A \rightarrow B$, en posant*

$$a \cdot n := \phi(a)n, \quad \forall a \in A, n \in N.$$

On notera ${}_A N$ ce A -module ; on dit que c'est le A -module obtenu à partir de N par restriction des scalaires.

Théorème 33.1.3 (Propriété universelle des modules étendus)

Soient M un A -module et N un B -module. On a une bijection

$$\theta(M, N) : \text{Hom}_A(M, {}_A N) \rightarrow \text{Hom}_B(B \otimes_A M, N)$$

défini par $\theta(M, N)(f)(b \otimes m) = bf(m)$, pour tout $f \in \text{Hom}_A(M, {}_A N)$ et $b \in B, m \in M$.

De plus, cette bijection est bifonctorielle, au sens suivant. Soient $\phi : M' \rightarrow M$ un A -morphisme et $\psi : N \rightarrow N'$ un B -morphisme. Alors le diagramme suivant est commutatif :

$$\begin{array}{ccc} \text{Hom}_A(M', {}_A N) & \xrightarrow[\sim]{\theta(M', N)} & \text{Hom}_B(B \otimes_A M', N) \\ \phi^* \uparrow & & \uparrow (\text{id}_B \otimes \phi)^* \\ \text{Hom}_A(M, {}_A N) & \xrightarrow[\sim]{\theta(M, N)} & \text{Hom}_B(B \otimes_A M, N) \\ \psi_* \downarrow & & \downarrow \psi_* \\ \text{Hom}_A(M, {}_A N') & \xrightarrow[\sim]{\theta(M, N')} & \text{Hom}_B(B \otimes_A M, N'), \end{array}$$

où $\phi^*(f) = f \circ \phi$ et $\psi_*(f) = \psi \circ f$, pour tout f .

Démonstration. Soit $f \in \text{Hom}_A(M, N)$. L'application

$$B \times M \rightarrow N, \quad (b, m) \mapsto bf(m)$$

est A -bilinéaire donc induit une application A -linéaire

$$\theta(f) : B \otimes_A M \rightarrow N, \quad b \otimes m \mapsto bf(m).$$

Pour tout $b, b' \in B, m \in M$, on a

$$\theta(f)(b \cdot (b' \otimes m)) = \theta(f)(bb' \otimes m) = bb'm = b\theta(f)(b' \otimes m).$$

Comme tout $x \in B \otimes_A M$ est somme de tenseurs $b' \otimes m$, ceci montre que $\theta(f)$ est B -linéaire. Ceci montre qu'on a une l'application bien définie $\theta = \theta(M, N) :$

$$\text{Hom}_A(M, {}_A N) \rightarrow \text{Hom}_B(B \otimes_A M, N).$$

D'autre part, pour tout $\gamma \in \text{Hom}_B(B \otimes_A M, N)$, notons $\gamma|_M$ l'application

$$M \rightarrow {}_A N, \quad m \mapsto \gamma(1 \otimes m).$$

On voit facilement que $\gamma|_M$ est A -linéaire, et que $\theta(f)|_M = f$. De plus, pour tout $b \in B$, $m \in M$, on a

$$\theta(\gamma|_M)(b \otimes m) = b\gamma|_M(m) = b\gamma(1 \otimes m) = \gamma(b \otimes m).$$

Ceci montre que $\theta(\gamma|_M) = \gamma$. La bijection annoncée en découle.

La vérification de la bifonctorialité est facile et est laissée au lecteur. \square

On peut alors définir le complexifié d'un \mathbb{R} -espace vectoriel V comme étant le \mathbb{C} -espace vectoriel obtenu par extension des scalaires :

$$V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V.$$

On laisse au lecteur le soin de vérifier, par exemple en utilisant la proposition précédente, que ceci coïncide avec les deux définitions données en 33.0.

33.2 Produit tensoriel par $S^{-1}A$

Un exemple important d'extension des scalaires est la localisation par rapport à une partie multiplicative S .

Soient A un anneau, S une partie multiplicative de A et soit M un A -module. On a construit au paragraphe 12.3 (Chap. 3) le $S^{-1}A$ -module $S^{-1}M$. Rappelons brièvement que $S^{-1}M$ est formé des "fractions" m/s , où $m \in M$, $s \in S$, et que l'on a :

$$\frac{m}{s} = \frac{m'}{t} \Leftrightarrow \text{il existe } u \in S \text{ tel que } u(tm - sm') = 0.$$

La structure de $S^{-1}A$ -module est définie par

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st},$$

et l'application $\tau_M : M \rightarrow S^{-1}M$, $m \mapsto m/1$ est un morphisme de A -modules.

De plus, via $A \rightarrow S^{-1}A$, tout $S^{-1}A$ -module N peut être vu, par restriction des scalaires, comme un A -module noté ${}_A N$. Avec cette notation, la propriété universelle de $S^{-1}M$ énoncée dans le théorème 12.3.1, se reformule comme suit.

Théorème 33.2.1 (Propriété universelle de $S^{-1}M$) *Pour tout $S^{-1}A$ -module N , l'application $\gamma \mapsto \gamma|_M$ est une bijection :*

$$\text{Hom}_{S^{-1}A}(S^{-1}M, N) \xrightarrow{\sim} \text{Hom}_A(M, {}_A N).$$

En d'autres termes, $S^{-1}M$ vérifie la même propriété universelle que le module étendu $S^{-1}A \otimes_A M$.

De ceci on déduit :

Théorème 33.2.2 *Il existe un unique isomorphisme de $S^{-1}A$ -modules*

$$\eta_M : S^{-1}M \xrightarrow{\sim} S^{-1}A \otimes_A M$$

tel que $\eta_M(m/1) = 1 \otimes m$, pour tout $m \in M$.

De plus, cet isomorphisme est fonctoriel en M , c.-à-d., si $f : M \rightarrow N$ est un morphisme de A -modules, alors le diagramme ci-dessous est commutatif :

$$\begin{array}{ccc} S^{-1}M & \xrightarrow[\sim]{\eta_M} & S^{-1}A \otimes_A M \\ S^{-1}f \downarrow & & \downarrow \text{id} \otimes f \\ S^{-1}N & \xrightarrow[\sim]{\eta_N} & S^{-1}A \otimes_A N. \end{array}$$

Démonstration. D'après la propriété universelle de $S^{-1}M$, il existe un unique $S^{-1}A$ -morphisme $\phi : S^{-1}M \rightarrow S^{-1}A \otimes_A M$ tel que $\phi(m/1) = 1 \otimes m$, pour tout $m \in M$.

De même, d'après la propriété universelle de $S^{-1}A \otimes_A M$, il existe un unique $S^{-1}A$ -morphisme $S^{-1}A \otimes_A M \rightarrow S^{-1}M$ tel que $\psi(1 \otimes m) = m/1$, pour tout $m \in M$. Il en résulte que $\psi \circ \phi = \text{id}$ et $\phi \circ \psi = \text{id}$. Ceci prouve la première assertion. La vérification de la fonctorialité est facile et laissée au lecteur. \square

33.3 Produit tensoriel par A/I

Soit I un idéal de A . Un autre exemple important d'extension des scalaires est le changement de base par le morphisme $A \rightarrow A/I$. (Même si l'anneau quotient A/I est "plus petit" que A , on parle encore d'extension des scalaires). Soit M un A -module, et formons le A -module M/IM . On a vu au paragraphe 9.6 (Chap. 2) que l'action de A sur M/IM , donnée par un morphisme d'anneaux

$$A \rightarrow \text{End}(M/IM),$$

se factorisait à travers A/I , munissant ainsi M/IM d'une structure de A/I -module.

Proposition 33.3.1 *On a un isomorphisme de A/I -modules : $(A/I) \otimes_A M \cong M/IM$.*

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

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

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

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

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

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

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

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

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

Par conséquent, τ se factorise en un A -morphisme

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

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

34 Algèbres tensorielles, symétriques, et extérieures

Un autre intérêt du produit tensoriel est qu'il permet de construire certaines algèbres associées à un k -espace vectoriel V ou, plus généralement, un A -module M . Dans la suite, A désignera un anneau **commutatif**.

34.1 A -algèbres non-commutatives

On va être amené à considérer des morphismes d'anneaux $A \rightarrow B$, où B est un anneau non nécessairement commutatif. Ceci conduit aux définitions suivantes.

Définition 34.1.1 (A -algèbres) Soit $\phi : A \rightarrow B$ un morphisme d'anneaux, B n'étant pas nécessairement commutatif. Alors ϕ définit deux structures de A -module sur B :

$$a \cdot b = \phi(a)b, \quad a * b = b\phi(a),$$

pour $a \in A$, $b \in B$. (On a $a' * (a * b) = (aa') * b = (a'a) * b$ car A est commutatif). On dit que B est une **A -algèbre** si ces deux structures de A -module coïncident, c.-à-d., si l'on a

$$\phi(a)b = b\phi(a), \quad \forall a \in A, b \in B.$$

Définition 34.1.2 (Centre d'un anneau) Soit B un anneau non nécessairement commutatif. On dit qu'un élément $b_0 \in B$ est **central** s'il commute à tout élément de B , c.-à-d., si $b_0b = bb_0$ pour tout $b \in B$. On note $Z(B)$ l'ensemble des éléments centraux de B ; il contient 1, et l'on voit facilement que c'est un sous-anneau de B . On l'appelle le **centre** de B .

Alors, un morphisme d'anneaux $A \rightarrow B$ fait de B une A -algèbre si et seulement si, $\phi(A) \subseteq Z(B)$.

34.2 Algèbre tensorielle d'un A -module

Soit M un A -module. Pour tout $n \in \mathbb{N}$, on pose

$$T_A^n(M) = M^{\otimes n} = M \otimes_A M \otimes_A \cdots \otimes_A M$$

(n facteurs), avec la convention $T_A^0(M) = A$.

Théorème 34.2.1 (L'algèbre tensorielle $T_A(M)$) On pose

$$T_A(M) = A \oplus M \oplus M^{\otimes 2} \oplus M^{\otimes 3} \oplus \cdots$$

C'est une A -algèbre associative, non-commutative, pour la multiplication définie par :

$$(1) \quad a \cdot w = aw = w \cdot a, \quad \forall a \in A, w \in T_A(M),$$

et, pour $p, q \geq 1$ et $x_1, \dots, x_p, y_1, \dots, y_q \in M$,

$$(2) \quad (x_1 \otimes \cdots \otimes x_p) \cdot (y_1 \otimes \cdots \otimes y_q) = x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q.$$

De plus, $T_A(M)$ vérifie la propriété universelle suivante : pour toute A -algèbre non nécessairement commutative B , et tout morphisme de A -modules $\tau : M \rightarrow B$, il existe un unique morphisme de A -algèbres $\phi : T_A(M) \rightarrow B$ tel que $\phi(m) = \tau(m)$, pour tout $m \in M$.

Démonstration. Soient $p, q \geq 1$. D'après le théorème 32.4.4, on a

$$\begin{array}{ccc} T_A^p(M) \otimes_A T_A^q(M) & \xrightarrow{\sim} & T_A^{p+q}(M) \\ (x_1 \otimes \cdots \otimes x_p) \otimes (y_1 \otimes \cdots \otimes y_q) & \mapsto & x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q. \end{array}$$

et ceci induit une application de multiplication A -bilinéaire

$$T_A^p(M) \times T_A^q(M) \rightarrow T_A^{p+q}(M)$$

vérifiant (2). On vérifie alors facilement que la multiplication est associative. Par définition, les éléments de A sont centraux, donc $T_A(M)$ est une A -algèbre.

Soient $f : A \rightarrow B$ une A -algèbre (non nécessairement commutative) et $\tau : M \rightarrow B$ un morphisme de A -modules. Pour tout $n \geq 1$, l'application

$$M^n \rightarrow B, \quad (x_1, \dots, x_n) \mapsto \tau(x_1) \cdots \tau(x_n)$$

(à droite, c'est le produit dans B), est A -multilinéaire donc induit une application A -linéaire $\phi_n = T_A^n(M) \rightarrow B$ telle que

$$(*) \quad \phi_n(x_1 \otimes \cdots \otimes x_n) = \tau(x_1) \cdots \tau(x_n).$$

Alors, on vérifie facilement que l'application $\phi : T_A(M) \rightarrow B$, égale à f sur $T_A^0(M) = A$ et à ϕ_n sur chaque $T_A^n(M)$, est un morphisme de A -algèbres, vérifiant $\phi(m) = \tau(m)$ pour tout $m \in M$. Enfin, un tel morphisme vérifie nécessairement (*), ce qui prouve l'unicité de ϕ . Le théorème est démontré. \square

Proposition 34.2.2 *Si M est un A -module libre de base (v_1, \dots, v_d) , alors chaque $T_A^n(M)$ est un A -module libre de base les éléments*

$$v_{i_1} \otimes \cdots \otimes v_{i_n}, \quad i_1, \dots, i_n \in \{1, \dots, d\}.$$

En particulier, $T_A^n(M)$ est libre de rang d^n .

Démonstration. Ceci résulte, par récurrence sur n , du théorème 32.5.4 (voir aussi la remarque 32.6.10). \square

34.3 Modules et algèbres gradués

Avant de définir l'algèbre symétrique de M , il est utile d'introduire la notion de A -module (resp. A -algèbre) gradué. Par définition, un A -module **gradué** est un A -module M somme directe de A -modules $(M_n)_{n \in \mathbb{N}}$:

$$M = \bigoplus_{n \in \mathbb{N}} M_n.$$

Dans ce cas, M_n s'appelle la composante de degré n de M . On dit qu'un élément $x \in M$ est **homogène** s'il est non nul et appartient à l'une des

composantes M_n ; dans ce cas, on dit que x est homogène de degré n , ou simplement **de degré n** .

Soit B une A -algèbre. Supposons que comme A -module B soit une somme directe $B = \bigoplus_n B_n$ et que la multiplication vérifie : $1 \in B_0$ et

$$B_p \cdot B_q \subseteq B_{p+q}, \forall p, q.$$

Dans ce cas, on dit que B est une **A -algèbre graduée**. En particulier, $T_A(M) = \bigoplus_n T_A^n(M)$ est une A -algèbre graduée.

On renvoie à 9.4 (Chap. 2) pour la notion d'idéal bilatère et d'anneau quotient dans le cas non-commutatif.

Définition et proposition 34.3.1 Soit $B = \bigoplus_n B_n$ une A -algèbre graduée et soit I un idéal bilatère de B . On dit que I est un **idéal homogène** s'il est engendré par des éléments homogènes de B . Dans ce cas, posant $I_n = I \cap B_n$ pour tout n , on a

$$(*) \quad I = \bigoplus_n (I \cap B_n),$$

et l'algèbre quotient B/I est graduée :

$$B/I = \bigoplus_n (B/I)_n, \quad \text{où } (B/I)_n = B_n/I_n.$$

Démonstration. Dans (*), l'inclusion \supseteq a toujours lieu, et il s'agit de montrer l'autre inclusion lorsque I est homogène. Soit (x_λ) un système de générateurs homogènes de I , chaque x_λ étant de degré d_λ . Tout élément de I est somme d'éléments de la forme $bx_\lambda c$, avec $b, c \in B$. Écrivons

$$b = b_1 + \cdots + b_r, \quad c = c_1 + \cdots + c_s,$$

avec chaque b_i , resp. c_j , homogène de degré p_i , resp. q_j . Alors

$$bx_\lambda c = \sum_{i=1}^r \sum_{j=1}^s b_i x_\lambda c_j,$$

et chaque $b_i x_\lambda c_j$ appartient à I et est homogène de degré $p_i + d_\lambda + q_j$, ou bien nul. Il en résulte que $I = \bigoplus_n I_n$.

Donc, $B/I \cong \bigoplus_n (B_n/I_n)$, d'après le corollaire 21.4.1, et l'on vérifie alors facilement que la multiplication de B/I (induite par celle de B) fait de B/I une A -algèbre graduée. \square

34.4 Algèbre symétrique d'un A -module

Soit M un A -module.

Définition et proposition 34.4.1 (L'algèbre symétrique $S_A(M)$) Soit $S_A(M)$ le quotient de la A -algèbre $T_A(M)$ par l'idéal homogène I engendré par les éléments de degré 2 :

$$x \otimes y - y \otimes x, \quad x, y \in M.$$

On a $S_A(M) = \bigoplus_{n \geq 0} S_A^n(M)$, avec $S_A^0(M) = A$ et $S_A^1(M) = M$, et $S_A(M)$ est une A -algèbre graduée **commutative**, appelée l'algèbre symétrique du A -module M . Elle vérifie la propriété universelle suivante : pour toute A -algèbre commutative B , et tout morphisme de A -modules $\tau : M \rightarrow B$, il existe un unique morphisme de A -algèbres $\psi : S_A(M) \rightarrow B$ tel que $\psi(m) = \tau(m)$, pour tout $m \in M$.

Démonstration. Posant $I_n = I \cap T_A^n(M)$ et $S_A^n(M) = T_A^n(M)/I_n$, il résulte de la proposition précédente que

$$S_A(M) = \bigoplus_{n \geq 0} S_A^n(M)$$

est une A -algèbre graduée. De plus, comme I est engendré par des éléments de degré 2, on a $I_0 = 0 = I_1$ et donc $S_A^0(M) = A$ et $S_A^1(M) = M$.

Pour $x, y \in M$, leur produit $xy \in S_A^2(M)$ est l'image dans $S_A^2(M)$ de $x \otimes y$. Mais, comme $x \otimes y - y \otimes x \in I_2$, on obtient que

$$(\dagger) \quad xy = yx, \quad \forall x, y \in M$$

On en déduit que $S_A(M)$ est commutative. En effet, tout élément de $S_A(M)$ est une somme finie de monômes $x_1 \cdots x_p$, où $x_i \in M$, et il résulte de (\dagger) que deux tels monômes commutent.

Enfin, la propriété universelle de $S_A(M)$ découle de celle de $T_A(M)$: soient B une A -algèbre commutative et $\tau : M \rightarrow B$ un morphisme de A -modules. Alors, il existe un unique morphisme de A -algèbres $\phi : T_A(M) \rightarrow B$ tel que

$$\phi(x_1 \otimes \cdots \otimes x_p) = \tau(x_1) \cdots \tau(x_p)$$

pour tout $p \geq 1$, $x_i \in M$. Comme B est commutative, on a $\phi(x \otimes y - y \otimes x) = 0$ pour tout $x, y \in M$, d'où $\phi(I) = 0$. Donc ϕ passe au quotient et définit un morphisme de A -algèbres $\psi : S_A(M) \rightarrow B$ tel que

$$(*) \quad \psi(x_1 \cdots x_p) = \tau(x_1) \cdots \tau(x_p)$$

pour tout $p \geq 1$ et $x_i \in M$. Ceci prouve l'existence. Enfin, tout morphisme de A -algèbres $\psi : S_A(M) \rightarrow B$ tel que $\psi(m) = \tau(m)$ pour $m \in M$, doit vérifier (*), d'où l'unicité. \square

Théorème 34.4.2 (Algèbre symétrique de A^r) *Soit M un A -module libre de rang r . On a un isomorphisme de A -algèbres*

$$S_A(M) \cong A[X_1, \dots, X_r].$$

En particulier, si (v_1, \dots, v_r) est une A -base de M alors, pour tout $n \geq 1$, les monômes

$$v_1^{t_1} \cdots v_r^{t_r}, \quad t_i \geq 0, \quad t_1 + \cdots + t_r = n,$$

forment une A -base de $S_A^n(M)$ et celui-ci est un A -module libre de rang $\binom{n+r-1}{r-1}$.

Démonstration. Soit (v_1, \dots, v_r) une A -base de M . Considérons le morphisme de A -modules $\tau : M \rightarrow k[X_1, \dots, X_r]$ défini par $\tau(v_i) = X_i$. D'après la propriété universelle de $S_A(M)$, il existe un unique morphisme de A -algèbres

$$\psi : S_A(M) \rightarrow A[X_1, \dots, X_r]$$

tel que $\psi(v_i) = X_i$ pour $i = 1, \dots, r$. Réciproquement, d'après la propriété universelle de $A[X_1, \dots, X_r]$, il existe un unique morphisme de A -algèbres

$$\phi : A[X_1, \dots, X_r] \rightarrow S_A(M)$$

tel que $\phi(X_i) = v_i$. Alors $\phi \circ \psi = \text{id}$ puisque $S_A(M)$ est engendrée comme A -algèbre par les v_i , et de même $\psi \circ \phi = \text{id}$. Donc ψ et ϕ sont des isomorphismes réciproques, et la deuxième assertion en découle.

Enfin, le calcul du rang s'effectue grâce à l'astuce suivante. Considérons une ligne formée de $n + r - 1$ cases, numérotées de 1 à $n + r - 1$ de gauche à droite, dans laquelle on veut noircir $r - 1$ cases. Il y a

$$\binom{n+r-1}{r-1}$$

choix possibles. D'autre part, chaque choix consiste en une suite strictement croissante

$$0 = k_0 < k_1 < \cdots < k_{r-1} < k_r = n$$

formée des numéros des cases noircies. Ce choix correspond au monôme

$$v_1^{t_1} \cdots v_r^{t_r},$$

où l'on a posé $t_i = k_i - k_{i-1}$ (le nombre de cases blanches entre k_{i-1} et k_i). On a bien $t_i \geq 0$ et $\sum_i t_i = n$, et réciproquement la donnée de tels t_i détermine de façon unique une suite de k_i . Ceci achève la preuve du théorème. \square

34.5 Algèbre extérieure et applications multilinéaires alternées

Soit M un A -module.

Définition et proposition 34.5.1 (L'algèbre extérieure $\bigwedge_A(M)$) Soit $\bigwedge_A(M)$ le quotient de la A -algèbre $T_A(M)$ par l'idéal homogène J engendré par les éléments de degré 2 :

$$x \otimes x, \quad x \in M.$$

On a $\bigwedge_A(M) = \bigoplus_{n \geq 0} \bigwedge_A^n(M)$, avec $\bigwedge_A^0(M) = A$ et $\bigwedge_A^1(M) = M$, et $\bigwedge_A(M)$ est une A -algèbre graduée, appelée l'algèbre extérieure du A -module M . Elle vérifie la propriété universelle suivante : pour toute A -algèbre B , et tout morphisme de A -modules $\tau : M \rightarrow B$ tel que

$$\tau(m)^2 = 0, \quad \forall m \in M,$$

il existe un unique morphisme de A -algèbres $\psi : \bigwedge_A(M) \rightarrow B$ tel que $\psi(m) = \tau(m)$, pour tout $m \in M$.

Démonstration. Posons $J_n = J \cap T_A^n(M)$ et $\bigwedge_A^n(M) = T_A^n(M)/J_n$. Comme J est engendré par des éléments de degré 2, c'est un idéal homogène, et il résulte de la proposition 34.3.1 que

$$\bigwedge_A(M) = \bigoplus_{n \geq 0} \bigwedge_A^n(M)$$

est une A -algèbre graduée. De plus, $J_0 = 0 = J_1$, d'où $\bigwedge_A^0(M) = A$ et $\bigwedge_A^1(M) = M$.

La propriété universelle de $\bigwedge_A(M)$ découle de celle de $T_A(M)$, exactement comme dans le cas de l'algèbre symétrique. Ceci ne présente pas de difficulté et est laissé au lecteur. \square

Notation 34.5.2 Soient $x_1, \dots, x_n \in M = \bigwedge_A^1(M)$. On désigne par

$$x_1 \wedge \cdots \wedge x_n$$

leur produit dans l'algèbre $\bigwedge_A(M)$. Par définition, c'est l'image dans $\bigwedge_A^n(M)$ de $x_1 \otimes \cdots \otimes x_n$.

On rappelle que S_n désigne le groupe des permutations de $\{1, \dots, n\}$, cf. 27.3 (Chap. 7).

Lemme 34.5.3 1) Pour tout $x, y \in M$, on a

$$(*) \quad x \wedge y = -y \wedge x.$$

2) Plus généralement, pour tout $n \geq 2$, $x_1, \dots, x_n \in M$ et $\tau \in S_n$, on a

$$(**) \quad x_{\tau(1)} \wedge \dots \wedge x_{\tau(n)} = \pm x_1 \wedge \dots \wedge x_n.$$

3) Pour tout $n \geq 2$, soit J'_n le sous- A -module de $T_A^n(M)$ engendré par les tenseurs $x_1 \otimes \dots \otimes x_n$ pour lesquels les x_i ne sont pas tous distincts (c.-à-d., il existe $i \neq j$ tel que $x_i = x_j$). Alors, $J'_n = J_n$.

Démonstration. Pour tout $x, y \in M$, on a

$$(x + y) \otimes (x + y) = x \otimes x + y \otimes y + x \otimes y + y \otimes x,$$

d'où $x \otimes y + y \otimes x \in J$, et donc $x \wedge y + y \wedge x = 0$. Ceci prouve 1).

Le point 2) en découle. En effet, si $1 = \tau(i)$, c.-à-d., si x_1 apparaît à la i -ème place dans le tenseur de gauche, alors on peut ramener x_1 à la 1ère place par $(i - 1)$ applications de (*), ce qui produit le signe $(-1)^{i-1}$. On procède ensuite de même avec x_2 , etc.

3) Il est clair que $J_n \subseteq J'_n$; montrons la réciproque. Soient $x_1, \dots, x_n \in M$; on suppose qu'il existe $i < j$ tel que $x_i = x_j$. Il s'agit de montrer que

$$x_1 \otimes \dots \otimes x_n \in J_n$$

ou, de façon équivalente, que $x_1 \wedge \dots \wedge x_n = 0$. Or, en utilisant 1) de façon répétée, puis l'égalité $x_i = x_j$, on obtient

$$x_i \wedge \dots \wedge x_j = (-1)^{j-1-i} x_i \wedge x_j \wedge x_{i+1} \wedge \dots \wedge x_{j-1} = 0.$$

□

Remarque 34.5.4 On renvoie à 27.5 (Chap. 7) pour la définition de la signature $\varepsilon(\tau)$ d'une permutation $\tau \in S_n$. En utilisant le théorème 27.4.3 et le fait que $\varepsilon : S_n \rightarrow \{\pm 1\}$ est un morphisme de groupes (Thm. 27.5.2), on peut montrer que le signe qui apparaît dans (***) est la signature $\varepsilon(\tau)$.

Proposition 34.5.5 Supposons que M soit engendré comme A -module par des éléments v_1, \dots, v_d . Alors, pour $1 \leq n \leq d$, $\bigwedge_A^n(M)$ est engendré comme A -module par les $\binom{d}{n}$ éléments

$$v_{i_1} \wedge \dots \wedge v_{i_n}, \quad 1 \leq i_1 < \dots < i_n \leq d,$$

et l'on a $\bigwedge_A^n(M) = 0$ pour $n > d$.

Démonstration. Soit $n \geq 1$. Par multilinéarité, tout élément de $\bigwedge_A^n(M)$ est combinaison linéaire des d^n éléments

$$v_{i_1} \wedge \cdots \wedge v_{i_n}, \quad 1 \leq i_1, \dots, i_n \leq d.$$

Or, d'après le point 1) du lemme précédent, cet élément est nul si deux indices i_j et i_k sont égaux. Ceci est forcément le cas si $n > d$, ce qui prouve déjà que $\bigwedge_A^n(M) = 0$ si $n > d$.

On peut donc supposer $n \leq d$ et les indices i_1, \dots, i_n deux à deux distincts. On peut de plus se ramener au cas où

$$i_1 < \cdots < i_n$$

puisque, d'après le point 2) du lemme précédent, effectuer des permutations ne fait que produire un changement de signe. Ceci prouve la proposition. \square

Définition 34.5.6 Soient M, N deux A -modules et $n \geq 1$. Une application A -multilinéaire $\phi : M^n \rightarrow N$ est dite **alternée** si elle vérifie, pour tout $x_1, \dots, x_n \in M$,

$$\phi(x_1, \dots, x_n) = 0 \text{ s'il existe } i \neq j \text{ tel que } x_i = x_j.$$

On note $\text{Alt}_n(M, N)$ l'ensemble des applications A -multilinéaires alternées $M^n \rightarrow N$.

Théorème 34.5.7 (Propriété universelle de $\bigwedge_A^n(M)$)

Pour tout morphisme de A -modules $f : \bigwedge_A^n(M) \rightarrow N$, l'application

$$\theta(f) : M^n \rightarrow N, \quad (x_1, \dots, x_n) \mapsto f(x_1 \wedge \cdots \wedge x_n)$$

est alternée, et θ définit une bijection

$$\theta : \text{Hom}_A(\bigwedge_A^n(M), N) \xrightarrow{\sim} \text{Alt}_n(M, N).$$

Démonstration. $\theta(f)$ est évidemment A -multilinéaire. Comme f s'annule sur $J_n = J'_n$, alors $\theta(f)$ est alternée. On a donc une application

$$\theta : \text{Hom}_A(\bigwedge_A^n(M), N) \rightarrow \text{Alt}_n(M, N).$$

Réciproquement, soit $\phi \in \text{Alt}_n(M, N)$. Comme ϕ est A -multilinéaire, il induit une application A -linéaire

$$\eta(\phi) : M^{\otimes n} \rightarrow N, \quad x_1 \otimes \cdots \otimes x_n \mapsto \phi(x_1, \dots, x_n).$$

Comme ϕ est alternée, alors $\eta(\phi)$ s'annule sur $J'_n = J_n$ donc passe au quotient et définit une application A -linéaire

$$\eta'(\phi) : \bigwedge_A^n(M) \rightarrow N, \quad x_1 \wedge \cdots \wedge x_n \mapsto \phi(x_1, \dots, x_n).$$

On voit alors que θ et η' sont des bijections réciproques. Ceci prouve le théorème. \square

Théorème 34.5.8 (Algèbre extérieure de A^d) *Si M est un A -module libre de base (v_1, \dots, v_d) alors $\bigwedge_A^d(M) = 0$ pour $n > d$ et, pour $n \leq d$, les monômes*

$$(\dagger) \quad v_{i_1} \wedge \cdots \wedge v_{i_n}, \quad 1 \leq i_1 < \cdots < i_n \leq d,$$

forment une A -base de $\bigwedge_A^n(M)$; celui-ci est donc un A -module libre de rang $\binom{d}{n}$. En particulier, $\bigwedge_A^d(M) \cong A$.

Démonstration. D'après la proposition 34.5.5, $\bigwedge_A^n(M) = 0$ pour $n > d$, et les éléments (\dagger) engendrent $\bigwedge_A^n(M)$ comme A -module pour $n \leq d$. Il s'agit donc de montrer que les éléments (\dagger) sont linéairement indépendants sur A .

Traitons d'abord le cas particulier $n = d$. Posons $C = \bigwedge_A^d(M)$; on sait que C est engendré comme A -module par l'élément

$$c := v_1 \wedge \cdots \wedge v_d.$$

Soit \mathfrak{a} l'annulateur de c , c.-à-d., le noyau du morphisme surjectif $A \rightarrow C$, $a \mapsto ac$. Il s'agit de montrer que $\mathfrak{a} = 0$. On va montrer plus bas qu'il existe un élément

$$(*) \quad f \in \text{Hom}_A(C, A) \text{ tel que } f(c) = 1.$$

Tenant ceci pour acquis, pour tout $a \in \mathfrak{a}$ on obtient $0 = f(ac) = af(c) = a$, d'où $\mathfrak{a} = 0$. Ceci montre que $\bigwedge_A^d(M)$ est librement engendré par c .

Maintenant, pour $n < d$, notons \mathcal{P}_n l'ensemble des parties de $\{1, \dots, d\}$ ayant n éléments. Si I est une telle partie, et si l'on désigne par $i_1 < \cdots < i_n$ ses éléments, rangés par ordre croissant, on pose

$$v_I := v_{i_1} \wedge \cdots \wedge v_{i_n}.$$

Supposons qu'on ait une relation de dépendance linéaire

$$(E) \quad 0 = \sum_{I \in \mathcal{P}_n} a_I v_I, \quad a_I \in A.$$

Fixons $I_0 \in \mathcal{P}_n$ et soit J_0 son complémentaire dans $\{1, \dots, d\}$. Alors $J_0 \in \mathcal{P}_{d-n}$ et, pour tout $I \in \mathcal{P}_n$, on a :

$$I \neq I_0 \Rightarrow I \cap J_0 \neq \emptyset.$$

Par conséquent, il résulte du lemme 34.5.3 qu'en multipliant (E) par v_{J_0} , on obtient

$$0 = a_{I_0} v_{I_0} \wedge v_{J_0} = \pm a_{I_0} c.$$

Comme C est librement engendré par c , ceci implique $a_{I_0} = 0$. Ceci montre que les v_I sont linéairement indépendants, donc forment une base de $\bigwedge_A^n(M)$, qui est donc un A -module libre de rang $\binom{d}{n}$. Ceci achève la preuve du théorème, modulo la preuve de l'assertion (*).

Or, d'après la propriété universelle 34.5.7, on a

$$\mathrm{Hom}_A(\bigwedge_A^d(M), A) \cong \mathrm{Alt}_d(M, A).$$

Par conséquent, pour trouver un tel f , il suffit de trouver une application A -multilinéaire alternée $\phi : M^d \rightarrow A$ telle que $\phi(v_1, \dots, v_d) = 1$. Considérons l'application ϕ définie comme suit. Pour tout d -uplet (x_1, \dots, x_d) d'éléments de M , on peut former la matrice

$$P(x_1, \dots, x_d) = \mathrm{Mat}_{(v_1, \dots, v_d)}(x_1, \dots, x_d)$$

exprimant les x_j dans la base (v_i) . C.-à-d., chaque x_j s'écrit de façon unique dans la base (v_i) :

$$x_j = \sum_{i=1}^d a_{ij} v_i;$$

on forme alors la matrice $P(x_1, \dots, x_d) = (a_{ij})_{1 \leq i, j \leq d}$. On pose alors

$$\phi(x_1, \dots, x_d) = \det P(x_1, \dots, x_d).$$

Il résulte des propriétés des déterminants que ϕ est une application multilinéaire alternée. (Pour la construction et les propriétés des déterminants, on renvoie, par exemple, à [BM, Ch. IV] ou [La, XIII, §4]). De plus, pour $(x_1, \dots, x_d) = (v_1, \dots, v_d)$, la matrice P est la matrice identité, de déterminant 1. On a donc bien $\phi(v_1, \dots, v_d) = 1$. Ceci achève la preuve du théorème.

□

Table des matières

Chapitre 0	1
1 Nombres entiers et rationnels	1
1.1 Notations et définitions	1
1.2 Division euclidienne et conséquences	2
1.3 Solutions entières de $x^2 + y^2 = z^2$	7
2 Entiers algébriques	8
2.1 Somme de deux carrés et entiers de Gauss	8
2.2 Les anneaux de nombres $\mathbb{Z}[\sqrt{n}]$	12
2.3 Les anneaux $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	15
2.4 Entiers algébriques	16
2.5 Anneaux noethériens	19
2.6 Éléments irréductibles dans un anneau intègre noethérien	21
Chapitre 1	23
3 \mathbb{C} est algébriquement clos	23
3.1 L'énoncé du théorème	23
3.2 La démonstration d'Argand	24
3.3 La cas de plusieurs polynômes	25
4 Le théorème des zéros	26
4.0 Courbes algébriques	26
4.1 Variétés algébriques	27
4.2 Vers la suite du cours	28
Chapitre 2	29
5 Anneaux et idéaux	29
5.1 Anneaux et corps	29
5.2 Idéaux	31
6 Modules	32

6.1	Groupes abéliens et \mathbb{Z} -modules	32
6.2	A -modules et sous- A -modules	32
6.3	Construction de modules (I) : sommes directes finies	35
6.4	Morphismes et isomorphismes	35
6.5	Modules de type fini	36
7	Modules et anneaux noethériens	38
7.1	Modules noethériens	38
7.2	Anneaux et modules noethériens	39
8	Anneaux de polynômes et théorème de transfert de Hilbert	40
8.1	L'anneau de polynômes $A[X]$	40
8.2	Le théorème de transfert de Hilbert	42
8.3	Construction de modules (II) : modules libres	43
8.4	Anneaux de polynômes en plusieurs variables	46
8.5	Morphismes d'anneaux et A -algèbres	48
8.6	A -algèbres et propriété universelle des algèbres de polynômes	49
9	Modules et anneaux quotients, théorèmes d'isomorphisme de Noether	50
9.1	Définition des modules quotients	50
9.2	Noyaux et images, théorèmes de Noether	52
9.3	Applications des modules quotients	55
9.4	Anneaux quotients	57
9.5	Algèbres de fonctions polynomiales	59
9.6	Anneaux d'endomorphismes et A/I -modules	61
10	Algèbres de type fini et noethérianité	63
10.1	Algèbres de type fini	63
10.2	Résultats de noethérianité	65
Chapitre 3		67
11	Idéaux premiers et maximaux, Lemme de Zorn	67
11.1	Idéaux premiers et maximaux	67
11.2	Sous-modules maximaux et lemme de Zorn	68
12	Anneaux de fractions, localisation	71
12.0	Motivation	72
12.1	Construction de l'anneau $S^{-1}A$	73
12.2	Le cas intègre	77
12.3	Localisation de modules	79
12.4	Idéaux premiers de $S^{-1}A$, anneaux locaux	83
12.5	Support et idéaux premiers associés	84

13	Idéaux irréductibles, radical d'un idéal et idéaux premiers minimaux	88
13.1	Idéaux irréductibles	88
13.2	Racine d'un idéal et idéaux premiers minimaux	90
14	Extensions entières et extensions de corps (I)	91
14.1	Morphismes entiers	91
14.2	Extensions de corps, multiplicativité du degré	93
14.3	Retour sur $K[X]$	94
15	Un aperçu de géométrie algébrique, théorème des zéros de Hilbert	95
15.1	Sous-variétés algébriques de k^n et topologie de Zariski	95
15.2	Le théorème des zéros de Hilbert	97
Chapitre 4		101
16	Anneaux factoriels	101
16.1	Éléments irréductibles et éléments associés	101
16.2	Anneaux factoriels, lemmes d'Euclide et Gauss	102
16.3	PPCM et PGCD dans un anneau factoriel	105
16.4	Le théorème de transfert de Gauss	107
17	Anneaux principaux et anneaux euclidiens	111
17.1	Les anneaux euclidiens sont principaux	111
17.2	Les anneaux principaux sont factoriels	112
18	Idéaux étrangers et théorème chinois	113
18.1	Idéaux étrangers	113
18.2	Théorème chinois des restes	115
19	Modules de torsion sur un anneau principal	116
19.1	Annulateurs et modules de torsion	116
19.2	Décomposition primaire des modules de torsion sur un anneau principal	118
Chapitre 5		125
20	A -modules libres de type fini, invariance du rang	125
20.1	Rang d'un module libre de type fini	125
20.2	Modules d'homomorphismes et module dual	127
21	Modules de type fini sur un anneau principal	128
21.1	Matrices échelonnées	128
21.2	Les résultats fondamentaux	129
21.3	Existence d'une base adaptée	130
21.4	Décomposition des modules de type fini	132
21.5	Unicité des facteurs invariants	134

22	Autre approche : réduction des matrices sur un anneau principal	137
22.1	Une conséquence de l'existence de bases adaptées . . .	137
22.2	Réduction des matrices	137
Chapitre 6		145
23	Caractéristique et extensions de corps	145
23.1	Les corps fondamentaux \mathbb{Q} et \mathbb{F}_p	145
23.2	Généralités sur les extensions	147
23.3	Extensions entières d'anneaux	148
23.4	Éléments algébriques ou bien transcendants	153
23.5	Extensions algébriques de corps et degré d'une extension	154
23.6	Bases de transcendances et extensions de type fini . .	156
24	Corps de rupture et corps de décomposition	160
24.1	Corps de rupture d'un polynôme	160
24.2	Corps de décomposition d'un polynôme	162
24.3	Le groupe des k -automorphismes d'une extension . . .	165
25	Extensions séparables et théorème de l'élément primitif . . .	167
25.1	Polynômes et extensions séparables	167
25.2	Racines multiples et séparabilité	168
25.3	Caractérisation de la séparabilité en termes de mor- phismes	170
25.4	Le théorème de l'élément primitif	172
26	Extensions galoisiennes et correspondance de Galois	174
26.1	Extensions galoisiennes	174
26.2	Indépendance des caractères	178
26.3	Invariants d'un groupe fini : théorème d'Artin	180
26.4	Autre démonstration du théorème d'Artin	182
26.5	Un rappel sur les groupes	182
26.6	Le couronnement : correspondance de Galois	183
26.7	Clôture normale ou galoisienne	185
Chapitre 7		189
27	Théorie des groupes	189
27.1	Ordre d'un élément, théorème de Lagrange	189
27.2	Groupes en action	190
27.3	Groupes symétriques et théorème de Cayley	192
27.4	Décomposition en cycles, engendrement par les trans- positions	193
27.5	Action sur $k[X_1, \dots, X_n]$ et signature	195

27.6	Conjugaison des cycles, générateurs de A_n	197
27.7	Groupes résolubles	198
27.8	A_n n'est pas résoluble, pour $n \geq 5$	200
27.9	Groupes abéliens finis	201
27.10	Centre d'un groupe et équation des classes	203
27.11	p -groupes et théorèmes de Sylow	204
28	Polynômes symétriques et groupes de Galois	206
28.1	Une application de Galois plus Sylow : \mathbb{C} est algébri- quement clos	206
28.2	Groupe de Galois d'un polynôme	208
28.3	Polynômes symétriques	209
28.4	Relations entre coefficients et racines d'un polynôme .	210
28.5	Le théorème fondamental des polynômes symétriques .	211
28.6	Invariants dans le corps des fractions	215
28.7	Fractions rationnelles symétriques	216
28.8	L'équation générale de degré n	217
28.9	Discriminant d'un polynôme	218
28.10	L'extension intermédiaire associée au discriminant . .	221
28.11	L'équation de degré 3	223
29	Équations résolubles par radicaux	224
29.1	Extensions radicales	225
29.2	Adjonction de racines de l'unité	226
29.3	P résoluble par radicaux $\Rightarrow \text{Gal}(P/k)$ résoluble	230
29.4	Un exemple de polynôme $P \in \mathbb{Q}[X]$ non résoluble par radicaux	231
29.5	Compléments sur le critère de résolubilité	233
Chapitre 8		235
30	Corps finis	235
30.1	Cardinal et groupe multiplicatif d'un corps fini	235
30.2	La formule du binôme	236
30.3	Endomorphismes de Frobenius	237
30.4	Existence et unicité des corps \mathbb{F}_{p^n}	238
30.5	Groupe de Galois de \mathbb{F}_{q^n} sur \mathbb{F}_q	239
30.6	Théorème de l'élément primitif, et polynômes irréduc- tibles sur \mathbb{F}_q	241
31	Clôtures algébriques	243
31.1	Corps algébriquement clos	243
31.2	Le corps $\overline{\mathbb{F}}_p$	243
31.3	Clôtures algébriques en général	246

Chapitre 9	249
32	Produit tensoriel 249
32.0	Remarque préliminaire 249
32.1	Applications bilinéaires 250
32.2	Produit tensoriel : définition et propriété universelle . 252
32.3	Premières propriétés du produit tensoriel 255
32.4	Applications multilinéaires et produits tensoriels itérés 257
32.5	Produits tensoriels d'algèbres et produits de variétés . 260
32.6	Produits et sommes directes 263
33	Extension des scalaires et changement de base 269
33.0	Complexifié d'un \mathbb{R} -espace vectoriel 269
33.1	Extension et restriction des scalaires 270
33.2	Produit tensoriel par $S^{-1}A$ 272
33.3	Produit tensoriel par A/I 273
34	Algèbres tensorielles, symétriques, et extérieures 274
34.1	A -algèbres non-commutatives 274
34.2	Algèbre tensorielle d'un A -module 275
34.3	Modules et algèbres gradués 276
34.4	Algèbre symétrique d'un A -module 278
34.5	Algèbre extérieure et applications multilinéaires alter- nées 280

Bibliographie

- [Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.
- [AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.
- [BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.
- [BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.
- [De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.
- [ChL] A. Chambert-Loir, A field guide to algebra, Springer, 2005; version française : Algèbre corporelle (sic!), Presses de l'École polytechnique, 2005.
- [Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.
- [Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.
- [Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.
- [Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.
- [Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.
- [Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.
- [Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).
- [La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.
- [Ne04] J. Nekovář, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~neko/var/co/ln
- [Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

- [Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.
- [Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.
- [Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.
- [St] J. Stillwell, Chapitre d'introduction dans [De].
- [Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.
- [vdW] B.L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.