1. *Définition des homomorphismes*

Soient L et M des modules à gauche sur un anneau K. On appelle **homomorphisme** ou **application linéaire** de L dans M toute application

$$f : \mathrm{L} \to \mathrm{M}$$

telle que l'on ait

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y) \quad \text{quels que soient } x, y \in \mathrm{L},\ \lambda, \mu \in \mathrm{K}.$$

On appelle **isomorphisme** de L sur M tout homomorphisme bijectif de L dans M; on dit que L et M sont **isomorphes** s'il existe un isomorphisme de L sur M.

Enfin, étant donné un K-module à gauche M, on appelle **endomorphisme de** M (ou parfois **opérateur linéaire dans** M) tout homomorphisme de M dans M, et **automorphisme** de M tout isomorphisme de M sur lui-même.

Soient L et M deux K-modules à gauche; pour qu'une application f de L dans M soit linéaire, il faut et il suffit qu'on ait les relations

$$f(x + y) = f(x) + f(y) \quad \text{quels que soient } x, y \in \mathrm{L}$$
$$f(\lambda x) = \lambda f(x) \quad \text{quels que soient } \lambda \in \mathrm{K},\ x \in \mathrm{L}.$$

En prenant $\lambda = 0$ dans la seconde relation, on voit donc que

$$f(0) = 0.$$

D'autre part, si f est un homomorphisme de L dans M, on a la relation

$$f(\lambda_1 x_1 + \cdots + \lambda_n x_n) = \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n) \tag{1}$$

quels que soient l'entier n, les vecteurs $x_1, \ldots, x_n \in \mathrm{L}$ et les scalaires $\lambda_1, \ldots, \lambda_n \in \mathrm{K}$; cette relation se réduit pour $n = 2$ à la définition même des homomorphismes, et se démontre dans le cas général par récurrence sur l'entier n :

$$\begin{aligned} f(\lambda_1 x_1 + \cdots + \lambda_n x_n) &= f[(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1}) + \lambda_n x_n] \\ &= f(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1}) + f(\lambda_n x_n) \\ &= \lambda_1 f(x_1) + \cdots + \lambda_{n-1} f(x_{n-1}) + \lambda_n f(x_n) \end{aligned}$$

comme annoncé.

Nous utiliserons constamment la relation (1) dans ce qui suit, et le plus souvent sans y référer explicitement.

THÉORÈME 1. *Si $f : L \to M$ et $g : M \to N$ sont des homomorphismes de modules, l'application composée $g \circ f$ est encore un homomorphisme, et c'est un isomorphisme si f et g sont des isomorphismes. L'application réciproque d'un isomorphisme de modules est un isomorphisme de modules.*

Soit $h = g \circ f$; on a

$$h(\lambda x + \mu y) = g[f(\lambda x + \mu y)] = g[\lambda f(x) + \mu f(y)] = \lambda g[f(x)] + \mu g[f(y)] = \lambda h(x) + \mu h(y),$$

ce qui montre que h est un homomorphisme; si de plus f et g sont des isomorphismes, i.e. sont bijectifs, il en est de même de h, qui est donc alors un isomorphisme.

Supposons que f soit un isomorphisme; pour montrer que l'application f^{-1} (qui est bijective) est un isomorphisme il suffit de prouver qu'elle est linéaire, autrement dit qu'on a

$$f^{-1}(\lambda u + \mu v) = \lambda f^{-1}(u) + \mu f^{-1}(v)$$

quels que soient $\lambda, \mu \in K$ et $u, v \in M$, ou enfin qu'on a $\lambda u + \mu v = f[\lambda f^{-1}(u) + \mu f^{-1}(v)]$; comme f est linéaire, cette relation s'écrit $\lambda u + \mu v = \lambda f[f^{-1}(u)] + \mu f[f^{-1}(v)]$, et est trivialement vérifiée, d'où le Théorème.

En raisonnant comme au § 7, n° 8, on déduit du Théorème 1 que « X et Y sont isomorphes » est une relation d'équivalence entre K-modules à gauche.

Dans la pratique, on regarde souvent deux modules isomorphes L et M comme identiques; plus exactement, si l'on choisit un isomorphisme f de L sur M, alors on peut traduire toute relation algébrique entre éléments de L en une relation analogue entre les images par f de ces éléments, et par suite transformer toute propriété de L en une propriété analogue de M. Le lecteur aura intérêt à vérifier ce fait aussi fréquemment que possible.

THÉORÈME 2. *Soit $f : L \to M$ un homomorphisme de modules. L'image par f d'un sous-module de L est un sous-module de M. L'image réciproque par f d'un sous-module de M est un sous-module de L.*

Soit L' un sous-module de L; supposons que $f(L')$ contienne deux éléments u, v de M; on peut donc écrire $u = f(x)$, $v = f(y)$ avec $x, y \in L'$; comme f est linéaire, on a $\lambda u + \mu v = f(\lambda x + \mu y) = f(z)$ avec $z = \lambda x + \mu y \in L'$ puisque L' est un sous-module de L; ainsi $f(L')$ contient $\lambda u + \mu v$ quels que soient les scalaires λ et μ, ce qui établit la première assertion de l'énoncé. La seconde se démontre de façon analogue.

En particulier, le **noyau** de f, i.e. l'ensemble des $x \in L$ tels que $f(x) = 0$, est un sous-module de L, qu'on note

$$\mathrm{Ker}(f)$$

conformément au n° 9 du § 7; et l'image

$$\mathrm{Im}(f) = f(L)$$

de f est un sous-module de M. Rappelons (§ 7, Théorème 8) que *f est injectif si et seulement si son noyau se réduit à 0.*

2. Homomorphismes d'un module libre de type fini dans un module quelconque

Le résultat suivant est fondamental :

THÉORÈME 3. *Soient L un K-module à gauche libre de type fini (*), $a_1, \ldots, a_p$ une base de L, M un K-module à gauche quelconque, et $c_1, \ldots, c_p$ des éléments donnés de M. Il existe alors un et un seul homomorphisme f de L dans M vérifiant*

$$f(a_i) = c_i \quad \text{pour} \quad 1 \leqslant i \leqslant p;$$

pour que f soit injectif (resp. surjectif) il faut et il suffit que les vecteurs $c_1, \ldots, c_p$ soient linéairement indépendants (resp. engendrent M).

Vu la relation (1) du n° 1 l'homomorphisme f, s'il existe, est nécessairement donné par la formule

$$f(\xi_1 a_1 + \cdots + \xi_p a_p) = \xi_1 c_1 + \cdots + \xi_p c_p, \tag{2}$$

ce qui montre déjà l'*unicité* de f.

Pour établir l'*existence* de f, notons que, pour tout $x \in L$, il existe un et un seul système de scalaires $\xi_i (1 \leqslant i \leqslant p)$ tel que

$$x = \xi_1 a_1 + \cdots + \xi_p a_p$$

du reste on a

$$\xi_i = f_i(x) \qquad (1 \leqslant i \leqslant p),$$

les applications $f_i : L \to K$ étant (§ 11, n° 4) les fonctions coordonnées du module L par rapport à la base $a_1, \ldots, a_p$. Cela dit, la formule (2) définit effectivement une application f de L dans M, d'ailleurs donnée d'après ce qui précède par la relation

$$f(x) = f_1(x)c_1 + \cdots + f_p(x)c_p,$$

ce qui revient à montrer que f est un *homomorphisme* transformant les vecteurs a_i en les vecteurs c_i.

La seconde assertion résulte aussitôt de la formule

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

(*) On peut étendre le Théorème 3 au cas d'un module libre quelconque, comme le lecteur le vérifiera facilement.

établie au § 11, n° 4, et de la relation

$$c_i = 0.c_1 + \cdots + 0.c_{i-1} + 1.c_i + 0.c_{i+1} + \cdots + 0.c_p.$$

Pour établir que f est un homomorphisme, remarquons d'abord qu'on a démontré au § 11, n° 4 que

$$f_i(\lambda x + \mu y) = \lambda f_i(x) + \mu f_i(y),$$

autrement dit que les fonctions coordonnées $f_i : \mathrm{L} \to \mathrm{K}$ sont des homomorphismes de K-modules à gauche. Par suite

$$\begin{aligned} f(\lambda x + \mu y) &= f_1(\lambda x + \mu y)c_1 + \cdots + f_p(\lambda x + \mu y)c_p \\ &= [\lambda f_1(x) + \mu f_1(y)]c_1 + \cdots + [\lambda f_p(x) + \mu f_p(y)]c_p \\ &= \lambda[f_1(x)c_1 + \cdots + f_p(x)c_p] + \mu[f_1(y)c_1 + \cdots + f_p(y)c_p] \\ &= \lambda f(x) + \mu f(y), \end{aligned}$$

ce qui prouve la linéarité de f.

Reste à déterminer les conditions pour que f soit injectif ou surjectif. Tout d'abord il est clair que l'image $f(\mathrm{L})$ est l'ensemble des combinaisons linéaires des vecteurs $c_1, \ldots, c_p$, autrement dit que f *applique* L *sur le sous-module de* M *engendré par* $c_1, \ldots, c_p$: pour que f soit surjectif il est donc nécessaire et suffisant que les vecteurs c_i engendrent M.

D'autre part, pour que f soit injectif il faut et il suffit que la relation $f(x) = 0$ implique $x = 0$, autrement dit que la relation

$$\xi_1 c_1 + \cdots + \xi_p c_p = 0$$

implique $\xi_1 a_1 + \ldots + \xi_p a_p = 0$, i.e. (puisque les a_i sont linéairement indépendants) implique

$$\xi_1 = 0, \ \ldots, \ \xi_p = 0.$$

Le Théorème 3 est donc démontré.

Corollaire 1. *Pour qu'un* K*-module* M *soit libre de type fini, il faut et il suffit qu'il existe un entier* n *tel que* M *soit isomorphe à* K^n. *Plus précisément, soient* $c_1, \ldots, c_n$ *des éléments de* M, *et* $e_1, \ldots, e_n$ *la base canonique de* K^n. *Pour que les vecteurs* c_i *forment une base de* M, *il faut et il suffit qu'il existe un isomorphisme de* K^n *sur* M *appliquant les vecteurs* e_i *sur les vecteurs* c_i.

D'après le Théorème 3, il existe toujours un et un seul homomorphisme

$$f : \mathrm{K}^n \to \mathrm{M}$$

tel que

$$f(e_i) = c_i \qquad (1 \leqslant i \leqslant p).$$

Pour que les c_i forment une base de M, il faut et il suffit qu'ils soient linéairement indépendants et engendrent M, autrement dit que f soit injectif et surjectif, d'où le Corollaire.

Corollaire 2. *Pour qu'un* K*-module* M *soit de type fini, il faut et il suffit qu'il existe un entier* n *et un homomorphisme* surjectif *de* K^n *dans* M.

Plus précisément, pour que des vecteurs $c_1, \ldots, c_n$ engendrent M, il faut et il suffit que l'homomorphisme $f : \mathrm{K}^n \to \mathrm{M}$ tel que $f(e_i) = c_i$ soit surjectif, d'où la nécessité de la condition. Le fait qu'elle soit suffisante résulte de ce que K^n est de type fini et de l'observation suivante : *soit*

$$f : \mathrm{L} \to \mathrm{M},$$

un homomorphisme de K*-modules; si* f *est surjectif et si* L *est de type fini, alors* M *est de type fini.* Soit en effet $a_1, \ldots, a_n$, un système de générateurs de L, et posons $b_i = f(a_i)$ $(1 \leqslant i \leqslant n)$; pour tout $y \in \mathrm{M}$, il existe un $x \in \mathrm{L}$ tel que $y = f(x)$; écrivant $x = \xi_1 a_1 + \cdots + \xi_n a_n$, et utilisant la relation (1) du n° 1 on voit que $y = \xi_1 b_1 + \ldots + \xi_n b_n$; les b_i engendrent donc M, qui est par suite de type fini.

3. Homomorphismes et matrices

Le Théorème 3 permet de construire tous les homomorphismes d'un module L *libre de type fini* dans un module quelconque M; pour aller plus loin, nous allons supposer que M est lui-même *libre de type fini*. Dans ce qui suit, on désignera par $a_1, \ldots, a_p$ une base de L et par $b_1, \ldots, b_q$, une base de M. D'autre part, nous supposerons que L et M sont des K-modules *à droite* (le lecteur examinera lui-même le cas des modules à gauche, qui ne diffère du reste pas du cas précédent si K est commutatif).

Soit donc un homomorphisme $f : \mathrm{L} \to \mathrm{M}$. Considérons un vecteur

$$x = a_1\xi_1 + \cdots + a_p\xi_p, \tag{3}$$

dans L, et son image

$$f(x) = y = b_1\eta_1 + \cdots + b_q\eta_q, \tag{4}$$

dans M; on se propose de trouver des formules permettant de *calculer les coordonnées* $\eta_1, \ldots, \eta_q$ *du vecteur* $f(x)$ *par rapport à la base* $b_1, \ldots, b_q$ *de* M *en fonction des coordonnées* $\xi_1, \ldots, \xi_p$ *de* x *par rapport à la base* $a_1, \ldots, a_p$ *de* L.

Pour cela, posons

$$\begin{cases} f(a_1) = c_1 = b_1\alpha_{11} + b_2\alpha_{12} + \cdots + b_q\alpha_{1q} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f(a_p) = c_p = b_1\alpha_{p1} + b_2\alpha_{p2} + \cdots + b_q\alpha_{pq}, \end{cases} \tag{5}$$

en mettant en évidence les coordonnées, par rapport à la base $b_1, \ldots, b_q$, des vecteurs $f(a_1), \ldots, f(a_p)$: ces coordonnées α_{ij} ne dépendent que de f et des deux bases choisies dans L et M. Cela dit, on a

$$\begin{aligned} f(x) &= c_1\xi_1 + \cdots + c_p\xi_p \\ &= (b_1\alpha_{11} + b_2\alpha_{12} + \cdots + b_q\alpha_{1q})\xi_1 \\ &+ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &+ (b_1\alpha_{p1} + b_2\alpha_{p2} + \cdots + b_q\alpha_{pq})\xi_p, \end{aligned}$$

et en effectuant colonne par colonne les additions figurant au dernier membre on obtient les valeurs cherchées pour les coordonnées de $f(x)$, à savoir

$$(6)\qquad \begin{cases} \eta_1 = \alpha_{11}\xi_1 + \alpha_{21}\xi_2 + \cdots + \alpha_{p1}\xi_p \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_q = \alpha_{1q}\xi_1 + \alpha_{2q}\xi_2 + \cdots + \alpha_{pq}\xi_p. \end{cases}$$

Ces formules s'appellent les **équations de f par rapport à la base $(a_i)_{1\leqslant i\leqslant p}$ de L et à la base $(b_j)_{1\leqslant j\leqslant q}$ de M**; on peut les écrire comme suit sous forme condensée :

$$(6\ bis)\qquad \eta_j = \sum_{i=1}^{i=p} \alpha_{ij}\xi_i.$$

Donnons-nous inversement des scalaires $\alpha_{ij} \in K$ $(1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q)$ et définissons une application f de L dans M par les formules (6) : f transforme donc chaque vecteur $x \in L$, de coordonnées $\xi_1, \ldots, \xi_p$ par rapport à la base donnée de L, en le vecteur de M dont les coordonnées $\eta_1, \ldots, \eta_q$ par rapport à la base donnée de M se calculent par les relations (6). Alors f est un *homomorphisme* de L dans M. On a en effet

$$\begin{aligned} f(x) &= b_1\eta_1 + \cdots + b_q\eta_q \\ &= b_1(\alpha_{11}\xi_1 + \cdots + \alpha_{p1}\xi_p) \\ &+ \cdots\cdots\cdots\cdots\cdots \\ &+ b_q(\alpha_{1q}\xi_1 + \cdots + \alpha_{pq}\xi_p) \\ &= c_1\xi_1 + \cdots + c_p\xi_p \end{aligned}$$

où les vecteurs c_i sont donnés par les formules (5), et on voit alors que f est l'homomorphisme dont le Théorème 3 affirme l'existence.

Remarquons enfin que, l'homomorphisme f étant donné, il existe *un seul* système de scalaires α_{ij} tel que f soit donné par les relations (6), car le calcul qu'on vient de faire montre qu'alors les α_{ij} sont nécessairement les coordonnées des vecteurs $f(a_i)$ par rapport à la base $(b_j)_{1\leqslant j\leqslant q}$ de M, ce qui les détermine entièrement.

Revenons maintenant aux formules (6) dont la connaissance permet de définir l'homomorphisme f. Il est clair que pour les retenir, il suffit de connaître le tableau

$$(7)\qquad \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{p1} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1q} & \alpha_{2q} & \cdots & \alpha_{pq} \end{pmatrix}$$

formé par les constantes α_{ij} (qu'on appelle les **coefficients** figurant dans les formules (6)). Un tableau de la forme (7) s'appelle une **matrice à p colonnes et q lignes à coefficients dans l'anneau** K (les α_{ij} s'appellent aussi les **termes** de la matrice en question), et on dit que (7) est la **matrice de l'homomorphisme f par rapport à la base $(a_i)_{1\leqslant i\leqslant p}$ de L et à la base $(b_j)_{1\leqslant j\leqslant q}$ de M**. La notion de matrice joue pour les homomorphismes un rôle analogue à celui que joue, pour les vecteurs, la notion de coordonnées.

Lorsqu'on n'a pas à faire de calculs explicites, on désigne souvent la matrice (7) par la notation condensée

$$(\alpha_{ij})_{1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q}.$$

qui a d'ailleurs le mérite de montrer qu'une matrice n'est autre qu'une *famille* d'éléments de K, famille indexée par l'ensemble de tous les couples (i, j) d'entiers tels que $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$.

Lorsque L = M, autrement dit lorsque f est un *endomorphisme* du module L, on utilise le plus souvent la même base $a_1, \ldots, a_p$ dans L et dans M, ce qui permet alors de parler de la **matrice d'un endomorphisme de L par rapport à une base de L**. La matrice en question a évidemment p lignes et p colonnes; on dit que c'est une **matrice carrée d'ordre p à coefficients dans K.**

Remarque 1. Étant donné un homomorphisme $f : L \to M$ de K-modules libres de type fini, on ne peut pas parler de « la » matrice de f; pour donner un sens à cette notion on doit d'abord choisir une base de L et une base de M, et « la » matrice obtenue dépend évidemment du choix des bases (on verra au § 15 ce qui se passe lorsqu'on change de bases dans L et dans M).

Toutefois, lorsque $L = K^p$ et $M = K^q$, il s'impose de choisir la base *canonique* de L et la base *canonique* de M (§ 11, *Exemple* 12); étant donné un homomorphisme

$$f : K^p \to K^q$$

il est donc légitime dans ce cas de parler de *la* matrice de f (sous-entendu : par rapport à la base canonique de K^p et à la base canonique de K^q); si l'on désigne cette matrice par $(\alpha_{ij})_{1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q}$, alors f n'est autre que l'application transformant chaque vecteur

$$x = (\xi_1, \ldots, \xi_p) \in K^p,$$

en le vecteur

$$f(x) = (\eta_1, \ldots, \eta_q) \in K^q$$

donné par les relations (6) ci-dessus.

En sens inverse, les mêmes constructions permettent d'attacher à chaque matrice $(\alpha_{ij})_{1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q}$ un homomorphisme bien déterminé de K^p dans K^q — à savoir celui dont *la* matrice est la matrice donnée.

Ces considérations montrent donc l'existence d'une bijection « canonique » de l'ensemble de tous les homomorphismes de K^p dans K^q sur l'ensemble de toutes les matrices à p colonnes et q lignes (à coefficients dans K). Nous utiliserons fréquemment cette correspondance, le plus souvent sans y référer explicitement.

Remarque 2. Soient L et M des K-modules à droite libres de type fini, $(a_i)_{1\leqslant i\leqslant p}$ une base de L et $(b_j)_{1\leqslant j\leqslant q}$ une base de M. Introduisons les isomorphismes

$$u : K^p \to L, \qquad v : K^q \to M$$

qui appliquent respectivement les bases canoniques de K^p et K^q sur les bases données de L et M (Corollaire 1 du Théorème 3).

Soit un homomorphisme $f : L \to M$; à l'aide de u et v, on en déduit (Théorème 1) un homomorphisme

$$\overline{f} = v^{-1} \circ f \circ u : K^p \to K^q;$$

cela dit, *la matrice de f par rapport à la base (a_i) de L et à la base (b_j) de M est identique à la matrice de $\overline{f}$* (par rapport aux bases canoniques de K^p et K^q). Considérons en effet les vecteurs

$$x = a_1\xi_1 + \cdots + a_p\xi_p,\ f(x) = b_1\eta_1 + \cdots + b_q\eta_q,$$

les τ_{ij} étant donnés en fonction des ξ_i par les formules (6) ci-dessus. Par construction de u on a

$$x = u(\xi_1, \ldots, \xi_p)$$

et de même

$$f(x) = v(\tau_{11}, \ldots, \tau_{1q});$$

donc

$$(\tau_{11}, \ldots, \tau_{1q}) = v^{-1}[f(x)] = v^{-1}\{f[u(\xi_1, \ldots, \xi_p)]\} = \bar{f}(\xi_1, \ldots, \xi_p);$$

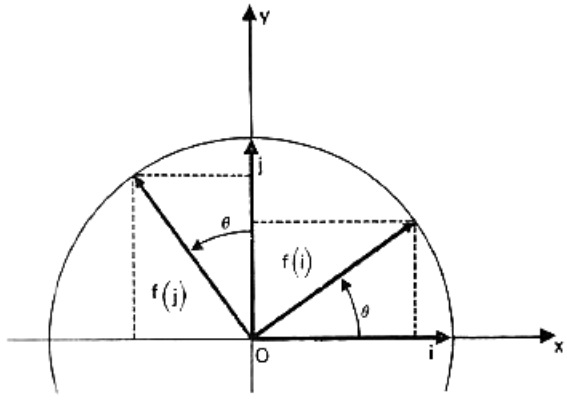
il s'ensuit que les formules (6) sont aussi les équations de $\bar{f}$ (par rapport aux bases canoniques), ce qui établit notre assertion.

On voit donc qu'on aurait encore pu introduire les matrices en montrant tout d'abord que tout homomorphisme de K^p dans K^q est donné par des relations du type (6), puis en observant que si l'on a un homomorphisme $f : L \to M$ de modules libres de type fini, alors le choix d'une base de L et d'une base de M permet d'identifier L à un module K^p, M à un module K^q, et par suite f à un homomorphisme $\bar{f}$ de K^p dans K^q, donc donné par des relations (6), et représenté de façon *canonique* par une matrice. On retrouverait ainsi la possibilité d'attacher une matrice à f une fois choisies des bases de L et M.

4. *Exemples d'homomorphismes et de matrices*

Nous allons indiquer maintenant quelques exemples d'homomorphismes, et de représentation d'un homomorphisme par une matrice.

Exemple 1. Soit L l'espace vectoriel réel formé des vecteurs d'origine donnée O dans le plan usuel, et considérons l'application $f : L \to L$ qui transforme tout vecteur d'origine O en celui qui s'en déduit par la rotation d'angle θ (donné) autour du point O. C'est évidemment une application linéaire (car une rotation transforme un parallélogramme en un parallélogramme, et une rotation de centre O commute à toute homothétie de centre O). Soit Ox, Oy un système de coordonnées *rectangulaires* dans le plan, i et j les vecteurs unité (*) de Ox et Oy; un raisonnement géométrique évident montre que l'on a les relations



$$f(i) = i.\cos\theta + j.\sin\theta$$
$$f(j) = -i.\sin\theta + j.\cos\theta;$$

par suite, la matrice de f par rapport à la base (i, j) de L n'est autre que

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

(*) Le vecteur i n'a évidemment aucun rapport avec le nombre complexe i...

(on n'oubliera pas que les *lignes* de la matrice (7) d'un homomorphisme s'obtiennent en considérant les *colonnes* figurant dans les relations (5), ce qui explique le résultat trouvé ici).

Exemple 2. Prenons L = M et supposons K commutatif; alors, pour tout $\lambda \in K$, l'application $x \to \lambda x$ (**homothétie de rapport** λ dans L) est linéaire. Comme elle transforme une base $a_1, \ldots, a_n$ de L en les vecteurs

$$\lambda.a_1 = \lambda.a_1 + 0.a_2 + \cdots + 0.a_n$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\lambda.a_n = 0.a_1 + 0.a_2 + \cdots + \lambda.a_n,$$

on voit que la matrice de l'homothétie de rapport λ, par rapport à une base quelconque de L, est

$$\begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 \\ 0 & \lambda & 0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix};$$

on dit que c'est une **matrice scalaire** à coefficients dans l'anneau K.

On notera qu'ici la matrice de f est indépendante du choix de la base $a_1, \ldots, a_n$ de L; on peut montrer facilement que les homothéties sont les *seuls* endomorphismes de L à posséder cette propriété.

Exemple 3. On appelle **forme linéaire** ou **covecteur** sur un K-module à droite L tout homomorphisme de L dans le K-module à droite, autrement dit toute application

$$f : L \to K$$

telle que l'on ait

$$f(x\lambda + y\mu) = f(x)\lambda + f(y)\mu \quad \text{quels que soient } \lambda, \mu \in K,\ x, y \in L.$$

Par exemple, le § 11, n° 4 montre que *les fonctions coordonnées de* L *par rapport à une base de* L *sont des formes linéaires sur* L.

Soit f une forme linéaire sur L, et choisissons (si c'est possible) une base $a_1, \ldots, a_p$ de L; pour attacher à f, comme à tout homomorphisme de modules libres de type fini, une matrice, il faut encore choisir une base du K-module à droite K : nous choisirons la base canonique de celui-ci, formée du vecteur (sic) 1. Pour calculer la matrice de f par rapport à ces deux bases, on doit écrire

$$f(a_1) = 1.\alpha_{11}$$
$$\cdots\cdots\cdots\cdots$$
$$f(a_p) = 1.\alpha_{p1};$$

il est clair qu'il est plus simple de poser

$$f(a_1) = \alpha_1$$
$$\cdots\cdots\cdots$$
$$f(a_p) = \alpha_p,$$

et alors f est représentée, par rapport aux bases considérées de L et K, par **la matrice ligne**

$$(\alpha_1, \ldots, \alpha_p);$$

la donnée de cette matrice détermine f grâce à la formule

$$f(a_1\xi_1 + \cdots + a_p\xi_p) = \alpha_1\xi_1 + \cdots + \alpha_p\xi_p;$$

on dit souvent que les α_i sont **les coefficients de f par rapport à la base $(a_i)_{1\leqslant i\leqslant p}$ de L.**

Si en particulier $L = K^p$, il s'impose de choisir la base canonique de L; les α_i s'appellent alors simplement les **coefficients de f** (sous-entendu : par rapport à la base canonique de K^p), et f est donnée par la relation

$$f(\xi_1, \ldots, \xi_p) = \alpha_1\xi_1 + \cdots + \alpha_p\xi_p.$$

Exemple 4. Soit M un K-module à droite, et considérons un homomorphisme

$$f: K \to M$$

de K-modules à droite; posant

$$f(1) = c \in M$$

on a

$$f(\xi) = f(1.\xi) = f(1)\xi = c\xi,$$

de sorte que la connaissance de c détermine entièrement f (dans la pratique on ne fait pas de différence entre l'homomorphisme f et l'élément c de M). Supposons que M admette une base $b_1, \ldots, b_q$; dans K, utilisons la base canonique; posant

$$c = f(1) = b_1\alpha_1 + \cdots + b_q\alpha_q$$

on voit que la matrice de f par rapport aux bases considérées de K et M est la **matrice colonne**

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_q \end{pmatrix}$$

formée avec les composantes du vecteur c par rapport à la base considérée de M.

Il nous arrivera parfois dans la suite d'identifier (une fois choisie une base de M) chaque vecteur de M avec la matrice *colonne* dont les termes sont les coordonnées du vecteur considéré par rapport à la base choisie dans M; ce point de vue sera justifié plus loin (§ 14, n° 4).

Les exemples précédents sont de nature purement algébrique (comme tout ce qui se rapporte aux modules *libres de type fini*). L'Analyse fournit par contre des exemples d'homomorphismes qu'il serait tout à fait artificiel de chercher à représenter par des matrices (même infinies). En voici quelques-uns.

Exemple 5. Soient a et b deux nombres réels tels que $a < b$, notons X l'ensemble des $t \in \mathbf{R}$ tels que $a \leqslant t \leqslant b$ (X n'est autre que l'intervalle $[a, b]$), et désignons par L l'espace vectoriel réel formé par toutes les applications $f: X \to \mathbf{R}$ qui sont continues quel que soit $t \in X$ (cf. § 10, *Exemples* 4 et 7). Soit $N(s, t)$ une fonction à valeurs réelles, définie et continue sur le carré $X \times X$. On peut démontrer (en utilisant le fait que la fonction N est *uniformément* continue sur le carré $X \times X$) que pour toute fonction $f \in L$, la fonction

$$f^*(s) = \int_a^b N(s, t) f(t) dt \qquad (a \leqslant s \leqslant b)$$

est encore continue sur l'intervalle X, autrement dit que $f^* \in L$. Cela fait, l'application $u: f \to f^*$ de L dans L est *linéaire*. Soient en effet $f, g \in L$ et posons $f + g = h$; on a

$$\begin{aligned} h^*(s) &= \int_a^b N(s, t)h(t)dt = \int_a^b N(s, t)[f(t) + g(t)]dt \\ &= \int_a^b N(s, t) f(t)dt + \int_a^b N(s, t)g(t)dt = f^*(s) + g^*(s), \end{aligned}$$

autrement dit $h^* = f^* + g^*$, de sorte qu'on a $u(f + g) = u(f) + u(g)$; on démontrerait de même la relation $u(\lambda f) = \lambda u(f)$ pour tout $\lambda \in \mathbf{R}$.

L'application u de L dans L s'appelle un **opérateur intégral;** l'étude (notamment par Hilbert et F. Riesz) de ces opérateurs a conduit à la création, dans le premier quart du XX^e siècle, de ce qu'on appelle aujourd'hui l'*Analyse Fonctionnelle*. Il va de soi — ce serait trop facile... — que les considérations purement algébriques, et essentiellement triviales, qui sont développées dans cet ouvrage ne sont d'aucun secours sérieux en Analyse Fonctionnelle, sauf pour fournir à celle-ci une terminologie raisonnable et une vague idée des directions dans lesquelles la recherche doit s'effectuer; en fait, les difficultés qu'on rencontre en Analyse Fonctionnelle pour établir des résultats non triviaux sont rarement de nature algébrique; elles sont le plus souvent de nature « analytique » et exigent, pour être surmontées, l'emploi de méthodes « topologiques » (i. e. fondées sur la notion de « continuité »). Il est du reste intéressant de remarquer que le développement de l'Algèbre linéaire élémentaire a été grandement influencé par celui de l'Analyse Fonctionnelle, alors qu'on aurait pu espérer voir plutôt le contraire...

Exemple 6. Prenons le même espace vectoriel réel L que ci-dessus; alors l'application

$$f \mapsto \int_a^b f(t)\,dt = I(f)$$

de L dans $\mathbf{R}$ est une *forme linéaire* sur L : si en effet f et g sont des fonctions continues sur l'intervalle $[a, b]$, l'intégrale de la fonction $f + g$ est la somme des intégrales des fonctions f et g; et si l'on multiplie f par une constante $\lambda \in \mathbf{R}$, son intégrale est aussi multipliée par λ.

Exemple 7. L'anneau de base étant toujours $\mathbf{R}$, considérons les deux espaces vectoriels réels L et M que voici : les éléments de L sont les applications $f: \mathbf{R} \to \mathbf{R}$ admettant une *dérivée seconde continue* f''; et ceux de M sont toutes les applications *continues* $g: \mathbf{R} \to \mathbf{R}$ (on n'impose aucune condition de dérivabilité). Bien entendu, les opérations vectorielles dans L et M sont définies comme au § 10, *Exemple* 4.

Choisissons une fois pour toutes des fonctions $a, b, c \in \mathrm{M}$ (i. e. des fonctions continues d'une variable réelle), et pour toute fonction $f \in \mathrm{L}$ formons la fonction

$$f^*(t) = a(t)f(t) + b(t)f'(t) + c(t)f''(t);$$

évidemment f^* appartient à M, d'où une application $\mathrm{D} : \mathrm{L} \to \mathrm{M}$ donnée par $\mathrm{D}(f) = f^*$ pour tout $f \in \mathrm{L}$. Cela dit, D est un *homomorphisme*. En effet

$$\begin{aligned} \mathrm{D}(f+g) &= a(f+g) + b(f+g)' + c(f+g)'' \\ &= af + bf' + cf'' + ag + bg' + cg'' = \mathrm{D}(f) + \mathrm{D}(g), \end{aligned}$$

et on montrerait de même que $\mathrm{D}(\lambda f) = \lambda \mathrm{D}(f)$.

Les homomorphismes de ce genre interviennent dans la théorie des *équations différentielles linéaires*.

Notons qu'il est aussi facile de construire des formes linéaires sur l'espace vectoriel L; c'est le cas par exemple de l'application

$$f \mapsto f''(0)$$

de L dans **R**, qui à chaque $f \in \mathrm{L}$ associe la valeur pour $t = 0$ de sa dérivée seconde.

§ 13. Addition des homomorphismes et matrices

1. *Les groupes additifs* Hom (L, M)

Soient L et M deux K-modules (à gauche par exemple) sur un anneau quelconque K. On désigne par la notation

$$\mathrm{Hom}\,(\mathrm{L}, \mathrm{M}) \qquad \text{ou} \qquad \mathfrak{L}(\mathrm{L}, \mathrm{M})$$

l'ensemble de toutes les applications linéaires de L dans M; on utilise aussi (lorsqu'il peut y avoir ambiguïté sur l'anneau de base) la notation

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M}) \qquad \text{ou} \qquad \mathfrak{L}_{\mathrm{K}}(\mathrm{L}, \mathrm{M}).$$

THÉORÈME 1. *Soient* L *et* M *deux* K*-modules à gauche. Si*

$$f,\ g : \mathrm{L} \to \mathrm{M}$$

sont des homomorphismes de L *dans* M, *il en est de même de l'application*

$$f + g : \ x \mapsto f(x) + g(x).$$

L'ensemble Hom (L, M), *muni de la loi de composition* $(f, g) \mapsto f + g$, *est un groupe commutatif.*

Posons $h = f + g$; alors

$$\begin{aligned} h(\lambda x + \mu y) &= f(\lambda x + \mu y) + g(\lambda x + \mu y) \\ &= \lambda f(x) + \mu f(y) + \lambda g(x) + \mu g(y) \\ &= \lambda[f(x) + g(x)] + \mu[f(y) + g(y)] \\ &= \lambda h(x) + \mu h(y), \end{aligned}$$

ce qui établit la première assertion de l'énoncé.

Pour établir la seconde, considérons l'ensemble E de *toutes* les applications (linéaires ou non) de L dans M; muni de la loi de composition $(f, g) \mapsto f + g$, c'est un groupe commutatif (§ 10, *Exemple* 4; le fait que L soit un module n'intervient pas, on regarde simplement L comme un ensemble). Il reste donc à faire voir

que Hom (L, M) est un *sous-groupe* de E; or Hom (L, M) contient évidemment l'élément neutre de E (à savoir l'application de L dans M qui prend partout la valeur 0), et si f, g sont des homomorphismes il en est de même de $f - g$, comme le montre la première partie de la démonstration, d'où le résultat cherché.

Le Théorème 1 permet d'appeler Hom (L, M) le **groupe des homomorphismes** de L dans M.

Lorsque l'anneau de base K est *commutatif*, on peut même considérer Hom (L, M) comme un nouveau K-module à gauche. Tout d'abord, reprenons l'ensemble E de toutes les applications (linéaires ou non) de L dans M; le § 10, *Exemple* 4 permet de considérer E non seulement comme un groupe additif, mais comme un K-module à gauche, le produit λf d'un scalaire $\lambda \in K$ et d'une application $f : L \to M$ étant l'application

$$x \mapsto \lambda f(x)$$

de L dans M (et cela ne suppose pas K commutatif). Or il se trouve que, K étant commutatif, l'ensemble Hom (L, M) est non seulement un sous-*groupe* mais un sous-*module* de E, autrement dit que si f est un homomorphisme de L dans M, il en est encore ainsi de $f' = \lambda f$; en effet, on a

$$\begin{aligned} f'(\alpha x + \beta y) &= \lambda f(\alpha x + \beta y) = \lambda\alpha . f(x) + \lambda\beta . f(y) \\ &= \alpha\lambda f(x) + \beta\lambda . f(y) = \alpha f'(x) + \beta f'(y), \end{aligned}$$

comme annoncé. On peut donc bien, dans ce cas, regarder Hom (L, M) comme un K-module à gauche.

Si par exemple L et M sont des espaces vectoriels réels (resp. complexes), alors on peut regarder Hom (L, M) comme un espace vectoriel réel (resp. complexe).

2. *Addition des matrices*

Dans ce qui précède, supposons que L et M soient des K-modules à droite libres de type fini; choisissons une base $(a_i)_{1 \leqslant i \leqslant p}$ de L et une base $(b_j)_{1 \leqslant j \leqslant q}$ de M; enfin, étant donnés deux homomorphismes f et g de L dans M, soient

$$\begin{aligned} A &= (\alpha_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q} \\ B &= (\beta_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q} \end{aligned}$$

leurs matrices par rapport aux bases considérées de L et M. On a donc

$$\begin{aligned} f(a_i) &= b_1\alpha_{i1} + \cdots + b_q\alpha_{iq}, \\ g(a_i) &= b_1\beta_{i1} + \cdots + b_q\beta_{iq}. \end{aligned}$$

Posant $h = f + g$, et désignant la matrice de h par rapport aux bases considérées par

$$C = (\gamma_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q},$$

on a

$$h(a_i) = f(a_i) + g(a_i) = b_1(\alpha_{i1} + \beta_{i1}) + \cdots + b_q(\alpha_{iq} + \beta_{iq}),$$

et par suite les termes de C sont donnés par les relations

$$\gamma_{ij} = \alpha_{ij} + \beta_{ij} \qquad (1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q). \tag{1}$$

Étant données deux matrices $A = (\alpha_{ij})$ et $B = (\beta_{ij})$ à coefficients dans K, on est ainsi conduit à appeler **somme des deux matrices** A et B la matrice $C = (\gamma_{ij})$ donnée par les relations (1); on la désigne par la notation

$$A + B.$$

On notera que la somme de deux matrices n'est définie que si celles-ci ont le même nombre de lignes, et le même nombre de colonnes.

Si l'on identifie une matrice $(\alpha_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q}$ à un élément de K^{pq}, il est clair que l'addition des matrices se réduit à celle des éléments de K^{pq}. Par suite, l'ensemble des matrices à p colonnes et q lignes, muni de la loi de composition $(A, B) \mapsto A + B$, est un *groupe commutatif*.

On a en outre — et pour cause — le résultat suivant :

THÉORÈME 2. *Soient* L *et* M *des* K*-modules libres de type fini, f et g des homomorphismes de* L *dans* M*; soient* A *et* B *les matrices de f et g par rapport à une base (a_i) de* L *et à une base (b_j) de* M. *Alors la matrice de $f + g$ par rapport à ces bases est* $A + B$.

Notons enfin qu'on peut regarder l'ensemble des matrices à p colonnes et q lignes à coefficients dans K non seulement comme un groupe additif, mais même comme un K-module à gauche (ou à droite); il suffit de définir, pour une matrice

$$A = (\alpha_{ij}),$$

les expressions λA et $A\lambda$ par les formules suivantes :

$$\lambda A = (\lambda\alpha_{ij}), \qquad A\lambda = (\alpha_{ij}\lambda).$$

§ 14. — Produits de matrices

1. *L'anneau des endomorphismes d'un module*

Établissons tout d'abord le résultat suivant :

THÉORÈME 1. *Soient* L, M, N *trois modules; étant donnés des homomorphismes*

$$f, g : \mathrm{L} \to \mathrm{M} \qquad et \qquad h : \mathrm{M} \to \mathrm{N},$$

on a la relation

$$h \circ (f + g) = h \circ f + h \circ g;$$

étant donnés des homomorphismes

$$f : \mathrm{L} \to \mathrm{M} \qquad et \qquad g, h : \mathrm{M} \to \mathrm{N},$$

on a la relation

$$(g + h) \circ f = g \circ f + h \circ f.$$

Établissons par exemple le premier résultat. Posant $u = f + g$, on a

$$h \circ u(x) = h[u(x)] = h[f(x) + g(x)] = h[f(x)] + h[g(x)]$$

ce qui montre que l'application $h \circ u$ est somme des applications $h \circ f$ et $h \circ g$, d'où le Théorème.

COROLLAIRE. *Soit* L *un module sur un anneau; l'ensemble* Hom (L, L) *des endomorphismes du module* L, *muni des lois de composition*

$$(f, g) \mapsto f + g, \qquad (f, g) \mapsto f \circ g,$$

est un anneau.

Le fait que Hom (L, L), muni de l'addition, soit un groupe commutatif résulte du § 13, Théorème 1. L'associativité de la multiplication résulte du § 2, Théorème 2, et l'existence d'un élément neutre du fait que l'application identique j_{L} appartient à Hom (L, L). Enfin, le Théorème 1 montre que les conditions de « distributivité » sont satisfaites, ce qui achève la démonstration.

L'ensemble Hom (L, L), muni des deux lois de composition en question, s'appelle **l'anneau des endomorphismes du module** L. Il est en général non commutatif (même si l'anneau de base K est commutatif), comme on le verra plus loin.

2. *Produit de deux matrices*

Soient L, M, N des modules à droite *libres de type fini*, et choisissons des bases $(a_1, \ldots, a_p)$, $(b_1, \ldots, b_q)$ et $(c_1, \ldots, c_r)$ de ces modules. Considérons des homomorphismes

$$f : \mathrm{M} \to \mathrm{N} \qquad et \qquad g : \mathrm{L} \to \mathrm{M}$$

et l'homomorphisme composé

$$h = f \circ g : \mathrm{L} \to \mathrm{N}.$$

Désignons la matrice de f par rapport aux bases (b_j) et (c_k) par

$$\mathrm{A} = (\alpha_{jk})_{1 \leqslant j \leqslant q,\, 1 \leqslant k \leqslant r},$$

celle de g par rapport aux bases (a_i) et (b_j) par

$$\mathrm{B} = (\beta_{ij})_{1 \leqslant i \leqslant p,\, 1 \leqslant j \leqslant q},$$

et celle de h par rapport aux bases (a_i) et (c_k) par

$$\mathrm{C} = (\gamma_{ik})_{1 \leqslant i \leqslant p,\, 1 \leqslant k \leqslant r};$$

on se propose de calculer C en fonction de A et B.

Soit

$$x = a_1\xi_1 + \cdots + a_p\xi_p$$

un élément de L; nous poserons

$$\begin{aligned} g(x) &= y = b_1\eta_1 + \cdots + b_q\eta_q \\ h(x) &= f(y) = c_1\zeta_1 + \cdots + c_r\zeta_r. \end{aligned}$$

Comme on connait les matrices A et B de f et g, les formules (6) du § 12, n° 3 montrent qu'on a

$$\begin{aligned} \zeta_k &= \alpha_{1k}\eta_1 + \cdots + \alpha_{qk}\eta_q \quad (1 \leqslant k \leqslant r) \\ \eta_j &= \beta_{1j}\xi_1 + \cdots + \beta_{pj}\xi_p \quad (1 \leqslant j \leqslant q), \end{aligned}$$

et par suite

$$\begin{aligned} \zeta_k = {} & \alpha_{1k}(\beta_{11}\xi_1 + \cdots + \beta_{p1}\xi_p) \\ & + \alpha_{2k}(\beta_{12}\xi_1 + \cdots + \beta_{p2}\xi_p) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + \alpha_{qk}(\beta_{1q}\xi_1 + \cdots + \beta_{pq}\xi_p); \end{aligned}$$

mais la matrice $\mathrm{C} = (\gamma_{ik})$ de h est aussi donnée par les formules

$$\zeta_k = \gamma_{1k}\xi_1 + \cdots + \gamma_{pk}\xi_p;$$

comparant les résultats obtenus on trouve donc les relations

$$\gamma_{1k} = \alpha_{1k}\beta_{11} + \alpha_{2k}\beta_{12} + \cdots + \alpha_{qk}\beta_{1q}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\gamma_{pk} = \alpha_{1k}\beta_{p1} + \alpha_{2k}\beta_{p2} + \cdots + \alpha_{qk}\beta_{pq}$$

ou, sous une forme plus condensée,

$$(1) \qquad \gamma_{ik} = \alpha_{1k}\beta_{i1} + \cdots + \alpha_{qk}\beta_{iq} = \sum_{j=1}^{j=q} \alpha_{jk}\beta_{ij}.$$

Ce résultat nous conduit à introduire la définition suivante : étant données des matrices

$$A = (\alpha_{jk})_{1\leqslant j\leqslant q,\ 1\leqslant k\leqslant r} \quad B = (\beta_{ij})_{1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q}$$

à coefficients dans l'anneau K, on appelle **produit de A et B** la matrice

$$AB = (\gamma_{ik})_{1\leqslant i\leqslant p,\ 1\leqslant k\leqslant r}$$

dont les coefficients sont donnés par les relations (1).

On notera que le produit AB n'est défini que si le nombre de *colonnes* de A est égal au nombre de *lignes* de B; et alors la matrice AB a autant de lignes que A, et autant de colonnes que B.

Il est clair qu'avec la définition précédente nous pouvons énoncer le résultat suivant :

Théorème 2. *Soient* L, M, N *des* K*-modules à droite libres de type fini,* (a_i), (b_j), (c_k) *des bases de* L, M, N *et* $f : M \to N$ *et* $g : L \to M$ *des homomorphismes. Soient* A *la matrice de* f *par rapport aux bases* (b_j) *et* (c_k), *et* B *celle de* g *par rapport aux bases* (a_i) *et* (b_j).

Alors la matrice de $f \circ g$ *par rapport aux bases* (a_i) *et* (c_k) *est* AB.

Donnons maintenant quelques exemples de multiplication de matrices.

Exemple 1. Prenons

$$A = (\alpha_1 \ \ldots \ \alpha_q), \qquad B = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_q \end{pmatrix};$$

le produit AB est défini et est une matrice à une ligne et une colonne, donc de la forme (γ) où γ est un scalaire; la relation (1) donne évidemment

$$\gamma = \alpha_1\beta_1 + \cdots + \alpha_q\beta_q,$$

et on dit, pour des raisons évidentes, que le scalaire γ est le produit de la « ligne » A par la « colonne » B.

Ce résultat permet de retenir facilement la règle générale de multiplication des matrices. En effet la formule (1), avec les conventions qu'on vient d'introduire, s'écrit encore

$$\gamma_{ik} = (\alpha_{1k} \ \ldots \ \alpha_{qk}) \cdot \begin{pmatrix} \beta_{i1} \\ \vdots \\ \beta_{iq} \end{pmatrix};$$

autrement dit, *les termes situés sur la* k^e *ligne de* AB *s'obtiennent en multipliant la* k^e *ligne de* A *par les colonnes de* B. C'est cette règle qu'on utilise toujours dans la pratique.

Exemple 2. La multiplication des matrices carrées d'ordre 2 est définie par la formule

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a'a'' + b'c'' & a'b'' + b'd'' \\ c'a'' + d'c'' & c'b'' + d'd'' \end{pmatrix}.$$

Par exemple, si x et y sont des nombres réels, on a

$$\begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix}\begin{pmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{pmatrix} = \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix};$$

compte-tenu du § 12, *Exemple* 1, ce résultat exprime qu'en composant, dans le plan, les rotations d'angles x et y autour d'un point 0, on trouve la rotation d'angle $x + y$ autour de 0.

Exemple 3. Pour tout anneau K et tout entier $n \geqslant 1$, considérons la matrice

$$1_n = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

à n lignes et n colonnes; on l'appelle la **matrice unité d'ordre** n. Cette terminologie est justifiée par le fait que, quelles que soient les matrices X et Y à coefficients dans K, les relations

$$1_n . X = X, \qquad Y . 1_n = Y$$

sont vraies (pourvu qu'elles aient un sens, i.e. si X a n lignes, et si Y a n colonnes) Ces relations s'obtiennent facilement sur les formules (1), et s'interprètent géométriquement comme suit. Soit L un K-module à droite libre de type fini, possédant une base $(a_i)_{1\leqslant i\leqslant n}$ formée de n vecteurs (on peut prendre par exemple $L = K^n$ et la base canonique); alors l'endomorphisme $j : L \to L$ ayant 1_n pour matrice par rapport à la base (a_i) n'est autre que l'*application identique* de L dans L, comme le montrent les formules (6) du § 12, n° 3 et le fait qu'ici on a

$$\alpha_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

Cela dit, pour établir par exemple la relation $1_n . X = X$, on introduit un second module M, une base (b_j) de M, et l'homomorphisme $f : M \to L$ ayant X pour matrice par rapport aux bases considérées de L et M; le Théorème 1 montre que $1_n . X$ est la matrice, par rapport à ces bases, de l'homomorphisme $j \circ f$; mais comme $j = j_L$ on a $j \circ f = f$, d'où la relation cherchée.

3. *Anneaux de matrices*

Les opérations d'addition et de multiplication des matrices, que nous avons définies dans ce § et le précédent, obéissent, dans la mesure où elles ont un sens, aux règles

de calcul usuelles. On le sait déjà pour l'addition (§ 13, n° 2). En ce qui concerne la multiplication, on a la relation d'*associativité*

$$A(BC) = (AB)C$$

toutes les fois que les deux membres sont définis; pour le voir, on introduit les homomorphismes

$$f : K^r \to K^s, \qquad g : K^q \to K^r, \qquad h : K^p \to K^q$$

dont les matrices (par rapport aux bases canoniques) sont A, B, C; alors, d'après le Théorème 2, la matrice A(BC) représente $f \circ (g \circ h)$, tandis que (AB)C représente $(f \circ g) \circ h$, d'où le résultat annoncé.

Enfin, on a les relations de *distributivité*

$$A(B + C) = AB + AC, \qquad (A + B)C = AC + BC,$$

qu'on démontre, comme la formule d'associativité, en remplaçant A, B, C par des homomorphismes de modules et en appliquant le Théorème 1.

En particulier, pour tout entier $n \geqslant 1$ et tout anneau K, désignons par la notation

$$M_n(K)$$

l'ensemble des matrices carrées d'ordre n (i.e. à n lignes et n colonnes) à coefficients dans K; on a sur cet ensemble deux lois de composition

$$(A, B) \mapsto A + B, \qquad (A, B) \mapsto AB;$$

cela dit, $M_n(K)$, muni de ces deux lois de composition, est un *anneau*. On sait en effet déjà que, relativement à l'addition, $M_n(K)$ est un groupe commutatif; d'autre part, on vient de démontrer que la multiplication est associative, et il est clair (*Exemple* 3 ci-dessus) qu'elle admet un élément neutre, à savoir 1_n; enfin, les formules précédentes montrent que, dans $M_n(K)$, la multiplication est distributive par rapport à l'addition.

On dit que $M_n(K)$ est l'**anneau des matrices d'ordre** n **à coefficients dans** K. Il est évidemment isomorphe à l'anneau des endomorphismes du K-module à droite K^n (ou de tout module admettant une base de n vecteurs).

Même lorsque K *est commutatif, l'anneau* $M_n(K)$ *n'est jamais commutatif si* $n \geqslant 2$; pour $n = 2$, il suffit pour le voir d'observer que

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & xy \\ 0 & 1 \end{pmatrix}$$

tandis que

$$\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix};$$

si l'anneau $M_2(K)$ était commutatif on aurait donc $xy = y$ quels que soient $x, y \in K$, ce qui a peu de chances de se produire si K possède au moins deux éléments...

Ce sont naturellement les anneaux $M_n(K)$ qui, historiquement, ont fourni les premiers exemples d'anneaux non commutatifs.

Comme dans tout anneau, on dit que deux matrices X et Y carrées d'ordre n **commutent** ou sont **permutables** lorsqu'on a

$$XY = YX.$$

Exemple 4. Prenons pour X une **matrice diagonale**, i.e. de la forme

$$X = \begin{pmatrix} x_1 & 0 & 0 & \dots & 0 \\ 0 & x_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & x_n \end{pmatrix}$$

et cherchons à quelle condition une matrice $Y = (y_{ij})_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n}$ commute à X; un calcul simple montre que

$$XY = (x_i y_{ij}), \qquad YX = (y_{ij} x_j);$$

il est donc nécessaire et suffisant que l'on ait

$$x_i y_{ij} = y_{ij} x_j \quad \text{pour} \quad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n.$$

Supposons que K soit un *anneau d'intégrité commutatif* et que les termes x_i de X soient *deux à deux distincts*; la condition précédente, qui s'écrit

$$(x_i - x_j)\, y_{ij} = 0$$

vu la commutativité de K, montre, puisque K est intègre et que $x_i \neq x_j$ pour $i \neq j$, que l'on doit avoir $y_{ij} = 0$ pour $i \neq j$, autrement dit que Y doit être une *matrice diagonale*; cette condition est du reste suffisante attendu que deux matrices diagonales, à coefficients dans un anneau commutatif K, commutent toujours comme le montre le calcul précédent.

4. *Écriture matricielle des homomorphismes*

Soient L et M des K-modules à droite libres de type fini, et f un homomorphisme de L dans M. Choisissons une base $(a_i)_{1 \leqslant i \leqslant p}$ de L et une base $(b_j)_{1 \leqslant j \leqslant q}$ de M, et soit

$$A = (\alpha_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q}$$

la matrice de f par rapport aux basses considérées. Étant donné un vecteur

$$x = a_1 \xi_1 + \dots + a_p \xi_p,$$

le vecteur

$$f(x) = b_1 \eta_1 + \dots + b_q \eta_q$$

est donnée par

$$\begin{aligned} \eta_1 &= \alpha_{11} \xi_1 + \dots + \alpha_{p1} \xi_p \\ &\dots\dots\dots\dots\dots\dots \\ \eta_q &= \alpha_{1q} \xi_1 + \dots + \alpha_{pq} \xi_p : \end{aligned}$$

or ces formules signifient visiblement qu'on a la relation

$$\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{p1} \\ \cdots & \cdots & \cdots \\ \alpha_{1q} & \cdots & \alpha_{pq} \end{pmatrix} \cdot \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_p \end{pmatrix} = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_q \end{pmatrix}.$$

Autrement dit, *si l'on identifie chaque* $x \in \mathrm{L}$ *à la matrice colonne formée avec ses coordonnées par rapport à la base* (a_i) *de* L, *et chaque* $y \in \mathrm{M}$ *à la matrice colonne formée avec ses coordonnées par rapport à la base* (b_j) *de* M, *la relation*

$$y = f(x)$$

entre les vecteurs x *et* y *est équivalente à la relation*

$$y = \mathrm{A}x$$

entre les matrices x *et* y. Ce résultat permet de calculer de façon quasi mécanique avec les homomorphismes de modules libres de type fini.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

1. On considère les matrices (à coefficients dans C)

$$I_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$
$$I_4 = \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \quad I_5 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad I_6 = \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix},$$

Établir les quinze relations suivantes :

$$\begin{array}{lll} [I_1, I_3] = 2I_3, & [I_1, I_4] = 2I_4, & [I_2, I_3] = 2I_4 \\ [I_1, I_5] = -2I_5, & [I_1, I_6] = -2I_6, & [I_2, I_5] = -2I_6 \\ [I_3, I_5] = I_1, & [I_3, I_6] = I_2, & [I_4, I_5] = I_2 \\ [I_2, I_4] = -2I_3, & [I_2, I_6] = 2I_5, & [I_4, I_6] = -I_1 \\ [I_1, I_2] = 0, & [I_3, I_4] = 0, & [I_5, I_6] = 0, \end{array}$$

où l'on pose d'une façon générale

$$[X, Y] = XY - YX.$$

Trouver toutes les matrices carrées d'ordre 2 qui commutent aux six matrices $I_1, \ldots, I_6$.

2. Établir les formules de l'*Exercice* précédent pour les matrices

$$I_1 = 2\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad I_2 = 2\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$I_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad I_5 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad I_6 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

3. Trouver toutes les matrices carrées d'ordre 3 commutant à la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 1 & 2 \end{pmatrix}$$

(on prendra comme anneau de base soit le corps **C**, soit un corps commutatif quelconque, soit un anneau arbitraire — au choix...).

4. Soit K un anneau commutatif. Montrer que l'application de $M_2(K)$ dans $M_4(K)$ qui transforme chaque matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en la matrice

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix}$$

est un isomorphisme de l'anneau $M_2(K)$ sur un sous-anneau de $M_4(K)$. Interprétation en termes de modules?

5. Calculer le produit des trois matrices

$$\begin{pmatrix} 0 & 2 & -1 \\ -2 & -1 & 2 \\ 3 & -2 & -1 \end{pmatrix}, \quad \begin{pmatrix} 70 & 34 & -107 \\ 52 & 26 & -68 \\ 101 & 50 & -140 \end{pmatrix}, \quad \begin{pmatrix} 27 & -18 & 10 \\ -46 & 31 & -17 \\ 3 & 2 & 1 \end{pmatrix}.$$

Effectuer le même calcul en prenant pour anneau de base l'anneau $\mathbf{Z}/7\mathbf{Z}$ des entiers modulo 7.

6. Calculer le cube de la matrice carrée d'ordre n

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

7. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2 à coefficients dans un anneau commutatif quelconque. Montrer qu'on a la relation

$$A^2 - (a+d)A + (ad - bc)1_2 = 0.$$

8. Étant donnée une matrice carrée

$$A = (\alpha_{ij})_{1 \leqslant i,j \leqslant n}$$

à coefficients dans un anneau *commutatif* K, on appelle **trace** de A le scalaire

$$\mathrm{Tr}(A) = \alpha_{11} + \alpha_{22} + \dots + \alpha_{nn},$$

somme des éléments diagonaux de A. Montrer qu'on a

$$\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B), \qquad \mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

quelles que soient les matrices A et B.
On suppose $K = \mathbf{C}$. Déduire de ce qui précède qu'il est impossible de trouver des matrices carrées X et Y d'ordre n telles que

$$XY - YX = 1_n.$$

9. Soient K un anneau commutatif et d un élément de K. Montrer que les matrices

$$\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

(où x et y sont des éléments arbitraires de K) forment un sous-anneau L de $M_2(K)$, et que L est isomorphe à l'anneau $K[\sqrt{d}]$ du § 9. Cas où $K = \mathbf{R}$, $d = -1$?

10. On dit qu'une matrice carrée X d'ordre n à coefficients dans un anneau K est **nilpotente** s'il existe un entier $r \geqslant 1$ tel que $X^r = 0$, et **unipotente** si la matrice $1_n - X$ est nilpotente. On suppose $K = \mathbf{C}$ dans ce qui suit. Étant données une matrice carrée nilpotente N, et une matrice carrée unipotente U, on pose (cf. § 8, *Exercice* 2)

$$\exp(N) = 1 + \frac{N}{1!} + \frac{N^2}{2!} + \dots \frac{N^k}{k!} + \dots,$$

$$\log(U) = -\frac{1-U}{1} - \frac{(1-U)^2}{2} - \dots - \frac{(1-U)^k}{k} - \dots.$$

On prend

$$N = \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix};$$

vérifier que N est nilpotente, que U est unipotente, et qu'on a les relations

$$\exp(\log(U)) = U, \qquad \log(\exp(N)) = N$$

[on calculera effectivement les matrices $\exp(\log(U))$ et $\log(\exp(N))$, sans utiliser le résultat général de l'*Exercice* 2 du § 8].

11. Pour tout nombre complexe t, on pose

$$U(t) = \begin{pmatrix} 1 & t & 2t + 2t^2 & 3t + \frac{17}{2}t^2 + 4t^3 \\ 0 & 1 & 4t & 5t + 12t^3 + 3t^4 \\ 0 & 0 & 1 & 6t \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

montrer qu'on a

$$U(s)\,U(t) = U(s+t)$$

quels que soient $s, t \in \mathbf{C}$ et que $U(t) = \exp(tN)$ où N est une matrice nilpotente qu'on calculera.

¶ **12.** Soit z un nombre algébrique, i.e. (§ 11, *Exemple* 11) un nombre complexe racine d'une équation algébrique à coefficients rationnels non tous nuls.

a) Montrer qu'il existe un entier $n \geqslant 1$ et des nombres rationnels $a_0, \dots, a_{n-1}$ tels que l'on ait une relation de la forme

$$z^n = a_0 + a_1 z + \dots + a_{n-1} z^{n-1}.$$

b) Soit K le sous-anneau de **C** engendré par **Q** et z; montrer que K, considéré comme espace vectoriel sur **Q**, est engendré par les éléments $1, z, \dots, z^{n-1}$.

c) On suppose n minimum dans ce qui précède. Montrer qu'alors $1, z, \dots, z^{n-1}$ forment une base de K regardé comme espace vectoriel sur **Q**.

d) Soit f l'application de K dans K donnée par

$$f(u) = zu \qquad \text{pour tout } u \in K.$$

Montrer que c'est un endomorphisme de K regardé comme espace vectoriel sur **Q**. Calculer la matrice de f par rapport à la base de K définie dans la question *c*).

¶ **13.** Soient L et M deux modules à gauche sur un anneau K ; on suppose donnés un sous-module L′ de L et un homomorphisme f de L dans M. Prouver que les deux conditions suivantes sont équivalentes : *a*) L′ est contenu dans le noyau de f, i.e. on a $f(x) = 0$ pour tout $x \in L'$; *b*) f est composé de l'application canonique de L sur le module quotient L/L′ (§ 10, *Exercice* 10) et d'un homomorphisme de L/L′ dans M.

14. Soient K un anneau, L, M et N trois K-modules à gauche, f un homomorphisme de L dans M, et p un homomorphisme de L dans N ; on suppose p surjectif. Montrer que les deux conditions suivantes sont équivalentes : *a*) on a $\mathrm{Ker}(f) \supset \mathrm{Ker}(p)$; *b*) f est composé de p et d'un homomorphisme de N dans M.

15. Soient L l'espace vectoriel réel formé des vecteurs d'origine donnée O dans l'espace usuel, et L′ le sous-espace vectoriel de L formé des vecteurs portés par une droite donnée (resp. un plan donné) passant par O. Pour tout $x \in L$, on note $f(x)$ le vecteur projection orthogonale de x sur L′. Montrer que l'application f de L dans L′ est linéaire. Quel est son noyau ?

¶¶ **16.** Soit K un anneau. On dit qu'un K-module à gauche M est **simple** ou **irréductible** s'il n'est pas réduit à 0 et si les seuls sous-modules de M sont $\{0\}$ et M tout entier.

a) Pour que M, supposé non nul, soit simple, il faut et il suffit que, quels que soient a, $b \in M$ avec $a \neq 0$, il existe un $\lambda \in K$ tel que $b = \lambda a$. En déduire que, si K est un *corps*, tout K-module simple est isomorphe à K.

b) Soit M un K-module simple. On choisit dans M un élément $a \neq 0$, et on note I l'ensemble des $\lambda \in K$ tels que $\lambda a = 0$. Montrer que I est un idéal à gauche *maximal* de K (§ 8, *Exercice* 7). Montrer que l'application $\lambda \to \lambda a$ de K dans M est composée de l'application canonique de K sur K/I, et d'un isomorphisme du K-module à gauche K/I sur M.
Montrer inversement que, pour tout idéal à gauche maximal I de K, le K-module à gauche K/I est simple.

c) Soient L et M deux K-modules à gauche simples, et f un homomorphisme de L dans M. Montrer que, si f n'est pas nul, c'est un isomorphisme de L sur M (lemme de Schur). (On examinera le noyau et l'image de f.)

d) Soit L un K-module à gauche simple. Montrer que l'anneau des endomorphismes de L est un *corps* (en général non commutatif).