Modules sur un anneau

La notion de module sur un anneau fournit un cadre général et abstrait permettant de traiter les aspects purement algébriques des problèmes « linéaires » qu'on rencontre dans toutes les branches des Mathématiques : théorie des nombres, algèbre linéaire classique, calcul tensoriel, formes différentielles, équations aux dérivées partielles, équations intégrales, géométrie algébrique, fonctions analytiques, topologie algébrique, etc...

Certains résultats de la théorie des modules sur un anneau K ne sont valables que moyennant certaines hypothèses concernant l'anneau K : par exemple, la théorie de la « dimension » suppose que K est un corps.

Par contre, les résultats les plus simples sont valables pour *tout* anneau K; ce sont ces résultats qu'on trouvera dans ce chapitre (§§ 10 à 17). Le lecteur qui trouverait trop général et abstrait le point de vue adopté ici, et qui préférerait supposer que l'anneau de base K, est, par exemple, le corps **R** des nombres réels, ne parviendrait pas à simplifier de façon très substantielle les §§ en question : en faisant l'hypothèse que $K = \mathbf{R}$, on pourra négliger les *Exemples* 5, 6, 9, 10 et le n° 4 du § 10, les *Exemples* 4, 5, 6, 11 du § 11, la *Remarque* 4 du § 16, et l'*Exemple* 2 du § 17, tout le reste demeurant sans aucun autre changement que le remplacement de la lettre K par la lettre **R**.

§ 10. Modules et espaces vectoriels

1. Définition des modules sur un anneau

Soit K un anneau; on appelle **module à gauche sur l'anneau K**, ou encore **K-module à gauche**, l'objet formé par un ensemble M, une loi de composition sur M, notée

$$(x, y) \mapsto x + y,$$

et une application de l'ensemble $K \times M$ dans M, notée

$$(\lambda, x) \mapsto \lambda x,$$

ces données étant assujetties à vérifier les deux conditions que voici :

(M 1) : *L'ensemble* M *muni de la loi de composition* $(x, y) \mapsto x + y$ *est un groupe commutatif;*

(M 2) : *on a les relations*

$$\lambda(\mu x) = (\lambda\mu)x; \qquad 1x = x;$$
$$(\lambda + \mu)x = \lambda x + \mu x; \qquad \lambda(x + y) = \lambda x + \lambda y$$

quels que soient $x, y \in M$ *et* $\lambda, \mu \in K$.

Dans la théorie des modules, l'anneau K est fixé une fois pour toutes, et s'appelle généralement **l'anneau de base**; ses éléments prennent alors le nom de **scalaires** (et on les désignera le plus souvent par des lettres grecques); les éléments des K-modules s'appellent au contraire des **vecteurs** (et on les désigne le plus souvent par des lettres latines, que de nombreuses personnes croient devoir surmonter d'une flèche, ce que l'immense majorité des mathématiciens a cessé de faire depuis longtemps). Mais la distinction entre « scalaires » et « vecteurs » n'a aucun sens mathématique précis (l'*Exemple* 1 ci-dessous montre en effet que les « scalaires » sont des « vecteurs » particuliers...), et son but est plutôt d'aider le lecteur à évoquer des images géométriques familières.

Lorsque l'anneau K est un *corps*, on dit **espace vectoriel à gauche sur** K au lieu de K-module à gauche. En particulier, un espace vectoriel sur le corps **R** des nombres réels s'appelle un **espace vectoriel réel**, et un espace vectoriel sur le corps **C** des nombres

complexes un **espace vectoriel complexe**; ces deux notions sont de loin les plus importantes en Analyse et en Physique; par contre, les espaces vectoriels sur des corps arbitraires, et les modules sur l'anneau **Z** (cf. *Exemple* 5 ci-dessous) ou sur un « anneau de polynômes », jouent dans beaucoup de branches des Mathématiques un rôle beaucoup plus important que les espaces vectoriels réels ou complexes. Mais même en Physique théorique on utilise des modules sur des anneaux qui ne sont pas des corps, et ne sont pas commutatifs (représentations linéaires du groupe de Lorentz, spineurs, etc...), bien que les physiciens n'utilisent pas encore le *langage* de la théorie des modules.

Notons que les identités figurant dans l'axiome (M 2) des modules impliquent les relations

$$\lambda 0 = 0 \quad \text{pour tout} \quad \lambda \in K, \qquad 0x = 0 \quad \text{pour tout} \quad x \in M$$

(dans ces relations le symbole 0 désigne tantôt l'élément nul de K, tantôt l'élément nul du groupe additif M; le lecteur trouvera facilement l'interprétation à choisir pour que les relations écrites aient un sens...). Pour établir la première, on observe que $\lambda 0 + \lambda x = \lambda(0 + x) = \lambda x$ pour tout $x \in M$; il vient donc $\lambda 0 = \lambda x - \lambda x = 0$ comme annoncé. La seconde relation résulte du fait que $0x + 1x = (0 + 1)x = 1x$, d'où $0x = x - x = 0$.

Nous utiliserons bien entendu sans référence les identités que nous venons de prouver, ainsi que celles qui figurent dans l'axiome (M 2) des modules.

Notons enfin qu'on définit la notion de **K-module à droite** comme suit : on appelle ainsi l'objet formé par un groupe additif M et par une application, notée

$$(x, \lambda) \mapsto x\lambda,$$

de $M \times K$ dans M, qui vérifie les conditions exprimées par les identités suivantes :

$$(x\lambda)\mu = x(\lambda\mu); \qquad x1 = x;$$
$$x(\lambda + \mu) = x\lambda + x\mu; \qquad (x + y)\lambda = x\lambda + y\lambda.$$

On peut montrer facilement (n° 4) que les K-modules *à droite* ne sont autres que les modules *à gauche* sur un anneau déduit de K par un procédé très simple (et du reste identique à K si K est commutatif, de sorte que la distinction entre les deux notions n'a d'intérêt que pour les anneaux non commutatifs). Il nous arrivera d'utiliser tantôt le langage des modules à gauche, tantôt celui des modules à droite; il va de soi qu'on peut passer de l'un à l'autre par des traductions triviales.

Nous allons maintenant donner quelques exemples importants de modules et d'espaces vectoriels.

2. Exemples de modules

Exemple 1. Pour tout anneau K et tout entier $n \geqslant 1$, on peut considérer l'ensemble

$$K^n = K \times \cdots \times K \quad (n \text{ facteurs})$$

comme un K-module à gauche, en posant, par définition,

$$(\xi_1, \ldots, \xi_n) + (\eta_1, \ldots, \eta_n) = (\xi_1 + \eta_1, \ldots, \xi_n + \eta_n)$$
$$\lambda.(\xi_1, \ldots, \xi_n) = (\lambda\xi_1, \ldots, \lambda\xi_n);$$

le fait que l'axiome (M 1) soit vérifié résulte du § 7, n° 2 (produit direct de groupes), et le lecteur vérifiera facilement, en utilisant les axiomes des anneaux, les identités figurant dans l'axiome (M 2) des modules.

Par la suite, quand nous parlerons de K^n comme d'un K-module à gauche, ce sera toujours du module ci-dessus qu'il s'agira.

Pour $n = 1$, la construction précédente permet de regarder K lui-même comme un K-module à gauche (ce qui montre que les « scalaires » sont aussi des « vecteurs »...).

On peut naturellement regarder aussi K^n comme un K-module *à droite*; il suffit pour cela de définir l'addition dans K^n comme ci-dessus, et de poser

$$(\xi_1, \ldots, \xi_n).\lambda = (\xi_1\lambda, \ldots, \xi_n\lambda).$$

C'est le K-module *à droite* K^n qui intervient naturellement dans la théorie des équations linéaires comme on le verra (mais il est clair, encore une fois, que la distinction est sans intérêt si K est commutatif !).

Exemple 2. Prenons $K = \mathbf{R}$, corps des nombres réels, et pour M l'ensemble des vecteurs usuels d'origine donnée O dans l'espace usuel; définissons la somme de deux vecteurs par la règle du parallélogramme, et le produit d'un vecteur x d'origine O et d'un nombre réel λ comme le vecteur obtenu en soumettant x à l'homothétie de centre O et de rapport λ; on obtient alors un espace vectoriel réel.

Bien entendu, on devrait prouver ici que les axiomes (M 1) et (M 2) sont vérifiés, ce qui ne peut se faire que dans le cadre de la Géométrie Élémentaire (et pour cause, puisque nous n'avons donné ici aucune définition mathématique rigoureuse de la notion usuelle de « vecteur »).

Cet Exemple est évidemment l'un de ceux qui ont donné naissance à la notion générale d'espace vectoriel ou de module, et explique l'emploi du mot « vecteur » pour désigner les éléments d'un module.

Exemple 3. Dans le plan rapporté à deux axes de coordonnées Ox et Oy, considérons l'ensemble M des vecteurs d'origine O dont les composantes dans le système de coordonnées considéré sont des nombres *rationnels*; il est clair que si $x, y \in M$ on a aussi $x + y \in M$, et que si $x \in M$ et $\lambda \in \mathbf{Q}$ on a aussi $\lambda x \in M$. Ceci permet de regarder M comme un espace vectoriel sur le corps $\mathbf{Q}$ des nombres rationnels.

Exemple 4. Soient K un anneau, M un K-module à gauche (par exemple K lui-même), et X un ensemble quelconque. Désignons par E l'ensemble de toutes les applications

$$f : X \to M;$$

on va en faire un K-module à gauche. Pour cela on doit définir la somme $f + g$ de deux applications de X dans M : ce sera la fonction $f(x) + g(x)$, dont la valeur en chaque $x \in X$ s'obtient en additionnant (dans M) les valeurs de f et g en x; on doit aussi définir le produit λf d'un scalaire $\lambda \in K$ et d'une

application f de X dans M : ce sera la fonction $\lambda f(x)$, dont la valeur en chaque $x \in X$ s'obtient en multipliant par λ la valeur de f en x.

On laisse au lecteur, à titre d'exercice, le soin de vérifier en détail les conditions (M 1) et (M 2) figurant dans la définition des modules.

On notera que si $M = K$ et si l'on prend $X = \{1, 2, \ldots, n\}$, une application f de X dans M n'est autre qu'une suite $(\xi_1, \ldots, \xi_n)$ d'éléments de K — à savoir $\xi_1 = f(1), \ldots, \xi_n = f(n)$; on retrouve alors le module K^n de l'*Exemple* 1.

Exemple 5. Montrons que *tout groupe commutatif* G *peut être regardé comme un* **Z***-module à gauche*. Pour cela, on écrit G additivement, ce qui permet déjà de définir la somme de deux éléments de G — et l'axiome (M 1) est alors trivialement vérifié. Il reste à définir le produit nx d'un $n \in \mathbf{Z}$ et d'un $x \in G$, ce qu'on fait comme au § 7, i.e. en posant

$$nx = \begin{cases} x + \cdots + x \ (n \text{ facteurs}) & \text{si } n \geqslant 1 \\ 0 & \text{si } n = 0 \\ (-n)\,(-x) & \text{si } n \leqslant -1. \end{cases}$$

L'axiome (M 2) se réduit alors aux règles de calcul établies dans l'*Exemple* 9 et la *Remarque* 1 du § 7.

Si le groupe G était écrit multiplicativement, il faudrait bien entendu définir la « somme » de deux éléments x et y de G comme étant xy, et le « produit » d'un $x \in G$ par un entier rationnel n comme étant x^n; il n'y a aucune différence avec ce qui précède, si ce n'est dans les *notations* adoptées.

Enfin, on peut facilement vérifier que *tout* **Z**-module s'obtient, par le procédé ci-dessus, à partir d'un groupe additif.

Cet Exemple montre que *la théorie des modules contient, entre autres, celle des groupes commutatifs*, ce qui n'est pas le cas de la théorie des espaces vectoriels (et encore moins si possible de celle des espaces vectoriels réels).

Exemple 6. Soit K un sous-anneau d'un anneau L; on peut alors regarder L comme un K-module à gauche, en définissant les opérations fondamentales des modules à l'aide de l'addition et de la multiplication données sur L. Autrement dit, si l'on considère deux éléments x et y de L, leur somme en tant que « vecteurs » sera simplement leur somme en tant qu'éléments de l'anneau L; et pour $\lambda \in K$ et $x \in L$, le produit du « scalaire » λ et du « vecteur » x sera le produit, dans l'anneau L, de λ par x. L'axiome (M 1) est ici vérifié parce que l'anneau L devient un groupe commutatif si l'on fait abstraction de son opération de multiplication; et quant à (M 2), il se déduit évidemment des règles d'associativité et de distributivité dans l'anneau L.

Par exemple, on peut regarder le corps $\mathbf{R}$ comme un espace vectoriel sur $\mathbf{Q}$, et le corps $\mathbf{C}$ comme un espace vectoriel sur $\mathbf{R}$, ou sur $\mathbf{Q}$.

Exemple 7. Prenons $K = \mathbf{R}$ et formons l'ensemble M de toutes les applications

$$f : \mathbf{R} \to \mathbf{R}$$

(fonctions réelles d'une variable réelle) qui sont continues partout. On démontre en Analyse que si f et g sont deux telles fonctions, la fonction $f + g$ est elle aussi partout continue, donc appartient à M; et que si $f \in M$, alors $\lambda f \in M$ pour tout scalaire $\lambda \in \mathbf{R}$ (les fonctions $f + g$ et λf sont définies comme dans l'*Exemple* 4 ci-dessus). Il est immédiat de voir que le triplet formé par

l'ensemble M, l'application $(f, g) \mapsto f + g$ de $M \times M$ dans M, et l'application $(\lambda, f) \mapsto \lambda f$ de $\mathbf{R} \times M$ dans M, est un espace vectoriel réel.

Cet Exemple (qui est à l'origine de l'introduction des espaces vectoriels en Analyse) est susceptible de nombreuses variantes; au lieu d'imposer aux fonctions f considérées d'être partout continues, on peut exiger qu'elles soient continues en un point donné, ou dérivables en un point donné, ou qu'elles admettent partout une dérivée seconde continue, etc...

3. *Sous-modules, sous-espaces vectoriels*

Soit M un module à gauche sur un anneau K. On appelle **sous-module de M** toute partie M′ de M vérifiant les deux conditions que voici :

(i) : M′ *est un sous-groupe du groupe additif* M;

(ii) : *les relations* $x \in M'$ *et* $\lambda \in K$ *impliquent* $\lambda x \in M'$.

Pour vérifier qu'une partie M′ de M est un sous-module, on doit vérifier que M′ est non vide (pratiquement on vérifie que $0 \in M'$), et que l'on a

$$\lambda x + \mu y \in M' \quad \text{quels que soient} \quad \lambda, \mu \in K \quad \text{et} \quad x, y \in M'.$$

Cette condition est évidemment nécessaire. Inversement, supposons-la vérifiée; faisant $\mu = 0$ on obtient déjà la condition (ii) ci-dessus; pour obtenir la condition (i), il suffit de faire $\lambda = 1$, $\mu = -1$, et de remarquer que dans un module on a

$$-x = (-1)x \quad \text{pour tout } x \in M$$

(en effet : $(-1)x + x = (-1)x + (+1)x = (-1+1)x = 0x = 0$).

Un module M possède toujours au moins deux sous-modules, à savoir M lui-même, et l'ensemble réduit au seul vecteur 0.

Soit M′ un sous-module d'un module M; la condition (i) ci-dessus permet déjà de regarder M′ comme un groupe additif ; la condition (ii) permet en outre de définir une application $(\lambda, x) \mapsto \lambda x$ de $K \times M'$ dans M′, et les identités qui figurent dans l'axiome (M 2) des modules, étant vérifiées dans M, le sont *a fortiori* dans M′. Par suite, *on peut regarder tout sous-module* M′ *de* M *comme un* K*-module à gauche.*

Lorsque K est un *corps*, on dit **sous-espace vectoriel** au lieu de sous-module.

Exemple 8. Prenons pour M l'espace vectoriel réel de l'*Exemple* 2 ci-dessus; on a alors dans M (en dehors de $\{0\}$ et de M lui-même) deux sortes de sous espaces vectoriels : *a*) l'ensemble des vecteurs d'origine O portés par une *droite* donnée passant par O; *b*) l'ensemble des vecteurs d'origine O contenus dans un *plan* donné passant par O. On voit du reste facilement qu'il n'y a pas d'autres sous-espaces vectoriels de M que ceux qu'on vient de décrire.

Exemple 9. Soit K un anneau et regardons-le (*Exemple* 1) comme un K-module à gauche; ses sous-modules sont donc les parties I de K qui sont non vides et telles que l'on ait

$$ux + vy \in I \quad \text{quels que soient} \quad u, v \in K \quad \text{et} \quad x, y \in I;$$

ce sont donc les *idéaux à gauche* de K définis au § 8, n° 6.

Exemple 10. Soit G un groupe commutatif écrit additivement, et regardons G comme un **Z**-module (*Exemple* 5); les sous-modules de G ne sont autres alors que ses sous-groupes, car si H est un sous-groupe de G on a $nx \in H$ pour tout $x \in H$ et tout $n \in \mathbf{Z}$.

Le résultat suivant est souvent utile :

THÉORÈME 1. *Soient* L *un module sur un anneau et* $(M_i)_{i \in I}$ *une famille de sous-modules de* L. *Alors l'intersection des* M_i *est encore un sous-module de* L. *Pour que la réunion des* M_i *soit un sous-module de* L, *il suffit que, quels que soient* $i, j \in I$, *il existe un* $k \in I$ *tel que l'on ait* $M_i \subset M_k$ *et* $M_j \subset M_k$.

Ce résultat se démontre exactement comme le Théorème 1 du § 7, et nous laisserons donc au lecteur le soin d'en rédiger lui-même une démonstration détaillée.

Il va de soi qu'en général une réunion de sous-modules n'est pas un sous-module : par exemple, dans la situation classique (*Exemple* 8), la réunion de deux droites distinctes passant par l'origine n'est pas un plan...

4. *Modules à droite et modules à gauche* (*)

Soit K un anneau. Nous allons construire un nouvel anneau qu'on appelle l'**opposé** de K, et qu'on désigne par la notation

$$K^o;$$

comme on le montrera ensuite, les modules *à droite* sur K ne sont autres que les module *à gauche* sur K^o.

Pour construire K^o, on doit se donner un ensemble, et deux lois de composition sur cet ensemble, une « addition » et une « multiplication ». Par définition, l'*ensemble* K^o sera *l'ensemble* K (les anneaux K et K^o ont donc les mêmes éléments), et l'*addition* sur K^o sera l'*addition* sur K (la somme $x + y$ de deux éléments de K a donc la même valeur, qu'on la calcule dans l'anneau K ou dans l'anneau K^o). Par contre, la *multiplication* dans K^o, au lieu d'être la multiplication $(x, y) \mapsto xy$ donnée sur K, sera l'application $(x, y) \mapsto yx$; autrement dit, si l'on désigne par xy le produit de deux éléments dans l'anneau K, et par $x * y$ leur produit dans l'anneau K^o, on a la relation

$$x * y = yx.$$

Il est facile de voir que l'ensemble K^o (= K !) muni des deux opérations qu'on vient de définir, est un anneau; par exemple la formule

$$(x + y) * z = x * z + y * z$$

se ramène évidemment à la relation $z(x + y) = zx + zy$ dans l'anneau K...

Il va de soi que, si K est un anneau commutatif, l'anneau K^o est identique à l'anneau K. La construction de K^o n'a donc d'intérêt que dans le cas non commutatif.

(*) Ce n° peut être négligé en première lecture; il n'est utilisé qu'à la fin du § 16, et le lecteur débutant pourra supposer à ce moment l'anneau K commutatif.

Soit maintenant M un module *à droite* sur l'anneau K. Définissons une application

$$(\lambda, \ x) \mapsto \lambda * x$$

de $K^0 \times M$ dans M en posant

$$\lambda * x = x\lambda \quad \text{pour tout } x \in M \text{ et tout } \lambda \in K.$$

Alors le groupe additif M, muni de l'application qu'on vient de construire, est un module *à gauche* sur l'anneau K^0 opposé à K. On a en effet

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

et enfin

$$1 * x = x1 = x,$$

ce qui établit le résultat annoncé.

Les constructions qu'on vient d'exposer montrent que les résultats établis pour les modules *à gauche* (resp. à droite) s'appliquent automatiquement aux modules *à droite* (resp. à gauche) : il suffit de passer de l'anneau de base donné à l'anneau opposé. On voit aussi que, lorsque l'anneau de base est *commutatif*, il est parfaitement indifférent, dans la théorie des modules, de placer les scalaires à gauche des vecteurs plutôt qu'à droite; c'est une simple question de *convention d'écriture*, qui n'a rien à voir avec la réalité mathématique elle-même, et dont on aurait tout à fait tort d'être l'esclave au point de ne pouvoir passer de l'écriture « droite » à l'écriture « gauche » et vice-versa.

§ 11. Relations linéaires dans un module

1. *Combinaisons linéaires*

Soient $a_1, \ldots, a_n$ des éléments d'un module à gauche M sur un anneau K; on appelle **combinaison linéaire de** $a_1, \ldots, a_n$ tout vecteur $x \in M$ possédant la propriété suivante : il existe des scalaires $\xi_1, \ldots, \xi_n \in K$ tels que l'on ait

$$x = \xi_1 a_1 + \cdots + \xi_n a_n.$$

On a bien entendu une notion analogue pour les modules à droite.

Exemple 1. Dans K^n (§ 10, *Exemple* 1) considérons les vecteurs

$$e_1 = (1, 0, 0, \ldots, 0, 0)$$
$$e_2 = (0, 1, 0, \ldots, 0, 0)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$e_n = (0, 0, 0, \ldots, 0, 1);$$

on a visiblement

$$\xi_1 e_1 = (\xi_1, 0, 0, \ldots, 0, 0)$$
$$\xi_2 e_2 = (0, \xi_2, 0, \ldots, 0, 0)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\xi_n e_n = (0, 0, 0, \ldots, 0, \xi_n)$$

et en ajoutant les résultats obtenus on trouve donc

$$\xi_1 e_1 + \cdots + \xi_n e_n = (\xi_1, \ldots, \xi_n). \tag{1}$$

Autrement dit, *tout* élément de K^n est combinaison linéaire des vecteurs $e_1, \ldots, e_n$; on a même un résultat plus précis : étant donné un vecteur $x \in K^n$, il existe *un et un seul* système de scalaires $\xi_1, \ldots, \xi_n$ tel que l'on ait

$$x = \xi_1 e_1 + \cdots + \xi_n e_n.$$

Exemple 2. Considérons le K-module *à droite* K^p pour un entier $p \geqslant 1$, et soient

$$a_1 = (\alpha_{11}, \alpha_{21}, \ldots, \alpha_{p1})$$
$$a_2 = (\alpha_{12}, \alpha_{22}, \ldots, \alpha_{p2})$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_n = (\alpha_{1n}, \alpha_{2n}, \ldots, \alpha_{pn})$$

des éléments donnés de ce module. Soit

$$b = (\beta_1, \beta_2, \ldots, \beta_p)$$

un élément de K^p; alors la relation

$$b = a_1\xi_1 + a_2\xi_2 + \cdots + a_n\xi_n \tag{2}$$

équivaut au **système de p équations linéaires à n inconnues** $\xi_1, \ldots, \xi_n$ que voici :

$$\left\{\begin{array}{l} \alpha_{11}\xi_1 + \alpha_{12}\xi_2 + \cdots + \alpha_{1n}\xi_n = \beta_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_{p1}\xi_1 + \alpha_{p2}\xi_2 + \cdots + \alpha_{pn}\xi_n = \beta_p. \end{array}\right. \tag{3}$$

On a en effet

$$a_1\xi_1 = (\alpha_{11}\xi_1, \ldots, \alpha_{p1}\xi_1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_n\xi_n = (\alpha_{1n}\xi_n, \ldots, \alpha_{pn}\xi_n),$$

de sorte que les premiers membres des relations (3) sont les composantes (*) du second membre de la relation (2).

Cet Exemple est à l'origine de la théorie « géométrique » des systèmes d'équations linéaires.

THÉORÈME 1. *Soient $a_1, \ldots, a_n$ des éléments d'un* K*-module à gauche* M, *et* M′ *l'ensemble des combinaisons linéaires de $a_1, \ldots, a_n$; alors* M′ *est le plus petit sous-module de* M *contenant $a_1, \ldots, a_n$.*

Tout d'abord, la relation

$$a_1 = 1.a_1 + 0.a_2 + \cdots + 0.a_n$$

et des relations analogues pour $a_2, \ldots, a_n$ montrent que M′ contient $a_1, \ldots, a_n$. D'autre part, tout sous-module de M contenant $a_1, \ldots, a_n$ contient aussi $\xi_1a_1, \ldots, \xi_na_n$ quels que soient $\xi_1, \ldots, \xi_n \in K$, donc contient $\xi_1a_1 + \ldots + \xi_na_n$; ainsi, tout sous-module de M contenant les vecteurs a_i ($1 \leqslant i \leqslant n$) contient M′.

Pour achever la démonstration, il reste donc à faire voir que M′ est effectivement un sous-module de M. Or soient

$$x = \xi_1a_1 + \cdots + \xi_na_n, \qquad y = \eta_1a_1 + \cdots + \eta_na_n$$

deux éléments de M′; un calcul trivial montre que

$$\lambda x + \mu y = \zeta_1a_1 + \cdots + \zeta_na_n$$

(*) Dans K^n on appelle composantes d'un vecteur $(\xi_1, \ldots, \xi_n)$ les scalaires $\xi_1, \ldots, \xi_n$; voir l'*Exemple* 12 ci-dessous.

avec

$$\zeta_1 = \lambda\xi_1 + \mu\eta_1, \ldots, \zeta_n = \lambda\xi_n + \mu\eta_n,$$

de sorte que $\lambda x + \mu y \in M'$ quels que soient les scalaires λ et μ, ce qui termine la démonstration.

Le sous-module M′ du Théorème 1 s'appelle le **sous-module de** M **engendré par** $a_1, \ldots, a_n$; lorsque $K = \mathbf{Z}$, de sorte que M est simplement un groupe commutatif écrit additivement, M′ n'est autre que le sous-groupe de M engendré par la partie $B = \{a_1, \ldots, a_n\}$ de M (§ 7, n° 4).

2. *Modules de type fini*

Soient M un K-module à gauche et M′ un sous-module de M; on dit que M′ est **de type fini** s'il existe des vecteurs $a_1, \ldots, a_n \in M'$ en nombre fini, tels que M′ soit engendré par ces vecteurs; on dit alors que $a_1, \ldots, a_n$ forment un **système de générateurs** de M′.

Cette définition s'applique en particulier au module M lui-même; autrement dit, on dit qu'un module est de type fini s'il contient des vecteurs $a_1, \ldots, a_n$ en nombre fini tels que tout $x \in M$ soit combinaison linéaire de $a_1, \ldots, a_n$.

Lorsque l'anneau de base K est un corps, on dit **espace vectoriel de dimension finie** au lieu de module de type fini.

Exemple 3. L'*Exemple* 1 montre que K^n est un K-module de type fini.

Exemple 4. Lorsque $K = \mathbf{Z}$, la notion de module de type fini se réduit à celle de groupe (commutatif) de type fini, introduite au § 7, n° 4.

Exemple 5. $\mathbf{Q}$ n'est pas de type fini comme $\mathbf{Z}$-module (§ 7, *Exemple* 10); par contre, $\mathbf{Q}$ est de type fini comme espace vectoriel sur $\mathbf{Q}$, vu l'*Exemple* 3 ci-dessus avec $K = \mathbf{Q}$, $n = 1$.

Exemple 6. Soit K un anneau; cherchons les sous-modules de type fini de K (regardé comme K-module à gauche); ce sont les idéaux à gauche (§ 10, *Exemple* 9) I de K qui possèdent la propriété suivante : *il existe des éléments $a_1, \ldots, a_n$ de* I, *en nombre fini, tels que tout $x \in I$ puisse se mettre sous la forme*

$$x = u_1a_1 + \ldots + u_na_n$$

pour un choix convenable de $u_1, \ldots, u_n \in K$. Un tel idéal est appelé un **idéal à gauche de type fini** de l'anneau K. Il est clair par exemple que tout idéal principal de K est de type fini, mais la réciproque est en général inexacte.

Étant donnés des éléments $a_1, \ldots, a_n$ de K, l'ensemble des éléments de K qui peuvent se mettre sous la forme $u_1a_1 + \ldots + u_na_n$ (autrement dit, le sous-module de K engendré par $a_1, \ldots, a_n$) s'appelle l'**idéal à gauche de K engendré par** $a_1, \ldots, a_n$.

Exemple 7. Les espaces vectoriels réels décrits au § 10, *Exemple* 7, ne sont pas de dimension finie.

3. Relations linéaires

Soient $a_1, \ldots, a_n$ des éléments d'un K-module à gauche M ; soit x une combinaison linéaire de ces vecteurs. Considérons deux façons d'écrire x comme combinaison linéaire des vecteurs donnés, soient

$$x = \xi_1 a_1 + \cdots + \xi_n a_n = \eta_1 a_1 + \cdots + \eta_n a_n ;$$

par différence, on trouve aussitôt la relation

$$(\xi_1 - \eta_1) a_1 + \ldots + (\xi_n - \eta_n) a_n = 0.$$

Ceci justifie l'introduction des notions suivantes.

On appelle **relation linéaire entre les vecteurs** $a_1, \ldots, a_n$ tout élément $(\lambda_1, \ldots, \lambda_n)$ du module K^n tel que l'on ait

$$\lambda_1 a_1 + \cdots + \lambda_n a_n = 0.$$

La relation linéaire $(0, \ldots, 0)$ est dite **triviale.** Enfin, on dit que les vecteurs $a_1, \ldots, a_n$ sont **linéairement indépendants,** ou que la famille $(a_i)_{1 \leqslant i \leqslant n}$ est **libre,** s'il n'existe pas d'autre relation linéaire entre $a_1, \ldots, a_n$ que la relation linéaire triviale.

Dire que $a_1, \ldots, a_n$ sont linéairement indépendants signifie donc que la relation

$$\lambda_1 a_1 + \cdots + \lambda_n a_n = 0 \quad \text{implique} \quad \lambda_1 = \cdots = \lambda_n = 0 ;$$

dire, au contraire, qu'ils ne sont pas linéairement indépendants (on dit alors que les vecteurs $a_1, \ldots, a_n$ sont **liés**) signifie qu'il existe des scalaires $\lambda_1, \ldots, \lambda_n$ *non tous nuls* tels que l'on ait

$$\lambda_1 a_1 + \cdots + \lambda_n a_n = 0.$$

Des vecteurs $a_1, \ldots, a_n$ linéairement indépendants sont nécessairement deux à deux distincts, car si l'on avait par exemple $a_1 = a_2$ l'élément $(1, -1, 0, \ldots, 0)$ de K^n serait évidemment une relation linéaire non triviale entre $a_1, \ldots, a_n$. Mais il ne suffit pas que les a_i soient deux à deux distincts pour qu'ils soient linéairement indépendants.

La façon dont nous avons été conduits à introduire la notion d'indépendance linéaire prouve immédiatement le résultat suivant :

THÉORÈME 2. *Soient $a_1, \ldots, a_n$ des éléments d'un* K*-module à gauche* M, *et x une combinaison linéaire des vecteurs $a_1, \ldots, a_n$. Les propriétés suivantes sont équivalentes :*

a) il existe un seul $(\xi_1, \ldots, \xi_n) \in K^n$ tel que l'on ait

$$x = \xi_1 a_1 + \cdots + \xi_n a_n ;$$

b) les vecteurs $a_1, \ldots, a_n$ sont linéairement indépendants.

Il suffit de remarquer que, si $(\lambda_1, \ldots, \lambda_n)$ est une relation linéaire entre $a_1, \ldots, a_n$, on a $\lambda_1 a_1 + \cdots + \lambda_n a_n = 0$ et par suite

$$\xi_1 a_1 + \cdots + \xi_n a_n = (\xi_1 + \lambda_1) a_1 + \cdots + (\xi_n + \lambda_n) a_n ;$$

et il est clair en fait que cette propriété *caractérise* les relations linéaires entre les vecteurs $a_1, \ldots, a_n$ donnés.

Exemple 8. Dans K^n, les vecteurs $e_1, \ldots, e_n$ de l'*Exemple* 1 sont linéairement indépendants.

Exemple 9. Prenons $K = \mathbf{R}$ et l'espace vectoriel M formé par les vecteurs d'origine donnée O dans l'espace usuel (§ 10, *Exemple* 2). Pour que des vecteurs $a_1, \ldots, a_n \in M$ soient linéairement indépendants, il faut et il suffit : (1) qu'ils ne soient pas nuls dans le cas $n = 1$; (2) qu'ils ne soient pas portés par une même droite dans le cas $n = 2$; (3) qu'ils ne soient pas contenus dans un même plan dans le cas $n = 3$. Pour $n \geqslant 4$, les vecteurs $a_1, \ldots, a_n$ ne peuvent jamais être linéairement indépendants (car s'ils l'étaient, il en serait déjà ainsi des trois vecteurs a_1, a_2, a_3, et les autres, par exemple a_4, seraient alors des combinaisons linéaires de ces trois vecteurs, ce qui contredit évidemment l'indépendance linéaire).

Exemple 10. Prenons $K = \mathbf{R}$ et pour M l'espace vectoriel de toutes les applications $f : \mathbf{R} \to \mathbf{R}$ (§ 10, *Exemple* 4 où l'on fait $X = M = K = \mathbf{R}$) ; soient $f_1, \ldots, f_n$ des éléments de M, i.e. des fonctions d'une variable réelle t, à valeurs réelles. Pour $\lambda_1, \ldots, \lambda_n \in \mathbf{R}$ la fonction $f = \lambda_1 f_1 + \cdots + \lambda_n f_n$ est donnée par

$$f(t) = \lambda_1 f_1(t) + \cdots + \lambda_n f_n(t)$$

pour tout $t \in \mathbf{R}$. Une relation linéaire entre $f_1, \ldots, f_n$ est donc une suite $(\lambda_1, \ldots, \lambda_n) \in \mathbf{R}^n$ de n nombres réels tels que l'on ait

$$\lambda_1 f_1(t) + \cdots + \lambda_n f_n(t) = 0 \quad \text{pour tout} \quad t \in \mathbf{R}.$$

Considérons par exemple les $n + 1$ fonctions $1, t, t^2, \ldots, t^n$; une relation linéaire entre ces fonctions est un système de $n + 1$ nombres réels $c_0, c_1, \ldots, c_n$ vérifiant

$$c_0 + c_1 t + \cdots + c_n t^n = 0$$

pour tout $t \in \mathbf{R}$. On verra plus loin, en étudiant le nombre de racines d'une équation algébrique, que la relation précédente implique $c_0 = \cdots = c_n = 0$, de sorte que, *quel que soit n, les fonctions $1, t, \cdots, t^n$ sont linéairement indépendantes* en tant qu'éléments de l'espace vectoriel réel M.

Exemple 11. Comme $\mathbf{Q}$ est un sous-corps de $\mathbf{C}$, on peut (§ 10, *Exemple* 6) considérer $\mathbf{C}$ comme un espace vectoriel sur $\mathbf{Q}$. Pour un $z \in \mathbf{C}$ considérons alors les $n + 1$ puissances $1, z, \ldots, z^n$ de z ; dire qu'il existe, entre ces $n + 1$ éléments de $\mathbf{C}$, une relation linéaire non triviale (à « coefficients » dans $\mathbf{Q}$) signifie qu'il existe des nombres *rationnels non tous nuls* $c_0, c_1, \ldots, c_n$ tels que z vérifie l'équation

$$c_0 + c_1 z + \ldots + c_n z^n = 0.$$

S'il en est ainsi pour au moins une valeur de n, on dit que z est un **nombre**

algébrique (*). Dans le cas contraire (i.e. si z ne vérifie aucune équation algébrique non triviale à coefficients *rationnels*) on dit que z est un **nombre transcendant**; c'est le cas de $\pi = 3{,}14159\ldots$

4. *Modules libres, bases*

Soit M un module à gauche sur un anneau K; on dit que M est **libre de type fini** s'il existe des éléments $a_1, \ldots, a_n$ de M en nombre fini qui sont *linéairement indépendants et engendrent* M. On dit alors que $a_1, \ldots, a_n$ forment une **base** de M (une base est donc un système fini de générateurs linéairement indépendants).

Soient $a_1, \ldots, a_n$ des éléments d'un K-module à gauche M; dire qu'ils engendrent M, c'est dire que pour tout $x \in M$ la relation

$$x = \xi_1 a_1 + \cdots + \xi_n a_n$$

est vérifiée pour *au moins* un $(\xi_1, \ldots, \xi_n) \in K^n$; d'autre part, dire que $a_1, \ldots, a_n$ sont linéairement indépendants signifie que, pour chaque $x \in M$, la relation ci-dessus est vérifiée pour un élément de K^n *au plus*.

Par suite, pour que les vecteurs $a_1, \ldots, a_n$ forment une base de M, il faut et il suffit que, pour chaque $x \in M$, il existe *un et un seul* $(\xi_1, \ldots, \xi_n) \in K^n$ tel que

$$x = \xi_1 a_1 + \cdots + \xi_n a_n;$$

les scalaires $\xi_1, \ldots, \xi_n$ s'appellent alors les **coordonnées** ou les **composantes de x par rapport à la base** $a_1, \ldots, a_n$ de M.

Ce qui précède montre que les coordonnées de x sont des fonctions de x, à valeurs dans K; notons-les $f_1, \ldots, f_n$, de sorte qu'on a

$$x = f_1(x)a_1 + \cdots + f_n(x)a_n$$

pour tout $x \in M$. On dit que les applications

$$f_i : M \to K$$

sont les **fonctions coordonnées du module M par rapport à la base** $a_1, \ldots, a_n$. On a les relations

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

car la relation

$$a_j = 0.a_1 + \cdots + 0.a_{j-1} + 1.a_j + 0.a_{j+1} + \cdots + 0.a_n$$

permet de calculer immédiatement les coordonnées du vecteur a_j par rapport à la base considérée.

(*) Rappelons que, comme on l'a déjà dit au § 5, n° 8, la notion de nombre algébrique définie ici n'a aucun rapport avec celle qu'on désigne sous ce nom dans l'Enseignement Secondaire (et qui n'est autre que celle de nombre réel).

On peut montrer que les nombres algébriques forment un sous-corps du corps C des nombres complexes (§ 26, n° 2); c'est l'étude de ces nombres au XIX^e siècle (surtout par Galois et les grands mathématiciens de l'école allemande : Gauss, Kummer, Jacobi, Lejeune-Dirichlet, Dedekind, Kronecker, Hilbert) qui a donné naissance à toute l'Algèbre moderne.

On a d'autre part les identités

$$f_i(x + y) = f_i(x) + f_i(y), \qquad f_i(\lambda x) = \lambda f_i(x);$$

en effet, les relations

$$x = f_1(x)a_1 + \cdots + f_n(x)a_n, \qquad y = f_1(y)a_1 + \cdots + f_n(y)a_n,$$

additionnées membre à membre, impliquent

$$x + y = [f_1(x) + f_1(y)]a_1 + \cdots + [f_n(x) + f_n(y)]a_n,$$

ce qui montre, comme annoncé, que les coordonnées du vecteur $x + y$ sont les scalaires $f_i(x) + f_i(y)$. La seconde relation s'établit de façon analogue.

Autrement dit, *pour additionner deux vecteurs, on additionne leurs coordonnées de même rang; et pour multiplier un vecteur par un scalaire, on multiplie chacune de ses coordonnées par ce scalaire.*

Exemple 12. Le K-module à gauche K^n est libre de type fini, et l'*Exemple* 1 montre que les vecteurs $e_1, \ldots, e_n$ forment une base de ce module; on l'appelle la **base canonique** de K^n. Étant donné un élément

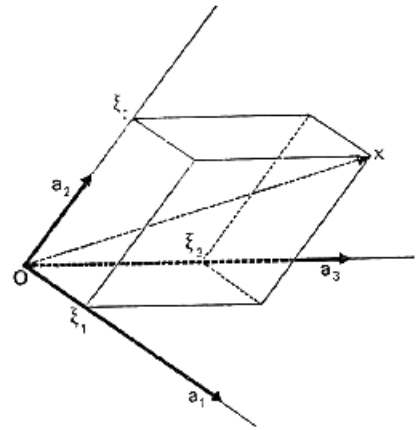
$$x = (\xi_1, \ldots, \xi_n),$$

la relation

$$x = \xi_1 e_1 + \cdots + \xi_n e_n$$

établie au n° 1 montre que les coordonnées de x par rapport à la base canonique de K^n sont les scalaires $\xi_1, \ldots, \xi_n$.

Exemple 13. Reprenons l'*Exemple* 9 ci-dessus; pour que $a_1, \ldots, a_n \in M$ forment une base de M, il faut et il suffit que $n = 3$ et que les vecteurs a_1, a_2, a_3 ne soient pas situés dans un même plan. Les coordonnées d'un vecteur x se calculent alors par la règle du « parallélipipède », que l'on comprendra en examinant la figure ci-dessous : on utilise les vecteurs a_i pour orienter et définir des « unités de longueur » sur les droites qui les portent.



Les définitions qui précèdent s'appliquent notamment aux groupes commutatifs; il suffit de faire $K = \mathbf{Z}$. On peut donc parler de **groupes commutatifs libres de type fini**

et de **bases** d'un groupe commutatif. Étant donné un groupe commutatif G (noté additivement — mais le lecteur aura intérêt à faire la traduction de ce qui va suivre en notation multiplicative), une base de G est une suite $a_1, \ldots, a_n$ d'éléments de G, en nombre fini (*), telle que l'application

$$(r_1, \ldots, r_n) \to r_1a_1 + \cdots + r_na_n$$

de $\mathbf{Z}^n$ dans G soit *bijective*; et on dit que G est libre de type fini s'il admet au moins une base.

Comme l'ensemble $\mathbf{Z}^n$ est infini, il est clair qu'un groupe commutatif libre de type fini est nécessairement infini. Un groupe commutatif fini est donc un $\mathbf{Z}$-module de type fini qui n'admet pas de base.

On voit donc qu'un module sur un anneau peut être de type fini *sans* être libre de type fini, i.e. sans posséder de base. Toutefois :

THÉORÈME 3. — *Tout espace vectoriel de dimension finie sur un corps* K *admet une base.*

Comme le présent Chapitre ne groupe que des résultats valables sur un anneau de base arbitraire, nous ne démontrerons pas ici le Théorème 3; le lecteur pourra, s'il le désire, se reporter au § 19, n° 1, attendu que la démonstration du Théorème 3 n'exige rien d'autre que le contenu du présent §.

Le Théorème 3 montre que l'assertion « tout K-module de type fini est libre de type fini », fausse si K est un anneau quelconque, est vraie si K est un *corps*.

Remarque 1. Pour assurer la validité de certains énoncés, on convient de dire que, pour tout anneau K, le K-module réduit à 0 est libre de type fini, et admet une base formée de 0 vecteurs.

Pour comprendre cette convention, on devrait définir comme suit la notion de base d'un K-module M : c'est une famille finie $(a_i)_{i\in I}$ de vecteurs linéairement indépendants qui engendrent M; cette définition autorise l'ensemble d'indices I à être vide, ce qu'on est en effet obligé de faire si l'on veut attribuer une base au module réduit à 0...

Il est de même indispensable de convenir que K^0 est le module réduit à un seul vecteur 0.

5. *Combinaisons linéaires infinies* (**)

Soient K un anneau, I un ensemble quelconque (fini ou non), et $(\lambda_i)_{i\in I}$ une famille indexée par I d'éléments de K; on dit que les scalaires λ_i sont **presque tous nuls** si l'ensemble des $i \in I$ tels que $\lambda_i \neq 0$ est *fini*; cette définition s'étend de façon évidente à une famille $(x_i)_{i\in I}$ d'éléments d'un module quelconque.

(*) Voir cependant le n° suivant.

(**) Le contenu de ce n° ne sera pas utilisé avant le § 26; le lecteur peut donc attendre d'en avoir besoin avant de l'étudier.

Il va de soit que la notion qu'on vient d'introduire n'a d'intérêt que si l'ensemble I est infini.

Soit $(x_i)_{i\in I}$ une famille d'éléments d'un K-module M; supposons les x_i presque tous nuls : il existe donc des parties *finies* J de I telles que l'on ait $x_i = 0$ pour $i \in \mathrm{I} - \mathrm{J}$; on pose alors, par définition,

$$\sum_{i\in I} x_i = \sum_{i\in J} x_i;$$

il est clair que la valeur du second membre ne dépend pas de J (pourvu que J satisfasse aux conditions énoncées ci-dessus).

Soit $(x_i)_{i\in I}$ une famille quelconque d'éléments d'un K-module M. On appelle **combinaison linéaire** des x_i tout $x \in \mathrm{M}$ possédant la propriété suivante : il existe une famille $(\xi_i)_{i\in I}$ de scalaires *presque tous nuls* telle que l'on ait

$$x = \sum_{i\in I} \xi_i x_i,$$

relation qui a un sens puisque les vecteurs $\xi_i x_i (i \in \mathrm{I})$ sont évidemment presque tous nuls.

On démontre facilement que l'ensemble M′ des combinaisons linéaires des x_i est le plus petit sous-module de M contenant tous les x_i, $i \in \mathrm{I}$; on l'appelle le **sous-module de M engendré par la famille** $(x_i)_{i\in I}$.

D'autre part, on appelle **relation linéaire entre les** $x_i (i \in \mathrm{I})$ toute famille $(\lambda_i)_{i\in I}$ de scalaires *presque tous nuls* tels que l'on ait

$$\sum_{i\in I} \lambda_i x_i = 0;$$

si cette relation implique $\lambda_i = 0$ pour tout $i \in \mathrm{I}$, on dit que les $x_i (i \in \mathrm{I})$ sont **linéairement indépendants,** ou que $(x_i)_{i\in I}$ est une **famille libre** d'éléments de M.

On appelle **base de** M toute famille libre $(x_i)_{i\in I}$ d'éléments de M engendrant le module M. Pour tout $x \in \mathrm{M}$, il existe alors une et une seule famille $(\xi_i)_{i\in I}$ de scalaires presque tous nuls telle que l'on ait

$$x = \sum_{i\in I} \xi_i x_i;$$

les ξ_i sont appelés les **coordonnées de** x **par rapport à la base** $(x_i)_{i\in I}$ **de** M.

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

On peut démontrer que *tout espace vectoriel sur un corps admet une base*; mais la démonstration de ce résultat est nettement plus difficile que celle du Théorème 3, et dépasse le cadre de cet ouvrage.

Exemple 14. L'*Exemple* 10 montre que la famille (infinie) des fonctions

$$t^n (n = 0, 1, 2, \ldots)$$

est *libre* dans l'espace vectoriel en question; les combinaisons linéaires de ces fonctions ne sont autres que les **fonctions polynomiales** d'une variable réelle (qui seront étudiées au § 28).

Exemple 15. Considérons $\mathbf{C}$ comme un espace vectoriel sur $\mathbf{Q}$; dire qu'un nombre $z \in \mathbf{C}$ est transcendant signifie que la famille (infinie) des puissances de z est libre.

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. Montrer que, dans $\mathbf{R}^3$, le vecteur $x = (6, 2, -7)$ est combinaison linéaire des vecteurs

$$a = (2, 1, -3), \qquad b = (3, 2, -5), \qquad c = (1, -1, 1);$$

les vecteurs a, b, c forment-ils une base de $\mathbf{R}^3$?
Mêmes questions dans $\mathbf{R}^4$ pour les vecteurs $x = (7, 14, -1, 2)$ et

$$a = (1, 2, -1, -2), \qquad b = (2, 3, 0, -1), \qquad c = (1, 2, 1, 3), \qquad d = (1, 3, -1, 0).$$

Montrer que les vecteurs a, b, c forment une base de $\mathbf{R}^3$, et trouver les coordonnées du vecteur x par rapport à cette base, dans chacun des cas suivants :

$a = (1, 1, 1)$, $b = (1, 1, 2)$, $c = (1, 2, 3)$, $x = (6, 9, 14)$,
$a = (2, 1, -3)$, $b = (3, 2, -5)$, $c = (1, -1, 1)$, $x = (6, 2, -7)$.

Même question dans $\mathbf{R}^4$ pour les vecteurs

$$a = (1, 2, -1, -2), \qquad b = (2, 3, 0, -1), \qquad c = (1, 2, 1, 4), \qquad d = (1, 3, -1, 0)$$

et

$$x = (7, 14, -1, 2).$$

2. Pour que deux vecteurs (a, b) et (c, d) de $\mathbf{R}^2$ forment une base de $\mathbf{R}^2$ il faut et il suffit que

$$ad - bc \neq 0.$$

3. Soit M l'espace vectoriel réel formé des vecteurs d'origine donnée O dans l'espace usuel. Soit $M' \subset M$ l'ensemble des vecteurs d'origine O dont l'extrémité est située sur un plan donné dans l'espace. M' est-il un sous-espace vectoriel de M?

4. Soit K un anneau. On considère dans K^n l'ensemble M des vecteurs $(x_1, \ldots, x_n)$ vérifiant la relation

$$x_1 + \cdots + x_n = 0;$$

est-ce un sous-module de K^n? Même question en remplaçant la relation précédente par

$$x_1 + \cdots + x_n = 1.$$

5. On considère dans $\mathbf{C}^n$ des vecteurs

$$x_k = (\xi_{k1}, \ldots, \xi_{kn}) \quad (1 \leqslant k \leqslant r)$$

dont les composantes vérifient les inégalités

$$|\xi_{kk}| > \sum_{\substack{1 \leqslant j \leqslant r \\ j \neq k}} |\xi_{kj}| \quad (1 \leqslant k \leqslant r);$$

montrer que ces vecteurs sont linéairement indépendants sur $\mathbf{C}$.

6. Quel est le sous-espace vectoriel de $\mathbf{R}^4$ engendré par les vecteurs

$$a = (1, -1, 1, 0), \qquad b = (1, 1, 0, 1), \qquad c = (2, 0, 1, 1)?$$

7. Traduire les notions de module de type fini, de module libre de type fini, et de base d'un tel module, dans le langage des groupes commutatifs écrits multiplicativement (un tel groupe étant regardé comme un $\mathbf{Z}$-module conformément à l'*Exemple* 5 du § 10).

¶ **8.** Soit V un espace vectoriel de dimension finie sur le corps $\mathbf{Q}$ des nombres rationnels. On dit qu'une partie M de V est un **réseau** dans V si M est un sous-groupe de type fini du groupe additif V, et si M contient un système de générateurs de V.

a) Soit M un sous-groupe de type fini de V. Pour que M soit un réseau de V, il faut et il suffit que, pour tout $x \in V$, il existe un entier rationnel $r \neq 0$ tel que $rx \in M$. Montrer qu'alors l'ensemble des $r \in \mathbf{Z}$ tels que $rx \in M$ est un idéal (non nul) de l'anneau $\mathbf{Z}$.

b) Soient p un nombre premier et M un réseau de V. On note M_p l'ensemble des $x \in V$ vérifiant la condition suivante : il existe un entier r non multiple de p tel que $rx \in M$. Montrer que M_p est un sous-module de V regardé comme module sur l'anneau $\mathbf{Z}_p$ du § 8, *Exercice* 5.

c) Montrer que, si M est un réseau de V, on a

$$M = \bigcap_{p \text{ premier}} M_p.$$

d) Soient M et N deux réseaux de V. Montrer que les nombres premiers p tels que

$$M_p \neq N_p$$

sont en nombre fini.
(On trouvera des propriétés supplémentaires des réseaux dans l'*Exercice* 1 du § 18.)

9. Soit A un sous-anneau d'un corps commutatif K; on suppose que tout élément de K puisse se mettre sous la forme uv^{-1} avec $u, v \in A$, $v \neq 0$, et que K soit un A-module de type fini. Montrer qu'alors $A = K$.

¶ **10.** Soient K un anneau, M un K-module à gauche et M' un sous-module de M.

a) Montrer que

$$x - y \in M'$$

est une relation d'équivalence sur l'ensemble M [on l'appelle la **congruence modulo** M' et on l'écrit souvent sous la forme

$$x \equiv y \pmod{M'};$$

voir § 7, n° 6].

b) On note M/M′ l'ensemble quotient de M par cette relation d'équivalence, et p l'application canonique de M sur M/M′. Montrer qu'il existe sur M/M′ une et une seule structure de K-module à gauche telle que l'on ait

$$p(x+y) = p(x) + p(y), \qquad p(\lambda x) = \lambda p(x)$$

quels que soient $x, y \in M$ et $\lambda \in K$ (utiliser le § 4, n° 3; voir aussi § 7, *Exercice* 16 et § 8, *Exercice* 7 pour des constructions analogues). On dit que M/M′, muni de cette structure de module, est le **module quotient** de M par le sous-module M′.

c) A chaque sous-module de M/M′ on associe son image réciproque par l'application p; montrer qu'on obtient ainsi une bijection de l'ensemble des sous-modules de M/M′ sur l'ensemble des sous-modules de M contenant M′.

d) Montrer que si M est de type fini il en est de même de M/M′ quel que soit M′. Si M est libre de type fini, en est-il de même de M/M′?

11. Soit M un module à gauche sur un anneau K.

a) Pour tout $x \in M$, on appelle **annulateur** de x l'ensemble des $\lambda \in K$ tels que $\lambda x = 0$. Montrer que c'est un idéal à gauche de K.

b) On suppose K intègre. Montrer que les $x \in M$ dont l'annulateur ne se réduit pas à 0 forment un sous-module T de M (on dit que T est le **sous-module de torsion** de M, et que M est **sans torsion** si $T = \{0\}$).

c) Montrer que le module quotient M/T (*Exercice* 10) est sans torsion.

d) Calculer T lorsque $K = \mathbf{Z}$ et $M = \mathbf{Z}^2/L$, où L est le sous-groupe de $\mathbf{Z}^2$ engendré par le vecteur (4,6).

12. On dit qu'un module à gauche M sur un anneau K est **de torsion** si, pour tout $x \in M$, il existe un scalaire *non nul* $\lambda \in K$ tel que $\lambda x = 0$.

a) Soient M un K-module à gauche et M′ un sous-module de K. On suppose que M′ et M/M′ sont des modules de torsion. Montrer que, si K est intègre, M est alors un module de torsion.

b) On suppose $K = \mathbf{Z}$. Montrer que, pour qu'un K-module de type fini soit de torsion, il faut et il suffit qu'il soit fini.

13. Soit M un module sur un anneau K. Une partie B de M (finie ou non) est appelée un **ensemble de générateurs** de M si le seul sous-module de M contenant B est M tout entier ou, ce qui revient au même, si chaque élément de M est combinaison linéaire d'éléments de B en nombre fini.
On suppose M de type fini. Montrer que l'on peut alors extraire de B un ensemble *fini* de générateurs de M (choisir dans M un système fini de générateurs x_i, et exprimer chaque x_i à l'aide d'éléments de B).

14. Soient K un corps commutatif et A un sous-anneau de K; on suppose que K est le corps des fractions de A i.e. que, pour tout $x \in K$, il existe des éléments u et v de A tels que $v \neq 0$ et

$$x = uv^{-1}.$$

Dans ce qui suit on regarde K comme un A-module, et on dit qu'une partie I de K est un **idéal fractionnaire** de l'anneau A si elle ne se réduit pas à 0, si c'est un sous-module de K, et si, enfin, il existe un élément $d \neq 0$ de K tel que l'on ait

$$dI \subset A$$

(où dI désigne l'ensemble des produits dx avec $x \in I$).

a) Pour qu'une partie I de K soit un idéal fractionnaire il faut et il suffit qu'il existe un idéal non nul J de l'anneau A et un $d \in A$ non nul tels que

$$I = d^{-1}J.$$

b) Soient I et J des idéaux fractionnaires, et soit $(I : J)$ l'ensemble des $x \in K$ tels que $xJ \subset I$; montrer que c'est un idéal fractionnaire (souvent appelé le **transporteur** de J dans I).

c) Soient I et J deux idéaux fractionnaires; on note $I + J$ l'ensemble des sommes $x + y$ avec $x \in I$ et $y \in J$, et IJ l'ensemble des éléments de K qui peuvent s'écrire comme somme (finie) de produits xy avec $x \in I$ et $y \in J$ (cf. § 8, *Exercice* 10 pour le cas où $I, J \subset A$). Montrer que $I + J$, IJ et $I \cap J$ sont des idéaux fractionnaires de l'anneau A. Étendre les formules du § 8, *Exercice* 10, (*a*).

d) On dit qu'un idéal fractionnaire I est **inversible** s'il existe un idéal fractionnaire J tel que

$$I.J = A;$$

montrer qu'alors J est unique, et donné par la relation

$$J = (A : I)$$

(on dit alors que J est l'**inverse** de I, et on le note I^{-1}). Autrement dit, pour que I soit inversible, il faut et il suffit que

$$(A : I).I = A.$$

e) Pour qu'un idéal I soit inversible il faut et il suffit qu'il existe des éléments $x_k \in I$ et $y_k \in (A : I)$ en nombre fini, tels que

$$1 = \sum x_k y_k;$$

les x_k forment alors un système de générateurs du A-module I (un idéal fractionnaire inversible est donc de type fini — on convient de dire qu'un idéal fractionnaire est **de type fini** s'il est de type fini comme A-module).

f) On dit que A est un **anneau de Dedekind** si tout idéal fractionnaire de A est inversible. Montrer que l'ensemble des idéaux fractionnaires de A, muni de la loi de composition $(I, J) \to I.J$, est alors un groupe.

g) Si A est un anneau de Dedekind, tout idéal *premier* non nul de A est *maximal*.
[Les anneaux de Dedekind se sont introduits d'abord dans la théorie des nombres algébriques — cf. § 34, *Exercice* — et on n'en a donné une définition générale et abstraite que beaucoup plus tard. La principale propriété de ces anneaux, est que *dans un anneau de Dedekind tout idéal s'écrit, d'une façon unique à des permutations près, sous la forme d'un produit d'idéaux premiers*; cf. § 18, *Exercice* 7. Inversement, cette propriété caractérise les anneaux de Dedekind. Une troisième caractérisation, beaucoup plus maniable dans la pratique, sera donnée au § 34, *Exercice* 50. Notons enfin que les anneaux de Dedekind interviennent non seulement dans la théorie des nombres algébriques, mais aussi dans l'étude des courbes algébriques et en beaucoup d'autres questions de Géométrie algébrique; c'est ce qui justifie l'introduction et l'étude des anneaux de Dedekind « abstraits ».
Comme exemple aussi élémentaire que possible d'un anneau de Dedekind, mis à part bien entendu l'anneau $\mathbf{Z}$, citons les anneaux $\mathbf{Z}[\sqrt{d}]$ où

$$d \equiv 2 \text{ ou } 3 \pmod 4.]$$

15. Soient K un anneau et X un ensemble. On désigne par

$$K^{(X)}$$

l'ensemble de toutes les applications

$$u : X \to K$$

telles que les $x \in X$ vérifiant $u(x) \neq 0$ soient en nombre *fini*. Montrer que $K^{(X)}$ est un sous-module du K-module à gauche K^X (formé de toutes les applications de K dans X). Pour chaque $x \in X$, on considère l'élément e_x de $K^{(X)}$ défini par

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

montrer que la famille $(e_x)_{x \in X}$ est une *base* du K-module à gauche $K^{(X)}$, et que les composantes par rapport à cette base de tout $u \in K^{(X)}$ sont les scalaires $u(x)$, autrement dit qu'on a

$$u = \sum_{x \in X} u(x) \cdot e_x$$

pour tout $u \in K^{(X)}$.
Soit f une application de X dans un K-module à gauche M; montrer qu'il existe un et un seul homomorphisme

$$\bar{f} : K^{(X)} \to M$$

tel que l'on ait

$$\bar{f}(e_x) = f(x) \quad \text{pour tout } x \in X.$$

(Les éléments du module $K^{(X)}$ sont généralement appelés les **combinaisons linéaires formelles** d'éléments de X à coefficients dans K, et on identifie le plus souvent l'élément de base e_x de ce module à l'élément $x \in X$ correspondant).

¶ **16.** Soient K et L deux anneaux commutatifs, et $j_1, \ldots, j_n$ des homomorphismes deux à deux distincts de K dans L. Montrer que $j_1, \ldots, j_n$ sont linéairement indépendants dans le L-module de toutes les applications de K dans L (théorème de Dedekind) (écrire une relation linéaire entre $j_1, \ldots, j_n$ et utiliser l'identité $j_k(xy) = j_k(x) j_k(y)$ pour se ramener au cas de $n - 1$ homomorphismes).

¶ **17.** Soient G un groupe commutatif, K un anneau commutatif, et $\rho_1, \ldots, \rho_n$ des homomorphismes deux à deux distincts de G dans le groupe multiplicatif K^*. Montrer que $\rho_1, \ldots, \rho_n$ sont linéairement indépendants sur K, i.e. que si $\alpha_1, \ldots, \alpha_n \in K$ vérifient

$$\alpha_1 \rho_1(s) + \ldots + \alpha_n \rho_n(s) = 0 \quad \text{pour tout } s \in G,$$

alors $\alpha_1 = \ldots = \alpha_n = 0$ (raisonner par récurrence sur n).
Exemple : soient $c_1, \ldots, c_n$ des nombres complexes deux à deux distincts; on considère les fonctions

$$e^{c_1 t}, \ldots, e^{c_n t}$$

pour $t \in \mathbf{R}$; montrer qu'elles sont linéairement indépendantes sur $\mathbf{C}$.