Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

THESIS / THÈSE

MASTER EN SCIENCES MATHÉMATIQUES

Des espaces vectoriels aux modules: une perspective didactique

HENROTTE, Maud

Award date:
2009

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026



FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX
NAMUR

Faculté des Sciences
Département de Mathématique

DES ESPACES VECTORIELS AUX MODULES : UNE PERSPECTIVE DIDACTIQUE

Mémoire présenté pour l'obtention

du grade académique de master en Sciences Mathématiques

Maud HENROTTE

Juin 2009

Promotrices : Suzanne THIRY et Valérie HENRY

Je remercie toutes les personnes qui, de près ou de loin, m'ont aidée à réaliser ce mémoire. Tout d'abord mes promotrices, Madame S. Thiry, pour son aide, pour tout ce qu'elle m'a appris au cours de l'année et pour les nombreuses heures qu'elle m'a consacrées, ainsi que Madame V. Henry, pour son soutien et ses précieux conseils. Ensuite, Madame M. Van Caenegem pour sa contribution en Latex et sa disponibilité. Enfin, je tiens à remercier ma famille et mes amis pour m'avoir encouragée durant ces cinq années.

Résumé

Dans ce mémoire, nous proposons une production didactique destinée à des étudiants de première année universitaire en mathématiques, familiarisés avec les notions de base d'algèbre linéaire. Elle a pour but de faire découvrir le concept de module et de mettre en place une comparaison entre celui-ci et celui d'espace vectoriel. Pour ce faire, nous commençons par rappeler les structures algébriques que sont les groupes, les anneaux et les corps. Ensuite, nous introduisons une nouvelle structure, le module, ainsi que quelques résultats fondamentaux. Enfin, nous présentons le concept de base dans le cadre général des modules. Les théorèmes d'existence et de caractérisation d'une base nous permettent de différencier davantage les espaces vectoriels des modules. Afin de faciliter la compréhension de ce travail auprès des étudiants, nous proposons des exemples et des exercices résolus. Tout au long de ce mémoire, nous explicitons également les réflexions et les choix inhérents à la présentation du sujet, au travers de commentaires didactiques.

Abstract

In this paper, we present a didactic production intended for first-year graduate students in mathematics, who have some basic knowledge in linear algebra. The aim of this production is to introduce the concept of module and draw a parallel between vector spaces and modules. For this purpose, we first remind the readers of algebraic structures as groups, rings and fields. Next, we introduce a new structure, the module, along with some fundamentals results. Finally, we bring forward the notion of basis within the framework of modules. Existence and characterization theorems enable us to emphasize the difference between vector spaces and modules. In order to make the students' understanding easier, we suggest examples and solved exercises. Through some didactic comments, we also formulate personal thoughts and choices that led to the way the subject is presented in this work.

Table des matières

Introduction **5**

1 Rappels des structures algébriques fondamentales **7**
1.1 Notion de groupe 8
1.1.1 Définition de groupe 8
1.1.2 L'élément neutre 10
1.1.3 La symétrisabilité 11
1.1.4 Groupe commutatif 12
1.1.5 Synthèse des différentes notations 12
1.1.6 Exemples de groupes 13
1.1.7 Produit direct de groupes 15
1.1.8 Homomorphisme de groupes 16
1.2 Notions d'anneau et corps 22
1.2.1 Définition d'anneau 22
1.2.2 Homomorphisme d'anneaux 25
1.2.3 Définition de corps 30

2 Introduction d'une structure algébrique nouvelle : le module **34**
2.1 Modules et espaces vectoriels 34
2.1.1 Définition de module 35
2.1.2 Relations fondamentales dans un module 42
2.1.3 Parallélisme entre modules à droite et modules à gauche 43
2.1.4 Définition d'espace vectoriel 45
2.1.5 Exemples de modules et espaces vectoriels 46
2.2 Sous-modules et sous-espaces vectoriels 54
2.3 Homomorphisme de modules 58
2.4 Exemples illustratifs 71

3 Bases dans les modules et espaces vectoriels **76**
3.1 Notion de base dans un module 77
3.1.1 Contexte et notations 77
3.1.2 Combinaisons linéaires 82
3.1.3 Systèmes générateurs et indépendance linéaire 87

3.1.4 Base d'un module 92
3.1.5 Base et homomorphisme de modules 96
3.2 Existence de bases dans les espaces vectoriels 105
3.2.1 Théorèmes d'existence de bases 105
3.2.2 Illustration des théorèmes d'existence 107
3.2.3 Corollaires du théorème d'existence 109
3.3 Notion de dimension d'un espace vectoriel 111
3.4 Comparaison entre modules et espaces vectoriels 119
3.4.1 Définitions 119
3.4.2 Sous-modules et sous-espaces vectoriels 120
3.4.3 Homomorphismes 121
3.4.4 Les bases 122

Conclusion **127**

Bibliographie **128**

Introduction

Le but de ce mémoire est de proposer un parcours qui permet d'élargir, au cadre général des modules, quelques notions relatives aux espaces vectoriels de dimension finie. Nous mettrons en place une comparaison entre ces deux structures algébriques.
Nous sommes conscients que les concepts abordés sont simples et maîtrisés depuis longtemps par les mathématiciens. Ce mémoire n'a donc aucune prétention d'amener quelque chose de nouveau dans ce domaine. L'objectif de ce travail est tout autre : mettre en place une présentation à caractère didactique. Les nouveaux concepts introduits ou les éléments distinctifs entre espaces vectoriels et modules font l'objet d'une explicitation particulière et sont illustrés par des exemples ou exercices résolus.

Ce travail comporte deux lectures distinctes. La première, constituée de la matière en elle-même, s'adresse à des étudiants de première année universitaire qui ont un premier bagage en algèbre linéaire. En effet, nous considérons qu'ils maîtrisent déjà les concepts d'espace vectoriel, de base et d'application linéaire dans les espaces de dimension finie. La deuxième lecture est destinée aux mathématiciens susceptibles d'enseigner le concept de module. Elle comprend des réflexions personnelles relatives aux choix didactiques effectués et à la construction des exemples proposés. Tout au long du mémoire, ces commentaires sont présentés dans des cadres ombrés afin de les distinguer du corps de texte.

Dans un premier chapitre, nous rappelons les structures algébriques de groupe, d'anneau et de corps ainsi quelques propriétés importantes, qui seront utiles pour la suite. Ce chapitre permet d'introduire les notations et de partir sur des bases communes à tous.

Dans un deuxième chapitre, nous étudions le module à droite et le module à gauche. Nous explicitons ces deux définitions en symboles mathématiques et en langage courant. Ensuite, nous présentons des relations fondamentales dans un module ainsi que le parallélisme existant entre module à droite et à gauche et finalement, nous nous intéressons à un cas particulier de module : l'espace vectoriel. Nous consacrons également des sections aux notions de sous-modules et d'homomorphisme de modules.

Dans un troisième chapitre, nous développons la notion de base dans les modules. D'abord, nous présentons les familles de vecteurs, les combinaisons linéaires, l'indépendance linéaire, les systèmes générateurs et enfin les bases. La notion de famille nous permet d'envisager un nouveau concept : celui des bases contenant un nombre infini de vecteurs. Ensuite, nous étudions l'existence des bases et leur caractérisation et introduisons la notion de dimension dans les espaces vectoriels. Enfin, une comparaison générale reprend les différences et analogies entre espaces vectoriels et modules repérées tout au long de ce mémoire.

Chapitre 1

Rappels des structures algébriques fondamentales

Afin d'introduire la notion de module, notion centrale de ce mémoire, nous allons commencer par présenter les différents concepts et mettre en place les outils préliminaires qui seront utiles pour la suite. Dans ce chapitre, nous rappellerons les structures algébriques de base que sont les groupes, les anneaux et les corps et nous énoncerons les résultats les plus importants concernant ces notions. Ensuite, après chaque notion théorique, nous proposerons un exemple ou un exercice résolu. Ils ont essentiellement pour buts de permettre une première manipulation des définitions et d'attirer l'attention sur les subtilités qui se cachent derrière certains concepts.
Ce premier chapitre est essentiellement basé sur les syllabi de P. Toint [8] et de S. Thiry [7].

Remarque : Ce premier chapitre peut paraître élémentaire à première vue puisqu'il a pour but de rappeler aux lecteurs les structures algébriques de base comme les groupes, les anneaux et enfin les corps. Nous sommes conscients que les étudiants en première année de bachelier connaissent déjà pour la plupart ces structures. Néanmoins, il est important que ces bases, clairement détaillées, soient communes à tous.
Ce rappel est aussi un moyen d'introduire en douceur les conventions de notations et de vocabulaire utilisées tout au long du travail et de laisser le temps aux étudiants de se familiariser avec elles. En effet, on remarque que certains problèmes de compréhension sont parfois dus aux notations spécifiques utilisées et à une trop grande quantité d'éléments nouveaux qui sont présentés simultanément. Dès lors, si les concepts sont connus, l'étudiant pourra se concentrer sur les notations et se les approprier avant d'aborder des notions plus complexes, comme celle de module par exemple.

1.1 Notion de groupe

1.1.1 Définition de groupe

Commençons par considérer un ensemble K non vide. Munissons cet ensemble K d'une loi de composition $*$, interne et partout définie[1] :

$$\begin{aligned} * : \quad K \times K &\longrightarrow K, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Dans la pratique, on rencontre souvent d'autres notations pour signifier une loi de composition, comme le symbole $+$ ou $\bullet$. On aurait donc pu noter la loi de composition définie ci-dessus comme suit :

$$\begin{aligned} + : \quad K \times K &\longrightarrow K, \\ (x, y) &\mapsto x + y. \end{aligned}$$

Malgré la notation équivoque, le symbole $+$ désigne une loi quelconque, sans rapport avec l'addition de nombres. On dit néanmoins que l'on utilise la notation additive.

On pourrait encore noter cette même loi de composition de la manière suivante :

$$\begin{aligned} \bullet : \quad K \times K &\longrightarrow K, \\ (x, y) &\mapsto x \bullet y = xy, \end{aligned}$$

dans ce cas, on dit que l'on utilise la notation multiplicative.

Il faut que le lecteur soit conscient qu'utiliser le symbole $+$, $\bullet$, l'absence de signe ou encore $*$ pour décrire la loi de composition est uniquement une convention d'écriture et ne change en rien la signification de la loi de composition en elle-même. Dans un premier temps, nous avons choisi d'utiliser le symbole $*$ pour désigner une loi de composition sur K.

Remarque

Par la suite, sauf mention explicite du contraire, nous ne considérerons que des lois de composition qui sont partout définies. Dès lors, lorsque nous parlerons de **loi de composition sur K**, il sera sous-entendu que cette loi est partout définie.

1. Une **loi de composition (interne) sur un ensemble K** est une fonction de $K \times K$ dans K. Une loi de composition est **partout définie** si c'est une application. En d'autres mots, une loi de composition interne et partout définie fait correspondre à tout couple $(x, y) \in K \times K$ un troisième élément de K qui dépend de x et de y.

Remarque : Notation de la loi de composition.
Nous trouvons qu'il est utile dans ce paragraphe d'insister sur les différentes notations que l'on peut choisir pour indiquer une loi de composition. Il y a plusieurs raisons à cela.
En premier lieu, utiliser différentes notations permet de faire comprendre à l'étudiant que les symboles utilisés sont uniquement des conventions d'écriture et ne changent pas la signification de la loi de composition. Il est en effet indispensable qu'il puisse en faire abstraction pour pouvoir comprendre en profondeur les concepts de loi de composition, de groupe, d'anneau et de module.
Ensuite, introduire le symbole $*$ permet d'éviter les notations $+$ et $\cdot$ utilisées habituellement dans la littérature. En effet, si on utilise directement ces dernières notations, l'étudiant risque d'associer ces symboles aux lois d'addition et multiplication usuelles, ce qui pourrait prêter à confusion.
Enfin, il est important qu'il soit capable de passer d'une notation à l'autre, c'est pourquoi nous insisterons sur ce point tout au long du paragraphe, notamment avec un tableau récapitulatif.

Lorsque l'on considère l'ensemble K et une loi de composition $(x, y) \mapsto x * y$ sur K, on les note généralement sous forme de couple : $\{K, *\}$.

Avec cette notation, introduisons la notion fondamentale de groupe.

Définition 1.1.1 (Groupe)
Le couple $\{K, *\}$ est un **groupe** s'il vérifie les conditions suivantes

1. $\forall\, x, y, z \in K$, $\quad x * (y * z) = (x * y) * z$ [Associativité]
2. $\exists\, e \in K,\ \forall\, x \in K$, $\quad e * x = x * e = x$ [Existence d'un élément neutre]
3. $\forall\, x \in K,\ \exists\, y \in K$, $\quad x * y = e = y * x$ [Symétrisabilité]

Remarque
Il est important de constater qu'un groupe est constitué de deux objets : un ensemble et une loi de composition. Néanmoins, en pratique, lorsqu'on parlera du groupe $\{K, *\}$, on le nommera simplement le groupe K, par la même lettre que l'ensemble qui en constitue l'une de ses données.

1.1.2 L'élément neutre

Définition 1.1.2 (Elément neutre)
Tout élément e dont il est question dans la propriété 2. de la définition 1.1.1 est appelé **élément neutre** de la loi de composition $*$. Autrement dit, un élément neutre de la loi $*$ est un élément e tel que

$$\forall\, x \in K, \quad e * x = x = x * e. \tag{1.1}$$

S'il y a une ambiguïté possible concernant le groupe auquel un élément neutre appartient, on le note e_G si e est un élément neutre pour la loi $*$ dans G.

Lorsqu'une loi de composition admet un élément neutre, elle n'en admet en fait qu'un seul, comme le spécifie le théorème suivant.

Théorème 1.1.1
Soit $*$ une loi interne et partout définie sur l'ensemble K.
Si cette loi de composition admet un élément neutre, alors il est unique.

Preuve :
Supposons que e' et e'' soient des éléments neutres pour la loi $*$ sur K. Ils vérifient donc les égalités (1.1).
Considérons le cas particulier où $x = e''$ dans l'égalité $e' * x = x$, on obtient :

$$e' * e'' = e''.$$

Considérons le cas particulier où $x = e'$ dans l'égalité $x * e'' = x$, on obtient :

$$e' * e'' = e'.$$

Et donc $e' = e''$. ∎

Remarques

1. Si l'on utilise la notation additive, l'élément neutre sera noté **0** plutôt que e, tandis que si la loi de composition est notée multiplicativement, le neutre est désigné par **1**.
2. Dorénavant, si une loi de composition admet un élément neutre, on dira ***l'*élément neutre** puisqu'on sait d'après le théorème précédent que s'il existe, il est unique.

1.1.3 La symétrisabilité

Définition 1.1.3 (Elément symétrique)
Si $x \in K$, alors tout élément $y \in K$ vérifiant la propriété 3. de la définition 1.1.1 est appellé **symétrique de x**. En d'autres mots, $y \in K$ est un symétrique de $x \in K$ si $x * y = e = y * x$.

Si l'élément $x \in K$ admet un symétrique, alors il n'y en a qu'un. C'est l'objet du théorème suivant.

Théorème 1.1.2
Soient $\{K, *\}$ un groupe et $x \in K$. Si l'élément x admet un symétrique, alors celui-ci est unique.

Preuve : Supposons que $y \in K$ et $y' \in K$ soient tous les deux des symétriques de x. Par définition, on peut écrire :

$$x * y = e = y * x \quad \text{et} \quad x * y' = e = y' * x$$

Par les égalités ci-dessus et par l'associativité de $*$, on obtient d'une part

$$(x * y) * y' = e * y' = y'.$$

et d'autre part

$$(x * y) * y' = (y * x) * y' = y * (x * y') = y * e = y.$$

Donc $y = y'$. ∎

Remarque
Dorénavant, s'il existe, nous noterons le symétrique de l'élément $x \in K$ pour la loi $*$ par x' afin d'insister sur le lien qui existe entre un élément et son symétrique.

Lorsqu'on utilise une loi de composition notée additivement, on prend comme convention de noter le symétrique de $x \in K$ par $-x$ plutôt que par x', et on l'appelle *opposé* plutôt que *symétrique*. Enfin, l'élément $x + (-y)$ du groupe K sera noté $x - y$.

Par contre, lorsqu'on a affaire à une loi de composition notée multiplicativement, on emploie le mot *inverse* au lieu du mot *symétrique* et on note l'inverse de l'élément $x \in K$ par x^{-1}. Par convention, l'élément $x \cdot (y^{-1})$ ou $x(y^{-1})$ du groupe K sera noté $x \cdot y^{-1}$ ou xy^{-1}.

1.1.4 Groupe commutatif

On ajoute souvent une nouvelle propriété à la définition de groupe : la commutativité de la loi de composition. On obtient alors la définition suivante.

Définition 1.1.4 (Groupe commutatif ou abélien)
$\{K, *\}$ est un **groupe commutatif** ou un **groupe abélien** si

1. $\{K, *\}$ est un groupe,
2. $\forall\, x, y \in K, \quad x * y = y * x$ [Commutativité]

1.1.5 Synthèse des différentes notations

Le tableau ci-dessous est tiré de [7] et donne un récapitulatif des notations que nous avons employées jusqu'à présent. Les notations addititive et multiplicative sont les plus fréquemment utilisées dans la littérature, il est donc intéressant de pouvoir passer aisément d'une notation à l'autre.

Notation de la loi	Composé	Elément neutre	Symétrique de x	Composé de x avec son symétrique
$*$	$x * y$	e	x'	$x * x'$
Notation additive $+$	$x + y$	0	$-x$ (opposé)	$x - x$
Notation multiplicative $\cdot$ ou absence de signe	$x \cdot y$ ou xy	1	x^{-1} (inverse)	xx^{-1}

Remarque
Dorénavant, par convention, nous écrirons *la loi de composition d'un groupe en notation additive*, et cela jusqu'à la fin de ce texte.

1.1.6 Exemples de groupes

Illustrons les différents concepts que nous avons vus jusqu'à présent par quelques exemples.

Objectifs des exemples 1.1.1 et 1.1.2 :
Le but visé par ces exemples est la manipulation de la définition de groupe. Le premier exemple permet à l'étudiant de faire le lien entre le concept abstrait de groupe et les ensembles de nombres munis des lois usuelles, qu'il manipule régulièrement.
Le deuxième exemple permet d'étudier un groupe qui est muni d'une loi moins intuitive pour les étudiants : la composition d'applications. Cette loi est un peu différente des lois usuelles d'addition et multiplication, notamment parce qu'elle n'est pas commutative. Elle incite donc plus à la réflexion.

Exemple 1.1.1
L'ensemble des nombres naturels $\mathbb{N}$ muni de la loi d'addition usuelle ne forme pas un groupe puisque les éléments de $\mathbb{N}$ n'admettent pas de symétrique dans $\mathbb{N}$. Par contre, l'ensemble des nombres entiers $\mathbb{Z}$ muni de la loi d'addition usuelle forme un groupe commutatif[2].

Exemple 1.1.2
Soit $K = \{1, 2 \ldots, n\}$ l'ensemble constitué par les naturels $1, 2, \ldots$ jusque n, et considérons les permutations[3] de K. Soit $\mathcal{S}_n$ l'ensemble de ces permutations, que l'on muni de la loi de composition d'applications usuelle $\circ$.

La formule $(f, g) \mapsto f \circ g$, où $f \circ g$ est la composée des applications f et g, définit bien une loi de composition interne et partout définie car $\forall f, g \in \mathcal{S}_n$, $h = f \circ g \in \mathcal{S}_n$: la composée de deux applications bijectives d'un ensemble dans lui-même est encore une application bijective.

Le couple $\{\mathcal{S}_n, \circ\}$ forme-t-il un groupe ?

Pour répondre à la question, nous proposons de résoudre ce problème sur un exemple plus concret : étudions le couple particulier $\{\mathcal{S}_3, \circ\}$.

2. Parfois, $\mathbb{Z}$ est aussi appelé l'ensemble des entiers rationnels et $\{\mathbb{Z}, +\}$ est appelé **groupe additif des entiers rationnels.**
3. On appelle une **permutation de K** toute application bijective de K dans K.

Prenons donc $K = \{1, 2, 3\}$. L'ensemble des permutations $\mathcal{S}_3$ comporte 6 éléments :

$$\begin{aligned} s_1 &: \ 1,2,3 \ \mapsto 1,2,3 \\ s_2 &: \ 1,2,3 \ \mapsto 2,3,1 \\ s_3 &: \ 1,2,3 \ \mapsto 3,1,2 \\ s_4 &: \ 1,2,3 \ \mapsto 1,3,2 \\ s_5 &: \ 1,2,3 \ \mapsto 3,2,1 \\ s_6 &: \ 1,2,3 \ \mapsto 2,1,3 \end{aligned}$$

De cette manière, nous avons répertorié tous les arrangements possibles des nombres $1, 2, 3$. Le nombre de permutations possibles de l'ensemble K est $3! = 6$.

Vérifions une à une les propriétés de la définition 1.1.1.

1. L'associativité est vérifiée car l'opération qui consiste à composer des applications est une loi de composition associative[4].

2. Peut-on trouver un élément neutre ? La permutation s_1 convient car c'est l'application identité sur K. En effet, on peut vérifier que $\forall\ s_i \in \mathcal{S}_3,\ s_1 \circ s_i = s_i = s_i \circ s_1,\ i = 1, \ldots, 6$.

3. En ce qui concerne la symétrisabilité, il faut vérifier que

$$\forall\ s_i \in \mathcal{S}_3,\ \exists\ s_j \in \mathcal{S}_3 : s_i \circ s_j = s_1 = s_j \circ s_i,\ i, j = 1, \ldots, 6.$$

   On peut vérifier que $s_1 \circ s_1 = s_1$, $s_4 \circ s_4 = s_1$, $s_5 \circ s_5 = s_1$, $s_6 \circ s_6 = s_1$, et enfin, $s_2 \circ s_3 = s_1 = s_3 \circ s_2$. Autrement dit, les éléments s_1, s_4, s_5, s_6 sont leur propre symétrique tandis que la permutation s_2 est le symétrique de s_3 et s_3 est le symétrique de s_2.

4. Enfin, on remarque que la loi $\circ$ n'est pas commutative.
   En effet, par exemple avec les permutations s_2 et $s_4 \in K$, $\underbrace{s_2 \circ s_4}_{=s_5} \neq \underbrace{s_4 \circ s_2}_{=s_6}$.

En conclusion, $\{\mathcal{S}_3, \circ\}$ est un groupe non-commutatif.

De manière générale, on peut montrer que $\{\mathcal{S}_n, \circ\}$ est un groupe[5], quel que soit le naturel n. Ceci clôture cet exemple.

4. Ce résultat ne sera pas démontré ici, mais une démonstration peut être trouvée dans [3], pg 61.
5. Une démonstration de cette affirmation peut être trouvée dans [3], à la page 114.

1.1.7 Produit direct de groupes

Par la suite, dans certains exemples, nous utiliserons des ensembles produits[6] ($\mathbb{R}^n, \mathbb{Z}^n, \dots$).
La propriété suivante nous sera alors utile.

Proposition 1.1.1 (Produit direct de groupe)
Soient $G_1, \dots, G_n$, n groupes. Considérons sur l'ensemble produit $G = G_1 \times \cdots \times G_n$ la loi de composition donnée par :

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n). \tag{1.2}$$

Alors, le couple formé par l'ensemble G et cette loi de composition est également un groupe. On l'appellera **le produit direct des groupes $G_1, \dots, G_n$.**

Ceci découle immédiatement du fait que $G_1, \dots, G_n$ sont des groupes.

Remarque
Observons que malgré leurs notations identiques (notation additive), les lois de compositions utilisées dans les deux membres de l'égalité (1.2) ne sont pas les mêmes. Dans le membre de gauche, le symbole $+$ représente la loi de composition sur G. Dans le membre de droite, les symboles $+$ représentent les lois définies respectivement sur $G_1, G_2, \dots, G_n$. La notation additive est utilisée pour chaque groupe rencontré mais elle peut cacher des réalités bien différentes de l'addition usuelle.
Cette subtilité est illustrée dans l'exemple suivant.

Objectif de l'exemple 1.1.3 :
Cet exemple a pour but d'illustrer la proposition ainsi que la remarque précédente et de faire prendre conscience à l'étudiant que les lois qui se cachent derrière les notations additives des différents groupes ne sont pas toujours la loi d'addition usuelle.
Cet exemple est présenté sous la forme d'un exercice résolu, comme beaucoup d'autres dans la suite du texte. De cette manière, l'étudiant peut s'exercer par lui-même et ensuite s'auto-contrôler.

6. L'ensemble produit $X \times Y$ est l'ensemble des couples (x, y) où $x \in X$ et $y \in Y$.
De plus, si X est un ensemble, on pose

$$X^n = \underbrace{X \times X \times \dots \times X}_{\text{produit de } n \text{ ensembles identiques}}.$$

Exemple 1.1.3
Soit G_1 et G_2 deux groupes définis comme suit :

- $G_1 = \{\mathcal{S}_3, \circ\}$: l'ensemble des permutations de l'ensemble $\{1, 2, 3\}$ muni de la composition usuelle d'applications, présenté dans l'exemple précédent ;
- $G_2 = \{\mathbb{Q}, \cdot\}$: l'ensemble des rationnels muni de la multiplication usuelle.

Considérons l'ensemble produit $G = G_1 \times G_2 = \{(s, \alpha) : s \in \mathcal{S}_3, \alpha \in \mathbb{Q}\}$, et munissons-le de la loi de composition définie par

$$(s_i, \alpha_1) + (s_j, \alpha_2) = (s_i \circ s_j, \alpha_1 \cdot \alpha_2).$$

Questions
a) **Le couple $\{G, +\}$ est-il un groupe ? Justifie.**
b) **Calculer $(s_2, 7) + (s_4, -3)$. Cet élément appartient-il à G ?**

Résolution

a) En premier lieu, vérifions que G_1 et G_2 ainsi définis sont des groupes.
On sait par l'exemple précédent que G_1 est un groupe, et on peut facilement vérifier que G_2 en est un également. De plus, la loi de composition sur G est définie selon la même structure que celle de la proposition 1.1.1. En effet,

$$\underbrace{(s_i, \alpha_1) + (s_j, \alpha_2)}_{\text{Loi définie sur } G} = (\quad \underbrace{s_i \circ s_j}_{\text{Loi définie sur } G_1} \quad , \quad \underbrace{\alpha_1 \cdot \alpha_2}_{\text{Loi définie sur } G_2} \quad).$$

Par la proposition 1.1.1, on peut donc conclure que $\{G, +\}$ est un groupe.

b) $(s_2, 7) + (s_4, -3) = (s_2 \circ s_4, 7 \cdot -3) = (s_5, -21)$. Par définition des lois de compositions sur G_1 et G_2 qui sont internes et partout définies, cet élément appartient à G.

Voilà qui clôture cet exemple.

1.1.8 Homomorphisme de groupes

Enfin, étudions maintenant la notion d'homomorphisme de groupes.

Définition 1.1.5 (Homomorphisme de groupes)
Soient K et L deux groupes. On appelle **homomorphisme de K dans L** toute application f de K dans L telle que

$$\forall\, x, y \in K, \qquad f(x + y) = f(x) + f(y). \tag{1.3}$$

Si l'homomorphisme est bijectif[7], on parlera d'**isomorphisme de K dans L**.
S'il existe un isomorphisme de K dans L, on dira que les groupes K et L sont **isomorphes**.

7. On considère que les notions d'application, d'injection, surjection et bijection sont connues. Des définitions claires de ces notions peuvent être trouvées dans [8], page 6.

Nous pouvons de nouveau observer que malgré leurs notations identiques (notation additive), les lois de compositions utilisées dans les deux membres de l'égalité (1.3) ne sont pas les mêmes. Dans le membre de gauche, le symbole $+$ représente la loi de composition sur K, tandis que dans le membre de droite, le symbole $+$ représente la loi définie sur L. Ces deux lois peuvent donc être totalement différentes, comme l'illustre l'exemple suivant.

Objectif de l'exemple 1.1.4 :
Dans cet exemple, nous voulons attirer l'attention de l'étudiant sur le fait que la définition d'homomorphisme de groupe implique deux groupes, un de départ et un d'arrivée, qui peuvent être totalement différents au point de vue de leur ensemble et de leur loi de composition. C'est pourquoi nous avons choisi pour le groupe de départ, l'ensemble des matrices 2×2 muni de la loi d'addition matricielle usuelle, et pour le groupe d'arrivée, l'ensemble des couples réels muni d'une loi de composition $\oplus$ assez particulière.
Cette loi diffère expressément de la loi $+$ usuelle pour mettre en lumière le fait que le symbole $+$ peut cacher des réalités parfois inattendues. Par exemple, la loi $\oplus$ n'admet pas l'élément $(0,0)$ comme neutre, comme c'est le cas pour l'addition usuelle de couples, mais elle admet le neutre $(-2,-2)$.

Exemple 1.1.4
Considérons l'application f définie par

$$f : \{M_2(\mathbb{R}), +\} \longrightarrow \{\mathbb{R}^2, \oplus\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = (a+d-2, c+b-2)$$

où

- $\{M_2(\mathbb{R}), +\}$ est l'ensemble des matrices 2×2, à éléments réels, muni de la loi d'addition matricielle usuelle[8].
- $\{\mathbb{R}^2, \oplus\}$ est l'ensemble des couples réels muni de la loi $\oplus : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ $((x_1, x_2), (y_1, y_2)) \mapsto (x_1 + y_1 + 2, x_2 + y_2 + 2)$, où $+$ désigne l'addition usuelle sur $\mathbb{R}$.

8. On définit l'addition matricielle usuelle sur $\{M_2(\mathbb{R}), +\}$ comme suit :

$$\begin{array}{rccc} + : & M_2(\mathbb{R}) \times M_2(\mathbb{R}) & \longrightarrow & M_2(\mathbb{R}) \\ & (A, B) & \mapsto & A + B, \end{array}$$

où, si a_{ij} désigne l'élément de A qui se trouve à la $i^{\text{ème}}$ ligne et à la $j^{\text{ème}}$ colonne, on définit

$$(A+B)_{ij} = a_{ij} + b_{ij}, \quad i, j = 1, 2.$$

Questions

a) **L'application f est-elle un homomorphisme de groupe ?**

b) **L'application f est-elle un isomorphisme de groupe ?**

Résolution

a) Vérifions que f est homomorphisme de groupe.

Pour commencer, remarquons que f est partout définie dans $M_2(\mathbb{R})$, c'est donc bien une application.
Ensuite, nous vérifierons que $\{M_2(\mathbb{R}), +\}$ et $\{\mathbb{R}^2, \oplus\}$ sont des groupes. Enfin, nous montrerons que f ainsi définie satisfait à l'égalité (1.3).

1) **$\{M_2(\mathbb{R}), +\}$ est un groupe (commutatif)**

En effet, l'addition matricielle est associative, commutative, l'élément neutre est la matrice nulle $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et enfin l'élément symétrique d'une matrice quelconque $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \{M_2(\mathbb{R}), +\}$ est la matrice opposée $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \in (M_2(\mathbb{R}), +)$.

2) **Le couple $\{\mathbb{R}^2, \oplus\}$ est-il un groupe ?**

Détaillons les propriétés de la définition 1.1.1 les unes après les autres.

. **[Associativité]** $\forall\, x = (x_1, x_2),\ y = (y_1, y_2),\ z = (z_1, z_2) \in \mathbb{R}^2,\ (x \oplus y) \oplus z =^{?} x \oplus (y \oplus z)$
Oui, car

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$
$$\Leftrightarrow (x_1 + y_1 + 2, x_2 + y_2 + 2) \oplus (z_1, z_2) = (x_1, x_2) \oplus (y_1 + z_1 + 2, y_2 + z_2 + 2)$$
$$\Leftrightarrow ((x_1+y_1+2)+z_1+2, (x_2+y_2+2)+z_2+2) = (x_1+(y_1+z_1+2)+2, x_2+(y_2+z_2+2)+2)$$
$$\Leftrightarrow (x_1 + y_1 + z_1 + 4, x_2 + y_2 + z_2 + 4) = (x_1 + y_1 + z_1 + 4, x_2 + y_2 + z_2 + 4)$$

. **[L'élément neutre]** $\exists\, e = (e_1, e_2) \in \mathbb{R}^2,\ \forall\, x = (x_1, x_2) \in \mathbb{R}^2,\ x \oplus e = x = e \oplus x.$
L'élément $(e_1, e_2) = (-2, -2) \in \mathbb{R}^2$ est le neutre de cette loi car

$$\forall (x_1, x_2) \in \mathbb{R}^2,\ (x_1 + e_1 + 2, x_2 + e_2 + 2) = (x_1, x_2) = (e_1 + x_1 + 2, e_2 + x_2 + 2)$$

. **[Symétrisabilité]** $\forall\, x = (x_1, x_2) \in \mathbb{R}^2,\ \exists\, x' = (x'_1, x'_2) \in \mathbb{R}^2,\ x \oplus x' = e = x' \oplus x.$
Soit $(x_1, x_2) \in \mathbb{R}^2$. Son symétrique est l'élément $x' = (x'_1, x'_2) = (-4 - x_1, -4 - x_2)$.
En effet, comme $e = (-2, -2)$, on doit trouver x' tel que

$$x \oplus x' = (-2, -2) = x' \oplus x$$

$$\Leftrightarrow (x_1 + x_1' + 2, x_2 + x_2' + 2) = (-2, -2) = (x_1' + x_1 + 2, x_2' + x_2 + 2)$$
$$\Leftrightarrow (x_1', x_2') = (-4 - x_1, -4 - x_2).$$

3) **Il reste à montrer que f vérifie la propriété** (1.3).

Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ deux éléments de $M_2(\mathbb{R})$.

Montrons que

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

Par les définitions de l'addition matricielle et de f, l'expression précédente est équivalente à

$$f(\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}) = (a+d-2, b+c-2) \oplus (a'+d'-2, b'+c'-2).$$

Par les définitions de f et de la loi $\oplus$, on obtient

$$(a+a'+d+d'-2, b+b'+c+c'-2) = ((a+d-2)+(a'+d'-2)+2, (b+c-2)+(b'+c'-2)+2).$$

En simplifiant le membre de droite, cette dernière égalité est encore équivalente à

$$(a + a' + d + d' - 2, b + b' + c + c' - 2) = (a + d + a' + d' - 2, b + c + b' + c' - 2).$$

En commutant les termes adéquats, on trouve finalement que les deux membres de l'expression ci-dessus sont égaux. Donc f est bien un homomorphisme de groupes.

b) **Vérifions que l'homomorphisme f est un isomorphisme.**

D'après la définition 1.1.5, il faut montrer que f est bijective.
Pour ce faire, montrons que f est

1. **Surjective** : par définition, f est surjective si et seulement si

$$\forall\ (x, y) \in \mathbb{R}^2,\ \exists \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \text{ tel que } f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = (x, y).$$

Par la définition de f,

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = (a + d - 2, c + b - 2)),$$

cela revient à se demander s'il existe une matrice dont les éléments vérifient le système

$$\begin{cases} a+d=x+2 \\ c+b=y+2, \end{cases}$$

quel que soit le couple $(x,y) \in \mathbb{R}^2$ choisi au départ.
On observe que c'est bien le cas, donc f est surjective.

2. **Injective** : par définition f est injective si et seulement si

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(\mathbb{R}),$$

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = f(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Par définition de f et par la définition de l'égalité de deux matrices[9], cela revient à vérifier que

$$(a+d-2, c+b-2) = (a'+d'-2, c'+d'-2) \Rightarrow \begin{cases} a=a' \\ b=b' \\ c=c' \\ d=d' \end{cases}.$$

Cependant, on observe que le système

$$\begin{cases} a+d-2=a'+d'-2 \\ c+b-2=c'=d'-2 \end{cases}$$

n'implique pas obligatoirement que

$$\begin{cases} a=a' \\ b=b' \\ c=c' \\ d=d' \end{cases}.$$

Donc, f n'est pas injective.

Par conséquent, f n'est pas un isomorphisme puisque cet homomorphisme n'est pas une bijection.

Voilà qui clôture cet exemple.

9. Soit A une matrice $n \times m$ et B une matrice $r \times p$.
A et B sont égales si elles ont même dimension ($n=r$ et $m=p$) et si leurs éléments dont égaux deux à deux $(a_{ij}=b_{ij},\ \forall i=1,\dots n,\ j=1,\dots m)$.

Terminons ce paragraphe sur les homomorphismes de groupes en explorant deux propriétés importantes.

Propriétés des homomorphismes de groupes

Soient K et L deux groupes. On constate que si f est un homomorphisme de groupes de K dans L, les propriétés suivantes sont toujours vérifiées.

Proposition 1.1.2 (Propriétés des homomorphismes de groupes)
Soient K et L deux groupes et f est un homomorphisme de groupes de K dans L.

1. *Le neutre de K est envoyé par l'homomorphisme de groupes sur le neutre de L.*
   En d'autres mots,
   $$f(0_K) = 0_L. \tag{1.4}$$

2. *L'image du symétrique de x dans K est le symétrique de $f(x)$ dans L.*
   Autrement dit,
   $$\forall\, x \in K, \qquad f(-x) = -f(x). \tag{1.5}$$

Preuve :

1. La première propriété est immédiate.
   En effet, en choisissant $y = 0_K$ dans la relation (1.3), on trouve pour tout x dans K :
   $$\begin{aligned} f(x + 0_K) = f(x) + f(0_K) &\Leftrightarrow f(x) = f(x) + f(0_K) \\ &\Leftrightarrow f(x) - f(x) = f(x) - f(x) + f(0_K) \\ &\Leftrightarrow 0_L = 0_L + f(0_K) \\ &\Leftrightarrow 0_L = f(0_K). \end{aligned}$$

2. Démontrons la deuxième propriété.
   En effet, en partant de l'égalité précédente, on obtient pour tout x dans K :
   $$\begin{aligned} 0_L = f(0_K) &\Leftrightarrow 0_L = f(-x + x) \\ &\Leftrightarrow 0_L = f(-x) + f(x) \quad \text{par (1.3)} \\ &\Leftrightarrow -f(x) = f(-x) + \underbrace{f(x) - f(x)}_{= 0_L} \\ &\Leftrightarrow -f(x) = f(-x). \end{aligned}$$

   ce qui implique le résultat annoncé. ∎

Ces propriétés clôturent le paragraphe relatif à la notion de groupe.

1.2 Notions d'anneau et corps

1.2.1 Définition d'anneau

Soit K un ensemble non vide muni de la loi de composition suivante :

$$\begin{aligned} + : \quad K \times K &\longrightarrow K, \\ (x, y) &\mapsto x + y. \end{aligned}$$

Pour définir un anneau, il est nécessaire d'introduire une deuxième loi de composition sur l'ensemble de départ.
Munissons donc K d'une deuxième loi de composition $*$ interne et partout définie :

$$\begin{aligned} * : \quad K \times K &\longrightarrow K, \\ (x, y) &\mapsto x * y. \end{aligned}$$

Considérons le triplet $\{K, +, *\}$ formé par l'ensemble K et les deux lois de compositions $+$ et $*$ et présentons la notion d'anneau.

Définition 1.2.1 (Anneau)
Le triplet $\{K, +, *\}$ est un **anneau** s'il vérifie les conditions suivantes

1. $\{K, +\}$ est un groupe commutatif,
2. $\forall\, x, y, z \in K, \quad x * (y * z) = (x * y) * z,$ [Associativité]
3. $\exists\, e \in K, \ \forall\, x \in K, \quad e * x = x = x * e,$ [Existence de l'élément neutre][10]
4. $\forall\, x, y, z \in K, \quad x * (y + z) = (x * y) + (x * z)$ et $(y + z) * x = (y * x) + (z * x).$
   [Distributivité à gauche et à droite de $*$ par rapport à $+$]

Comme nous l'avons fait avec la première loi pour définir un groupe commutatif, on peut exiger que la deuxième loi $*$ soit commutative. On obtient alors la définition suivante :

Définition 1.2.2 (Anneau commutatif)
Le triplet $\{K, +, *\}$ est un **anneau commutatif** si

1. $\{K, +, *\}$ est un **anneau**,
2. $\forall\, x, y \in K, \quad x * y = y * x$ [Commutativité]

10. Certains auteurs omettent l'existence d'un neutre dans la définition d'anneau et parlent d'**anneau unitaire** lorsque l'élément neutre existe.

Remarques

1. Pour introduire le concept d'anneau, nous avons besoin de deux lois de compositions sur K. Dans la littérature, on trouve les notations et appellations suivantes, que nous adopterons dans la suite.
   a) La première loi est souvent notée additivement $(+)$ et est appelée **addition sur K**. Le neutre associé à cette loi est noté 0.
   b) La deuxième loi que nous avons notée jusqu'ici par $*$ est plutôt notée multiplicativement (par $\cdot$ ou par l'absence de symbole) et est appelée **multiplication sur K.** L'élément neutre associé à cette loi est noté par $\mathbf{1}$ au lieu de e.

   Rappelons que malgré leur notation et leur nom, ces deux lois peuvent n'avoir aucun rapport avec les lois d'addition et de multiplication habituelles.
2. Observons que nous avons utilisé deux symboles différents pour les deux neutres : 0 pour de la loi d'addition et $\mathbf{1}$ pour la loi de multiplication.
   a) Le neutre pour l'addition est **absorbant** c'est-à-dire que pour tout élément x de l'anneau K, $0x = x0 = 0$.

   En effet, on vérifie que

   $$x = 1x = (1+0)x = 1x + 0x = x + 0x.$$

   L'égalité $x = x + 0x$ obtenue permet de conclure que $0 = 0x$. L'autre identité se démontre de la même façon.
   b) **Les deux neutres 0 et 1 peuvent-ils être identiques ?**
   Supposons que $0 = \mathbf{1}$. Dans ce cas, on obtient, pour tout x dans K :

   $$x = x \cdot \mathbf{1} = x \cdot 0 = 0$$

   où la dernière égalité s'obtient grâce au fait que 0 est absorbant. On observe donc que K se réduit à un seul élément, 0. Il est qualifié dans ce cas d'**anneau trivial.**

Illustrons la définition d'anneau par quelques exemples.

Objectifs de l'exemple 1.2.1 :
Nous introduisons ici l'ensemble des matrices muni des lois usuelles d'addition et de multiplication. Cet ensemble est intéressant pour illustrer la notion d'anneau, d'une part car les matrices sont des objets connus des élèves depuis la 6ème année de l'enseignement secondaire, et d'autre part, parce que cet ensemble muni de ces deux lois forme un anneau non commutatif, sans être un corps. Pour ces deux raisons, de nombreux exemples ayant trait à cet anneau, seront développés dans la suite du travail.

Exemple 1.2.1

1. L'ensemble des nombres entiers $\mathbb{Z}$ muni des lois d'addition et de multiplication habituelles est un anneau commutatif[11]. On peut par contre vérifier que l'ensemble des nombres entiers naturels $\mathbb{N}$, muni des mêmes lois n'est pas un anneau puisque $\{\mathbb{N}, +\}$ n'est pas un groupe commutatif.

2. Soit K un anneau quelconque. Précisons quelques notations : on note par $M_{m,n}(K)$ l'ensemble des matrices à m lignes, n colonnes et à éléments dans K, et par $M_m(K)$ l'ensemble des matrices carrées d'ordre m à éléments dans K.

   Considérons l'ensemble des matrices $M_n(K)$ et munissons cet ensemble des lois de composition d'addition et de multiplication matricielles usuelles, définies comme suit

$$\begin{aligned} + : \quad M_n(K) \times M_n(K) &\longrightarrow M_n(K) \\ (A, B) &\mapsto A + B, \end{aligned}$$

   où, si a_{ij} désigne l'élément de A qui se trouve à la $i^{\text{ème}}$ ligne et à la $j^{\text{ème}}$ colonne, on définit

$$(A + B)_{ij} = a_{ij} + b_{ij}, \qquad i, j = 1, \ldots, n.$$

   où $a_{ij} + b_{ij}$ est obtenu grâce à la loi de composition de $+$ dans l'anneau K,

   et

$$\begin{aligned} \cdot : \quad M_n(K) \times M_n(K) &\longrightarrow M_n(K) \\ (A, B) &\mapsto A \cdot B = AB, \end{aligned}$$

   où, si a_{ij} désigne l'élément de A qui se trouve à la $i^{\text{ème}}$ ligne et à la $j^{\text{ème}}$ colonne, on définit

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \qquad i, j = 1, \ldots, n.$$

   où $a_{ik} b_{kj}$ est obtenu grâce à la loi de multiplication dans l'anneau K.

Alors, on peut vérifier que $M_n(K)$ muni de ces deux lois de composition est un anneau.
Le 0 de $M_n(K)$ est la matrice dont tous les coefficients sont égaux au 0 de K. Le $\mathbf{1}$ de $M_n(K)$ est la matrice dont les éléments diagonaux sont égaux au $\mathbf{1}$ de K et dont tous les autres éléments sont égaux au 0 de K.

11. On l'appelle parfois **l'anneau des entiers rationnels.**

1.2.2 Homomorphisme d'anneaux

Tout comme nous l'avons fait pour les groupes, on peut définir un homomorphisme d'anneaux.

Définition 1.2.3 (Homomorphisme d'anneaux)
Soient K et L deux anneaux. On appelle **homomorphisme de K dans L** toute application f de K dans L telle que

$$\forall\, x, y \in K, \qquad f(x+y) = f(x) + f(y), \quad f(x \cdot y) = f(x) \cdot f(y) \quad \text{et} \quad f(1_K) = 1_L.$$

Si l'homomorphisme est bijectif, on parlera d'**isomorphisme de K sur L**.
S'il existe un isomorphisme de K dans L, on dira que les anneaux K et L sont **isomorphes**.

Remarque
On observe que tout homomorphisme d'anneaux satisfait automatiquement la définition d'homomorphisme de groupes, puisque la première égalité de la définition 1.2.3 est la même que dans la définition 1.1.5.

Illustrons cette définition par un exemple.

Exemple 1.2.2
Considérons l'application f de l'exemple 1.1.4 définie sur M, un sous-ensemble de $M_2(\mathbb{R})$ (et non plus sur $M_2(\mathbb{R})$ tout entier) :

$$f : \{M, +, \cdot\} \longrightarrow \{\mathbb{R}^2, \oplus, \otimes\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = (a+d-2, c+b-2)$$

où les ensembles de départ et d'arrivée sont chacun munis, cette fois-ci, de deux lois de composition :

- $\{M, +, \cdot\}$ où $M = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix},\ a, b \in \mathbb{R} \right\}$ est muni de la loi d'addition matricielle usuelle et de la loi de multiplication suivante :

$$\cdot : M \times M \longrightarrow M$$

$$\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}\right) \mapsto \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' & bb' \\ bb' & aa' \end{pmatrix},$$

où l'absence de symbole représente la multiplication usuelle sur $\mathbb{R}$.

- $\{\mathbb{R}^2, \oplus, \otimes\}$ est l'ensemble des couples réels muni de la loi $\oplus : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$
  $((x_1, y_1), (x_2, y_2)) \mapsto (x_1 + y_1 + 2, x_2 + y_2 + 2)$,

  et de la loi $\otimes : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$
  $((x_1, x_2), (y_1, y_2)) \mapsto (x_1 + y_1 + \frac{x_1 y_1}{2}, x_2 + y_2 + \frac{x_2 y_2}{2})$, où $+$ désigne l'addition usuelle sur $\mathbb{R}$.

Question : l'application f est-elle un homomorphisme d'anneaux ?

Résolution

Vérifions que f est un homomorphisme d'anneaux.
Pour ce faire, montrons que

1. $\{M, +, \cdot\}$ et $\{\mathbb{R}^2, \oplus, \otimes\}$ sont des anneaux, ce que nous ferons en premier lieu.
2. f ainsi définie satisfait aux égalités de la définition 1.2.3 :

$$\forall\, A, B \in M, \quad f(A+B) = f(A) + f(B), \quad f(A \cdot B) = f(A) \cdot f(B) \quad \text{et} \quad f(\mathbb{I}) = \mathbf{1},$$

où $\mathbb{I} \in M$ est le neutre pour la loi $\cdot$ et $\mathbf{1} \in \mathbb{R}^2$ est le neutre pour la loi $\otimes$.

1. Montrons que $\{M, +, \cdot\}$ et $\{\mathbb{R}^2, \oplus, \otimes\}$ sont des anneaux en vérifiant les propriétés de la définition 1.2.1.

a. $\{M, +, \cdot\}$ est un anneau.

. $\{M, +\}$ est un groupe commutatif. Nous laissons cette vérification au soin du lecteur. Elle se fait de la même manière que dans l'exemple 1.1.4.

. **[Associativité]** $\forall \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \in M,$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} \cdot \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \right) = \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} \right) \cdot \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a'a'' & b'b'' \\ b'b'' & a'a'' \end{pmatrix} = \begin{pmatrix} aa' & bb' \\ bb' & aa' \end{pmatrix} \cdot \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a(a'a'') & b(b'b'') \\ b(b'b'') & a(a'a'') \end{pmatrix} = \begin{pmatrix} (aa')a'' & (bb')b'' \\ (bb')b'' & (aa')a'' \end{pmatrix}$$

Par l'associativité de la multiplication dans $\mathbb{R}$, on conclut que les éléments des matrices sont égaux deux à deux. La loi $\cdot$ est donc associative.

. **[L'élément neutre]** $\exists\, \mathbb{I} = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \in M,\ \forall \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M,$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

L'élément $\mathbb{I} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ est le neutre de cette loi car $\forall \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M$:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a \cdot 1 & b \cdot 1 \\ b \cdot 1 & a \cdot 1 \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

L'autre membre de l'égalité se montre de manière similaire.

. **[Distributivité de $+$ par rapport à $\cdot$] :**

$$\forall \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \in M,$$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \right) \stackrel{?}{=} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix}$$

et

$$\left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \right) \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Démontrons la première égalité, la deuxième se montre de manière similaire.

Elle est vérifiée car

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix} \right) = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a'' & b'' \\ b'' & a'' \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a'+a'' & b'+b'' \\ b'+b'' & a'+a'' \end{pmatrix} = \begin{pmatrix} aa' & bb' \\ bb' & aa' \end{pmatrix} + \begin{pmatrix} aa'' & bb'' \\ bb'' & aa'' \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a(a'+a'') & b(b'+b'') \\ b(b'+b'') & a(a'+a'') \end{pmatrix} = \begin{pmatrix} aa'+aa'' & bb'+bb'' \\ bb'+bb'' & aa'+aa'' \end{pmatrix}.$$

et par la distributivité de $\cdot$ par rapport à $+$ dans $\mathbb{R}$, cette égalité est toujours vraie.

b. $\{\mathbb{R}^2, \oplus, \otimes\}$ est un anneau.

. $\{\mathbb{R}^2, \oplus\}$ est un groupe commutatif d'après l'exemple 1.1.4.

. **[Associativité]** $\forall\, x = (x_1, x_2),\ y = (y_1, y_2),\ z = (z_1, z_2) \in \mathbb{R}^2,\ (x \otimes y) \otimes z =^{?} x \otimes (y \otimes z)$
Oui, car

$$(x \otimes y) \otimes z = x \otimes (y \otimes z)$$
$$\Leftrightarrow (x \otimes y) + z + \frac{(x \otimes y)z}{2} = x + (y \otimes z) + \frac{x(y \otimes z)}{2}$$
$$\Leftrightarrow x + y + \frac{xy}{2} + z + \frac{xz + yz + \frac{xyz}{2}}{2} = x + y + z + \frac{yz}{2} + \frac{xy + xz + \frac{xyz}{2}}{2}$$
$$\Leftrightarrow x + y + z + \frac{xy}{2} + \frac{xz}{2} + \frac{yz}{2} + \frac{xyz}{4} = x + y + z + \frac{xy}{2} + \frac{xz}{2} + \frac{yz}{2} + \frac{xyz}{4}$$

. **[L'élément neutre]** $\exists\, e = (e_1, e_2) \in \mathbb{R}^2,\ \forall\, x = (x_1, x_2) \in \mathbb{R}^2,\ x \otimes e = x = e \otimes x.$

L'élément $(e_1, e_2) = (0, 0) \in \mathbb{R}^2$ est le neutre de cette loi car

$$\forall (x_1, x_2) \in \mathbb{R}^2,\ (x_1 + 0 + \frac{x_1 \cdot 0}{2}, x_2 + 0 + \frac{x_2 \cdot 0}{2}) = (x_1, x_2) = (0 + x_1 + \frac{0 \cdot x_1}{2}, 0 + x_2 + \frac{0 \cdot x_2}{2})$$

. **[Distributivité de $\oplus$ par rapport à $\otimes$] :**
$\forall\ x = (x_1, x_2),\ y = (y_1, y_2),\ z = (z_1, z_2) \in \mathbb{R}^2,\ x \otimes (y \oplus z) \stackrel{?}{=} (x \otimes y) \oplus (x \otimes z)$ et
$(y \oplus z) \otimes x \stackrel{?}{=} (y \otimes x) \oplus (z \otimes x)$

La première égalité est vérifiée car

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$
$$\Leftrightarrow x + (y \oplus z) + \frac{x(y \oplus z)}{2} = (x \otimes y) + (x \otimes z) + 2$$
$$\Leftrightarrow x + y + z + 2 + \frac{xy + xz + 2x}{2} = x + y + \frac{xy}{2} + x + z + \frac{xz}{2} + 2$$
$$\Leftrightarrow 2x + y + z + 2 + \frac{xy}{2} + \frac{xz}{2} = 2x + y + z + 2 + \frac{xy}{2} + \frac{xz}{2}.$$

La deuxième égalité se montre de manière similaire.

2. Montrons que f ainsi définie satisfait aux deux dernières égalités de la définition 1.2.3.

1. $\forall\, A, B \in M,\quad f(A + B) = f(A) + f(B)$. Cette égalité a été vérifiée dans l'exemple 1.1.4 dans le cas général où $A, B \in M_2(\mathbb{R})$. Comme M est un groupe et un sous-ensemble de $M_2(\mathbb{R})$, cette égalité est vérifiée dans le cas où $A, B \in M$.

2. Soit $\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} \in M$:

$$f\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}\right) \stackrel{?}{=} f\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) \otimes f\left(\begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix}\right)$$

Oui car, par la définition de f et par la définition de la loi de composition $\cdot$, cette égalité peut s'écrire comme suit

$$f\left(\begin{pmatrix} aa' & bb' \\ bb' & aa' \end{pmatrix}\right) = (2a-2, 2b-2) \otimes (2a'-2, 2b'-2)$$

Par la définition de f et de la loi $\otimes$, cette dernière égalité est équivalente à

$$(2aa'-2, 2bb'-2) = (2a-2, 2b-2) + (2a'-2, 2b'-2) + \frac{(2a-2, 2b-2)(2a'-2, 2b'-2)}{2}$$

ou encore, après simplification du membre de droite, à

$$(2aa'-2, 2bb'-2) = (2a+2a'-4+\frac{1}{2}(4aa'-4a-4a'+4), 2b+2b'-4+\frac{1}{2}(4bb'-4b-4b'+4))$$

$$\Leftrightarrow (2aa'-2, 2bb'-2) = (2aa'-2, 2bb'-2).$$

3. Si $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ est le neutre pour la loi $\cdot$ sur M et $e = (0,0)$ est le neutre pour la loi $\otimes$ sur $\mathbb{R}^2$,

$$f\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right) \stackrel{?}{=} (0,0)$$

Oui car par la définition de f, on obtient

$$(1+1-2, 1+1-2) = (0,0).$$

En conclusion, f est bien un homomorphisme d'anneaux.

- $\{\mathbb{R}^2, \oplus, \otimes\}$ l'ensemble des couples réels muni de la loi $\oplus : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$
  $((x_1, y_1), (x_2, y_2)) \mapsto (x_1 + y_1 + 2, x_2 + y_2 + 2)$,

  et de la loi $\otimes : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$
  $((x_1, x_2), (y_1, y_2)) \mapsto (x_1 + y_1 + \frac{x_1 y_1}{2}, x_2 + y_2 + \frac{x_2 y_2}{2})$, où $+$ désigne l'addition usuelle sur $\mathbb{R}$.

Question : $\{M, +, \cdot\}$ et $\{\mathbb{R}^2, \oplus, \otimes\}$ sont-ils des corps ? Sont-ils des champs ?

Résolution

1. Commençons par le triplet $\{M, +, \cdot\}$. Nous savons déjà que ce triplet est un anneau par l'exemple 1.2.2.

De plus, cet anneau est non trivial. En effet, le neutre de la loi d'addition (la matrice nulle $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$) est différent du neutre de la loi de multiplication ($\mathbb{I} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$).

D'après la définition 1.2.4, il reste à montrer que

$$\forall \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}, \ \exists \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M,$$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a' & b' \\ b' & a' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

Soit $\begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

On vérifie que le symétrique est donné par la matrice $\begin{pmatrix} \frac{1}{a} & \frac{1}{b} \\ \frac{1}{b} & \frac{1}{a} \end{pmatrix}$ qui existe toujours puisque $\mathbb{R}$ est un corps et $a, b \neq 0$.

De plus, cette matrice appartient bien à M puisqu'elle est de la forme $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$, où $x, y \in \mathbb{R}$.

En conclusion, $\{M, +, \cdot\}$ est un corps.

C'est également un champ puisque la loi de composition $\cdot$ est commutative. En effet,

$$\forall \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M,$$

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

car par la définition de $\cdot$ cette égalité est équivalente à

$$\begin{pmatrix} aa' & bb' \\ bb' & aa' \end{pmatrix} = \begin{pmatrix} a'a & b'b \\ b'b & a'a \end{pmatrix}$$

qui est toujours vraie car la multiplication usuelle sur $\mathbb{R}$ est commutative.

2. A présent, intéressons-nous au triplet $\{\mathbb{R}^2, \oplus, \otimes\}$. Nous savons déjà que ce triplet est un anneau par l'exemple 1.2.2.

De plus, cet anneau est non trivial.
En effet, le neutre de la loi d'addition ($(-2,-2) \in \mathbb{R}^2$) est différent du neutre de la loi de multiplication ($(0,0) \in \mathbb{R}^2$).

Il reste à montrer que
$\forall\, x = (x_1, x_2) \in \mathbb{R}^2 \setminus \{(-2,-2)\}$, $\exists\, x' = (x'_1, x'_2) \in \mathbb{R}^2$,

$$(x_1, x_2) \otimes (x'_1, x'_2) = (0,0) = (x_1, x_2) \otimes (x'_1, x'_2)$$

Or, l'expression précédente peut s'écrire comme suit, par la définition de $\otimes$:

$$(x_1 + x'_1 + \frac{x_1 x'_1}{2}, x_2 + x'_2 + \frac{x_2 x'_2}{2}) = (0,0) = (x'_1 + x_1 + \frac{x'_1 x_1}{2}, x'_2 + x_2 + \frac{x'_2 x_2}{2})$$

ou encore

$$(x'_1(1 + \frac{x_1}{2}), x'_2(1 + \frac{x_2}{2})) = (-x_1, -x_2).$$

Autrement dit, $\forall\, x = (x_1, x_2) \in \mathbb{R}^2 \setminus \{(-2,-2)\}$, il faut pouvoir trouver un élément $x' = (x'_1, x'_2) \in \mathbb{R}^2$ tel que

$$(x'_1, x'_2) = (\frac{-x_1}{1 + \frac{x_1}{2}}, \frac{-x_2}{1 + \frac{x_2}{2}}).$$

Comme c'est toujours possible, sauf pour le couple $(-2,-2)$, le triplet $\{\mathbb{R}^2, \oplus, \otimes\}$ est bien un corps.

C'est également un champ, puisque la loi de composition $\otimes$ est commutative. En effet,

$$\forall\ x = (x_1, x_2),\ y = (y_1, y_2) \in \mathbb{R}^2,\ x \otimes y = y \otimes x$$

car

$$x + y + \frac{xy}{2} = y + x + \frac{yx}{2},$$

et l'addition et la mulitiplication usuelles dans $\mathbb{R}$ sont commutatives.

Cet exemple clôture la section sur les anneaux.

Nous avons à présent tous les outils pour introduire, dans le chapitre suivant, la nouvelle notion de module.

Chapitre 2

Introduction d'une structure algébrique nouvelle : le module

2.1 Modules et espaces vectoriels

Maintenant que nous avons mis en place les concepts de base, les conventions de notation et de vocabulaire, nous pouvons entrer dans le vif du sujet et introduire la notion de module.
Pour commencer, nous détaillerons la construction du concept de module, en utilisant les notions rappelées au chapitre précédent. Nous verrons alors comment relier cette nouvelle notion à celle, déjà connue, d'espace vectoriel. Ensuite, nous nous intéresserons aux théorèmes fondamentaux concernant les modules en général. Enfin, nous consacrerons deux sections particulières aux sous-modules et aux homomorphismes de modules.
Pour permettre une première manipulation des nouvelles définitions et résultats, nous proposerons quelques exemples et exercices résolus, et cela, tout au long du chapitre.
Ce chapitre et le suivant sont essentiellement basés sur l'ouvrage de R. Godement [3].

Commentaires didactiques : Un des objectifs de ce travail est de faire découvrir aux étudiants la distinction entre un module et un espace vectoriel. Même si la comparaison entre ces deux concepts est exposée dans le chapitre suivant, elle trouve sa source dans les définitions que nous allons présenter et détailler abondamment ici.
Afin d'attirer l'attention de l'étudiant, chaque formulation en langage symbolique sera suivie de son explication en langage courant. En effet, les formules mathématiques paraissent assez simples d'un premier abord mais cachent des subtilités dont il n'est pas toujours conscient. Nous faisons donc le choix de « mettre des mots » sur ces subtilités.

2.1.1 Définition de module

Introduisons les concepts de module à droite et de module à gauche.

Commentaires didactiques
Des choix didactiques réfléchis se cachent derrière la manière de présenter la définition de module.
Dans un premier temps, nous commençons par introduire la notion de module à gauche avec un symbole différent pour chaque loi de composition, afin que l'étudiant repère bien la différence qu'il existe entre chacune d'entre elle. Ces notations sont, pour la plupart, extraites du syllabus de P. Toint [8]. Ensuite, nous présentons avec ces notations le concept de module à droite, afin que l'étudiant puisse bien discerner la différence entre module à droite et module à gauche et faire des parallèles entre les deux concepts. Enfin, nous avons explicitons en language courant les différences qui distinguent les deux définitions, pour aider l'étudiant à les repérer.

Pour définir un module, deux ensembles, munis chacun d'un certain nombre de lois de composition, sont nécessaires :

- premièrement, un **anneau** $\{K, +, *\}$ fixé une fois pour toutes et appelé **anneau de base.** Nous y puiserons des éléments que nous appellerons « **scalaires** » et que nous noterons dorénavant par des lettres grecques.
- deuxièmement, un **groupe commutatif** $\{M, \#\}$. Nous appellerons les éléments de ce groupe des « **vecteurs** » et nous les noterons par des lettres latines.

Enfin, il nous faut une loi qui relie ces deux ensembles : nous munissons le groupe commutatif M d'une loi de composition ***externe*** et partout définie $\bullet$, appelée **multiplication scalaire**, que l'on définit comme suit :

$$\begin{array}{rccc} \bullet : & K \times M & \longrightarrow & M \\ & (\lambda, x) & \mapsto & \lambda \bullet x. \end{array}$$

Considérons le triplet $\{M, \#, \bullet\}$ et introduisons les définitions de K-module à gauche et de K-module à droite.

Définition 2.1.1 (Module à gauche)
On appelle **module à gauche sur l'anneau K**, ou encore **K-module à gauche**, le triplet $\{M, \#, \bullet\}$ dont les éléments vérifient :

1. $\forall\ \alpha, \beta \in K,\ \forall\ x \in M,$ $(\alpha * \beta) \bullet x = \alpha \bullet (\beta \bullet x)$ [Associativité mixte]
2. $\forall\ x \in M,$ $\mathbf{1} \bullet x = x$
3. $\forall\ \alpha \in K,\ \forall\ x, y \in M,$ $\alpha \bullet (x \# y) = (\alpha \bullet x) \# (\alpha \bullet y)$ [Double
4. $\forall\ \alpha, \beta \in K,\ \forall\ x \in M,$ $(\alpha + \beta) \bullet x = (\alpha \bullet x) \# (\beta \bullet x)$ distributivité]

Définition 2.1.2 (Module à droite)
On appelle **module à droite sur l'anneau K**, ou encore **K-module à droite**, le triplet $\{M, \#, \bullet\}$ dont les éléments vérifient :

1. $\forall\ \alpha, \beta \in K,\ \forall\ x \in M,$ $(\alpha * \beta) \bullet x = \beta \bullet (\alpha \bullet x)$ [Associativité mixte]
2. $\forall\ x \in M,$ $\mathbf{1} \bullet x = x$
3. $\forall\ \alpha \in K,\ \forall\ x, y \in M,$ $\alpha \bullet (x \# y) = (\alpha \bullet x) \# (\alpha \bullet y)$ [Double
4. $\forall\ \alpha, \beta \in K,\ \forall\ x \in M,$ $(\alpha + \beta) \bullet x = (\alpha \bullet x) \# (\beta \bullet x)$ distributivité]

On observe immédiatement qu'il n'y a que la première propriété de chaque définition qui différencie un K-module à gauche d'un K-module à droite. Les trois autres propriétés des deux définitions sont en effet identiques que l'on soit dans un module à gauche ou à droite.

Remarque
Si l'on suppose que K est commutatif, la première propriété de chaque définition est identique que l'on soit dans un module à gauche ou un module à droite. Par conséquent, *si K est commutatif, tout K-module à gauche est automatiquement un K-module à droite et réciproquement.* Dans ce cas, on parlera simplement de **K-module**.

Traduction en langage courant des définitions.

Explicitons en français et une à une les propriétés qui caractérisent un K-module à gauche et un K-module à droite.

1. Dans un module à gauche (définition 2.1.1), la première propriété signifie que

Prendre deux scalaires dans K, un premier α et un deuxième β ,

- les composer entre eux par la deuxième loi sur K $[\alpha * \beta]$

- puis composer ce scalaire résultant avec un vecteur x par la loi externe $[(\alpha * \beta) \bullet x]$

revient à

- *multiplier scalairement le vecteur x avec le deuxième scalaire β* $[\beta \bullet x]$
- *puis multiplier scalairement ce vecteur résultant avec le premier scalaire α* $[\alpha \bullet (\beta \bullet x)]$

Dans un module à droite (définition 2.1.2), la première propriété nous dit que

Prendre deux scalaires dans K, un premier α et un deuxième β ,

- *les composer entre eux par la deuxième loi sur K* $[\alpha * \beta]$
- *puis composer ce scalaire résultant avec un vecteur x par la loi externe* $[(\alpha * \beta) \bullet x]$

revient à

- *multiplier scalairement le vecteur x et avec le premier scalaire α* $[\alpha \bullet x]$
- *puis multiplier scalairement ce vecteur résultant avec le deuxième scalaire β* $[\beta \bullet (\alpha \bullet x)]$

On remarque que ces deux propriétés ne sont pas équivalentes. Dans un module à gauche, le vecteur x est composé d'abord avec β puis avec α, tandis que dans un module à droite, le vecteur x est composé d'abord avec le scalaire α puis par le scalaire β. Comme nous n'avons pas supposé que l'anneau K était commutatif, $\alpha * \beta$ n'est pas obligatoirement égal à $\beta * \alpha$ et donc les premières propriétés respectives des deux définitions sont fondamentalement différentes. Il faut donc veiller à ne pas confondre les deux définitions.

2. La deuxième propriété signifie que, dans un K-module (à droite ou à gauche),

composer par la loi externe un vecteur $x \in M$ avec le neutre de l'anneau des scalaires ne change pas le vecteur x.

3. La troisième propriété dit que, dans un K-module à droite ou à gauche

- *composer deux vecteurs entre eux par la loi sur M* $[x\#y]$
- *puis composer par la loi externe le vecteur résultant avec un scalaire α* $[\alpha \bullet (x\#y)]$

donne le même résultat que

- *multiplier scalairement le vecteur x et le scalaire α* $[\alpha \bullet x]$
- *d'autre part, multiplier scalairement le vecteur y avec ce même scalaire α* $[\alpha \bullet y]$
- *enfin composer par la loi sur M les deux vecteurs résultants entre eux* $[(\alpha \bullet x)\#(\alpha \bullet y)]$

4. Enfin, la quatrième propriété signifie que dans un K-module à droite ou à gauche

- *composer deux scalaires entre eux par la première loi sur* K $[\alpha + \beta]$
- *puis multiplier scalairement le vecteur* x *et ce résultat scalaire* $[(\alpha + \beta) \bullet x]$

revient à

- *multiplier scalairement le vecteur* x *et le scalaire* α $[\alpha \bullet x]$
- *d'autre part, multiplier scalairement le même vecteur* x *avec le scalaire* β $[\beta \bullet x]$
- *enfin composer par la loi interne sur* M *les deux vecteurs résultants* $[(\alpha \bullet x)\#(\beta \bullet x)]$

Quelques améliorations de notations

Dans la littérature, on trouvera souvent les définitions de module à gauche et à droite présentées un peu différement que ci-dessus. Pour des raisons que nous expliciterons, les conventions utilisées par les auteurs sont plus commodes à l'usage. C'est pourquoi nous consacrons à présent un paragraphe particulier pour introduire unes à unes les formulations des définitions qu'ils utilisent. Nous attirons l'attention sur le fait que ces différences de formulation sont uniquement des conventions d'écriture et ne changent en rien la signification des définitions.

Commentaires didactiques :
Les conventions que les auteurs ont l'habitude d'employer, bien que plus commodes, auraient vraissemblablement été à l'origine de confusions chez les étudiants si nous les avions introduites directement. C'est pourquoi nous préférons introduire progressivement ces changements d'écriture.

Le premier changement concerne la notation de la loi externe lorsqu'on définit un module à droite. Les raisons de ce changement sont explicitées dans le texte ci-dessous. Si nous avions introduit cette notation dès le départ, faire le parallèle entre les définitions de modules à gauche et à droite aurait peut-être été moins évident pour les étudiants.

Le deuxième changement concerne les symboles utilisés pour noter les différentes lois de composition. Les symboles que nous avons choisis dans un but didactique ne sont pas ceux utilisés habituellement. Nous opérons donc un changement de notation en le précisant à chaque fois en français. Enfin, nous réécrivons les définitions de module à droite et à gauche dans ces nouvelles notations.

Le premier changement de notation se situe au niveau de la définition de module à droite uniquement.

Pour des questions de commodité, on choisit d'utiliser une notation différente pour la loi de composition externe, lorsque l'on définit un module à droite.

Soit $\{K, +, *\}$ l'anneau de base et $\{M, \#\}$ un groupe commutatif.
On munit le groupe commutatif M de la loi de composition ***externe*** et partout définie $\bullet$, mais cette fois, nous la noterons de la manière suivante :

$$\begin{array}{rccc} \bullet : & K \times M & \longrightarrow & M \\ & (\lambda, x) & \mapsto & x \bullet \lambda. \end{array}$$

Dans ce cas, la définition de module à droite s'écrit de la manière suivante.

Définition 2.1.3 (Module à droite)
On appelle **module à droite sur l'anneau K**, ou encore **K-module à droite**, le triplet $\{M, \#, \bullet\}$ dont les éléments vérifient :

1. $\forall\, \alpha, \beta \in K,\ \forall\, x \in M,$ $\quad x \bullet (\alpha * \beta) = (x \bullet \alpha) \bullet \beta$
2. $\forall\, x \in M,$ $\quad x \bullet \mathbf{1} = x$
3. $\forall\, \alpha \in K,\ \forall\, x, y \in M,$ $\quad (x \# y) \bullet \alpha = (x \bullet \alpha) \# (y \bullet \alpha)$
4. $\forall\, \alpha, \beta \in K,\ \forall\, x \in M,$ $\quad x \bullet (\alpha + \beta) = (x \bullet \alpha) \# (x \bullet \beta)$

Nous n'avons donc pas changé le sens de la définition de module à droite, seulement sa notation.

En effet, la première propriété de la définition, dans un module à droite signifie que

Prendre deux scalaires dans K, un premier α et un deuxième β ,

- *les composer entre eux par la deuxième loi sur K* $\quad [\alpha * \beta]$
- *composer ce résultat scalaire avec un vecteur x par la loi externe* $\quad [x \bullet (\alpha * \beta)]$

est équivalent à

- *multiplier scalairement le vecteur x et le* **premier scalaire α** $\quad [x \bullet \alpha]$
- *puis multiplier scalairement ce résultat avec* **le deuxième scalaire β** $\quad [(x \bullet \alpha) \bullet \beta]$

La signification des trois autres propriétés de la définition de module à droite est également inchangée.

La raison de ce changement est simple : l'écriture de la première propriété de la définition 2.1.2 est plus commode lorsqu'on choisit la notation $x \bullet \alpha$.

En effet, avec le choix précédent de la loi externe, notée $\alpha \bullet x$, la première propriété qui consiste à composer le vecteur x, d'abord avec le scalaire α, puis par le scalaire β, s'écrivait en inversant l'ordre des scalaires d'un membre de l'égalité à l'autre : $(\alpha * \beta) \bullet x = \beta \bullet (\alpha \bullet x)$.
La notation de cette propriété est un peu contre-intuitive.

Ce problème disparait lorsque l'on utilise la nouvelle notation de la loi de composition $x \bullet \alpha$.
En effet, cette propriété s'écrit maintenant : $x \bullet (\alpha * \beta) = (x \bullet \alpha) \bullet \beta$.
On observe que l'ordre des scalaires est gardé d'un membre de l'égalité à l'autre; il suffit de décaler les parenthèses, ce qui est plus pratique.

Par contre dans un module à gauche, dans la première propriété de la définition 2.1.1, c'est le contraire, le vecteur x est composé d'abord avec β puis avec α. Avec le choix précédent d'écriture de la loi externe $\alpha \bullet x$, on garde l'ordre des scalaires d'un membre de l'égalité à l'autre : $(\alpha * \beta) \bullet x = \alpha \bullet (\beta \bullet x)$.
C'est donc la notation de la loi externe $\alpha \bullet x$ qui reste la plus commode dans le cas d'un module à gauche.

Le deuxième changement de notations se situe au niveau des lois de composition, dans les modules à gauche aussi bien que dans les modules à droite.

En effet, en pratique, on constate que les notations $\#$, $\bullet$ et $*$ sont relativement lourdes à utiliser. C'est pourquoi, dans la plupart des ouvrages traitant de ce sujet, on trouvera les changements de convention d'écriture suivants.

- En premier lieu, on prend l'habitude de noter **la loi de composition interne $\#$ sur M** par $+$ et on la définit comme **l'addition des vecteurs**. Il faut veiller à ne pas confondre cette loi d'addition des vecteurs avec la loi de composition interne $+$ **définie sur l'anneau K** que l'on appellera dorénavant **l'addition des scalaires**. En effet, malgré leur notation identique, ces deux lois ne sont pas les mêmes car définies sur des ensembles différents.

- En deuxième lieu, on choisit **d'omettre le symbole $*$** qui représentait la loi de composition interne sur K. Cette loi, que l'on définit comme **la multiplication des scalaires**, associe à deux scalaires un nouveau scalaire.
  De la même manière, on prend la convention **d'omettre le symbole $\bullet$** qui représentait la loi de composition externe. Cette loi, que nous avons appelée **la multiplication scalaire**, associe à un scalaire et à un vecteur un nouveau vecteur.

Avec ces nouvelles conventions d'écriture, réécrivons les définitions de modules à gauche et de modules à droite.

Définition 2.1.4 (Module à gauche)
Soient $\{K,+,\cdot\}$ un anneau et $\{M,+\}$ un groupe commutatif.
On appelle **module à gauche sur l'anneau K**, ou encore **K-module à gauche**, le triplet $\{M,+,\cdot\}$ où la loi de composition externe est une application donnée par

$$\begin{array}{rccc} \cdot : & K \times M & \longrightarrow & M \\ & (\lambda, x) & \mapsto & \lambda x, \end{array}$$

et dont les éléments vérifient :

1. $\forall\ \alpha,\beta \in K,\ \forall\ x \in M,$ $\quad (\alpha\beta)x = \alpha(\beta x)$
2. $\forall\ x \in M,$ $\quad \mathbf{1}\ x = x$
3. $\forall\ \alpha \in K,\ \forall\ x,y \in M,$ $\quad \alpha(x+y) = \alpha x + \alpha y$
4. $\forall\ \alpha,\beta \in K,\ \forall\ x \in M,$ $\quad (\alpha+\beta)x = \alpha x + \beta x$

Définition 2.1.5 (Module à droite)
Soient $\{K,+,\cdot\}$ un anneau et $\{M,+\}$ un groupe commutatif.
On appelle **module à droite sur l'anneau K**, ou encore **K-module à droite**, le triplet $\{M,+,\cdot\}$ où la loi de composition externe est une application donnée par

$$\begin{array}{rccc} \cdot : & K \times M & \longrightarrow & M \\ & (x, \lambda) & \mapsto & x\lambda, \end{array}$$

et dont les éléments vérifient :

1. $\forall\ \alpha,\beta \in K,\ \forall\ x \in M,$ $\quad x(\alpha\beta) = (x\alpha)\beta$
2. $\forall\ x \in M,$ $\quad x\ \mathbf{1} = x$
3. $\forall\ \alpha \in K,\ \forall x,y \in M,$ $\quad (x+y)\alpha = x\alpha + y\alpha$
4. $\forall\ \alpha,\beta \in K,\ \forall\ x \in M,$ $\quad x(\alpha+\beta) = x\alpha + x\beta$

Avec ces nouvelles notations, présentons maintenant quelques propriétés importantes des modules.

2.1.2 Relations fondamentales dans un module

Les propriétés qui définissent un K-module à gauche impliquent les relations importantes suivantes.

Proposition 2.1.1 (Relations fondamentales dans un module)
Soit M un K-module à gauche. Alors, les relations suivantes sont vérifiées :

1. $\forall\, \lambda \in K,\ \lambda 0_M = 0_M$
2. $\forall\, x \in M,\ 0_K x = 0_M$

Nous pouvons bien sûr démontrer les relations similaires dans le cas d'un K-module à droite.

Preuve :

1. Soit $\lambda \in K$. Observons que, pour tout x dans M :

$$\begin{aligned} \lambda 0_M + \lambda x = \lambda(0_M + x) &\Leftrightarrow \lambda 0_M + \lambda x = \lambda x \\ &\Leftrightarrow \lambda 0_M + \lambda x - \lambda x = \lambda x - \lambda x \\ &\Leftrightarrow \lambda 0_M = 0_M. \end{aligned}$$

2. Soit $x \in M$. La deuxième égalité provient du fait que

$$0_K x + 1x = (0_K + 1)x = 1x = x$$

et d'autre part

$$0_K x + 1x = 0_K x + x.$$

Donc finalement, on obtient

$$0_K x + x = x.$$

L'égalité précédente est équivalente à

$$0_K x + x - x = x - x$$

ou encore à

$$0_K x + 0_M = 0_M.$$

Finalement, on obtient

$$0_K x = 0_M,$$

ce qui termine cette preuve. ∎

2.1.3 Parallélisme entre modules à droite et modules à gauche

Le raisonnement qui suit est particulièrement important et intéressant car il illustre le fait que les théories des modules à gauche et des modules à droite sont entièrement parallèles.

Considérons un K-module à droite M. Grâce à quelques constructions spécifiques, montrons que l'on peut envisager M comme un K^{op}-module à gauche, où K^{op} est l'anneau opposé de K défini comme suit.

Définition 2.1.6 (L'anneau opposé de K)
Soit $\{K, +, \cdot\}$ un anneau arbitraire et M un module à droite sur K.
L'anneau opposé de K est le nouvel anneau $\{K^{op}, +, \circ\}$ construit comme suit :

- *les éléments de l'anneau K^{op} sont identiques à ceux de l'anneau K. Autrement dit, les scalaires de K^{op} sont ceux de K,*
- *la loi $+$ d'addition des scalaires sur K^{op} est l'addition sur K,*
- *par contre, la multiplication des scalaires $\circ$ sur K^{op} est donnée par*

$$a \circ b \ = \ ba,$$

où a et b sont des scalaires de l'ensemble $K = K^{op}$ et la multiplication utilisée dans le second membre de cette égalité est la multiplication des scalaires sur K.

Vérifions, sous forme d'exercice, que le triplet $\{K^{op}, +, \circ\}$ ainsi défini est bien un anneau.

Question : $\{K^{op}, +, \circ\}$ est-il un anneau ?

Résolution

Vérifions que $\{K^{op}, +, \circ\}$ est bien un anneau en examinant les propriétés de la définition 1.2.1.

1. $\{K^{op}, +\}$ est un groupe commutatif car $\{K^{op}, +\} = \{K, +\}$ et $\{K, +\}$ est un groupe commutatif.

2. Associativité : $\forall\, x, y, z \in K^{op}$,

$$x \circ (y \circ z) = x \circ (zy) = \underbrace{(zy)x = z(yx)}_{\text{par associativité de la multiplication dans } K} = z(x \circ y) = (x \circ y) \circ z$$

3. Existence d'un élément neutre :

$$\exists\, e \in K^{op},\ \forall x \in K^{op}, \quad e \circ x = xe = x = ex = x \circ e.$$

On remarque immédiatement que si $\mathbf{1}$ est le neutre de l'anneau K, alors il est aussi le neutre de K^{op}.

4. Distributivité de $\circ$ par rapport à $+$: $\forall\, x, y, z \in K^{op}$,

$$x \circ (y+z) = \underbrace{(y+z)x \;=\; yx + zx}_{\text{distributivité de } \cdot \text{ par rapport à } + \text{ dans } K} = x \circ y + x \circ z$$

et $$(y+z) \circ x = \underbrace{x(y+z) \;=\; xy + xz}_{\text{distributivité de } \cdot \text{ par rapport à } + \text{ dans } K} = y \circ x + z \circ x.$$

En conclusion, $\{K^{op}, +, \circ\}$ est bien un anneau.

Construction d'un K^{op}-module à gauche

Définissons une loi de composition externe comme suit :

$$\begin{aligned} \circ : \quad K^{op} \times M &\longrightarrow M \\ (\lambda, x) &\mapsto \lambda \circ x = x\lambda, \end{aligned}$$

où la multiplication scalaire utilisée dans le second membre de cette égalité est la multiplication scalaires sur K.

Dans ce cas, le groupe commutatif $\{M, +\}$, muni de l'application ci-dessus, est un K^{op}-module à gauche.

Vérifions, sous forme d'exercice, que le triplet $\{M, +, \circ\}$ ainsi défini est bien un K^{op}-module à gauche.

Question : $\{M, +, \circ\}$ est-il un K^{op}-module à gauche ?

Résolution

Vérifions les propriétés de la définition 2.1.4 :

1. $\forall\, \alpha, \beta \in K,\ \forall\, x \in M,$

$$\alpha \circ (\beta \circ x) = (\beta \circ x)\alpha = \underbrace{(x\beta)\alpha \;=\; x(\beta\alpha)}_{\text{Associativité mixte dans } M} = (\beta\alpha) \circ x = (\alpha \circ \beta) \circ x,$$

2. $\forall\, x \in M,$

$$\mathbf{1} \circ x = x\mathbf{1} = x,$$

3. $\forall\, \alpha \in K,\ \forall\, x, y \in M,$

$$\alpha \circ (x+y) = \underbrace{(x+y)\alpha \;=\; x\alpha + y\alpha}_{\text{Double distributivité dans } M} = \alpha \circ x + \alpha \circ y,$$

4. $\forall\, \alpha, \beta \in K,\ \forall\, x \in M,$

$$(\alpha+\beta) \circ x = \underbrace{x(\alpha+\beta) \;=\; x\alpha + x\beta}_{\text{Double distributivité dans } M} = \alpha \circ x + \beta \circ x.$$

En conclusion, M est bien un K^{op}-module à gauche.

Conclusion

Tout K-module à droite M peut donc être considéré comme un K^{op}-module à gauche. Ce raisonnement nous permet de montrer que, en passant par l'anneau opposé, on peut appliquer des résultats établis dans le cadre des modules à droite directement aux modules à gauche (et vice-versa). Les théories des K-modules à gauche et des K-modules à droite sont donc totalement parallèles. Pour éviter de refaire le travail inutilement, nous choisissons de travailler uniquement avec des K-modules à gauche.

Remarque

Comme nous venons de le montrer, les théories que l'on construit dans les K-modules à droite ont leur équivalent dans les K-modules à gauche. Par la suite, nous choisissons de travailler dans **les modules à gauche** plutôt que dans les modules à droite. Il y a en fait une raison didactique simple à ce choix.

Nous avons vu que, avec les conventions d'écriture de la loi externe choisies à la page 41 dans les définitions 2.1.4 et 2.1.5, les notations sont plus simples et plus intuitives lorsqu'on est dans un module à gauche. Par exemple, considérons un $\mathbb{Z}$-module contenant un vecteur x quelconque. Nous avons l'habitude d'écrire $3x$ plutôt que $x3$ lorsqu'on compose le vecteur x avec le scalaire 3 par la loi de composition externe. Or, ce choix d'écriture de la loi externe est celui que nous avons convenu, par commodité, pour définir un de module à gauche.

2.1.4 Définition d'espace vectoriel

A présent intéressons-nous à un cas particulier de module en imposant que l'anneau K soit un corps. Nous obtenons la définition suivante.

Définition 2.1.7 (Espace vectoriel à gauche (à droite))

Lorsque l'anneau de base K est un corps, un K-module à gauche (à droite) est appelé **espace vectoriel à gauche (à droite) sur K**.

Remarque

Si K est un champ, un K-module est simplement appelé **espace vectoriel** sur K (puisque la distinction entre espace vectoriel à gauche et à droite n'a plus lieu d'être si K est commutatif). On observe que *le concept d'espace vectoriel*, est en fait ***un cas particulier*** **du concept de module.**

2.1.5 Exemples de modules et espaces vectoriels

Dans les deux exemples suivants, nous nous intéressons aux ensembles de matrices et essayons de construire des modules de matrices. Le premier, plus théorique, introduit des modules de matrices en général. Le deuxième est un exercice résolu qui présente un exemple particulier de module de matrices sur l'anneau des entiers muni de lois non usuelles.

Objectif de l'exemple 2.1.1 :
Cet exemple permet à l'étudiant d'accrocher le concept de module à des ensembles rencontrés auparavant : les ensembles de matrices. Ainsi l'étudiant ne doit pas faire face à d'autres difficultés que celles liées au nouveau concept de module. Ensuite, si K est un anneau, les K-modules de matrices permettent d'illustrer exclusivement le concept de module car ils ne peuvent généralement pas être considérés comme des espaces vectoriels.
Dans cet exemple, nous considérons également le cas particulier où K est l'anneau des matrices (avec les lois matricielles usuelles). Cela permet de montrer qu'il est indispensable de faire la distinction entre un K-module à gauche et un K-module à droite car la multiplication matricielle n'est pas commutative.

Comme les étudiants ont eu l'occasion de travailler des exemples semblables dans le cadre des espaces vectoriels en première année de bachelier, nous nous permettons de présenter l'exemple qui suit de manière plus théorique. Cela permet de rester général et de couvrir ainsi un maximum de cas.

Exemple 2.1.1
Soit K un anneau arbitraire. Considérons $M_{m,n}(K)$ l'ensemble des matrices à m lignes, n colonnes et à éléments dans K.

Le groupe des matrices $\{M_{m,n}(K), +\}$, où $+$ désigne la loi usuelle d'addition matricielle définie dans l'exemple 1.2.1, peut être considéré comme un K-module à gauche si on choisit comme loi de composition externe l'application :

$$\begin{aligned} \cdot : \quad & K \times M_{m,n}(K) \longrightarrow M_{m,n}(K) \\ & (\lambda, A) \mapsto \lambda A, \end{aligned} \tag{2.1}$$

où, si a_{ij} désigne l'élément de A situé à la $i^{\text{ème}}$ ligne et à la $j^{\text{ème}}$ colonne, on définit

$$(\alpha A)_{ij} = \alpha a_{ij}, \qquad i = 1, \ldots, n \ , \ j = 1, \ldots, m \quad \text{et } \alpha \in K.$$

Si K est un corps, le triplet $\{M_{m,n}(K), +, \cdot\}$ est un espace vectoriel à gauche.

Par contre, si on définit la loi de composition externe comme suit :

$$\begin{aligned} \cdot : \quad & K \times M_{m,n}(K) \longrightarrow M_{m,n}(K) \\ & (\lambda, A) \mapsto A\lambda, \end{aligned} \tag{2.2}$$

où, si a_{ij} désigne l'élément de A situé à la $i^{\text{ème}}$ ligne et à la $j^{\text{ème}}$ colonne, on définit

$$(A\alpha)_{ij} = a_{ij}\alpha, \qquad i = 1, \ldots, n \ , j = 1, \ldots, m \quad \text{et } \alpha \in K,$$

le triplet $\{M_{m,n}(K), +, \cdot\}$ est un K-module à droite.

Si K est un anneau commutatif, comme par exemple l'anneau des entiers $\mathbb{Z}$, alors, $\{M_{m,n}(K), +, \cdot\}$ est un K-module.

On peut particulariser la situation exposée ci-dessus en choisissant pour l'anneau K l'anneau des matrices présenté dans l'exemple 1.2.1 et en définissant comme loi de composition externe suivante :

$$\begin{aligned} \cdot : \quad M_m(K) \times M_{m,n}(K) &\longrightarrow M_{m,n}(K) \\ (A, B) &\mapsto A \cdot B = AB, \end{aligned}$$

où $\cdot$ désigne la multiplication matricielle usuelle. Cette définition permet de considérer $M_{m,n}(K)$ comme un $M_m(K)$-module à gauche.

A l'inverse, si on choisit comme loi de composition externe l'application

$$\begin{aligned} \cdot : \quad M_{m,n}(K) \times M_n(K) &\longrightarrow M_{m,n}(K) \\ (A, B) &\mapsto A \cdot B = AB, \end{aligned}$$

on considère $M_{m,n}(K)$ comme un $M_n(K)$-module à droite.

Comme la multiplication matricielle usuelle n'est pas une loi commutative, le triplet $\{M_{m,n}(K), +, \cdot\}$ ne peut pas être considéré comme un module sur $M_n(K)$ ou $M_m(K)$.

Ici, exiger que K soit un corps ne suffit pas pour que le triplet $\{M_{m,n}(K), +, \cdot\}$ soit un espace vectoriel à gauche sur $M_m(K)$ ou un espace vectoriel à droite sur $M_n(K)$.
En effet, pour avoir un espace vectoriel, il faut non seulement que K soit un corps mais aussi que l'ensemble des matrices carrées muni des lois d'addition et multiplication matricielle usuelles soit un corps. Or, ce n'est pas le cas en général, puisqu'il existe des matrices qui ne sont pas inversibles dans K. Une manière de faire de cet ensemble un corps serait donc de restreindre l'ensemble des matrices carrées aux matrices carrées inversibles et de munir cet ensemble des mêmes lois de composition (restreintes au nouvel ensemble).

Objectif de l'exemple 2.1.2 :
Cet exemple contient deux parties distinctes et se présente sous la forme d'un exercice résolu. Il permet à l'étudiant de manipuler les définitions de module et d'espace vectoriel de manière plus calculatoire.

Dans la première partie, l'exercice proposé est une application plus concrète de la première partie de l'exemple précédent (exemple 2.1.1). Néanmoins, la structure de la loi de composition externe a été consciemment choisie un peu différente de cet exemple, afin de susciter la réflexion et la vigilence chez l'étudiant. De même, l'anneau $\mathbb{Z}$ d'une loi de multiplication un peu différente de la multiplication usuelle.

Le deuxième partie de cet exemple comporte une difficulté supplémentaire car on ne considère plus le module formé de toutes les matrices à éléments réels, mais seulement quatre ensembles de matrices particuliers, munis de la multiplication usuelle. Il faut donc penser à vérifier que ces matrices munies de cette loi de composition forme un groupe commutatif, ce qui est le cas. Par contre, on découvre que les conditions de la définition de module ne sont pas vérifiées, ce qui oblige l'étudiant à être vigilant jusqu'au bout de l'exercice.

Exemple 2.1.2

1. Considérons dans un premier temps les deux ensembles suivants

   - l'ensemble des entiers $\mathbb{Z}$, muni de la loi d'addition usuelle des entiers $(+)$ et de la loi $* : \mathbb{Z} \to \mathbb{Z}$, $(\alpha, \beta) \mapsto \alpha * \beta = \frac{\alpha.\beta}{2} = \frac{\alpha\beta}{2}$ (où $.$ désigne la multiplication usuelle des entiers).
   - $M_2(\mathbb{R})$, l'ensemble des matrices 2×2 à coefficients réels. Munissons cet ensemble de la loi usuelle d'addition des matrices $(+)$.

   Enfin, construisons une loi qui relie ces deux ensembles comme suit

$$\begin{array}{rccl} \circ : & \mathbb{Z} \times M_2(\mathbb{R}) & \longrightarrow & M_2(\mathbb{R}) \\ & (\lambda, A) & \mapsto & \lambda \circ A = \frac{1}{2}\lambda \bullet A = \frac{1}{2}\lambda A. \end{array}$$

   où $\bullet$ est la multiplication scalaire définie en (2.1).

   Question 1

   Le triplet $\{M_2(\mathbb{R}), +, \circ\}$ forme-t-il un $\mathbb{Z}$-module à gauche ? Est-il un $\mathbb{Z}$-module à droite ?
   Peut-on dire que le triplet $\{M_2(\mathbb{R}), +, \circ\}$ forme un espace vectoriel (à droite et/ou à gauche) sur $\mathbb{Z}$?
   Sinon, que pourrait-on changer au niveau de l'anneau de base pour que le triplet $\{M_2(\mathbb{R}), +, \circ\}$ soit un espace vectoriel ?

2. Considérons dans un deuxième temps les ensembles particuliers suivants

- l'ensemble des entiers $\mathbb{Z}$, muni de la loi d'addition usuelle des entiers $(+)$ et de la loi $* : \mathbb{Z} \to \mathbb{Z},\ (\alpha, \beta) \mapsto \frac{\alpha.\beta}{2} = \frac{\alpha\beta}{2}$ (où $.$ désigne la multiplication usuelle des entiers), comme dans l'exemple précédent.
- Un autre ensemble M muni de la loi usuelle de multiplication matricielle $\cdot$ où $M = \{\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}\}$ avec

$$\mathcal{A} = \left\{ \begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix},\ a \in \mathbb{R}_0 \right\} \quad , \mathcal{B} = \left\{ \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix},\ b \in \mathbb{R}_0 \right\} \quad ,$$

$$\mathcal{C} = \left\{ \begin{pmatrix} 0 & -c \\ c & 0 \end{pmatrix},\ c \in \mathbb{R}_0 \right\} \quad , \mathcal{D} = \left\{ \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix},\ d \in \mathbb{R}_0 \right\}.$$

Enfin, considérons la même loi externe que dans l'exemple précédent

$$\begin{array}{rccl} \circ : & \mathbb{Z} \times M & \longrightarrow & M \\ & (\lambda, P) & \mapsto & \lambda \circ P = \frac{1}{2}\lambda \bullet P = \frac{1}{2}\lambda P. \end{array}$$

où $\bullet$ est la multiplication scalaire définie en (2.1).

Question 2

Le triplet $\{M, \cdot, \circ\}$ forme-t-il un $\mathbb{Z}$-module à gauche ? Est-il un $\mathbb{Z}$-module à droite ?

Résolution

Question 1

Montrons que le triplet $\{M_2(\mathbb{R}), +, \circ\}$ forme un $\mathbb{Z}$-module à gauche.

Pour ce faire, nous devons tout d'abord montrer que $\{M_2(\mathbb{R}), +\}$ est un groupe commutatif et que $(\mathbb{Z}, +, *)$ est un anneau. Enfin, il restera à montrer que le triplet $\{M_2(\mathbb{R}), +, \circ\}$ vérifie les conditions de la définition 2.1.4.

1. $\{M_2(\mathbb{R}), +\}$ est un groupe commutatif : c'est immédiat.
En effet, on sait par l'exemple 1.1.4 que l'addition matricielle est associative, commutative, admet un élément neutre (la matrice nulle) et vérifie la symétrisabilité.

2. $\{\mathbb{Z}, +, *\}$ est un anneau où le neutre de la loi $*$ est 2.

Cette vérification est laissée au soin du lecteur.

3. $\{M_2(\mathbb{R}), +, \circ\}$ vérifie les conditions de la définition 2.1.4.

- **[Associativité mixte]** $\forall\ \alpha, \beta \in \mathbb{Z},\ \forall\ A \in M,\ (\alpha * \beta) \circ A \stackrel{?}{=} \alpha \circ (\beta \circ A)$.
  Oui, car
  $$(\frac{\alpha\beta}{2}) \circ A = \alpha \circ (\frac{1}{2}\beta A)$$
  $$\Leftrightarrow \frac{1}{2}\frac{\alpha\beta}{2}A = \frac{1}{2}\alpha(\frac{1}{2}\beta A)$$
  $$\Leftrightarrow \frac{\alpha\beta}{4}A = \frac{1}{4}\alpha\beta A.$$

- $\forall\ A \in M,\ 2 \circ A \stackrel{?}{=} A$.
  Oui, car
  $$2 \circ A = A \Leftrightarrow \frac{1}{2} \cdot 2A = A.$$

- **[Double distributivité]** $\forall\ \alpha \in \mathbb{Z},\ \forall\ A, B \in M,\ \alpha \circ (A + B) \stackrel{?}{=} (\alpha \circ A) + (\alpha \circ B)$.
  Oui, car l'égalité
  $$\frac{1}{2}\alpha(A + B) = \frac{1}{2}\alpha A + \frac{1}{2}\alpha B$$
  est toujours vérifiée dans $M_2(\mathbb{R})$.

- **[Double distributivité]** $\forall\ \alpha, \beta \in \mathbb{Z},\ \forall\ A \in M,\ (\alpha + \beta) \circ A \stackrel{?}{=} (\alpha \circ A) + (\beta \circ A)$.
  Oui, car l'égalité
  $$\frac{1}{2}(\alpha + \beta)A = (\frac{1}{2}\alpha A) + (\frac{1}{2}\beta A)$$
  est toujours vérifiée dans $M_2(\mathbb{R})$.

En conclusion, le triplet $\{M_2(\mathbb{R}), +, \circ\}$ forme bien un $\mathbb{Z}$-module à gauche.

Comme $\mathbb{Z}$ est commutatif, le triplet $\{M_2(\mathbb{R}), +, \circ\}$ est aussi un $\mathbb{Z}$-module à droite.

4. Le triplet $\{M_2(\mathbb{R}), +, \circ\}$ est-il un espace vectoriel sur $\mathbb{Z}$?

Pour montrer que $\{M_2(\mathbb{R}), +, \circ\}$ est un espace vectoriel, il faut vérifier que l'anneau de base $\{\mathbb{Z}, +, *\}$ est un corps (définition 1.2.4).

1. $\{\mathbb{Z}, +, *\}$ est un anneau ***non trivial*** puisque le neutre de l'addition (0) est différent du neutre de $*$ (2).

2. **[Symétrisabilité]** $\forall\ x \in \mathbb{Z} \setminus \{0\},\ \exists\ y \in \mathbb{Z},\quad x * y = 2 = y * x$
   Or, cette égalité peut s'écrire comme suit, par la définition de $*$:
   $$\frac{xy}{2} = 2 = \frac{yx}{2}$$
   $$\Leftrightarrow xy = 4 = yx.$$
   Donc, quel que soit $x \in \mathbb{Z} \setminus \{0\}$, son symétrique est l'élément $y = \frac{4}{x}$. Mais, on remarque que y est une fraction, et donc n'appartient pas obligatoirement à $\mathbb{Z}$. Il n'y a donc pas toujours de symétrique pour x.

En conclusion, $\{\mathbb{Z}, +, *\}$ n'est pas un corps et donc le triplet $\{M_2(\mathbb{R}), +, \circ\}$ n'est pas un espace vectoriel sur $\mathbb{Z}$.

Une solution pour faire de $\{M_2(\mathbb{R}), +, \circ\}$ un espace vectoriel serait de choisir comme anneau de base l'ensemble $\mathbb{Q}$, muni des mêmes lois de composition $+$ et $*$ définies cette fois sur $\mathbb{Q}$. On peut vérifier facilement que $\mathbb{Q}$ est un champ et donc que le triplet $\{M_2(\mathbb{R}), +, \circ\}$ est un espace vectoriel (à gauche et à droite) sur $\mathbb{Q}$.

Question 2

Il faut montrer que le triplet $\{M, \cdot, \circ\}$ forme un $\mathbb{Z}$-module.

Comme nous savons déjà par la question 1 que $\{\mathbb{Z}, +, *\}$ est un anneau, il reste à vérifier que $\{M, \cdot\}$ est un groupe commutatif. Ensuite, nous vérifierons si le triplet $\{M, \cdot, \circ\}$ satisfait aux conditions de la définition 2.1.4.

1. $\{M, \cdot\}$ est un groupe commutatif

. **[Associativité]** C'est immédiat puisque la multiplication matricielle est associative.

. **[L'élément neutre]** $\exists\, I \in M,\ \forall\, A \in M,\ A \cdot I = A = I \cdot A$

On vérifie facilement que la matrice identité $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est le neutre pour cette loi. De plus, $\mathbb{I}$ est une matrice de M puisque elle appartient au sous-ensemble $\mathcal{D}$.

. **[Symétrisabilité]** $\forall\, A \in M,\ \exists\, A' \in M,\ A \cdot A' = \mathcal{I} = \mathcal{A}' \cdot \mathcal{A}$.

Considérons une matrice quelconque de chaque sous-ensemble $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ et essayons de trouver son symétrique dans M.

1. Soit $\begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix}$ une matrice de $\mathcal{A}$ avec $a \in \mathbb{R}_0$.

   Alors, on peut vérifier que le symétrique de cette matrice est la matrice $\begin{pmatrix} -\frac{1}{a} & 0 \\ 0 & -\frac{1}{a} \end{pmatrix}$

   qui existe toujours puisque $\mathbb{R}$ est un corps et que a est non nul.
   De plus, cette matrice appartient bien à M puisqu'elle appartient au sous-ensemble $\mathcal{A}$.

2. Soit $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$ une matrice de $\mathcal{B}$ avec $b \in \mathbb{R}_0$.

   Alors, le symétrique de cette matrice est la matrice $\begin{pmatrix} 0 & -\frac{1}{b} \\ \frac{1}{b} & 0 \end{pmatrix}$. Cette matrice, qui existe toujours dans $\mathbb{R}$ puisque $b \neq 0$, appartient bien à M puisqu'elle est dans le sous-ensemble $\mathcal{C}$.

Pour les matrices des sous-ensembles $\mathcal{C}$ et $\mathcal{D}$, on procède de manière similaire.

. **[Commutativité]** $\forall\, A, B \in M,\ A \cdot B = B \cdot A$.

En choisissant deux matrices de M, dans des sous-ensembles différents, on peut montrer qu'elles vérifient la propriété de la commutativité.

Par exemple, en prenant une matrice $\begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix}$ dans $\mathcal{A}$ et une matrice $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$ dans $\mathcal{B}$ avec $(a, b \in \mathbb{R}_0)$, la propriété de commutativité s'écrit :

$$\begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix} \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} \begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix}$$

ou encore

$$\begin{pmatrix} 0 & (-a)b \\ (-a)(-b) & 0 \end{pmatrix} = \begin{pmatrix} 0 & b(-a) \\ (-b)(-a) & 0 \end{pmatrix}.$$

Or, cette dernière égalité est toujours vérifiée puisque $\mathbb{R}$ est un corps commutatif.

Les autres cas se vérifient de manière similaire.

2.2 Sous-modules et sous-espaces vectoriels

Intéressons-nous à présent à des parties particulières des modules que nous appelerons des sous-modules.
Pour présenter la définition de sous-module, nous rappelons tout d'abord la notion de sous-groupe.

Définition 2.2.1 (Sous-groupe)
Soit $\{G, +\}$ un groupe. **Un sous-groupe de G** est une partie de G qui est encore un groupe.
Traduisons cette définition en termes mathématiques.

Une partie H de G est **un sous-groupe de G** si elle vérifie les propriétés suivantes :

1. $\forall\, x, y \in H, \quad x + y \in H,$
2. l'élément neutre e de G est dans H,
3. $\forall\, x \in H, \quad -x \in H.$

En pratique, pour vérifier que H est un sous-groupe de G, on utilise souvent la propriété qui suit.

Proposition 2.2.1 (Caractérisation d'un sous-groupe)
Soient $\{G, +\}$ un groupe et H une partie de G.
Alors, H est un sous-groupe de G si et seulement si

1. *H est non vide*
2. *$\forall\, x, y \in H,\ x - y \in H.$*

Cette proposition ne sera pas démontrée ici mais le lecteur pourra trouver une preuve à la page 118 de [3].

Nous pouvons à présent définir un sous-module.

Définition 2.2.2 (Sous-modules)
Soit M un K-module à gauche.
On appelle **sous-module de M** toute partie M' de M qui est encore un K-module à gauche.
Si on traduit cette définition en termes mathématiques, on obtient la définition équivalente suivante.

Une partie M' de M est **un sous-module de M** si

1. M' est un sous-groupe du groupe M ;
2. $\forall\, x \in M',\ \forall\, \lambda \in K,\ \lambda x \in M'.$

Lorsque K est un corps, M' sera appelé **sous-espace vectoriel de M**.

Si on considère un K-module à gauche M, alors tous ses sous-modules sont non-vides, car ils contiennent tous le neutre de M. C'est l'objet de la proposition suivante.

Proposition 2.2.2
Soit M un K-module à gauche.
Le neutre de M, noté 0_M, appartient à tous les sous-modules de M.

Preuve : Supposons que M' soit un sous-module de M. D'une part, M' vérifie la deuxième propriété de la définition 2.2.2, à savoir

$$\forall\, x \in M',\ \forall \lambda \in K,\ \lambda x \in M'.$$

En choisissant le cas particulier $\lambda = 0_K$ (le neutre de K), dans la propriété précédente, on observe que le vecteur $0_K x$ appartient à M'. D'autre part, par la deuxième relation de la proposition 2.1.1, on sait que

$$\forall\, x \in M,\ 0_K x = 0_M.$$

Par conséquent, 0_M appartient à M'. ∎

Tout comme pour les sous-groupes, il existe une propriété qui permet de vérifier rapidement si une partie d'un module est un sous-module.

Proposition 2.2.3 (Caractérisation d'un sous-module)
Soient M un module à gauche sur un anneau K et M' une partie de M.
La partie M' est un sous-module de M si et seulement si elle vérifie les deux conditions suivantes :

1. *M' est non vide*[a],
2. $\forall\, \alpha, \beta \in K,\ \forall\, x, y \in M',\qquad \alpha x + \beta y \in M'.$

a. En pratique, pour vérifier cette propriété, on montrera souvent que $0 \in M'$.

Preuve :
Il est évident que la définition 2.2.2 implique cette propriété.
Inversement, supposons que les deux conditions ci-dessus sont vérifiées et montrons que M' satisfait à la définition de sous-module.
En choisissant $\beta = 0$, on obtient la deuxième condition de la définition.
Il reste à montrer que M' est un sous-groupe de M, ce que nous allons faire en utilisant la proposition 2.2.1.
Premièrement, l'ensemble M' est non vide par hypothèse. Deuxièmement, si $x, y \in M$, en prenant $\alpha = 1$ et $\beta = -1$, on obtient que $x - 1y \in M'$. Or, dans un module, l'égalité suivante est toujours vérifiée

$$\forall\, y \in M,\qquad -y = -(1)y.$$

En effet, $(-\mathbf{1})y + y = (-\mathbf{1})y + (+\mathbf{1})y = (-\mathbf{1}+\mathbf{1})y = 0y = 0$, où la dernière égalité est obtenue par la proposition 2.1.1.
Donc, $x - y \in M'$, ce qui clôture cette preuve. ∎

Remarques

1. Soit M un K-module à gauche. Alors, M possède toujours au moins deux sous-modules : $\{0\}$ et M lui-même.
2. Si on suppose que K est un corps, les deux propositions précédentes (propositions 2.2.2 et 2.2.3) peuvent être énoncées et démontrées pour des sous-espaces vectoriels.

A présent, illustrons le concept de sous-module par un exemple.

Exemple 2.2.1
Considérons le $\mathbb{Z}$-module à gauche $\{M_2(\mathbb{R}), +, \circ\}$ défini dans l'exemple 2.1.2 où $+$ est l'addition matricielle usuelle et $\circ$ est la loi

$$\begin{array}{rccl} \circ : & \mathbb{Z} \times M_2(\mathbb{R}) & \longrightarrow & M_2(\mathbb{R}) \\ & (\lambda, A) & \mapsto & \lambda \circ A = \frac{1}{2}\lambda \bullet A = \frac{1}{2}\lambda A. \end{array}$$

Considérons également une partie particulière M' de l'ensemble $M_2(\mathbb{R})$ où M' est l'ensemble des matrices diagonales à éléments dans $\mathbb{R}$:

$$M' = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{avec} \quad a, b \in \mathbb{R} \right\}.$$

Munissons cet ensemble de la loi d'addition matricielle usuelle et de la loi externe suivante :

$$\begin{array}{rccl} \circ : & \mathbb{Z} \times M' & \longrightarrow & M' \\ & (\lambda, A) & \mapsto & \lambda \circ A = \frac{1}{2}\lambda \bullet A = \frac{1}{2}\lambda A. \end{array}$$

où $\bullet$ est la multiplication scalaire définie en (2.1).

Question

Le triplet $\{M', +, \circ\}$ forme-t-il un sous-module de $\{M_2(\mathbb{R}), +, \circ\}$?

Résolution

Vérifions que $\{M', +, \circ\}$ est un sous-module de $\{M_2(\mathbb{R}), +, \circ\}$ en montrant que $\{M', +, \circ\}$ satisfait aux conditions de la proposition 2.2.3.

1. **M' est non vide.**

   En effet, M' est non vide puisque la matrice identité $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartient à M'.

2. $\forall\, \alpha, \beta \in \mathbb{Z},\ \forall\, A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ A' = \begin{pmatrix} a' & 0 \\ 0 & b' \end{pmatrix} \in M',\ \alpha \circ A + \beta \circ A' \in M'.$

   En effet,

$$\alpha \circ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \beta \circ \begin{pmatrix} a' & 0 \\ 0 & b' \end{pmatrix} = \begin{pmatrix} \frac{\alpha a + \beta a'}{2} & 0 \\ 0 & \frac{\alpha b + \beta b'}{2} \end{pmatrix}.$$

   La matrice obtenue est également une matrice diagonale à éléments réels, elle appartient donc à M'.

En conclusion, $\{M', +, \circ\}$ est bien un sous-module de $\{M_2(\mathbb{R}), +, \circ\}$.

Traduction en langage courant de la définition 2.3.1

Soient M et N des modules à gauche sur un même anneau K.
Dire que f est un homomorphisme de M dans N signifie deux choses.

1. *Additionner deux vecteurs x et y de M $[\boldsymbol{x+y}]$ puis prendre l'image par f du vecteur résultant $[\boldsymbol{f(x+y)}]$*

   revient à

   prendre l'image par f des deux vecteurs x et y de M $[\boldsymbol{f(x)}$ et $\boldsymbol{f(y)}]$ puis additionner leur image dans N $[\boldsymbol{f(x)+f(y)}]$.

   Cette propriété est illustrée par le fait que le diagramme ci-dessous est commutatif.
   Dire que ce diagramme est commutatif signifie que parcourir le chemin en trait plein (——) revient à parcourir le chemin en traits pointillés (· · · · ·), ou encore

$$f \circ +_M = +_N \circ (f \times f).$$

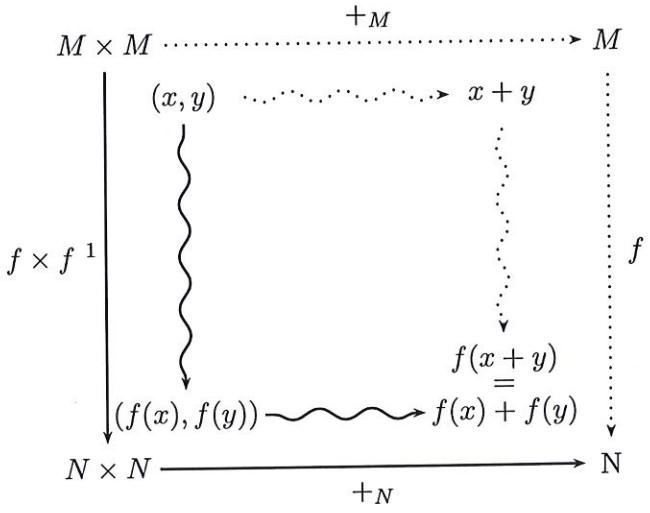


Figure 2.1 – Si f est un homomorphisme de modules, le diagramme ci-dessus est commutatif.

1. Lorsque $f : M \to N$, on définit $f \times f$ par $f \times f$: $M \times M \longrightarrow N \times N$
   $(x, y) \mapsto (f(x), f(y))$

2. *Multiplier un vecteur x de M par un scalaire α de K* $[\alpha x]$, *puis prendre l'image par f de ce nouveau vecteur* $[f(\alpha x)]$

donne le même résultat que

prendre l'image par f du vecteur x de M $[f(x)]$, *puis multiplier cette image par le scalaire α de K* $[\alpha f(x)]$.

Cette propriété est illustrée par le fait que le diagramme ci-dessous est commutatif.
De nouveau, dire que ce diagramme est commutatif signifie que parcourir le chemin en trait plein (——) revient au même que parcourir le chemin en traits pointillés (· · · · ·), ou encore, si on note par $\cdot$ la multiplication scalaire et par id_K l'application identité sur K :

$$f \circ \cdot_M = \cdot_N \circ (id_K \times f).$$

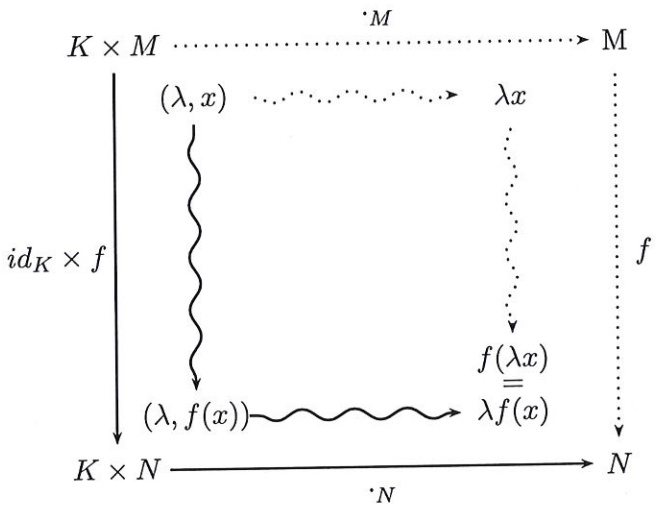


Figure 2.2 – Si f est un homomorphisme de modules, le diagramme ci-dessus est commutatif.

En pratique, pour vérifier qu'une application f est un homomorphisme de modules, on utilise souvent la propriété suivante.

Proposition 2.3.1 (Caractérisation d'un homomorphisme de modules)
Soient M et N des modules à gauche sur un même anneau K.
Alors,

f est un homomorphisme de M dans N

$$\Updownarrow$$

$$\forall\, x, y \in M,\ \forall\, \alpha, \beta \in K,\ f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) \tag{2.3}$$

Preuve :
Commençons par montrer la condition nécessaire. Supposons que f est un homomorphisme de M dans N et montrons qu'on obtient la relation (2.3).
Supposons que $\alpha, \beta \in K$ et que $x, y \in M$. Dès lors, puisque M est un module, les vecteurs αx et βy sont dans M. En utilisant successivement les deux conditions de la définition d'homomorphisme de modules, on obtient la relation souhaitée :

$$f(\alpha x + \beta y) = f(\alpha x) + f(\beta y) = \alpha f(x) + \beta f(y).$$

Pour démontrer la condition suffisante, supposons par hypothèse que la propriété (2.3) est vérifiée et montrons que f satisait à la définition 2.3.1 d'homomorphisme de modules.
Il suffit de choisir dans la relation (2.3)

- $\alpha = \beta = 1$ pour obtenir la première propriété de la définition 2.3.1,
- $\beta = 0$ pour obtenir la deuxième propriété de la définition 2.3.1. ∎

Remarque
On peut noter que pour toute application linéaire $f : M \to N$, l'égalité

$$f(0_M) = 0_N. \tag{2.4}$$

est vérifiée. En effet, pour vérifier cette affirmation, il suffit de prendre $\alpha = \beta = 0_K$ dans l'équation (2.3).

De nouveau, tout comme avec les groupes ou les anneaux, lorsqu'un homomorphisme est bijectif, on l'appelle isomorphisme. On obtient la définition qui suit.

Définition 2.3.2 (Ismomorphisme de modules)
Soient M et N des modules à gauche sur un même anneau K.
Un **isomorphisme** de M dans N est un homomorphisme bijectif de M dans N. S'il existe un isomorphisme de M dans N, on dira que M et N sont **isomorphes**.

Remarque
En pratique, deux modules isomorphes sont deux modules totalement similaires. En effet, puisqu'un isomorphisme est une bijection de M dans N, on peut dire qu'à tout élément de M correspond toujours un et un seul élément de N et réciproquement. De plus, puisqu'un isomorphisme est aussi un homomorphisme, à toute relation entre les éléments de M correspond une relation entre les éléments de N et réciproquement (un homomorphisme étant caractérisé par le fait qu'il conserve les structures d'addition et de multiplication externe).
Comme R. Godement l'explique clairement dans [3], « [grâce à l'isomorphisme, on va pouvoir] *traduire toute relation algébrique entre éléments de M en une relation algébrique analogue entre les images par f de ces éléments, et par suite transformer toute propriété de M en une propriété analogue de N.* »

L'exercice résolu suivant propose de vérifier si une application f particulière est un homorphisme de modules.

Objectif de l'exemple 2.3.1 :
Cet exemple a pour but de permettre à l'étudiant de se familiariser avec la définition d'homorphisme de modules sur un exercice résolu à caractère calculatoire. Par ailleurs, l'exemple porte sur l'ensemble des nombres complexes, ensemble qui a déjà été étudié dans d'autres contextes (en humanités et en première bachelier). Cet exemple permettra donc à l'étudiant de faire éventuellement certains liens avec un ensemble qu'il a déjà eu l'occasion de rencontrer.

Exemple 2.3.1

Considérons le $\mathbb{Z}$-module à gauche $\{M_2(\mathbb{R}), +, \circ\}$ défini dans l'exemple 2.1.2 ainsi que l'anneau $(\mathbb{Z}, +, *)$ muni de la loi usuelle d'addition et de la loi de multiplication $* : \mathbb{Z} \to \mathbb{Z}, (\alpha, \beta) \mapsto \alpha * \beta = \frac{\alpha.\beta}{2} = \frac{\alpha\beta}{2}$ (où . désigne la multiplication usuelle des entiers), et enfin le triplet $(\mathbb{C}^2, +, \bullet)$ où :

- $\mathbb{C}^2$ est l'ensemble des couples de nombres complexes.
- La loi $+$ est la loi d'addition définie par $+ : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}^2$
  $((x_1, x_2), (y_1, y_2)) \mapsto (x_1 + y_1, x_2 + y_2)$, avec $+$ qui est la loi d'addition usuelle sur $\mathbb{C}$.
  Rappelons que la somme de deux complexes $x = a + ib$ et $y = c + id$ est définie par $x + y = (a + c) + i(b + d)$ (où $i^2 = 1$)
- La loi $\bullet$ est une loi externe qui relie $\mathbb{C}^2$ à un anneau de base que nous choisissons égal à $\mathbb{Z}$:

$$\begin{array}{rccc} \bullet : & \mathbb{Z} \times \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ (\lambda, (a + ib, a' + ib')) & \mapsto & \lambda \bullet (a + ib, a' + ib') = (\dfrac{\lambda(a + ib)}{2}, \dfrac{\lambda(a' + ib')}{2}). & \end{array}$$

Enfin, définissons une application f comme suit :

$$f : \{M_2(\mathbb{R}), +, \circ\} \longrightarrow \{\mathbb{C}^2, +, \bullet\}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = (a + id, c + ib).$$

Questions

1. **Le triplet $\{\mathbb{C}^2, +, \bullet\}$ est-il un module à gauche sur le corps $\{\mathbb{Z}, +, *\}$? Est-il un module à droite ?**
2. **L'application f est-elle un homomorphisme de modules ?**

- par le point précédent, nous savons que $(\mathbb{C}^2, +, \bullet)$ est $\mathbb{Z}$-module.

Vérifions que f satisfait à l'égalité (2.3) de la proposition 2.3.1.

Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(\mathbb{R})$ et soit $\alpha,\ \beta \in \mathbb{Z}$. Montrons que

$$f\left(\alpha \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \beta \circ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = \alpha \bullet f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) + \beta \bullet f\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)$$

Or, cette égalité peut encore s'écrire, par la définition de f et de la loi externe $\circ$ sur $M_2(\mathbb{R})$, comme

$$f\left(\frac{1}{2}\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \frac{1}{2}\beta \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = \alpha \bullet (a + id, c + ib) + \beta \bullet (a' + id', c' + ib')$$

ou encore, par définition de f et la loi externe $\bullet$ sur $\mathbb{C}^2$

$$(\tfrac{1}{2}\alpha a + i\tfrac{1}{2}\alpha d, \tfrac{1}{2}\alpha c + i\tfrac{1}{2}\alpha b) + (\tfrac{1}{2}\beta a' + i\tfrac{1}{2}\beta d', \tfrac{1}{2}\beta c' + i\tfrac{1}{2}\beta b')$$
$$= (\tfrac{\alpha(a+id)}{2}, \tfrac{\alpha(c+ib)}{2}) + (\tfrac{\beta(a'+id')}{2}, \tfrac{\beta(c'+ib')}{2}).$$

Or, cette égalité est toujours vérifiée dans $\mathbb{C}^2$.

En conclusion, f est bien un homomorphisme de modules, ce qui clôture cet exemple.

A présent, considérons un cas particulier d'homomorphisme $f : M \to N$ en choisissant $M = N$. Cela nous amène à de nouvelles définitions.

Définition 2.3.3 (Endomorphisme-automorphisme)
Soit M un K-module à gauche.
- Un homomorphisme de M dans M est appelé **endomorphisme de M.**
- Un isomorphisme de M dans M est appelé **automorphisme de M.**

L'ensemble de tous les endomorphismes sur M sera noté par

$$\boldsymbol{End_K(M,N)} \qquad \textbf{ou} \qquad \boldsymbol{End(M,N)}$$

s'il n'y a aucune ambiguïté sur l'anneau de base.

Lien entre la notion d'homomorphisme de modules et celle de sous-module

Intéressons-nous à présent à ce que devient l'image d'un sous-module par un homomorphisme de modules. Obtient-on automatiquement un sous-module du module d'arrivée ?
La réponse à cette question est contenue et démontrée dans le théorème suivant, qui relie la notion de sous-module à celle d'homomorphisme de modules.

Théorème 2.3.1 (Image de sous-modules)
Considérons M et N deux modules à gauche sur un même anneau K et soit $f : M \to N$ un homomorphisme de modules.
Alors,

1. *l'image par f d'un sous-module de M est un sous-module de N.*
2. *l'image réciproque*[a] *d'un sous-module de N est un sous-module de M.*

a. Soit f une application de l'ensemble X dans l'ensemble Y, et considérons A une partie de Y. On appelle **image réciproque de A par f** l'ensemble $\{x \in X \mid f(x) \in A\}$.

Preuve :

1. Soit M' un sous-module de M. Montrons que $f(M')$ est un sous-module de N, et cela grâce à la caractérisation d'un sous-module (proposition 2.2.3).
   - L'ensemble $f(M')$ est non vide car 0_N, le neutre du module N appartient à $f(M')$. En effet, d'une part, on sait par la proposition 2.2.2 que le neutre de M, noté 0_M, appartient à M'. D'autre part, on sait que $f(0_M) = 0_N$. Le vecteur 0_N est donc dans $f(M')$.
   - Supposons que u et v se trouvent dans $f(M')$ et montrons que
   $$\forall\ \alpha, \beta \in K,\ \alpha u + \beta v \in f(M').$$
   Comme par hypothèse, u et v se trouvent dans $f(M')$, on peut trouver des vecteurs $x, y \in M'$ tels que $u = f(x)$ et $v = f(y)$.
   D'autre part, on sait que le vecteur $z = \alpha x + \beta y$ appartient à M' vu que M' est un sous-module de M.
   Comme f est une application linéaire, on obtient
   $\forall\ \alpha, \beta \in K$,
   $$\begin{aligned} f(z) &= f(\alpha x + \beta y) \\ &= \alpha f(x) + \beta f(y) \\ &= \alpha u + \beta v \end{aligned}$$
   En conclusion, $\forall\ \alpha, \beta \in K,\ \alpha u + \beta v \in f(M')$, ce qui termine la preuve de la première partie du théorème.

2. Soit N' un sous-module de N. Considérons l'ensemble M' défini comme suit

$$M' = \{x \in M \mid f(x) \in N'\}.$$

Autrement dit, M' est l'ensemble des vecteurs de M dont les images par f appartiennent au sous-module N'.

Montrons que l'ensemble M' ainsi défini est un sous-module de M. Pour ce faire, utilisons à nouveau la proposition 2.2.3.

- M' est non vide. En effet, comme N' est un sous-module de N, il comprend le neutre de N noté par 0_N (proposition 2.2.2). D'autre part, $f(0_M) = 0_N$, où 0_M est le neutre de M. Donc, 0_M appartient à M'.
- Supposons que a et b se trouvent dans M' et montrons que $\forall\ \alpha, \beta \in K,\ \alpha a + \beta b \in M'$. Dire que a et b sont des éléments de M' signifie que $f(a)$ et $f(b)$ sont des vecteurs de N'. Comme N' est un sous module de N, on obtient que

$$\forall\ \alpha, \beta \in K,\ \alpha f(a) + \beta f(b) \in N'.$$

Comme l'application f est linéaire par hypothèse, cette dernière propriété peut encore s'écrire :

$$\forall\ \alpha, \beta \in K,\ f(\alpha a + \beta b) \in N',$$

ce qui montre, par définition de M' que le vecteur $\alpha a + \beta b$ est bien dans M'.

Ceci clôture la preuve de ce théorème. ∎

Appliquons à présent le théorème précédent à deux sous-ensembles des modules M et N, rencontrés régulièrement, à savoir : $Kerf$ et Imf. Commençons par définir rigoureusement ces sous-ensembles dans le cadre des modules.

Définition 2.3.4 (Noyau et image d'un homomorphisme de module)
Soient M et N deux modules à gauche sur un même anneau K et $f : M \to N$ un homomorphisme de modules.

Le sous-ensemble de M, $Kerf = \{x \in M \mid f(x) = 0\}$ est appelé **noyau de f.**

Le sous-ensemble de N, $Imf = \{y \in N \mid \exists\ x \in M,\ y = f(x)\}$ est appelé **image de f.**

Enonçons le théorème important suivant.

Théorème 2.3.2 (Noyau et ensemble image d'un homomorphisme de modules)
Considérons M et N deux modules à gauche sur un même anneau K ainsi que $f : M \to N$ un homomorphisme de modules.

Alors, les ensembles $Kerf$ et Imf sont des sous-modules de M et N respectivement.

Preuve :

- Montrons que l'ensemble $Kerf$ est un sous-module de M.
  En appliquant la deuxième propriété du théorème précédent (théorème 2.3.1), on peut affirmer que $Kerf$ est un sous-module de M. En effet, il est l'image réciproque par f de $\{0_N\}$, qui est le plus petit sous-module de N.
- Montrons que l'ensemble Imf est un sous-module de N.
  On peut conclure, par la première propriété du théorème 2.3.1, que l'ensemble image de f, $Imf = f(M)$, est un sous-module de N puisque M est lui-même un sous-module de M. ∎

Remarque

Dans le cas où M et N sont des espaces vectoriels sur un même corps K, le théorème 2.3.1 et son corollaire peuvent être adaptés.
Si $f : M \to N$ est un homomorphisme d'espaces vectoriels, alors l'image par f d'un sous-espace vectoriel de M est un sous-espace vectoriel de N, et l'image réciproque d'un sous-espace vectoriel de N est un sous-espace vectoriel de M. Et donc, les ensembles $Kerf$ et Imf sont des sous-espaces vectoriels de M et N respectivement.
Il suffit de prendre K qui est un corps dans les preuves du théorème 2.3.1 et son corollaire.

L'ensemble des homomorphismes de modules

Pour terminer le paragraphe sur les homomorphismes de modules, présentons un résultat important concernant l'ensemble des homorphismes $Hom(M, N)$ du K-module M dans le K-module N.

Théorème 2.3.3

Soient M et N deux K-modules à gauche et $f, g \in Hom(M, N)$.

1. Alors, l'application

$$f + g : M \longrightarrow N, \quad x \mapsto (f + g)(x) = f(x) + g(x), \tag{2.5}$$

où le symbole $+$ dans le second membre de l'égalité représente l'addition sur N,
est appelée **somme des homomorphismes f et g** *et est aussi un homomorphisme de M dans N.*

De plus, l'ensemble $Hom(M, N)$, muni de la loi de composition

$$\begin{aligned} + : \quad & Hom(M,N) \times Hom(M,N) \longrightarrow Hom(M,N) \\ & (f, g) \mapsto f + g, \end{aligned} \tag{2.6}$$

est un groupe commutatif, appelé **le groupe des homomorphismes de M dans N.**

2. Si K est **commutatif**, le groupe $\{Hom(M,N),+\}$, muni de la loi de composition externe $\cdot$ définie comme suit :

$$\begin{aligned} \cdot : \quad & K \times Hom(M,N) \longrightarrow Hom(M,N) \\ & (\lambda, f) \mapsto \lambda f, \end{aligned} \tag{2.7}$$

avec

$$\lambda f : M \longrightarrow N, \quad x \mapsto (\lambda f)(x) = \lambda \cdot f(x) \tag{2.8}$$

où $\cdot$ représente la multiplication scalaire sur N, est un $\boldsymbol{K}$**-module.**

Preuve :

1. **Premièrement, montrons que l'application $f+g$ est bien un homomorphisme.**

   Pour ce faire, posons $h = f + g$. En utilisant la caractérisation d'un homomorphisme (proposition 2.3.1), on vérifie que h est un homomorphisme :
   $\forall\, x, y \in M,\ \forall\, \alpha, \beta \in K,$

$$\begin{aligned} h(\alpha x + \beta y) &= (f+g)(\alpha x + \beta y) \\ &= f(\alpha x + \beta y) + g(\alpha x + \beta y) \quad \text{par (2.5)} \\ &= \alpha f(x) + \beta f(y) + \alpha g(x) + \beta g(y) \quad \text{car } f \text{ et } g \text{ sont des homomorphismes} \\ &= \alpha[f(x) + g(x)] + \beta[f(y) + g(y)] \\ &= \alpha[(f+g)(x)] + \beta[(f+g)(y)] \quad \text{par (2.5)} \\ &= \alpha h(x) + \beta h(y) \end{aligned}$$

   Deuxièmement, montrons que l'ensemble $Hom(M,N)$, muni de la loi de composition $(f,g) \mapsto f+g$ (interne et partout définie par le point précédent) est un groupe commutatif.

   Pour cela vérifions unes à unes les propriétés de la définition de groupe commutatif (définitions 1.1.1 et 1.1.4) pour le couple $\{Hom(M,N),+\}$.

   . **[Associativité]** $\forall\, f,g,h \in Hom(M,N) :\ (f+g)+h \stackrel{?}{=} f+(g+h)$.

   Oui, car l'égalité $(f+g)+h = f+(g+h)$ est équivalente à

$$\begin{aligned} & \forall x \in M,\ [(f+g)+h](x) = [f+(g+h)](x) \\ \Leftrightarrow \quad & \forall x \in M,\ (f+g)(x) + h(x) = f(x) + (g+h)(x) \quad \text{par (2.5)} \\ \Leftrightarrow \quad & \forall x \in M,\ (f(x)+g(x)) + h(x) = f(x) + (g(x)+h(x)) \quad \text{par (2.5)} \end{aligned}$$

   Or, cette dernière égalité est toujours vraie car $\{N,+\}$ est un groupe commutatif (vu que N est un K-module à gauche par hypothèse).

. **[L'élément neutre]** $\exists\, e \in Hom(M,N),\ \forall\, f \in Hom(M,N),\ f+e=f=e+f.$

L'application nulle qui à chaque élément de M fait correspondre le neutre de N :

$$0 : M \longrightarrow N,\ x \mapsto 0_N$$

convient. En effet, $\forall\, f \in Hom(M,N),\ \forall\, x \in M$, l'égalité

$$(f+0)(x) = f(x) = (0+f)(x)$$

est équivalente, par la définition de la somme d'homomorphismes (2.5), à

$$f(x) + 0(x) = f(x) = 0(x) + f(x)$$

ou encore, par la définition de l'application nulle, à

$$f(x) + 0_N = f(x) = 0_N + f(x).$$

Cette dernière égalité est toujours vérifiée par définition de l'élément neutre 0_N dans N.

. **[Symétrisabilité]** $\forall\, f \in Hom(M,N),\ \exists\, f' \in Hom(M,N),\ f+f'=0=f'+f.$

Soit $f \in Hom(M,N)$. Son symétrique est l'application qui à tout élément x de M fait correspondre l'opposé de son l'image par f dans N :

$$(-f) : M \longrightarrow N$$

$$x \mapsto (-f)(x) = -f(x).$$

En effet, pour tout élément x dans M,

$$(f+(-f))(x) = 0(x) = ((-f)+f)(x),$$

$$\Leftrightarrow f(x) + (-f)(x) = 0_N = (-f)(x) + f(x), \quad \text{par (2.5)}$$

$$\Leftrightarrow f(x) - f(x) = 0_N = -f(x) + f(x), \quad \text{par définition de } (-f).$$

Cette dernière égalité est toujours vérifiée puisque l'élément symétrique de $f(x)$ dans N est $-f(x)$, $\forall\, x \in M$.

. **[Commutativité]** $\forall\, f,g \in Hom(M,N),\ f+g=g+f.$

Cela s'obtient directement par le fait que N est un groupe commutatif.
En effet, $\forall\, x \in M,\ (f+g)(x) = (g+f)(x)$ car dans N, $\forall x \in M,\ f(x)+g(x) = g(x)+f(x)$.

$\{Hom(M,N),+\}$ est donc un groupe commutatif.

2. **Montrons à présent que l'ensemble $Hom(M,N)$, muni de la loi de composition $(\lambda, f) \mapsto \lambda f$ est un K-module à gauche.**

Pour cela, vérifions tout d'abord que $f' = \lambda f$ est un homomorphisme par la propriété 2.3.1 : $\forall\, x, y \in M,\ \forall\, \alpha, \beta \in K$,

$$\begin{aligned} f'(\alpha x + \beta y) &= \lambda f(\alpha x + \beta y) \\ &= \lambda\alpha f(x) + \lambda\beta f(y) \quad \text{car } f \text{ est un homomorphisme} \\ &= \alpha\lambda f(x) + \beta\lambda f(y) \quad \textbf{car } K \textbf{ est commutatif} \\ &= \alpha f'(x) + \beta f'(y) \end{aligned}$$

La loi de composition définie en (2.7) est donc bien une loi de composition externe sur $Hom(M,N)$, si l'on suppose que K est commutatif.

Enfin, montrons que le triplet $\{Hom(M,N), +, \cdot\}$ est un K-module à gauche.

Pour cela, montrons que ce triplet satisfait aux propriétés de la définition de module à gauche (définition 2.1.4) :

. **[Associativité mixte]** $\forall\, \alpha, \beta \in K,\ \forall\, f \in Hom(M,N),\ (\alpha\beta)f \stackrel{?}{=} \alpha(\beta f)$
Oui, car l'égalité $(\alpha\beta)f = \alpha(\beta f)$ est équivalente, par (2.5) et par (2.8) à :

$$\begin{aligned} &\forall\, x \in M,\ [(\alpha\beta)f](x) = [\alpha(\beta f)](x) \\ \Leftrightarrow\ &\forall\, x \in M,\ (\alpha\beta)f(x) = \alpha(\beta f)(x) \\ \Leftrightarrow\ &\forall\, x \in M,\ (\alpha\beta)f(x) = \alpha(\beta f(x)). \end{aligned}$$

Or, la dernière égalité est toujours vraie vu que N est un K-module à gauche.

. $\forall\, f \in Hom(M,N),\ 1f \stackrel{?}{=} f$, où 1 est le neutre de K pour la multiplication.
Puisque N est un K-module à gauche, c'est immédiat car

$$\forall\, x \in M,\ (1f)(x) = 1f(x) = f(x).$$

. **[Double distributivité]** $\forall\, \alpha, \beta \in K, \forall\, f, g \in Hom(M,N),\ \alpha(f+g) \stackrel{?}{=} \alpha f + \alpha g$ et $(\alpha+\beta)f \stackrel{?}{=} \alpha f + \beta f$.

Démontrons la première propriété, la seconde se démontrant de manière similaire.
De nouveau, c'est immédiat car
$\forall\, x \in M$,

$$\begin{aligned} &[\alpha(f+g)](x) = [\alpha f + \alpha g](x) \\ \Leftrightarrow\ &\alpha(f+g)(x) = \alpha f(x) + \alpha g(x), \end{aligned}$$

et cette dernière égalité est toujours vraie dans N puisque N est un K-module à gauche.

En conclusion, le triplet $\{Hom(M,N), +, \cdot\}$ est un K-module à gauche, si K est commutatif.

Ceci termine la preuve du théorème 2.3.3. ∎

Remarque
Si M et N sont des modules à gauches sur un même anneau K, on peut vérifier que l'ensemble des applications de M dans N, que l'on note $App(M,N)$, muni des lois de composition usuelles d'addition d'applications et de multiplication scalaire[2] est aussi un K-module à gauche.
Dès lors, $Hom(M,N)$ est un sous-module de $App(M,N)$.
En effet, $Hom(M,N)$ est une partie de $App(M,N)$ et est encore un K-module à gauche (comme nous venons de démontrer dans le théorème précédent).

2.4 Exemples illustratifs

Terminons ce paragraphe sur le concept de module et les résultats importants qui en découlent, en donnant deux exemples récapitulatifs des notions vues jusqu'à présent.

Exemple 2.4.1
Pour tout anneau K et pour tout entier $n \geq 1$, l'ensemble

$$K^n = K \times \cdots \times K$$

muni des lois de composition définies par

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

peut être considéré comme un K-module à gauche.
En effet, il vérifie la définition 2.1.4 : on sait que K^n est un groupe commutatif grâce à la proposition 1.1.1, avec comme neutre pour l'addition, l'élément $(0, \ldots, 0)$. La vérification des autres conditions sont laissées au soin du lecteur (on utilise le fait que K est un anneau).

On peut aussi évidemment considérer K^n comme un K-module à droite en notant la loi de composition externe comme suit :

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

Enfin, on observe que lorsque $n = 1$, **K lui-même peut être considéré comme un K-module à gauche ou un K-module à droite.**

D'après cet exemple, les ensembles comme $\mathbb{R}^n$ et $\mathbb{Z}^n$ munis des lois définies ci-dessus peuvent être considérés comme des modules sur $\mathbb{R}$ et $\mathbb{Z}$ respectivement, pour tout n dans $\mathbb{N}_0$.

2. Ces lois sont identiques à celles définies en (2.6) et (2.7), à ceci près que leur domaine de définition n'est plus $Hom(M,N)$, mais bien $App(M,N)$.

Exemple 2.4.2

Dans cet exemple[3], nous montrerons que tout groupe commutatif G peut être regardé comme un $\mathbb{Z}$-module. Ensuite, nous nous intéresserons aux sous-modules de G et aux homomorphismes entre deux groupes commutatifs considérés comme des $\mathbb{Z}$-modules.

Soit G un groupe commutatif quelconque.

Commençons par définir deux lois de composition sur G, pour en faire un $\mathbb{Z}$-module à gauche.

1. Pour la loi interne, prenons la loi d'addition définie sur G, que l'on notera $+$.
2. Pour la loi externe, définissons l'application $\cdot : \mathbb{Z} \times G \to G : (\alpha, x) \mapsto \alpha \cdot x = \alpha x$ en posant

$$\alpha x = \begin{cases} x + \cdots + x \quad (\alpha \text{ termes}) & \text{si } \alpha \geq 1, \\ 0 & \text{si } \alpha = 0, \\ (-\alpha)(-x) & \text{si } \alpha \leq -1. \end{cases}$$

Questions

1. **Le triplet $\{G, +, \cdot\}$ est-il un $\mathbb{Z}$-module à gauche ?**
2. **Si oui, quels sont ses sous-modules ?**
3. **Considérons I et J deux groupes commutatifs et $f : I \to J$ un homomorphisme de groupes. Montrez que f est également un homomorphisme de $\mathbb{Z}$-modules.**

<u>Résolution</u>

1. Vérifions que $\{G, +, \cdot\}$ est un $\mathbb{Z}$-module à gauche.

Nous savons que $\mathbb{Z}$ muni des loi d'addition et de multiplication usuelles est un anneau et que $\{G, +\}$ est un groupe commutatif, par hypothèse. Il nous reste donc à montrer que les quatre propriétés de la définition 2.1.4 sont vérifiées.

· **[Associativité mixte]** $\forall\, \alpha, \beta \in \mathbb{Z},\ \forall\, x \in G,\ (\alpha\beta)x \stackrel{?}{=} \alpha(\beta x)$

Comme les scalaires α, β sont pris dans $\mathbb{Z}$, ils peuvent être aussi bien positifs que négatifs. Comme la loi de composition change selon les signes de α, β, il faut distinguer quatre cas.

Cas 1 : $\alpha > 0$ et $\beta > 0$

On a

$$\begin{aligned} \alpha(\beta x) &= \alpha(\overbrace{x + x + \ldots + x}^{\beta \text{ termes}}) \\ &= \underbrace{\overbrace{(x + x + \ldots + x)}^{\beta \text{ termes}} + \overbrace{(x + x + \ldots + x)}^{\beta \text{ termes}} + \ldots + \overbrace{(x + x + \ldots + x)}^{\beta \text{ termes}}}_{\alpha \text{ termes}} \\ &= \underbrace{x + x + \ldots + x}_{\alpha\beta \text{ termes}} \\ &= (\alpha\beta)x. \end{aligned}$$

3. Cet exemple est inspiré de l'exemple (1.5) page 109 de [1]

Cas 2 : $\alpha < 0$ et $\beta > 0$

On a

$$\alpha(\beta x) = (-\alpha)(\overbrace{(-x)+(-x)+\ldots+(-x)}^{\beta \text{ termes}})$$

$$= \underbrace{\overbrace{((-x)+(-x)+\ldots+(-x))}^{\beta \text{ termes}} + \overbrace{((-x)+(-x)+\ldots+(-x))}^{\beta \text{ termes}} + \ldots + \overbrace{((-x)+(-x)+\ldots+(-x))}^{\beta \text{ termes}}}_{(-\alpha) \text{ termes}}$$

$$= \underbrace{(-x)+(-x)+\ldots+(-x)}_{-(\alpha\beta) \text{ termes}}$$

$$= -(\alpha\beta)(-x)$$

$$= (\alpha\beta)x.$$

Le **cas 3 : $\alpha > 0$ et $\beta < 0$** et le **cas 4 : $\alpha < 0$ et $\beta < 0$** se montrent de manière similaire et sont laissés au lecteur.

· $\forall\, x \in G,\ 1x = x$, où 1 est le neutre de $\mathbb{Z}$ pour la multiplication.
Cela découle immédiatement de la définition de la loi externe sur G.

· **[Double distributivité]** $\forall\, \alpha, \beta \in \mathbb{Z},\ \forall\, x, y \in G,\ \alpha(x+y) \stackrel{?}{=} \alpha x + \alpha y$ et $(\alpha+\beta)x \stackrel{?}{=} \alpha x + \beta x$.

Démontrons la première propriété de la double distributivité, dans le cas où $\alpha < 0$, le cas où $\alpha > 0$ est laissé au lecteur.
On a

$$\begin{aligned}
\alpha(x+y) &= (-\alpha)\,[-(x+y)] \\
&= \overbrace{-(x+y)-(x+y)-\ldots-(x+y)}^{(-\alpha) \text{ termes}} \\
&= \underbrace{-x-x-\ldots-x}_{(-\alpha) \text{ termes}} + \underbrace{-y-y-\ldots-y}_{(-\alpha) \text{ termes}} \\
&= (-\alpha)(-x)+(-\alpha)(-y) \\
&= \alpha x + \alpha y.
\end{aligned}$$

Démontrons la deuxième propriété de la double distributivité, dans le cas où $(\alpha+\beta) > 0$, avec $\alpha > 0$ et $\beta < 0$, les autres cas sont laissés au lecteur mais se démontrent de manière similaire.
On a

$$\begin{aligned}
(\alpha+\beta)x &= \overbrace{x+x+\ldots+x}^{(\alpha+\beta) \text{ termes}} \\
&= \underbrace{x+x+\ldots+x}_{\alpha \text{ termes}} + \underbrace{-x-x-\ldots-x}_{(-\beta) \text{ termes}} \\
&= \alpha x + (-\beta)(-x) \\
&= \alpha x + \beta x.
\end{aligned}$$

Le groupe G peut donc est vu comme un $\mathbb{Z}$-module à gauche. Comme $\mathbb{Z}$ est commutatif, G peut être vu comme *un $\mathbb{Z}$-module.*
Notons que G ne peut **pas** être considéré comme un espace vectoriel sur $\mathbb{Z}$ étant donné que l'ensemble des entiers n'est pas un champ mais seulement un anneau.

2. Montrons que les sous-modules de G sont ses sous-groupes.

En effet, si on suppose que H est un sous-groupe de G, alors la première condition de la définition 2.2.2 de sous-module est automatiquement vérifiée.

De plus, par la définition de sous-groupe, l'élément $\overbrace{x+x+\ldots+x}^{n \text{ termes}} \in H$ et donc par définition de la loi externe, $\forall\, n \in \mathbb{Z},\ \forall\, x \in H,\ nx \in H$. La deuxième condition de la définition 2.2.2 est vérifiée.
H est donc un sous-module du $\mathbb{Z}$-module G.

3. A présent, considérons I et J deux groupes commutatifs et $f : I \to J$ un homomorphisme de groupes et montrons que f est également un homomorphisme de $\mathbb{Z}$-modules.

Montrons que f vérifie la relation (2.3) de la caractérisation d'homomorphisme de modules (proposition 2.3.1), pour tout $\alpha, \beta \in \mathbb{Z}$.
Avec $\alpha, \beta \in \mathbb{Z}$ positifs et $g, b \in I$,

$$\begin{aligned} f(\alpha g + \beta b) &= f(\overbrace{g+\cdots+g}^{\alpha \text{ termes}} + \overbrace{b+\cdots+b}^{\beta \text{ termes}}) \\ &= f(g)+\cdots+f(g)+f(b)+\cdots+f(b) \quad \text{car } f \text{ est un homomorphisme de groupes} \\ &= \alpha f(g) + \beta f(b) \quad \text{car } f(g) \text{ et } f(b) \text{ sont des éléments du groupe } J. \end{aligned}$$

A présent, considérons le cas où α est négatif. Cela ne pose pas de problème puisque par la relation (1.5), on sait que

$$f(-g) = -f(g).$$

Donc, par définition de la loi de composition externe lorsque n est négatif,

$$\begin{aligned} f(\alpha x) &= f((-\alpha)(-x)) \\ &= f(-x-x-\cdots-x) \\ &= -f(x)-f(x)-\cdots-f(x) \\ &= (-\alpha)(-f(x)) \\ &= \alpha f(x). \end{aligned}$$

On peut donc conclure que f est un homomorphisme de I dans J, avec I et J qui sont considérés comme des $\mathbb{Z}$-modules.

Maintenant que nous avons présenté le concept de module et découvert quelques-unes de ses propriétés, nous allons nous concentrer sur les différences qu'il existe entre un module et un espace vectoriel. Nous savons déjà que par définition, un espace vectoriel est un cas particulier de module, lorsque l'anneau de base est un corps.
Dans le chapitre 3, nous allons reprendre des concepts déjà connus dans les espaces vectoriels de dimension finie (concept de combinaison linéaire, de base,...) et les élargir afin de les considérer dans le cadre général des modules. Certains résultats resteront inchangés, mais d'autres seront modifiés, juste par le fait que pour définir la notion de module nous n'avons pas imposé la symétrisabilité à la multiplication des scalaires.

Chapitre 3

Bases dans les modules et espaces vectoriels

Dans ce chapitre, nous étudierons le concept fondamental de base. Bien connu dans les espaces vectoriels de dimension finie, il va être élargi au cadre général des modules. Pour cela, nous présenterons tout d'abord les notions de combinaison linéaire, de vecteurs linéairement indépendants et générateurs. Ensuite, nous définirons ce qu'est une base dans un module, et nous présenterons des résultats importants à ce sujet. Enfin, nous étudierons l'existence des bases dans un module, grâce à quelques théorèmes fondamentaux et nous introduirons la notion de dimension. Nous illustrerons des conséquences de l'élargissement du concept de base grâce à quelques exemples et exercices résolus.

Commentaires didactiques : La notion de base et ses propriétés fondamentales, ont pour la plupart déjà été rencontrées par les étudiants dans le cours d'algèbre linéaire de première année universitaire, dans le cadre des espaces vectoriels de dimension finie. Ce chapitre risque donc d'un premier abord de leur donner une impression de « déjà vu ». Cependant, il contient deux nouveautés importantes.

La première porte sur le fait que nous allons travailler dans les modules en général et non plus dans les espaces vectoriels uniquement. Des théorèmes qui étaient démontrables dans le cadre des espaces vectoriels ne seront pas transposables dans le cadre des modules. Par exemple, si l'on n'impose pas que l'anneau de base soit un corps, l'existence de bases ne sera plus garantie. Dès que possible, nous illustrerons les différences entre modules et espaces vectoriels par des exemples concrets dans le but de permettre aux étudiants de mieux cerner les enjeux de cet élargissement.

La deuxième nouveauté concerne le fait que nous allons travailler dans les modules qui peuvent admettre des bases composées d'un nombre infini d'éléments. Or, jusqu'ici, les étudiants de première année n'ont étudié le concept de base que dans le cadre des espaces vectoriels de dimension finie. C'est pourquoi, nous commencerons par consacrer un paragraphe aux définitions de la notion d'ensemble infini et de la notion de famille. Ces définitions vont nous permettre d'introduire la notion de combinaison linéaire infinie.

Remarque préliminaire

Dans ce chapitre, tout comme dans le précédent, nous choisissons de travailler dans des modules à gauche. Néanmoins, toutes les notions et théorèmes que nous exposerons peuvent être présentés de manière similaire dans des modules à droite.

3.1 Notion de base dans un module

Dans ce paragraphe, nous introduisons et étudions la notion de base dans le cadre des modules. Nous envisageons le cadre le plus général possible pour construire une base : nous considérons des bases qui peuvent contenir un nombre infini ou non de vecteurs.

Pour ce faire, nous commençons par présenter quelques conventions de notations et par définir rigoureusement les notions d'ensemble infini et de famille.

3.1.1 Contexte et notations

La notion d'ensemble infini se définit à partir de celle d'ensemble fini comme suit :

Définition 3.1.1 (Ensembles finis et infinis)

Un ensemble X est dit **fini** s'il est vide ou s'il existe un naturel non nul n ainsi qu'une bijection de X dans l'ensemble $\{1, 2, \ldots, n\}$ [1].

Un **ensemble infini** est un ensemble qui n'est pas fini. Autrement dit, l'ensemble X est infini s'il est différent du vide et s'il n'existe pas de naturel n tel que X soit en bijection avec l'ensemble $\{1, 2, \ldots, n\}$

Un ensemble est dit **infini dénombrable** s'il existe une bijection entre cet ensemble et $\mathbb{N}$.

1. On dit aussi que X est fini si $X \neq \emptyset$ et $\exists\, n \in \mathbb{N}_0$ tel que X soit *équipotent* à l'ensemble $\{1, 2, \ldots, n\}$. Par définition, un ensemble X est *équipotent* à un ensemble Y s'il existe une bijection de X dans Y.

Par la suite, nous utiliserons fréquemment *la notion de famille* pour parler d'un ensemble d'éléments indexés. Cette notion peut se construire selon le raisonnement suivant.

Lorsqu'on veut présenter deux éléments de façon à pouvoir distinguer leur rôle, on donne un couple (a, b), de premier élément a et de deuxième élément b.

De manière générale, si l'on veut donner un nombre fini n d'éléments et pouvoir dire qu'à la $i^{\text{ème}}$ place se trouve l'élément $a_i (i = 1, \ldots, n)$, on donne un n-uplet $(a_1, a_2, \ldots, a_n)$.

Si l'on veut aller encore plus loin et donner un ensemble dénombrable d'éléments, on doit trouver une technique pour préciser quel est le premier élément, le deuxième,... On peut procéder en associant le premier élément à 1, le deuxième élément à 2, et ainsi de suite en donnant à chaque fois un couple.

Ainsi, donner le quadruplet (a, b, c, d) revient à donner l'ensemble

$$G = \{(1, a), (2, b), (3, c), (4, d)\}$$

c'est-à-dire un graphe fonctionnel.

De même, pour donner un ensemble dénombrable d'éléments $x_0, x_1, x_2, \ldots$, en distinguant leur rôle, on peut donner un graphe

$$G = \{(0, x_0), (1, x_1), (2, x_2), \ldots\}, \tag{3.1}$$

ce que l'on peut encore noter par

$$G = \{(n, x_n) \mid n \in \mathbb{N}\}.$$

Plus généralement encore, si G est un graphe fonctionnel, on peut imaginer que sa première projection ne soit pas $\mathbb{N}$ comme ci-dessus mais un ensemble I quelconque, fini ou infini.
On obtient la définition de famille.

Définition 3.1.2 (Famille)
Le graphe fonctionnel $G = \{(i, x_i) \mid i \in I\}$, où les éléments x_i sont des objets quelconques dépendant de i (pour chaque $i \in I$), est appelé **famille indexée par I**, **famille d'index I** ou encore **famille ayant I pour ensemble d'indices**.

Si l'on note x_i l'objet associé à l'élément i de I, on désigne généralement la famille considérée par $(x_i)_{i \in I}$.

L'ensemble I est appelé l'**index** de la famille et les x_i sont appelés **valeurs** ou **membres** de la famille.

Remarques

1. Il faut veiller à bien distinguer la famille $(x_i)_{i\in I}$ de l'ensemble de ses valeurs $\{x_i \mid i \in I\}$ qui en est simplement la deuxième projection. Comme J. Mersch l'explique clairement dans [4], « *intuitivement,* $(x_i)_{i\in I}$ *est l'ensemble* $\{x_i \mid i \in I\}$ *muni d'un arrangement déterminé par* I . »
2. Au lieu de l'expression *valeur d'une famille*, on utilise parfois abusivement *élément d'une famille*. Ainsi, une famille $(x_i)_{i\in I}$ est appelée **famille d'éléments d'un ensemble X** si $\forall\, i \in I,\ x_i \in X$.
   De plus, si on applique à une famille une définition ou une propriété relative aux ensembles, on sous-entend qu'on l'applique à l'ensemble des valeurs de la famille, et non au graphe fonctionnel en entier.

Illustrons cette définition par deux exemples qui s'inspirent de l'exemple 4B.5 et de l'exemple 4B.6 de [5], page 4.2 et 4.3.

Objectif de l'exemple 3.1.1 :
Cet exercice a pour but de permettre à l'étudiant de se familiariser avec la définition de famille. Etant donné que c'est une notion qu'il rencontre pour la première fois en algèbre, nous proposons un exercice résolu où la famille est finie. Il permet d'insister sur le fait qu'une famille est un graphe *fonctionnel* et que c'est un objet qui ne peut se restreindre à l'ensemble des valeurs de la famille.

Exemple 3.1.1
Considérons les ensembles A, B, C définis comme suit :

$$\begin{aligned} A &= \{x \in \mathbb{R} : x \geq 5\} \\ B &= \{x \in \mathbb{R} : x < 100\} \\ C &= \{x \in \mathbb{R} : 7 \leq x \leq 8\} \end{aligned}$$

ainsi que les graphes F, G et H suivants :

$$\begin{aligned} F &= \{(1, A), (2, B), (3, C)\} \\ G &= \{(1, A), (2, B), (3, B), (4, C), (5, A)\} \\ H &= \{(1, A), (2, B), (2, C), (3, C)\} \end{aligned}$$

Questions

1. **Les graphes F, G et H représentent-ils des familles ?**
2. **Si oui, préciser quel est leur index et leur ensemble de valeurs.**
3. **Les graphes F, G et H représentent-ils la même famille ?**

Résolution

1. Pour que ces graphes soient des familles, il faut qu'ils vérifient le caractère fonctionnel (à un élément de l'index doit correspondre au plus une valeur). On observe que F et G sont des familles mais H n'en n'est pas une, car à l'élément 2 correspondent deux valeurs différentes B et C.
   On remarque que la nature des objets A, B, C n'intervient pas danslorsqu'il faut vérifier que F, G et H sont des familles. La notion de famille est totalement indépendante de la nature de ses valeurs.
2. Index de $F = \{1, 2, 3\}$ et ensemble des valeurs de $F = \{A, B, C\}$.
   Index de $G = \{1, 2, 3, 4, 5\}$ et ensemble des valeurs de $G = \{A, B, C\}$.
3. Les familles F et G, bien qu'ayant le même ensemble de valeurs, ne possèdent pas le même index. Elles sont donc différentes. On observe qu'il est indispensable, lorsqu'on s'intéresse à une famille, de ne pas se restreindre à l'ensemble de ses valeurs.

Objectif de l'exemple 3.1.2 :
Dans l'exercice précédent, les familles proposées pouvaient s'écrire la sous-forme de n-uplet, écriture déjà connue des étudiants. Elles ne nécessitaient pas les conventions d'écriture utilisées pour noter une famille. Dans l'exemple suivant, l'étudiant est confronté à une famille contenant une infinité d'éléments. Cet exemple est conçu pour lui faire prendre conscience que, dans le cas infini, la notion de n-uplet ne suffit plus. La notion de famille et les conventions d'écriture de celle-ci deviennent indispensables pour décrire le graphe proposé.

Exemple 3.1.2
Considérons les ensembles $A, B, C, D, \ldots, AA, AB, \ldots$, définis comme suit :

$$\begin{aligned} A &= \{x \in \mathbb{R} : x \geq 1\} \\ B &= \{x \in \mathbb{R} : x \geq 2\} \\ C &= \{x \in \mathbb{R} : x \geq 3\} \\ D &= \{x \in \mathbb{R} : x \geq 4\} \\ \vdots &\quad\quad \vdots \\ AA &= \{x \in \mathbb{R} : x \geq 27\} \\ \vdots &\quad\quad \vdots \end{aligned}$$

ainsi que le graphe $F = \{(1, A), (2, B), (3, C), (4, D), \ldots, (27, AA), \ldots\}$.

Questions

1. **Le graphe F constitue-t-il une famille ?**
2. **Si oui, préciser quel est son index et son ensemble de valeurs.**
3. **Le graphe F représente-il un n-uplet ? Si oui, lequel ?**
4. **Pourrait-on écrire F de manière plus concise ? Si oui, comment ?**

Résolution

1. Le graphe F est une famille car il est fonctionnel (à un élément de l'index correspond au plus une valeur).
2. L'index de $F = \{1, 2, 3, 4, \ldots\} = \mathbb{N}_0$ et l'ensemble des valeurs de $F = \{A, B, C, D, \ldots\}$.
3. On se rend compte que si l'on essaie de représenter la famille F sous la forme d'un n-uplet $(A, B, C, D, \ldots)$, il est impossible de déterminer la valeur de n. En effet, on observe que dans ce cas n n'est pas fini. On ne peut donc pas écrire F sous la forme d'un n-uplet.
4. Comme l'index de F est $\mathbb{N}_0$, la famille F contient un ensemble dénombrable d'éléments. On peut donc introduire le même principe de notation que celui introduit pour G en (3.1). Si on pose $A_1 = A$, $A_2 = B$, $A_3 = C$, $A_4 = D, \ldots$, le graphe F peut s'écrire

$$F = \{(1, A_1), (2, A_2), (3, A_3), (4, A_4), \ldots\},$$

ou encore, de manière plus concise

$$F = \{(n, A_n) \mid n \in \mathbb{N}_0\}.$$

Si l'on utilise les conventions de notations pour une famille, F peut encore s'écrire

$$F = (A_n)_{n \in \mathbb{N}_0}, \quad \text{avec } A_n = \{x \in \mathbb{R} : x \geq n\}.$$

Ceci clôture cet exercice.

Les ensembles que nous rencontrerons le plus souvent dans la suite sont les ensembles utilisés dans le cadre des modules. Nous en avons distingué deux types : les ensembles de scalaires (éléments de l'anneau de base) et les ensembles de vecteurs (éléments du groupe commutatif). Les familles auxquelles nous serons confrontés seront donc presque exclusivement des familles de vecteurs ou de scalaires.

Remarques

1. Dans le cas particulier où l'ensemble d'indices I d'une famille est l'ensemble $\mathbb{N}$, on dit que cette famille est une **suite**, et on la désignera par la notation

$$(x_i)_{i \geq 0} \quad \text{ou} \quad (x_i)_{i \in \mathbb{N}}.$$

2. Dans le cas particulier où l'ensemble d'indices I d'une famille est une partie $\{a, a+1, a+2, \ldots, b\}$ de l'ensemble $\mathbb{N}$, on notera plutôt cette famille par

$$(x_i)_{i=a}^{b}.$$

Elargissons maintenant la définition de combinaison linéaire à un nombre infini de vecteurs. On obtient la définition suivante.

Définition 3.1.5 (Combinaisons linéaires dans le cas infini)
Soit $(a_i)_{i\in I}$ une famille de vecteurs d'un K-module M.
On dira que le vecteur $x \in M$ est **combinaison linéaire** des vecteurs a_i $(i \in I)$ s'il existe une famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls de K telle que l'on puisse écrire

$$x = \sum_{i\in I} \lambda_i a_i. \tag{3.2}$$

On observe que cette définition a bien un sens puisque, par la propriété 2.1.1, les vecteurs $\lambda_i a_i$ sont presque tous nuls et donc la somme (3.2) est en réalité une somme finie.
Si l'ensemble I est fini, on retrouve la définition 3.1.3.

Considérons à présent un cas particulier de combinaison linéaire, les combinaisons linéaires du vecteur nul.

Définition 3.1.6 (Relation linéaire)
Soit $(a_i)_{i\in I}$ une famille de vecteurs d'un K-module M.
Supposons que le neutre de M soit combinaison linéaire de ces vecteurs, c'est-à-dire qu' il existe une famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls dans K tels que

$$0 = \sum_{i\in I} \lambda_i a_i.$$

Alors, la famille de scalaires $(\lambda_i)_{i\in I}$ est appelée **relation linéaire** entre les vecteurs a_i $(i \in I)$.

Remarque
Soit $(a_i)_{i\in I}$ une famille de vecteurs d'un K-module M.
Dans le cas particulier où $I = \{1, \ldots, n\}$, une *relation linéaire entre les vecteurs* a_i $(i = 1, \ldots, n)$ est un élément $(\lambda_1, \ldots, \lambda_n)$ de K^n tel que l'on ait

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

Observons qu'il peut y avoir plusieurs relations linéaires différentes (c'est-à-dire plusieurs n-uplet de K^n) entre les vecteurs de la famille $(a_i)_{i=1}^n$.
Il est évident que la relation linéaire $(0, \ldots, 0)$ entre les vecteurs a_i $(i = 1, \ldots, n)$ existe toujours, mais elle peut ne pas être unique.

La relation linéaire particulière $(0, \ldots, 0)$ est dite **triviale**.

Illustrons par un exemple particulier les concepts de combinaison linéaire et de relation linéaire.

Objectif de l'exemple 3.1.3 :
Dans cet exemple, nous avons consciemment choisi des fonctions comme vecteurs du module M. Les étudiants n'ont pas l'habitude de considérer des fonctions comme des vecteurs, ce qui permet d'insister sur le fait que des vecteurs d'un module peuvent avoir n'importe quelle forme.
Ensuite, cet exemple permet la manipulation d'une famille infinie ainsi que la construction de combinaisons linéaires et de relations linéaires dans le cas infini.
Il est assez général et sera à la base d'exercices résolus dans la suite de ce chapitre.

Exemple 3.1.3 (Exemple de combinaison linéaire et de relation linéaire)
Considérons un $\mathbb{R}$-module M où M est l'ensemble formé de toutes les applications partout continues

$$f: \quad \mathbb{R} \longrightarrow \mathbb{R}.$$

Des théorèmes d'analyse permettent d'affirmer que les applications $f+g$ et λf sont également des applications partout continues. Ces applications appartiennent donc à M, quelles que soient f, g dans M et $\lambda \in \mathbb{R}$.
Considérons le triplet constitué par l'ensemble M, l'application

$$\begin{array}{rccc} + : & M \times M & \longrightarrow & M \\ & (f,g) & \mapsto & f+g \end{array}$$

et l'application

$$\begin{array}{rccc} \cdot : & \mathbb{R} \times M & \longrightarrow & M \\ & (\lambda, f) & \mapsto & \lambda \cdot f = \lambda f. \end{array}$$

On peut montrer, en suivant les mêmes démarches que dans la preuve du théorème 2.3.3 que le triplet $\{M, +, \cdot\}$ est un $\mathbb{R}$-module. De plus, comme $\mathbb{R}$ est un champ, on constate que le triplet $\{M, +, \cdot\}$ est un espace vectoriel.

Construisons des combinaisons linéaires dans cet espace vectoriel.

Soit $(f_i)_{i\in I}$ une famille d'applications de M. Alors, l'application $f \in M$ est combinaison linéaire de ces fonctions s'il existe une famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls dans $\mathbb{R}$ tels que

$$f = \sum_{i\in I} \lambda_i f_i.$$

Alors, $\forall\ \lambda, \mu \in K,\ \ \lambda x + \mu y \in M'$ car

$$\lambda x + \mu y = \xi_1 a_1 + \ldots + \xi_n a_n$$

où

$$\xi_1 = \lambda\alpha_1 + \mu\beta_1, \ldots, \xi_n = \lambda\alpha_n + \mu\beta_n$$

sont des éléments de l'anneau K.
L'élément $\lambda x + \mu y$ peut s'écrire comme combinaison linéaire des vecteurs a_i $(i = 1, \ldots, n)$ et donc appartient à M'.

2. Montrons que M' **est le plus petit sous-module** qui contient la famille $(a_i)_{i=1}^n$.

Observons tout d'abord que les vecteurs a_i $(i = 1, \ldots, n)$ sont des vecteurs qui appartiennent à M'. En effet, ils peuvent s'écrire comme combinaison linéaire des vecteurs de la famille $(a_i)_{i=1}^n$ puisque $a_1 = \mathbf{1}.a_1 + 0.a_2 + \cdots + 0.a_n$, $a_2 = 0.a_1 + \mathbf{1}.a_2 + \ldots + 0.a_n$ et ainsi de suite pour $a_3, \ldots, a_n$.
D'autre part, $\forall\, \alpha_1, \ldots, \alpha_n \in K$, tout sous-module de M qui contient les vecteurs $a_1, \ldots, a_n$, contient aussi, par définition de module, les vecteurs $\alpha_1 a_1, \ldots, \alpha_n a_n$, et donc le vecteur $x = \alpha_1 a_1 + \cdots + \alpha_n a_n$. Donc, tout sous-module de M contenant les vecteurs a_i $(i = 1, \ldots, n)$ contient également toutes les combinaisons linéaires des vecteurs $a_1, \ldots, a_n$, c'est-à-dire M'.
Donc, l'ensemble M' est bien le plus petit sous-module à contenir la famille $(a_i)_{i=1}^n$, puisqu'il est inclus dans tous les autres sous-modules qui vérifient cette propriété. ∎

Soit M un K-module à gauche. Par le théorème précédent, nous savons que l'ensemble M' des combinaisons linéaires des vecteurs de la famille $(a_i)_{i\in I}$ de M a un statut particulier : c'est le plus petit sous-module qui contient la famille $(a_i)_{i\in I}$.
Donnons-lui un nom spécifique. C'est l'objet de la définition suivante.

Définition 3.1.7 (Sous-modules engendrés)
Soit $(a_i)_{i\in I}$ une famille de vecteurs d'un K-module à gauche M, et soit M' l'ensemble des combinaisons linéaires des vecteurs a_i $(i \in I)$.

Alors M' est appellé **le sous-module de M engendré par les vecteurs de la famille** $(a_i)_{i\in I}$.

Remarque
Soit M un K-module à gauche et $(a_i)_{i\in I}$ une famille de vecteurs de M.
Puisque M est aussi un sous-module de M, la définition précédente peut s'étendre à M lui-même : on dira donc que M **est engendré par les vecteurs a_i $(i \in I)$** si M est l'ensemble des combinaisons linéaires de ces vecteurs ou encore si M est le plus petit sous-module qui contient la famille $(a_i)_{i\in I}$.

3.1.3 Systèmes générateurs et indépendance linéaire

Le concept de base dans les espaces vectoriels est construit grâce aux notions de vecteurs linéairement indépendants et générateurs. Une base dans un module se définit de manière similaire. Nous commençons donc par étendre et présenter les concepts de système de générateurs puis d'indépendance linéaire dans le cadre des modules.

Définition 3.1.8 (Module de type fini et système générateur)
Soit M un K-module à gauche et M' un sous-module de M.
On dira que M' est un sous-module **de type fini** s'il existe une famille de vecteurs $(a_i)_{i=1}^n \in M'$ en nombre fini qui engendrent M'.
Dans ce cas, on dira que les vecteurs de la famille $(a_i)_{i=1}^n$ forment **un système de générateurs** de M'.

Remarque
De nouveau, cette définition s'applique en particulier au module M lui-même.
Donc, le module M est dit de **type fini** s'il contient des vecteurs $a_1, \ldots, a_n$ en nombre fini tel que tout vecteur x de M puisse s'écrire comme combinaison linéaire des vecteurs $a_1, \ldots, a_n$.
Les vecteurs $a_1, \ldots, a_n$ sont un **système de générateurs** de M.

Lorsque l'anneau de base est un corps et que M est engendré par un nombre fini de vecteurs, on parlera **d'espace vectoriel de dimension finie**, plutôt que de module de type fini.

Définissons la notion d'indépendance et de dépendance linéaire dans un module.

Définition 3.1.9 (Vecteurs linéairement indépendants)
Soient M un K-module à gauche et $(a_i)_{i\in I}$ une famille de vecteurs de M.
On dit que les vecteurs a_i $(i \in I)$ sont **linéairement indépendants**, ou que la famille $(a_i)_{i\in I}$ est **libre**, si l'égalité

$$\sum_{i\in I} \lambda_i a_i = 0$$

implique que $\forall\, i \in I,\ \lambda_i = 0$, quelle que soit la famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls de K.

Dans le cas particulier où I est fini, cela signifie qu'il n'existe pas d'autre relation linéaire que la relation linéaire triviale entre les vecteurs a_i $(i = 1, \ldots, n)$.

Au contraire, les vecteurs a_i $(i \in I)$ sont dits **liés** ou **linéairement dépendants** s'il existe des scalaires λ_i $(i \in I)$ *non tous nuls* tels que l'on ait

$$\sum_{i\in I} \lambda_i a_i = 0.$$

Autrement dit, dans le cas où I est fini, dire que des vecteurs sont linéairement dépendants signifie qu'il existe une relation linéaire non triviale entre eux.

Remarque

On considère que l'ensemble vide est libre car la proposition suivante
$\forall\, a_1, \ldots, a_n \in \emptyset,\ \forall \alpha_1, \ldots, \alpha_n \in K$:

$$\sum_{i=1}^{n} \alpha_i a_i = 0 \Rightarrow \alpha_1 = \ldots = \alpha_n = 0$$

est toujours vraie.

A présent, énonçons un premier résultat qui différencie les espaces vectoriels des modules.

Dans un espace vectoriel E, dire que des vecteurs de la famille $(a_i)_{i=1}^n$ de E sont linéairement dépendants est équivalent à dire que l'on peut exprimer un de ces vecteurs en fonction des autres. C'est l'objet de la propriété suivante[3].

Proposition 3.1.1

Soient E un espace vectoriel à gauche sur un corps K et $(a_i)_{i=1}^n$, une famille de vecteurs non nuls de E.

Alors, les vecteurs de la famille $(a_i)_{i=1}^n$ sont linéairement dépendants

$\Leftrightarrow$

Il existe un naturel k compris entre 1 et n tel que a_k soit combinaison linéaire des vecteurs $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n$.

Preuve :

Condition nécessaire

Supposons que les vecteurs a_i $(i = 1, \ldots, n)$ soient linéairement dépendants et montrons que l'on peut écrire l'un d'eux comme combinaison linéaire des autres.
Dire que les vecteurs a_i $(i = 1, \ldots, n)$ sont linéairement dépendants signifie qu'il existe une relation linéaire non triviale entre ces vecteurs. Autrement dit, nous avons l'égalité

$$\sum_{i=1}^{n} \alpha_i a_i = 0, \tag{3.3}$$

où les scalaires $\alpha_1, \ldots, \alpha_n$ sont non tous nuls.

Choisissons k comme étant le premier entier entre 2 et n tel que les vecteurs a_i $(i = 1, \ldots, k-1)$ soient linéairement dépendants et considérons son coefficient scalaire α_k.
Nous savons que α_k est différent de 0, sinon les $k-1$ premiers vecteurs seraient linéairement dépendants, ce qui est contradictoire avec la définition de l'entier k. Dès lors, comme K est un corps, nous pouvons considérer l'inverse de α_k, le scalaire α_k^{-1}.

3. Cette proposition et son corollaire sont présentés dans le cas fini, pour des facilités d'écriture, mais ils peuvent être étendus au cas infini.

Isolons le terme $\alpha_k a_k$ dans l'égalité (3.3) :

$$\alpha_k a_k = \alpha_1 a_1 + \ldots + \alpha_{k-1} a_{k-1} + \alpha_{k+1} a_{k+1} + \ldots + \alpha_n a_n$$

puis multiplions les deux membres de cette dernière égalité par α_k^{-1} :

$$a_k = \alpha_k^{-1}\alpha_1 a_1 + \ldots + \alpha_k^{-1}\alpha_{k-1} a_{k-1} + \alpha_k^{-1}\alpha_{k+1} a_{k+1} + \ldots + \alpha_k^{-1}\alpha_n a_n.$$

Nous avons donc réussi à écrire le vecteur a_k comme combinaison linéaire des autres vecteurs.

Condition suffisante

Considérons la famille de vecteurs $(a_i)_{i=1}^n$.
Supposons qu'il existe un entier k tel que le vecteur a_k soit combinaison linéaire des autres vecteurs a_i $(i = 1, \ldots, n,\ i \neq k)$ et montrons que la famille $(a_i)_{i=1}^n$ est non libre.

Par hypothèse, nous avons que

$$a_k = \lambda_1 a_1 + \ldots + \lambda_{k-1} a_{k-1} + \lambda_{k+1} a_{k+1} + \ldots + \lambda_n a_n,$$

où les scalaires $\lambda_1, \ldots, \lambda_n$ sont non tous nuls. Or, cette dernière relation peut encore s'écrire comme

$$0 = \lambda_1 a_1 + \ldots + \lambda_{k-1} a_{k-1} + (-1) a_k + \lambda_{k+1} a_{k+1} + \ldots + \lambda_n a_n.$$

Nous avons trouvé une relation linéaire non triviale $(\lambda_1, \ldots, \lambda_{k-1}, -1, \lambda_{k+1}, \ldots, \lambda_n)$ entre les vecteurs a_i $(i = 1, \ldots, n)$. Ils sont donc linéairement dépendants. ∎

Il existe un corollaire à cette proposition, que nous utiliserons par la suite.

Corollaire 3.1.1
Soient E un espace vectoriel à gauche sur un corps K et $(a_i)_{i=1}^n$, une famille de vecteurs non nuls de E.

Alors, les vecteurs de la famille $(a_i)_{i=1}^n$ sont linéairement dépendants

$$\Leftrightarrow$$

il existe un naturel k compris entre 2 et n tel que a_k soit combinaison linéaire des vecteurs $a_1, a_2, \ldots a_{k-1}$.

D'après ce corollaire, dire que des *vecteurs sont linéairement dépendants* est équivalent à dire que *l'un d'eux peut s'écrire comme combinaison linéaire des vecteurs précédents.*

La preuve de ce corollaire est fort semblable à celle du théorème précédent. Nous ne la présenterons pas ici, mais elle peut-être trouvée dans [8], à la page 12.

Remarque

Il est important de souligner que la proposition 3.1.1 est valable uniquement dans les espaces vectoriels mais pas dans les modules en général. En effet, on constate que dans la preuve de cette proposition, il est indispensable d'avoir l'hypothèse « $\boldsymbol{K}$ **est un corps** » pour pouvoir considérer l'inverse du scalaire α_k.

Dans l'exemple qui suit, illustrons le fait que dans un module, la proposition 3.1.1 n'est pas toujours valable.

Objectif de l'exemple 3.1.4 :
Cet exemple a pour but d'illustrer le fait que la proposition 3.1.1 n'est valable que dans les espaces vectoriels. Dans un module, dire que des vecteurs sont linéairement dépendants n'implique pas obligatoirement que l'on puisse exprimer un de ces vecteurs en fonction des autres. Ce résultat devrait étonner les étudiants, étant donné qu'ils ont l'habitude d'appliquer cette proposition par réflexe, dans les espaces vectoriels.

Exemple 3.1.4

Considérons dans cet exemple le module $\mathbb{Q}$ sur l'anneau $\mathbb{Z}$ où les lois d'addition, de multiplication et de multiplication scalaire choisies sont les lois de composition usuelles sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Choisissons deux vecteurs quelconques de $\mathbb{Q}$, par exemple les rationnels $\frac{3}{2}$ et $\frac{-6}{7}$.

Essayons de trouver une relation linéaire non triviale entre ces vecteurs. Il y en a une infinité. Choisissons par exemple $(\alpha_1, \alpha_2) = (8, 14)$.

On vérifie que 8 et 14 sont bien des entiers et que

$$\frac{3}{2} \cdot \alpha_1 + \frac{-6}{7} \cdot \alpha_2 = \frac{3}{2} \cdot 8 + \frac{-6}{7} \cdot 14 = 0.$$

Essayons à présent d'exprimer un des deux vecteurs en fonction de l'autre :

$$\exists\, ?\ \lambda, \eta \in \mathbb{Z}, \quad \tfrac{3}{2} = \lambda \cdot \tfrac{-6}{7} \quad \text{ou} \quad \tfrac{-6}{7} = \eta \cdot \tfrac{3}{2}.$$

Ces égalités seraient possibles si et seulement si les scalaires λ et η valaient respectivement $\frac{-7}{4}$ et $\frac{-4}{7}$. Or, ces scalaires n'appartiennent pas à $\mathbb{Z}$.
Il est donc impossible de trouver des entiers tels que l'un des deux rationnels puisse s'écrire comme une combinaison linéaire de l'autre.

Si, au lieu du $\mathbb{Z}$-module $\mathbb{Q}$, nous avions considéré l'espace vectoriel $\mathbb{Q}$ sur le corps $\mathbb{Q}$, nous n'aurions pas eu ce problème. S'il existait une relation non triviale entre des rationnels, nous aurions pu exprimer l'un d'entre eux comme combinaison linéaire des autres, comme l'affirme la proposition 3.1.1.

Montrons à présent la condition suffisante.

Supposons que les vecteurs a_i $(i = 1, \ldots, n)$ soient linéairement indépendants, et montrons que le n-uplet $(\lambda_1, \ldots, \lambda_n) \in K^n$, formé des coefficients de la combinaison linéaire du vecteur x, est unique.
Supposons par l'absurde qu'il existe deux façons différentes d'écrire x comme combinaison linéaire des vecteurs donnés :

$$x = \lambda_1 a_1 + \cdots + \lambda_n a_n = \xi_1 a_1 + \cdots + \xi_n a_n,$$

on obtient donc

$$(\lambda_1 - \xi_1)a_1 + \cdots + (\lambda_n - \xi_n)a_n = 0.$$

Comme par hypothèse les vecteurs a_i $(i = 1, \ldots, n)$ sont linéairement indépendants, cette dernière relation implique que $(\lambda_1 - \xi_1) = \ldots = (\lambda_n - \xi_n) = 0$ ou encore

$$(\lambda_1, \ldots, \lambda_n) = (\xi_1, \ldots, \xi_n).$$

Le n-uplet $(\lambda_1, \ldots, \lambda_n)$ est donc unique. ∎

3.1.4 Base d'un module

Nous avons à présent tous les outils pour définir une base dans le cadre des modules.

Définition 3.1.10 (Module libre de type fini – Base)
Soit M un K-module à gauche.

Une **base de** M est une famille $(a_i)_{i \in I}$ d'éléments de M qui est *libre* et dont les vecteurs *engendrent* le module M.
Si le module M admet une base, on dira que M est **un module libre.**

De plus, lorsqu'une base de M est formée d'*un nombre fini de vecteurs*, on dira que M est **un module libre de type fini.**

Remarque
On prend comme convention que, pour tout anneau K, le K-module réduit à 0 est un module *libre de type fini*, et admet une base formée de 0 vecteurs.

Énonçons une propriété fondamentale des bases.

Théorème 3.1.3 (Caractérisation d'une base)
Soit M un K-module à gauche.
Alors, la famille de vecteurs $(a_i)_{i\in I}$ est une base de M

si et seulement si

pour tout vecteur x de M, il existe une et une seule famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls telle que

$$x = \sum_{i\in I} \lambda_i a_i. \tag{3.4}$$

Preuve :
En effet, d'une part, le caractère générateur de la famille $(a_i)_{i\in I}$ signifie par définition (définition 3.1.8) qu'il existe une famille de scalaires $(\lambda_i)_{i\in I}$ tel que l'on ait (3.4).
D'autre part, par le théorème 3.1.2, dire que la famille de vecteurs $(a_i)_{i\in I}$ est libre revient à affirmer l'unicité de la famille de scalaires $(\lambda_i)_{i\in I}$. ∎

L'existence et l'unicité des scalaires $(\lambda_i)_{i\in I}$ dans la relation (3.4) nous amène à la définition suivante.

Définition 3.1.11 (Composantes)
Soient $(a_i)_{i\in I}$ une base d'un K-module à gauche M et x un vecteur de M.
Les scalaires λ_i ($i \in I$ définis par la relation (3.4) sont appelés **les coordonnées** ou **les composantes de x par rapport à la base $(a_i)_{i\in I}$ de M.**

La définition précédente et la relation (3.4) nous permettent d'associer à chaque vecteur x de M ses coordonnées de manière univoque.
Nous pouvons donc construire des applications bijectives à valeurs dans K qui, à chaque vecteur x, feraient correspondre ses composantes.
Cela nous conduit à définir les applications coordonnées.

Définition 3.1.12 (Applications coordonnées)
Soient M un K-module à gauche et $(a_i)_{i\in I}$ une base de M.
Les applications

$$\begin{aligned} f_i \ : \quad & M \longrightarrow K \qquad (\ i \in I\ ) \\ & x \ \mapsto \ f_i(x) = \lambda_i \end{aligned} \tag{3.5}$$

où les λ_i ($\in I$) sont les composantes du vecteurs x, sont appelées **les applications coordonnées du module M par rapport à la base $(a_i)_{i\in I}$.**

Par conséquent, les applications coordonnées peuvent également être définies par la relation

$$x = \sum_{i \in I} f_i(x) a_i,$$

pour tout $x \in M$.

Présentons quelques résultats importants qui découlent de la définition des applications coordonnées.

Plaçons-nous dans le cas particulier où $I = \{1, \ldots, n\}$, pour des facilités d'écriture[4].
Supposons que $(a_i)_{i=1}^n$ soit une base du K-module M.

- Dans un premier temps, essayons de caractériser les applications coordonnées.

  Comme le vecteur $a_j \in M$ $(j = 1, \ldots, n)$, il peut s'écrire de manière unique comme combinaison linéaire des vecteurs de la base $(a_i)_{i=1}^n$ de M. En effet, on peut écrire

  $$a_j = 0 \cdot a_1 + \cdots + 0 \cdot a_{j-1} + \mathbf{1} \cdot a_j + 0 \cdot a_{j+1} + \cdots + 0 \cdot a_n, \quad 1 \leq j \leq n.$$

  Les composantes des vecteurs de base sont donc données par

  $$(0, 0, \ldots, 0, \underbrace{1}_{j^e place}, 0, \ldots, 0), \quad 1 \leq j \leq n.$$

  Nous pouvons généraliser ces résultats par les relations suivantes, qui caractérisent les applications coordonnées

  $$f_i(a_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j, \end{cases} \tag{3.6}$$

  où δ_{ij} est le symbole de Kroenecker.

- Dans un deuxième temps, montrons que les applications coordonnées sont en fait des homomorphismes de modules, et cela, en montrant qu'elles satisfont à la définition 2.3.1.

  Tout d'abord, remarquons que les ensembles de départ et d'arrivée sont des K-modules. En effet, M est un K-module à gauche par hypothèse, et K est lui-même un K-module d'après l'exemple 2.4.1.

  Ensuite, les identités suivantes sont vérifiées pour tout $x, y \in M$:

  $$f_i(x + y) = f_i(x) + f_i(y), \qquad f_i(\lambda x) = \lambda f_i(x). \tag{3.7}$$

  En effet, considérons le vecteur $x + y$, où x et y appartiennent à M.
  D'une part, les coordonnées du vecteur $x + y$ sont données par la relation

  $$\forall\, x, y \in M,\ x + y = f_1(x + y)a_1 + \ldots + f_n(x + y)a_n.$$

4. Il est possible de faire le même raisonnement dans le cas où I est infini.

D'autre part, pour $x, y \in M$, on peut écrire par définition des applications coordonnées :

$$x = f_1(x)a_1 + \cdots + f_n(x)a_n \quad \text{et} \quad y = f_1(y)a_1 + \cdots + f_n(y)a_n,$$

on obtient donc en additionnant membre à membre ces deux égalités

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

Par unicité des scalaires dans l'expression d'un vecteur par rapport à une base, le scalaire $f_i(x+y)$, c'est-à-dire la $i^{\text{ème}}$ coordonnée de $x+y$, doit être égale à $[f_i(x)+f_i(y)]$, $i = 1, \ldots, n$.

On procède de manière similaire pour montrer la deuxième identité.

A présent, illustrons les notions vues jusqu'ici sur un exemple général : considérons le K-module K^n et essayons de trouver une base.

Objectif de l'exemple 3.1.5 :
Cet exemple a pour but d'illustrer les notions de vecteurs linéairement indépendants, générateurs ainsi que les notions de base et de composantes par rapport à une base. Il est général et recouvre quelques cas déjà connus des étudiants comme le $\mathbb{Z}$-module $\mathbb{Z}^n$ et l'espace vectoriel $\mathbb{R}^n$ sur $\mathbb{R}$, c'est pourquoi nous nous permettons de le présenter de manière plus théorique.

Exemple 3.1.5
Soit K un anneau. Dans le K-module K^n, on considère les vecteurs

$$e_1 = (1, 0, 0, \ldots, 0), \quad e_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad e_n = (0, 0, 0, \ldots, 1).$$

En multipliant ces vecteurs respectivement par les scalaires $\alpha_1, \ldots, \alpha_n$ et ensuite en les additionnant, on obtient l'égalité suivante :

$$\alpha_1 e_1 + \ldots + \alpha_n e_n = (\alpha_1, \ldots, \alpha_n).$$

On observe que *tout* élément de K^n peut s'écrire comme combinaison linéaire des vecteurs $e_1, \ldots, e_n$. Le K-module K^n est donc un *K-module de type fini* puisqu'il est engendré par un nombre fini de vecteurs.

De plus, étant donné un vecteur $x = (\alpha_1, \ldots, \alpha_n) \in K^n$, il s'écrit de manière unique comme combinaison linéaire des vecteurs e_1, $\ldots$, e_n puisque

$$x = (\alpha_1, \ldots, \alpha_n) = \alpha_1 e_1 + \cdots + \alpha_n e_n.$$

Autrement dit, les vecteurs e_1, $\ldots$, e_n forment une *famille libre* de K^n.

En résumé, ces vecteurs forment une *base* de K^n, qui est donc un *module libre de type fini.* Cette base est appelée la **base canonique** de K^n.
Les *coordonnées* du vecteur x par rapport à la base canonique sont les scalaires $\alpha_1, \ldots, \alpha_n$ et les *applications coordonnées* sont les applications

$$f_i : \quad K^n \longrightarrow K \qquad (\, i = 1, \ldots, n \,)$$

$$x \;\mapsto\; f_i(x) = \alpha_i.$$

De plus, les relations suivantes sont vérifiées

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

pour $i = 1, \ldots, n$.

3.1.5 Base et homomorphisme de modules

A présent, intéressons-nous au lien entre le concept de base d'un module et le concept d'homomorphisme de modules. On peut se poser plusieurs questions.
Par exemple, si l'on considère l'image d'une famille libre du module de départ par un homomorphisme de modules, obtient-on une famille libre du module d'arrivée ? Et, si l'on considère l'image d'une base du module de départ par un homomorphisme de modules, obtient-on une base du module d'arrivée ?

Les réponses à ces questions se trouvent dans le théorème et ses corollaires, énoncés et démontrés ci-dessous.

Théorème 3.1.4
Soient M un K-module à gauche, libre et de type fini[a], *ainsi que $(a_i)_{i=1}^n$ une base de M. Soient N un K-module à gauche quelconque et $c_1, \ldots, c_n$ des éléments de N.*
Alors, il existe une et une seule application linéaire de M dans N qui vérifie

$$f(a_i) = c_i, \quad 1 \leq i \leq n.$$

De plus, on a les équivalences suivantes :

1. *f est injective $\iff$ Les vecteurs $c_1, \ldots, c_n$ sont linéairement indépendants*
2. *f est surjective $\iff$ Les vecteurs $c_1, \ldots, c_n$ engendrent N.*

a. On peut étendre ce théorème et sa démonstration au cas d'un module libre quelconque.

Preuve :
Commençons par montrer la première partie du théorème à savoir qu'il existe une seule application linéaire $f : M \to N$ telle que

$$f(a_i) = c_i, \quad 1 \leq i \leq n.$$

- Construisons une telle application f.
  L'application f sera définie si pour tout vecteur x de M, on définit $f(x)$.

  Soit $x \in M$. Comme les vecteurs $a_1, \ldots, a_n$ forment une base de M, on peut exprimer x de la manière suivante

$$x = \alpha_1 a_1 + \ldots + \alpha_n a_n, \tag{3.8}$$

  où les scalaires $\alpha_1, \ldots, \alpha_n$ sont déterminés de manière unique.
  Ces scalaires peuvent être donnés par

$$\alpha_1 = f_1(x), \ldots, \alpha_n = f_n(x)$$

  où les applications $f_i : M \to N$, $x \mapsto f_i(x) = \alpha_i$ sont les fonctions coordonnées du module M par rapport à la base $(a_i)_{i=1}^n$.

  Posons

$$f(x) = f_1(x)c_1 + \ldots + f_n(x)c_n.$$

- On vérifie facilement que $f(a_i) = c_i$.
  En effet, puisque

$$f_j(a_i) = \begin{cases} 1 \text{ si } i = j, \\ 0 \text{ si } i \neq j, \end{cases}$$

  on obtient

$$f(a_i) = 0.c_1 + \ldots + 0.c_{i-1} + 1.c_i + 0.c_{i+1} + \ldots + 0.c_n = c_i.$$

- Montrons que f ainsi définie est bien une application linéaire.
  Les égalités (3.7) et la définition de f permettent d'écrire :

$$\begin{aligned} f(\lambda x + \mu y) &= f_1(\lambda x + \mu y)c_1 + \ldots + f_n(\lambda x + \mu y)c_n \\ &= [\lambda f_1(x) + \mu f_1(y)]c_1 + \ldots + [\lambda f_n(x) + \mu f_n(y)]c_n \\ &= \lambda[f_1(x)c_1 + \ldots + f_n(x)c_n] + \mu[f_1(y)c_1 + \ldots + f_n(y)c_n] \\ &= \lambda f(x) + \mu f(y) \end{aligned}$$

- Il reste à montrer que f est l'unique application linéaire qui vérifie $f(a_i) = c_i$, $i = 1, \ldots, n$.
  Supposons qu'il existe une autre application linéaire $g : M \to N$ tel que $g(a_i) = c_i$, $i = 1, \ldots, n$ et montrons que $\forall x \in M : \ g(x) = f(x)$.

  Soit $x \in M$. On sait par l'égalité (3.8) que x s'écrit de manière unique comme

$$x = \alpha_1 a_1 + \ldots + \alpha_n a_n.$$

On obtient, par la linéarité et la définition de g

$$g(x) = g(\alpha_1 a_1 + \ldots + \alpha_n a_n) = \alpha_1 g(a_1) + \ldots + \alpha_n g(a_n) = \alpha_1 c_1 + \ldots + \alpha_n c_n.$$

Comme les scalaires $\alpha_1, \ldots, \alpha_n$ sont uniques, on peut conclure par la définition de f que

$$g(x) = \alpha_1 c_1 + \ldots + \alpha_n c_n = f(x).$$

Montrons à présent les deux équivalences.

1. Supposons que f est injective et montrons que cela revient à dire que les vecteurs $c_1, \ldots, c_n$ sont linéairement indépendants.

   Tout d'abord, f est injective est équivalent à dire que $[f(x) = 0 \Rightarrow x = 0]$.
   Autrement dit, f est injective si et seulement si

   $$\left[f(x) = \alpha_1 c_1 + \ldots \alpha_n c_n = 0 \Longrightarrow x = \alpha_1 a_1 + \ldots + \alpha_n a_n = 0\right]. \tag{3.9}$$

   Comme par hypothèse, les vecteurs a_i $(i = 1, \ldots, n)$ forment une base, ils sont linéairement indépendants, c'est-à-dire $\alpha_1 a_1 + \ldots + \alpha_n a_n = 0$ est équivalent à $\alpha_1 = \ldots = \alpha_n = 0$. Donc l'implication (3.9) est équivalente à l'implication suivante

   $$\left[\alpha_1 c_1 + \ldots + \alpha_n c_n = 0 \Longrightarrow \alpha_1 = 0, \ldots, \alpha_n = 0\right].$$

   Mais cette implication est la définition même de l'indépendance linéaire des vecteurs $c_1, \ldots, c_n$.
   Donc, f injective $\Leftrightarrow$ les vecteurs $c_1, \ldots, c_n$ sont linéairement indépendants.

2. Montrons l'équivalence entre la surjectivité de f et le fait que N soit engendré par les vecteurs $c_1, \ldots, c_n$.

   Comme

   $$f(x) = f(\alpha_1 a_1 + \ldots \alpha_n a_n) = \alpha_1 f(a_1) + \ldots + \alpha_n f(a_n) = \alpha_1 c_1 + \ldots \alpha_n c_n,$$

   on observe que $f(M)$ est l'ensemble des combinaisons linéaires de $c_1, \ldots, c_n$.
   Une condition nécessaire et suffisante pour que les vecteurs $c_1, \ldots, c_n$ engendrent N tout entier est donc que f soit surjective.
   Ceci termine la preuve de ce théorème. ∎

Ce théorème possède deux corollaires particulièrement intéressants, qui permettent respectivement de vérifier si un K-module est libre de type fini ou simplement de type fini.
Enonçons et démontrons-les ci-dessous.

Corollaire 3.1.2
Soit M un K-module à gauche.
Alors,

$$M \text{ est libre de type fini} \iff \exists n \in \mathbb{N} : M \text{ soit isomorphe à } K^n.$$

Autrement dit, si $c_1, \ldots, c_n$ sont des vecteurs de M et $(e_i)_{i=1}^n$ est la base canonique de K^n, alors

$$\text{la famille formée par les vecteurs } c_1, \ldots, c_n \text{ est une base de } M$$
$$\iff$$
$$\text{il existe un isomorphisme } f \text{ de } K^n \text{ sur } M \text{ tel que } f(e_i) = c_i,\ i = 1, \ldots, n.$$

Preuve :
On sait, d'après le théorème précédent, qu'on peut toujours trouver un homomorphisme $f : K^n \to M$ tel que $f(e_i) = c_i,\ i = 1, \ldots, n,$ et que celui-ci est unique.
De plus, dire que f *est bijective (autrement dit f est surjective et injective)* est équivalent à dire que les *vecteurs $c_1, \ldots, c_n$ sont linéairement indépendants et engendrent M*, c'est-à-dire qu'ils forment une base de M. ∎

Corollaire 3.1.3
Soit M un K-module à gauche.
Alors, ces deux propositions sont équivalentes.
- *M est de type fini, c'est-à-dire engendré par un nombre fini de vecteurs $c_1, \ldots, c_n$.*
- *Il existe un entier n et un homomorphisme* **surjectif** *de K^n dans M tels que*

$$f(e_i) = c_i,\ i = 1, \ldots, n,$$

où $(e_i)_{i=1}^n$ est la base canonique de K^n.

Preuve :
Commençons par montrer la condition nécessaire.

Supposons que M est de type fini et montrons qu'il existe un homorphisme surjectif, comme décrit dans l'énoncé.
D'après le théorème 3.1.4, on sait qu'il existe un homomorphisme $f : K^n \to M$ tel que $f(e_i) = c_i,\ i = 1, \ldots, n.$
D'autre part, comme M est de type fini, il existe des vecteurs $c_1, \ldots, c_n$ en nombre fini qui engendrent M. Donc, toujours par le théorème 3.1.4, l'homomorphisme f est nécessairement surjectif.

Démontrons à présent la condition suffisante

Supposons qu'il existe un homomorphisme surjectif de K^n dans M tel que $f(e_i) = c_i,\ i = 1, \ldots, n$ et montrons que M est de type fini.

Pour ce faire, utilisons la propriété suivante.

Soit $f : L \to M$ un homomorphisme entre deux K-modules à gauche.

Si f est surjectif et si L est de type fini, alors M est de type fini.

Comme on sait que K^n est de type fini par l'exemple 3.1.5 et que f est surjectif par hypothèse, on peut conclure que M est de type fini.

Il nous reste donc à montrer que la propriété ci-dessus est vérifiée.

Pour cela, supposons que les vecteurs $a_1, \ldots, a_n$ engendrent L et posons

$$f(a_i) = b_i, \quad i = 1, \ldots, n.$$

Considérons y un vecteur de M. Comme f est surjectif par hypothèse, on sait qu'il existe un vecteur x dans L tel que $y = f(x)$.

Comme $x \in L$, on peut écrire $x = \alpha_1 a_1 + \ldots + \alpha_n a_n$.

Comme f est une application linéaire,

$$f(x) = y = \alpha_1 b_1 + \ldots + \alpha_n b_n.$$

Par conséquent, vu que y est arbitraire dans M, les b_i engendrent M.

M est donc de type fini. ∎

Exemples illustratifs

Terminons cette section sur la notion de base en illustrant ce concept par deux exemples récapitulatifs. Ils se présentent sous forme d'exercices résolus et sont inspirés de [3].

Objectif de l'exemple 3.1.6 :
Ce premier exemple a pour objectif de montrer l'importance de l'anneau dans lequel on puise les scalaires pour construire un module. Des caractéristiques fondamentales d'un module peuvent être modifiées si l'on change l'anneau de base.
En effet, dans cet exemple, on considère le module des nombres rationnels $\mathbb{Q}$ muni des lois usuelles. Ce module est de type fini si l'anneau de base est $\mathbb{Q}$ mais n'est pas de type fini si son anneau de base est $\mathbb{Z}$.

Exemple 3.1.6

Intéressons-nous au module $\mathbb{Q}$ sur un anneau K. L'anneau K sera dans un premier temps l'anneau des entiers $\mathbb{Z}$, et dans un deuxième temps l'anneau des nombres rationnels $\mathbb{Q}$ lui-même.

Les lois de compositions internes et externes choisies sont les lois de composition usuelles.

Questions

1. **Le $\mathbb{Z}$-module $\mathbb{Q}$ est-il un module de type fini ?**
2. **Et qu'en est-il du $\mathbb{Q}$-module $\mathbb{Q}$?**

Résolution

a. Considérons $\mathbb{Q}$ comme un $\mathbb{Z}$-module et supposons que ce module est de type fini.
Par définition, cela signifie que $\mathbb{Q}$ doit être engendré par un nombre fini de vecteurs.
Supposons donc que $\mathbb{Q}$ est engendré par un nombre fini de nombres rationnels :

$$a_1 = \frac{p_1}{q_1}, \quad \ldots, \quad a_n = \frac{p_n}{q_n}.$$

Cela signifie que pour chaque vecteur x dans $\mathbb{Q}$, il existe une famille d'entiers $(\lambda_i)_{i=1}^n$ telle que

$$\begin{aligned} x &= \lambda_1 a_1 + \cdots + \lambda_n a_n \\ &= \lambda_1 \frac{p_1}{q_1} + \cdots + \lambda_n \frac{p_n}{q_n} \end{aligned}$$

On observe que tout nombre rationnel x de $\mathbb{Q}$ peut s'écrire sous forme d'une fraction ayant pour dénominateur $q_1 \cdot \ldots \cdot q_n$. Autrement dit, cela signifie que l'on peut réduire au même dénominateur tous les éléments de $\mathbb{Q}$, ce qui est évidemment une absurdité.

Donc, comme il ne peut pas être engendré par un nombre fini de rationnels, $\mathbb{Q}$ **n'est pas un $\mathbb{Z}$-module de type fini.**

b. Considérons à présent $\mathbb{Q}$ comme un $\mathbb{Q}$-module. Dans ce cas, on obtient que $\mathbb{Q}$ est un module de type fini.

En effet, en choisissant l'anneau $K = \mathbb{Q}$ et $n = 1$ dans l'exemple 3.1.5, on obtient que $\mathbb{Q}$ est un $\mathbb{Q}$-module de type fini. D'après ce même exemple, la base de ce module est formée d'un seul vecteur e_1, qui est le neutre pour la multiplication de l'anneau $\mathbb{Q}$.
La base de $\mathbb{Q}$ est donc $\{1\}$.
Comme les scalaires sont choisis dans $\mathbb{Q}$ (et non dans $\mathbb{Z}$ comme le point précédent), tout rationnel $\frac{p}{q}$ de $\mathbb{Q}$ peut s'écrire comme une combinaison linéaire du vecteur $e_1 = 1$:

$$\frac{p}{q} = \lambda_1 . 1$$

Il suffit de choisir $\lambda_1 \in \mathbb{Q}$ qui vaut $\frac{p}{q}$.

De plus, puisque tout élément (excepté le neutre de l'addition 0) de $\mathbb{Q}$ admet un inverse dans $\mathbb{Q}$, autrement dit puisque $\mathbb{Q}$ est un corps, on observe que $\mathbb{Q}$ **est un espace vectoriel de dimension finie sur $\mathbb{Q}$.**

Objectif de l'exemple 3.1.7 :
L'objectif de ce deuxième exemple est de montrer qu'il existe des bases constituées d'un nombre infini de vecteurs. Pour ce faire, nous introduisons l'espace vectoriel formé des applications polynomiales. Les polynômes sont des objets déjà bien connus des étudiants dans le cadre des espaces vectoriels de dimension finie. Cet exemple leur permet donc d'élargir leurs connaissances à ce sujet.
Un intéret de cet exercice est de réaliser une synthèse entre les notions du chapitre 2 (comme la notion de sous-espace vectoriel) et du chapitre 3 (indépendance linéaire, vecteurs générateurs, base,...).
Cet exemple se base sur l'exemple général 3.1.3.

Exemple 3.1.7

1. Considérons les applications $1,\ t,\ t^2,\ \ldots,\ t^N : \mathbb{R} \to \mathbb{R}$ où $N \in \mathbb{N}$ est un naturel fixé, ainsi que l'espace vectoriel $\{M, +, \bullet\}$, défini dans l'exemple 3.1.3, constitué par l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ partout continues, muni des lois usuelles.

Questions 1

a) **Les applications $1,\ t,\ t^2,\ \ldots,\ t^N$ ($N \in \mathbb{N}$) sont-elles linéairement indépendantes ?**

b) **Forment-elles une base de l'espace vectoriel M ?**

2. A présent, intéressons-nous à un sous-ensemble[5] M' de M où M' est l'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$.
Un vecteur de M' est donc une application

$$\begin{array}{rccl} p: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & t & \mapsto & p(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n, \end{array}$$

où n peut prendre toutes les valeurs dans $\mathbb{N}$.

Questions 2

a) **L'ensemble M' forme-t-il un sous-espace vectoriel de M ?**

b) **La famille d'applications $(t^i)_{i\in\mathbb{N}}$ forme-t-elle une base de M' ?**

5. L'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ est bien une partie de M puisqu'il est formé d'applications $\mathbb{R} \to \mathbb{R}$ et partout continues.

Résolution

Questions 1

Les $N+1$ applications $1,\ t,\ t^2,\ \ldots,\ t^N$ sont partout continues, à variables réelles et à valeurs réelles, elles font donc bien partie de l'espace vectoriel M.

a) Une relation linéaire entre ces applications est une famille de nombres réels $\lambda_0,\ \lambda_1,\ \lambda_2,\ \ldots,\ \lambda_N$ vérifiant

$$\forall\, t \in \mathbb{R},\ \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_N t^N = 0.$$

Or, cette relation implique obligatoirement que $\lambda_0 = \cdots = \lambda_N = 0$.
Autrement dit, les applications $1,\ t,\ t^2,\ \ldots,\ t^N$ sont linéairement indépendantes dans l'espace vectoriel M. La famille d'applications $\left(t^i\right)_{i=1}^N$ est donc une famille libre de M.

b) Pour que les applications $1,\ t,\ t^2,\ \ldots,\ t^N$ forment une base de M, il faut qu'elles forment un système de générateurs de M. Autrement dit, il faut que toute application f de M puisse s'écrire comme combinaison linéaire de $1,\ t,\ t^2,\ \ldots,\ t^N$. On peut montrer qu'il existe des applications partout continues de $\mathbb{R}$ dans $\mathbb{R}$ qui ne peuvent pas s'écrire comme une combinaison linéaire des applications $1,\ t,\ t^2,\ \ldots,\ t^N$, comme par exemple les applications $t \mapsto \cos t$, $t \mapsto e^t$ ou encore l'application $t \mapsto t^{N+1}$.
En conclusion, les applications $1,\ t,\ t^2,\ \ldots,\ t^N$ sont linéairement indépendantes, mais ne forment pas une base de M.

Questions 2

Considérons M' l'ensemble des applications polynomiales de $\mathbb{R}$ dans $\mathbb{R}$.

a) Montrons que M' est un sous-espace vectoriel de M par la proposition 2.2.2 (caractérisation d'un sous-module).

Tout d'abord, M' est non vide puisqu'il contient l'application nulle qui à tout $t \in \mathbb{R}$ fait correspondre 0. L'application nulle peut en effet s'écrire sous la forme d'une application polynomiale p_0 :

$$\begin{array}{rccl} p_0 : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & t & \mapsto & p_0(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n, \qquad \text{où} \quad \alpha_0 = \alpha_1 = \ldots = \alpha_n = 0. \end{array}$$

Ensuite, vérifions que $\forall\, \alpha, \beta \in \mathbb{R},\ \forall\, p, q \in M',\ \alpha p + \beta q \in M'$.
Si on suppose que $\forall\, t \in \mathbb{R},\ p(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n$, et $q(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n'} t^{n'}$, où $n, n' \in \mathbb{N}$ avec $n > n'$, on obtient $\forall\, t \in \mathbb{R}$,

$$\begin{aligned} \alpha p(t) + \beta q(t) &= \alpha(\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n) + \beta(\alpha_0 + \alpha_1 t + \cdots + \alpha_{n'} t^{n'}) \\ &= \alpha_0(\alpha + \beta) + \alpha_1(\alpha + \beta)t + \ldots + \alpha_{n'}(\alpha + \beta)t^{n'} + \alpha_{n+1}\alpha t^{n+1} \ldots + \alpha_n \alpha t^n. \end{aligned}$$

Autrement dit, l'application $\alpha p + \beta q$ peut aussi s'écrire sous la forme d'une application polynomiale et donc appartient à M'.

Puisque $\mathbb{R}$ est un corps, nous avons montré que M' est bien un sous-espace vectoriel de M.

b) La famille d'applications $(t^i)_{i\in\mathbb{N}}$ forme-t-elle une base de M' ?

En suivant le même raisonnement qu'à la question 1, on peut dire que les applications $1,\ t,\ t^2,\ \ldots,\ t^n$ $(n \in \mathbb{N})$ sont linéairement indépendantes.

D'autre part, il est évident que tout polynôme $p \in M'$ de degré n peut s'écrire comme une combinaison linéaire des fonctions $1,\ t,\ t^2,\ \ldots,\ t^n$ $(\forall n \in \mathbb{N})$; il est donc engendré par ces applications.

En général, on peut dire que la famille d'applications $(t^i)_{i\in\mathbb{N}}$ définie ci-dessus est non seulement une famille libre dans M' mais forme également un système de générateurs de M'. Cette famille est donc une base de M'.

Les *coordonnées* d'un polynôme $p \in M'$ par rapport à cette base ne sont rien d'autre que les coefficients du polynôme p.

Remarquons que comme il existe un nombre infini dénombrable de vecteurs dans cette base, M n'est pas un espace vectoriel de dimension finie. *Cette exemple nous montre qu'un espace vectoriel qui n'est pas de dimension finie peut aussi admettre une base.*

3.2 Existence de bases dans les espaces vectoriels

3.2.1 Théorèmes d'existence de bases

Dans cette section, nous présentons quelques résultats fondamentaux qui vont nous permettre de différencier davantage les espaces vectoriels des modules. En effet, les théorèmes que nous énonçons sont spécifiques aux espaces vectoriels et ne sont pas valables dans les modules.
Nous illustrons les conséquences de ces différences dans plusieurs exemples.

Le théorème qui suit est de toute première importance.

Théorème 3.2.1
Tout espace vectoriel sur un corps K admet une base.

Remarque
Il est important de savoir que les théorèmes et propriétés que nous exposons ici sont valables pour **tous les espaces vectoriels, qu'ils soient de dimension finie ou non.**
Néanmoins, nous ne les démontrerons que dans le cas particulier des espaces vectoriels de dimension finie, étant donné que les démonstrations générales dépassent le cadre de ce travail.

Reformulons le théorème précédent dans le cas fini.

Théorème 3.2.2
Tout espace vectoriel de dimension finie sur un corps K admet une base.

Pour prouver ce résultat fondamental, nous utilisons le théorème suivant.

Théorème 3.2.3
Soit E un espace vectoriel de dimension finie sur un corps K. Considérons G un ensemble fini de générateurs de E et L une partie de G dont les éléments sont linéairement indépendants. Alors, il existe une base B de E telle que

$$L \subset B \subset G.$$

Dans un premier temps, nous réalisons la preuve du théorème 3.2.3. Dans un deuxième temps, nous verrons comment le théorème fondamental 3.2.2 se démontre presque immédiatement à partir du théorème 3.2.3.

Preuve du théorème 3.2.3

Pour prouver ce théorème, commençons par considérer toutes les parties de G. En particulier, intéressons-nous aux parties de G qui sont libres et qui contiennent L [6].

Parmi ces parties, certaines possèdent plus d'éléments que d'autres. Pour cette preuve, considérons uniquement celles qui comportent le plus grand nombre d'éléments.
Posons B l'une de ces parties et montrons que B ainsi défini forme une base de E.

Par construction, nous savons que B **est libre**, donc, pour prouver que B est une base de E, il suffit de montrer que les éléments de B **engendrent** E.
Par définition d'un système de générateurs, cela revient à montrer que tout élément $y \in E$ s'écrit comme combinaison linéaire des éléments de B. Comme G est un ensemble fini de générateurs de E, on observe qu'il est suffisant de montrer que tout élément $x \in \boldsymbol{G}$ s'écrit comme combinaison linéaire des éléments de B.

Soit $x \in G$. Essayons d'exprimer x comme combinaison linéaire des éléments de B.

Pour cela, distinguons deux cas :

- Soit $x \in B$.
  Dans ce cas c'est évident.
- Soit $x \notin B$.
  Dans ce cas, on pose $B' = B \cup \{x\}$.
  L'ensemble B' ainsi construit est contenu dans l'ensemble générateur G et contient strictement plus d'éléments que B.

  L'ensemble B' n'est donc pas libre puisque B contient par construction un maximum d'éléments linéairement indépendants.
  Autrement dit, si on note $x_1, \ldots, x_n$ les éléments de B, on peut écrire l'égalité suivante

$$\lambda_1 x_1 + \ldots + \lambda_n x_n + \lambda x = 0 \tag{3.10}$$

  où les scalaires $\lambda_1, \ldots, \lambda_n$ et λ sont non tous nuls.
  De plus, on sait que $\lambda \neq 0$, sinon $(\lambda_1, \ldots, \lambda_n)$ constituerait une relation linéaire non triviale entre les éléments x_i de B, ce qui contredirait le fait que B est libre.

  La relation (3.10) peut encore s'écrire

$$-\lambda_1 x_1 - \ldots - \lambda_n x_n = \lambda x. \tag{3.11}$$

  Puisque $\lambda \neq 0$ et que par hypothèse, **l'anneau de base $\boldsymbol{K}$ est un corps**, λ est inversible dans K.
  On peut donc multiplier les deux membres de l'égalité (3.11) par λ^{-1}, l'inverse de λ dans K.
  On obtient

$$-\lambda^{-1}\lambda_1 x_1 - \ldots - \lambda^{-1}\lambda_n x_n = \lambda^{-1}\lambda x$$

6. On remarque qu'il est toujours possible de trouver une telle partie, ne serait-ce que L elle-même puisque les éléments de L sont linéairement indépendants par hypothèse.

ou encore

$$-\lambda^{-1}\lambda_1 x_1 - \ldots - \lambda^{-1}\lambda_n x_n = x,$$

ce qui montre que $x \in G$ est bien combinaison linéaire des éléments de B.

En conclusion, B est non seulement formé de vecteurs linéairement indépendants mais ces vecteurs constituent aussi un système de générateurs de E. Donc B est bien une base de E.■

Preuve du théorème 3.2.2

Considérons E un espace vectoriel de dimension finie et montrons qu'il admet une base B.
Le théorème 3.2.2 est en fait un cas particulier du théorème 3.2.3.
En effet, choisissons, dans l'énoncé du théorème 3.2.3, L qui vaut l'ensemble vide $\emptyset$ et G qui est un ensemble fini de générateurs de E.
L'ensemble vide est bien une partie de G dont les vecteurs sont linéairement indépendants par la remarque de la page 88 et E possède bien un ensemble fini de générateurs G, puisque que c'est un espace vectoriel de dimension finie. Avec ce choix particulier, on obtient qu'il existe une base B de l'espace vectoriel E.

Remarque
Rappelons que les théorèmes 3.2.3 et 3.2.2 sont valables uniquement dans les espaces vectoriels mais pas dans les modules en général. En effet, on constate que dans la preuve du théorème 3.2.3, il est indispensable d'avoir l'hypothèse « $\boldsymbol{K}$ **est un corps** » pour être certain de pouvoir considérer l'inverse du scalaire λ.

3.2.2 Illustration des théorèmes d'existence

Les théorèmes de la section précédente constituent une différence fondamentale entre module et espace vectoriel. Alors qu'un espace vectoriel possède toujours une base, ce n'est pas le cas pour les modules, comme l'illustre l'exemple suivant.

Exemple 3.2.1
Nous avons vu dans l'exemple 2.4.2 page 72 que tout groupe commutatif pouvait être considéré comme un $\mathbb{Z}$-module.

Soit G un groupe commutatif considéré comme un $\mathbb{Z}$-module. Nous voudrions savoir si G peut être un $\mathbb{Z}$-module libre de type fini et si oui, dans quels cas.

Supposons que G est libre de type fini. Par définition, cela signifie que G admet au moins une base qui contient un nombre fini d'éléments.

Cette base est une suite d'éléments de G (en nombre fini) $a_1, \ldots, a_n$ telle que l'application de $\mathbb{Z}^n$ dans G

$$(\alpha_1, \ldots, \alpha_n) \longmapsto \alpha_1 a_1 + \ldots + \alpha_n a_n$$

est bijective.

Or, nous savons que l'ensemble $\mathbb{Z}^n$ est infini. Par conséquent, l'ensemble G est nécessairement infini.

Autrement dit, nous avons l'implication suivante

$$G \text{ admet une base formée d'un nombre fini d'éléments} \implies \text{l'ensemble } G \text{ est infini}$$

ou encore,

$$G \text{ est un module libre de type fini} \implies \text{l'ensemble } G \text{ est infini.}$$

Prenons à présent la contraposée de cette dernière implication. On obtient

$$\text{l'ensemble } G \text{ est fini} \implies \text{le module } G \text{ n'est pas « libre de type fini »}$$

ce qui revient à dire

$$\text{l'ensemble } G \text{ est fini} \implies \underbrace{\text{le module } G \text{ n'est pas de type fini}}_{\text{impossible puisque } G \text{ est fini}} \text{ ou le module } G \text{ n'est pas libre}$$

et donc

$$\textit{l'ensemble } G \textit{ est fini} \implies \textit{le module } G \textit{ n'est pas libre}$$

On arrive donc à la conclusion suivante : un groupe commutatif fini considéré comme un $\mathbb{Z}$-module est donc un module de type fini (forcément, puisque G est fini) qui n'admet jamais de base.

Il ne sera donc jamais libre de type fini.

Nous sommes donc en présence d'un module qui n'admet pas de base. De plus, nous pouvons faire la constatation suivante :

ce n'est donc pas parce qu'un module sur un anneau est de *type fini* (i.e engendré par un nombre fini d'éléments) qu'il possède nécessairement une base (i.e libre de type fini).

3.2.3 Corollaires du théorème d'existence

Ce théorème possède de nombreux corollaires. Nous en présentons deux qui nous semblent particulièrement intéressants.

Corollaire 3.2.1
Soient E un espace vectoriel de dimension finie et $(x_i)_{i=1}^n$ une famille quelconque de vecteurs linéairement indépendants dans E.

Alors, une des deux propositions suivantes est vraie.

1. *$(x_i)_{i=1}^n$ est une base de E.*
2. *Il est possible de trouver une famille de vecteurs $(x_i)_{i=n+1}^{n+m}$ de E tels que la famille de vecteurs $(x_i)_{i=1}^{n+m}$ soit une base de E.*

Ce premier corollaire nous dit que tout ensemble de vecteurs linéairement indépendants de E peut être completé pour former une base de E.

Preuve :
Pour prouver ce théorème, considérons deux cas.

. **Les vecteurs de la famille $(x_i)_{i=1}^n$ sont générateurs de E.**
Comme, par hypothèse, les vecteurs $x_1, \ldots, x_n$ sont linéairement indépendants, ces n vecteurs forment donc une base de E.
On obtient la première proposition du théorème.

. **Les vecteurs de la famille $(x_i)_{i=1}^n$ ne sont pas générateurs de E.**
Dans ce cas, nous voudrions trouver une base de E qui contient les vecteurs $x_1, \ldots, x_n$.
Pour ce faire, appliquons le théorème 3.2.3 à des ensembles G et L particuliers :

- G doit être un ensemble fini de vecteurs générateurs de E. Choisissons

$$G = Y \cup \{x_1, \ldots, x_n\},$$

où $Y = \{y_1, \ldots, y_m\}$ est un système fini de générateurs quelconques de E.

- L doit être une partie de G dont les éléments sont linéairement indépendants. Choisissons

$$L = \{x_1, \ldots, x_n\}.$$

Grâce au théorème 3.2.3, on peut conclure qu'il existe (au moins) une base de E incluse dans G et qui comprend les vecteurs $\{x_1, \ldots, x_n\}$.
Notons B l'une de ces bases.

A présent, essayons de trouver une expression explicite de B. On procède comme suit.

Observons tout d'abord que l'ensemble $G = \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$ est un ensemble de vecteurs linéairement dépendants. En effet, comme par hypothèse les vecteurs y_i, $(i = 1, \ldots, m)$ sont générateurs de E, les vecteurs $x_i \in E$ peuvent s'écrirent comme combinaison linéaire des y_i.

Soit z le premier vecteur de G qui est combinaison linéaire des vecteurs précédents (ce vecteur existe toujours par le corollaire 3.1.1). Puisque par hypothèse, les vecteurs x_i sont linéairement indépendants, il existe $1 \leq j \leq m$ tel que $z = y_j$. Considérons maintenant le nouvel ensemble

$$G' = G \setminus \{y_j\} = \{x_1, \ldots, x_n, y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_m\}.$$

Ensuite, observons que les vecteurs de G' sont encore générateurs de E tout entier.
C'est évident puisque les vecteurs y_i forment un système de générateurs de E et que y_j est combinaison linéaire des éléments de G'.

Nous avons alors deux possibilités.

1. *Soit les vecteurs de G' sont linéairement indépendants.*
   Dans ce cas, nous avons trouvé une expression de la base B : il suffit de choisir les vecteurs $\{x_i\}_{i=n+1}^{n+p}$ égaux aux y_i restant dans G' (avec $p = m - 1$).
2. *Soit les vecteurs de G' sont linéairement dépendants.*
   Dans ce cas, on recommence la même procédure que ci-dessus en enlevant un nouveau vecteur y_i de l'ensemble G', pour obtenir un nouvel ensemble G'' de générateurs de E et ainsi de suite, jusqu'à obtenir un ensemble de vecteurs linéairement indépendants. On aura ainsi obtenu une base B qui contient tous les vecteurs de départ $\{x_i\}_{i=1}^{n}$ ainsi que les $\{x_i\}_{i=n+1}^{n+p}$ qui sont choisis identiques aux vecteurs y_i restant dans cet ensemble. ∎

Corollaire 3.2.2
Soit E un espace vectoriel de dimension finie sur un corps K.
Alors, des éléments donnés de E font partie d'une base de E si et seulement si ils sont linéairement indépendants.

Ce deuxième corollaire est intéressant parce qu'il nous donne une condition nécessaire et suffisante pour que des vecteurs d'un module fassent partie d'une base.

Preuve : La condition nécessaire est évidente. En effet, s'il existe une base B de E qui contient ces éléments, alors, par définition de base, ces éléments sont linéairement indépendants. Pour la condition suffisante, supposons que les vecteurs $\{x_i\}_{i=1}^{n}$ soient linéairement indépendants. Nous avons vu par le corollaire précédent, que dans ce cas, ils font partie d'une base. ∎

Ceci clôture cette section sur l'existence de bases dans les espaces vectoriels. Dans la section suivante, nous caractérisons ces bases.

3.3 Notion de dimension d'un espace vectoriel

Dans cette section, nous commençons par présenter un théorème fondamental de l'algèbre linéaire concernant les bases des espaces vectoriels. Ce théorème nous permettra d'introduire la notion de dimension d'un espace vectoriel.

Théorème 3.3.1
Soit E un espace vectoriel de dimension finie sur un corps K.
***Toutes** les bases de E possèdent **le même nombre** de vecteurs.*

La preuve de ce théorème est inspirée de [8].

Preuve :
Soient $X = (x_i)_{i=1}^n$ et $Y = (y_i)_{i=1}^m$ deux familles finies de vecteurs de E.
Supposons d'une part que Y soit *une famille libre* de E et d'autre part que X soit un *ensemble de générateurs* de E, c'est-à-dire que tout vecteur de E est combinaison linéaire des vecteurs de X.

Considérons l'ensemble

$$A_1 = \{y_m, x_1, \ldots, x_n\}.$$

On observe que tout vecteur de E est combinaison linéaire des vecteurs de A_1 puisque les vecteurs x_i sont générateurs de E par hypothèse. En particulier le vecteur y_m peut s'écrire comme une combinaison linéaire des vecteurs x_i. Donc, les vecteurs de A_1 sont linéairement dépendants.

D'après le théorème 3.1.1, on peut trouver un vecteur $z \in A_1$ qui soit combinaison linéaire des vecteurs précédents. Le vecteur z est dans ce cas-ci évidemment égal à l'un des vecteurs x_i.

Soit $z = x_j$ avec $1 \leq j \leq n$ et considérons maintenant l'ensemble A_1 auquel on a retiré le vecteur z. Appelons ce nouvel ensemble A_1' :

$$A_1' = \{y_m, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n\}.$$

Observons que les vecteurs de A_1' sont encore générateurs de E.
C'est évident puisque les vecteurs x_i sont générateurs de E et que le vecteur enlevé $z = x_j$ est combinaison linéaire des éléments de A_1'.
Donc, en particulier, le vecteur $y_{m-1} \in E$ peut s'écrire comme combinaison linéaire des vecteurs de A_1'.

Construisons à présent l'ensemble A_2 comme suit :

$$A_2 = A_1' \cup \{y_{m-1}\} = \{y_{m-1}, y_m, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n\}.$$

On obtient que A_2 est un ensemble de vecteurs linéairement dépendants et générateurs de E.

On remarque que A_2 est un ensemble de vecteurs de E qui a les mêmes propriétés que A_1.
On peut donc lui appliquer le même raisonnement : par le théorème 3.1.1, on peut trouver un vecteur $z \in A_2$ qui soit combinaison linéaire des vecteurs précédents. Le vecteur z est égal à l'un des vecteurs x_i, puisque nous avons supposé les vecteurs y_i linéairement indépendants.
Par le même procédé que précédemment, on peut ainsi retirer un des x_i de A_2 et lui rajouter un des y_i pour obtenir l'ensemble A_3 qui aura les mêmes propriétés que A_2.

En continuant de cette manière, on va incorporer tous les y_i avant d'avoir épuisé tous les x_i.
En effet, dans le cas contraire, les y_i restant seraient combinaisons linéaires des y_i se trouvant dans l'ensemble, ce qui contredirait le fait qu'ils forment une famille libre.

On obtient finalement, après m opérations, un ensemble avec les mêmes propriétés que A_1 mais dont m x_i ont été remplacés par des y_i.
Ceci démontre que

$$n \geq m.$$

Supposons à présent que les familles X et Y soient toutes les deux des bases de E. Elles satisfont a fortiori les hypothèses du début de la preuve.
De plus, on peut inverser les rôles de X et Y : prendre comme famille libre la famille X et comme ensemble de générateurs la famille Y. En effectuant le même résonnement précédemment, on déduit que

$$m \geq n.$$

En conclusion, $m = n$, autrement dit, les bases X et Y contiennent bien le même nombre d'éléments. ∎

Remarque
L'hypothèse que E soit un espace vectoriel est indispensable pour montrer que les bases contiennent le même nombre d'éléments. En effet, dans la preuve de ce théorème, on utilise plusieurs fois la proposition 3.1.1 et son corollaire 3.1.1, qui nécessitent tous les deux l'hypothèse que K soit un corps.
Nous n'avons donc pas de théorème équivalent dans le cadre des modules.

Remarque : Il aurait été intéréssant d'approfondir le sujet du nombre de vecteurs dans deux bases distinctes d'un module. Nous aurions souhaité nous pencher sur l'existence d'un module qui possèderait deux bases contenant un nombre différent de vecteurs et présenter, s'il en existe, un exemple d'un tel module. Mais faute de temps, nous avons décidé de ne pas nous attarder sur ce point.

Maintenant que nous savons que toutes les bases d'un espace vectoriel ont le même nombre d'éléments, nous pouvons introduire la notion de dimension dans un espace vectoriel de dimension finie.

Définition 3.3.1 (Dimension d'un espace vectoriel de dimension finie)
Soit E un espace vectoriel de dimension finie sur un corps K.

La dimension de E est le nombre de vecteurs dans une base quelconque de cet espace.
On dira que E est de dimension n sur le corps K ou encore que n est la dimension de E sur le corps K si cette base contient n vecteurs.
On notera la dimension de E sur le corps K par

$$dim_K(E).$$

S'il n'y a aucune ambiguïté possible sur le corps de base, on dira simplement que E est de dimension n ou que n est la dimension de E et on la notera par $dim(E)$.

Remarque
Lorsque l'espace vectoriel $E = \{0\}$, on convient de prendre $\dim(E) = 0$.

L'exemple suivant est un exercice résolu qui illustre la notion de dimension.

Objectif de l'exemple 3.3.1 :
Dans cet exemple, nous présentons un espace vectoriel E sur le corps des complexes puis des réels, dans le but de montrer que la dimension d'un espace vectoriel dépend du corps des scalaires. Cet exemple illustre sur un exercice concret la propriété générale suivante : $\dim_{\mathbb{R}}(E) = 2\dim_{\mathbb{C}}(E)$.

Exemple 3.3.1
Considérons l'espace vectoriel $\mathbb{C}^3$ sur deux corps différents et étudions sa dimension.

Questions

1. Quelle est la dimension de cet espace vectoriel si le corps des scalaires est $\mathbb{C}$?
2. La réponse à la question précédente change-t-elle si le corps des scalaires est $\mathbb{R}$?

Résolution

1. Dimension de l'espace vectoriel $\mathbb{C}^3$ sur le corps $\mathbb{C}$.

Par l'exemple 3.1.5, nous savons qu'une base possible de l'espace vectoriel $\mathbb{C}^3$ sur le corps $\mathbb{C}$ est la base canonique $(1,0,0),(0,1,0),(0,0,1)$.

Si le triplet $(a+ib, c+id, e+if) \in \mathbb{C}^3$, il peut s'écrire comme combinaison linéaire des trois vecteurs de la base canonique :

$$(a+ib, c+id, e+if) = \alpha(1,0,0) + \beta(0,1,0) + \gamma(0,0,1)$$

où $\alpha, \beta, \gamma \in \mathbb{C}$. On observe que $\alpha = a+ib, \beta = c+id, \gamma = e+if$; ce sont bien des scalaires complexes.

Puisqu'une base de l'espace vectoriel $\mathbb{C}^3$ contient trois vecteurs, $dim_{\mathbb{C}}(\mathbb{C}^3) = 3$.

2. Dimension de l'espace vectoriel $\mathbb{C}^3$ sur le corps $\mathbb{R}$.

Dans ce cas-ci, les trois vecteurs $(1,0,0), (0,1,0), (0,0,1)$ n'engendrent plus $\mathbb{C}^3$.
En effet, si le triplet $(a+ib, c+id, e+if) \in \mathbb{C}^3$, il ne peut pas s'écrire comme combinaison linéaire de ces trois vecteurs car les scalaires de la combinaison linéaire doivent être puisés dans $\mathbb{R}$. Les parties imaginaires des nombres complexes constituant le triplet ne peuvent pas être engendrées par des vecteurs à composantes réelles uniquement.

Introduisons donc trois autres vecteurs linéairement indépendants avec des composantes complexes. Le plus simple est d'ajouter les trois vecteurs $(i,0,0), (0,i,0), (0,0,i)$.

Nous laissons au lecteur le soin de vérifier que les six vecteurs
$(1,0,0), (0,1,0), (0,0,1), (i,0,0), (0,i,0), (0,0,i)$ sont linéairement indépendants.
A présent, le triplet $(a+ib, c+id, e+if)$ peut s'écrire comme combinaison linéaire des vecteurs de la base :

$$(a+ib, c+id, e+if) = \alpha(1,0,0) + \beta(0,1,0) + \gamma(0,0,1) + \delta(i,0,0) + \eta(0,i,0) + \epsilon(0,0,i)$$

où $\alpha, \beta, \gamma, \delta, \eta, \epsilon \in \mathbb{R}$.
On obtient en effet que $\alpha = a$, $\delta = b$, $\beta = c$, $\eta = d$, $\gamma = e$ et $\epsilon = f$; les scalaires sont bien des réels. Ces six vecteurs forment un système de générateurs de $\mathbb{C}^3$.

Puisqu'on a trouvé une base de $\mathbb{C}^3$ qui contient six vecteurs, $dim_{\mathbb{R}}(\mathbb{C}^3) = 6$.

En conclusion, la dimension de $\mathbb{C}^3$ peut changer selon le corps de base.
De plus, la relation suivante est vérifiée :

$$dim_{\mathbb{R}}(\mathbb{C}^3) = 2.dim_{\mathbb{C}}(\mathbb{C}^3).$$

Généralisons ce que nous venons de découvrir grâce à cet exemple.

Un espace vectoriel E complexe (c'est-à-dire dont le corps de base est $\mathbb{C}$) peut être vu comme un espace vectoriel réel (c'est-à-dire dont le corps de base est $\mathbb{R}$).

On peut démontrer la relation générale suivante

$$\dim_{\mathbb{R}}(E) = 2\dim_{\mathbb{C}}(E).$$

Le théorème suivant nous fournit plusieurs caractérisations utiles des bases d'un espace vectoriel de dimension finie.

Théorème 3.3.2 (Caractérisations des bases dans un espace vectoriel)
Soient E un espace vectoriel quelconque sur un corps K et $(x_i)_{i=1}^n$ une famille de vecteurs de E.
Alors, les propriétés suivantes sont équivalentes.

1) *Les vecteurs de la famille $(x_i)_{i=1}^n$ forment une base de E.*
2) *Les vecteurs $x_1, \ldots, x_n$ sont linéairement indépendants et E est de dimension n.*
3) *Les vecteurs $x_1, \ldots, x_n$ sont linéairement indépendants et toute partie libre de E comporte au plus n éléments.*
4) *Les vecteurs $x_1, \ldots, x_n$ engendrent E et E est de dimension n.*
5) *Les vecteurs $x_1, \ldots, x_n$ engendrent E et tout système générateur de E comporte au moins n éléments.*

Preuve :

Nous prouverons ce théorème en montrant que 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 4) $\Rightarrow$ 5) et enfin, nous terminerons en montrant que 5) $\Rightarrow$ 1).

1) $\Rightarrow$ 2) Evident

2) $\Rightarrow$ 3) On sait par le corollaire 3.2.1 qu'une famille libre fait toujours partie d'une base. Une famille libre contient donc au plus n vecteurs, étant donné que E est de dimension n par hypothèse.

3) $\Rightarrow$ 4) Soit $x \in E$ et montrons qu'il peut s'écrire comme une combinaison linéaire des vecteurs $x_1, \ldots, x_n$.
Par hypothèse, nous savons que toute partie libre possède au plus n éléments, donc il existe une relation non triviale qui relie les $n+1$ vecteurs $x_1, \ldots, x_n, x$

$$\lambda_1 x_1 + \ldots + \lambda_n x_n + \lambda x = 0$$

où le scalaire $\lambda \neq 0$. Sinon, on aurait une relation non triviale entre les vecteurs x_i, ce qui contredirait l'hypothèse selon laquelle ils sont linéairement indépendants. On peut donc inverser λ dans le corps K, et par conséquent, on obtient

$$x = -\lambda^{-1}\lambda_1 x_1 + \ldots + \lambda^{-1}\lambda_n x_n.$$

Le vecteur x s'écrit comme combinaison linéaire des vecteurs x_i, ce qui prouve que les x_i forment un système de générateurs de E.
Comme ils sont linéairement indépendants, ils forment aussi une base de E, qui est par conséquent de dimension n.

4) $\Rightarrow$ 5) Par le théorème 3.2.3, on sait que tout système de générateurs de E contient une base de E. Comme par hypothèse, $\dim(E) = n$, tout système de générateurs possède au moins n vecteurs.

5) $\Rightarrow$ 1) D'après le théorème 3.2.3, tout système de générateurs d'un espace vectoriel comprend une base de cet espace. La famille $(x_i)_{i=1}^n$ contient donc une base de E.
Or par hypothèse, tout système de générateurs comporte au moins n éléments. Par conséquent, les vecteurs de la famille $(x_i)_{i=1}^n$ forment nécessairement une base de E et le théorème est démontré. ∎

De nouveau, on remarque que l'hypothèse « ***E* est un espace vectoriel** » est une hypothèse indispensable pour démontrer le théorème précédent. Ce dernier théorème n'est effectivement pas valable dans un module en général, comme l'illustre l'exemple suivant.

Objectif de l'exemple 3.3.2 :
Le premier objectif de cet exemple est de montrer que le théorème précédent n'est pas valable dans un module. Dans un espace vectoriel, ce théorème affirme que n vecteurs forment une base si et seulement si ils sont linéairement indépendants et l'espace est de dimension n.
Mais ici, nous considérons le $\mathbb{Z}$-module $\mathbb{Z}^3$, qui possède une base de 3 vecteurs et montrons que 3 vecteurs linéairement indépendants ne forment pas obligatoirement une base.

Le deuxième objectif de cet exemple est de montrer que, dans un $\mathbb{Z}$-module $\mathbb{Z}^3$, des vecteurs linéairement indépendants ne font pas partie obligatoirement d'une base de ce module. Cet exemple montre donc que le corollaire 3.2.1 n'est pas valable dans les modules.

Exemple 3.3.2
Soit le $\mathbb{Z}$-module $\mathbb{Z}^3$. Essayons de trouver trois vecteurs qui forment une base de ce module.

Question
Les vecteurs suivants forment-ils une base du $\mathbb{Z}$-module $\mathbb{Z}^3$:

1. $(2,3,1)$, $(1,2,3)$, $(4,5,-3)$?
2. $(2,1,1)$, $(1,2,2)$, $(1,2,1)$?
3. $(1,1,1)$, $(1,1,0)$, $(1,0,0)$?

Si non, ces triplets de vecteurs font-ils partie d'une base du $\mathbb{Z}$-module $\mathbb{Z}^3$?

Résolution

D'après la définition 3.2.3, des vecteurs de $\mathbb{Z}^3$ forment une base du module $\mathbb{Z}^3$ s'ils sont linéairement indépendants et s'ils engendrent $\mathbb{Z}^3$.

1. Considérons les trois vecteurs $(2,3,1)$, $(1,2,3)$, $(4,5,-3)$.
   On vérifie aisément que ces trois vecteurs sont liés et ne forment donc pas une base de $\mathbb{Z}^3$. Comme des vecteurs d'une base sont nécessairement linéairement indépendants, cet ensemble de vecteurs ne peut pas faire partie d'une base.

2. Considérons les trois vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$.
   On vérifie que ces vecteurs sont linéairement indépendants. Par contre, ils ne sont pas générateurs de $\mathbb{Z}^3$. En effet, si on écrit tout élément de $\mathbb{Z}^3$ comme combinaison linéaire de ces vecteurs c'est-à-dire si

$$\forall\ (x,y,z) \in \mathbb{Z}^3, \quad (x,y,z) = \lambda_1(2,1,1) + \lambda_2(1,2,2) + \lambda_3(1,2,1),$$

   on peut montrer que les scalaires λ_1, λ_2 et λ_3 ne sont pas (en général) des éléments de $\mathbb{Z}$.

   Ces trois vecteurs linéairement indépendants font-ils partie d'une base du $\mathbb{Z}$-module $\mathbb{Z}^3$? Autrement dit, pourrait-on ajouter un vecteur (ou plus) à ce triplet pour que l'ensemble des vecteurs forment une base ?

   Pour répondre à cette question, ajoutons à ce triplet un quatrième vecteur quelconque (a,b,c) de $\mathbb{Z}^3$, et considérons la combinaison linéaire suivante entre les quatre vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$, (a,b,c) :

$$\alpha(2,1,1) + \beta(1,2,2) + \gamma(1,2,1) + \delta(a,b,c) = (0,0,0), \quad \text{avec } \alpha,\beta,\gamma,\delta \in \mathbb{Z}. \tag{3.12}$$

   Si l'on trouve une relation non triviale entre ces quatre vecteurs, c'est-à-dire si on peut trouver un quadruplet de scalaires $(\alpha,\beta,\gamma,\delta) \neq (0,0,0,0)$, cela signifie que les quatres vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$, (a,b,c) sont linéairement dépendants.

   Or, on peut vérifier que le quadruplet $(\alpha,\beta,\gamma,\delta) = (b-2a, b+a-3c, 3(c-b), 3)$ est une relation linéaire entre les vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$, (a,b,c) c'est-à-dire qu'il vérifie l'égalité 3.12. De plus, cette relation linéaire est non triviale puisque $(b-2a, b+a-3c, 3(c-b), 3)$ est toujours différent de $(0,0,0,0)$.
   Les vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$, (a,b,c) sont donc linéairement dépendants, et cela quel que soit le vecteur (a,b,c) de $\mathbb{Z}^3$.

   Donc, les trois vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$ ne pourront jamais être complétés pour former une base.
   Cet exemple montre que le corollaire 3.2.1, que nous avons démontré dans le cadre des espaces vectoriels, n'est pas valable en général dans les modules.

3. Considérons les trois vecteurs $(1,1,1)$, $(1,1,0)$, $(1,0,0)$.
   Dans ce cas, on peut vérifier que ces vecteurs sont non seulement linéairement indépendants mais aussi générateurs de $\mathbb{Z}^3$. Par définition, ils forment une base de $\mathbb{Z}^3$.

On constate d'après cet exemple que trois vecteurs linéairement indépendants ne forment pas toujours une base de $\mathbb{Z}^3$, ce qui est un résultat quelque peu déroutant si on le confronte aux propriétés connues des espaces vectoriels.
En effet, dans un espace vectoriel de dimension 3 (c'est-à-dire dont les bases contiennent toutes 3 vecteurs), 3 vecteurs linéairement indépendants forment automatiquement une base. Ce n'est pas le cas ici. On sait que les 3 vecteurs $(1,1,1)$, $(1,1,0)$, $(1,0,0)$ forment une base du $\mathbb{Z}$-module $\mathbb{Z}^3$ mais, les 3 vecteurs $(2,1,1)$, $(1,2,2)$, $(1,2,1)$ qui sont linéairement indépendants n'en forment pas une.

Enfin, nous terminons cette section sur la dimension d'un espace vectoriel en énonçant un théorème qui permet de faire le lien entre dimension et isomorphisme d'espaces vectoriels.

Théorème 3.3.3
Soit E et F deux espaces vectoriels de dimension finie sur un même corps K.
Alors, L *et* M *sont isomorphes*

$$\Leftrightarrow$$

$$dim(E) = dim(F).$$

Preuve :

Si l'on suppose qu'il existe un isomorphisme f (c'est-à-dire une application linéaire bijective) entre E et F, alors, par le théorème 3.1.4, on sait que toute base de E est transformée par f en une base de F. Donc, $dim(E) = dim(F)$.

Inversément, si l'on suppose que $dim(E) = dim(F) = n$, alors, E et F sont isomorphes à K^n d'après le corollaire 3.1.2.
Puisque E et F sont isomorphes tous les deux à K^n, ils sont isomorphes entre eux. ∎

3.4 Comparaison entre modules et espaces vectoriels

Pour clôturer ce travail, nous proposons, en guise de synthèse, une comparaison entre les concepts de module et d'espace vectoriel. Pour ce faire, nous reprenons les différentes notions et résultats abordés et mettons en évidence des similitudes ou des différences entre ces deux objets mathématiques. Pour chaque thème, nous présentons la comparaison sous forme de tableau.

3.4.1 Définitions

La différence entre les définitions de module et d'espace vectoriel se situe uniquement au niveau de l'anneau de base, puisque, pour un espace vectoriel, on impose à cet anneau d'être un corps (définition 1.2.4).
Le fait que les scalaires d'un module ne soient pas toujours inversibles a d'importantes conséquences dans la suite.

Espaces vectoriels	**Modules**
Un espace vectoriel *[à droite]* sur K **est un triplet $\{E, +, \bullet\}$ tel que**	**Un K-module à gauche *[à droite]*** **est un triplet $\{M, +, \bullet\}$ tel que**
- $\{E, +\}$ est un groupe commutatif	- $\{M, +\}$ est un groupe commutatif
- $\forall\ \alpha, \beta \in K, \forall\ x \in E,\ (\alpha\beta)x = \alpha(\beta x)$ $[\ x(\alpha\beta) = (x\alpha)\beta\ ]$	- $\forall\ \alpha, \beta \in K, \forall\ x \in M,\ (\alpha\beta)x = \alpha(\beta x)$ $[\ x(\alpha\beta) = (x\alpha)\beta\ ]$
- $\forall\ x \in E,\ \mathbf{1}\ x = x$	- $\forall\ x \in M,\ \mathbf{1}\ x = x$
- $\forall\ \alpha \in K, \forall\ x, y \in E,\ \alpha(x+y) = \alpha x + \alpha y$	- $\forall\ \alpha \in K, \forall\ x, y \in M,\ \alpha(x+y) = \alpha x + \alpha y$
- $\forall\ \alpha, \beta \in K, \forall\ x \in E,\ (\alpha+\beta)x = \alpha x + \beta x$	- $\forall\ \alpha, \beta \in K, \forall\ x \in M,\ (\alpha+\beta)x = \alpha x + \beta x$
et où $\bullet$ représente la loi externe définie par : $\bullet : \{K, +, \cdot\} \times \{E, +\} \longrightarrow \{E, +\}$ $(\lambda, x) \mapsto \lambda \bullet\ x = \lambda x$ où $\{K, +, \cdot\}$ est **UN CORPS.**	et où $\bullet$ représente la loi externe définie par : $\bullet : \{K, +, \cdot\} \times \{M, +\} \longrightarrow \{M, +\}$ $(\lambda, x) \mapsto \lambda \bullet\ x = \lambda x$ où $\{K, +, \cdot\}$ est **UN ANNEAU.**
La multiplication des scalaires de K vérifie la symétrisabilité : $\forall\ \alpha \in K \setminus \{0\},\ \exists\ \beta \in K,\ \alpha \cdot \beta = \mathbf{1} = \beta \cdot \alpha$ Tous les scalaires sont inversibles (sauf le neutre de l'addition sur K).	La multiplication des scalaires de K ne vérifie pas obligatoirement la symétrisabilité. Il se peut que certains scalaires (autres que le neutre de l'addition sur K) ne soient pas inversibles.

Espaces vectoriels (e.v.)	**Modules**
K n'est pas trivial.	K peut être l'anneau trivial.
Si K est commutatif, tout e.v. à gauche sur K est un e.v. à droite sur K et réciproquement. On parle alors d'espace vectoriel sur K.	**Si K est commutatif,** tout K-module à gauche est un K-module à droite et réciproquement. On parle alors de K-module.

3.4.2 Sous-modules et sous-espaces vectoriels

Les définitions ainsi que les caractérisations sont tout à fait semblables pour les sous-modules et les sous-espaces vectoriels mis à part le fait que, dans le cas d'un sous-espace vectoriel, K est un corps.

Sous-espaces vectoriels (s.e.v)	**Sous-modules (s.m.)**
Soit E un espace vectoriel à gauche sur K.	Soit M un K-module à gauche.
Définition	
Un s.e.v. est une partie de E qui est encore un espace vectoriel sur K.	Un s.m. est une partie de M qui est encore un K-module.
Une partie E' de E est **un sous-espace vectoriel de E** si - E' est un sous-groupe du groupe E - $\forall x \in M'$, $\forall \lambda \in \underbrace{K}_{\text{CORPS}}$, $\lambda x \in E'$.	Une partie M' de M est **un sous-module de M** si - M' est un sous-groupe du groupe M - $\forall x \in M'$, $\forall \lambda \in \underbrace{K}_{\text{ANNEAU}}$, $\lambda x \in E'$.
Le neutre de E appartient à tous les s.e.v. de E.	Le neutre de M appartient à tous les s.m. de M.
Caractérisation	
La partie E' est un sous-espace vectoriel de $E \Leftrightarrow$ - E' est non vide - $\forall\ \alpha, \beta \in K, \forall\ x, y \in E'$, $\alpha x + \beta y \in E'$.	La partie M' est un s.m. de $M \Leftrightarrow$ - M' est non vide - $\forall\ \alpha, \beta \in K, \forall\ x, y \in M'$, $\alpha x + \beta y \in M'$.

3.4.3 Homomorphismes

Les notions d'homomorphisme de modules et d'homomorphisme d'espaces vectoriels sont totalement semblables. En effet, le seul changement se situe dans la deuxième définition : K est un corps dans le cas des homomorphismes d'espaces vectoriels.

De plus, on observe que la caractérisation d'homomorphisme ainsi que les théorèmes cités ci-dessous sont similaires que l'on soit dans un module ou dans un espace vectoriel.

Homomorphisme d'espaces vectoriels	**Homomorphisme de modules**
Soient E et F deux espaces vectoriels à gauche sur le même corps K.	Soient M et N deux modules à gauche sur le même anneau K.
Définition	
Une application $f : E \to F$ est un **homomorphisme d'espaces vectoriels** ou une **application linéaire de E dans F** si - $\forall\, x, y \in E,\ f(x+y) = f(x) + f(y)$ - $\forall\, \alpha \in \underbrace{K}_{\text{CORPS}},\ \forall\, x \in E,\ f(\alpha x) = \alpha f(x)$	Une application $f : M \to N$ est un **homomorphisme de modules** ou une **application linéaire de M dans N** si - $\forall\, x, y \in M,\ f(x+y) = f(x) + f(y)$ - $\forall\, \alpha \in \underbrace{K}_{\text{ANNEAU}},\ \forall\, x \in M,\ f(\alpha x) = \alpha f(x)$
Caractérisation	
f est un homomorphisme de E dans $F \Leftrightarrow$ $\forall\, x, y \in E,\ \forall\, \alpha, \beta \in K,$ $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$	f est un homomorphisme de M dans $N \Leftrightarrow$ $\forall\, x, y \in M,\ \forall\, \alpha, \beta \in K,$ $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$

Homomorphisme d'espaces vectoriels	**Homomorphisme de modules**
Soient E et F deux espaces vectoriels à gauche sur le même corps K.	Soient M et N deux modules à gauche sur le même anneau K.
Théorème 2.3.1 et son corollaire	
Soit f un homomorphisme de E dans F . L'image par f d'un s.e.v. de E est un s.e.v de F. . L'image réciproque d'un s.e.v. de F est un s.e.v. de E. . $Kerf$ et Imf sont des s.e.v. de E et F respectivement.	Soit f un homomorphisme de M dans N . L'image par f d'un s.m. de M est un s.m. de N. . L'image réciproque d'un s.m de N est un s.m. de M. . $Kerf$ et Imf sont des s.m. de M et N respectivement.
Théorème 2.3.3	
Si K est commutatif, $\{Hom(E,F),+,\cdot\}$ est un espace vectoriel sur K.	Si K est commutatif, $\{Hom(M,N),+,\cdot\}$ est un K-module.

3.4.4 Les bases

Dans le troisième chapitre, on observe que les notions de combinaison linéaire, de famille de scalaires presque tous nuls, de relation linéaire, de système générateur, d'indépendance linéaire ou encore de base sont définies dans le cadre général des modules, et sont donc valables dans le cadre particulier des espaces vectoriels.

Espaces vectoriels (e.v.)	**Modules**
Définitions	
Soit E un e.v à gauche sur K, et $(a_i)_{i\in I}$ une famille de vecteurs de E, $x \in E$ est **combinaison linéaire** des vecteurs a_i $(i \in I)$ si $\exists\,(\lambda_i)_{i\in I}$, une famille de scalaires presque tous nuls de K tel que $x = \sum_{i\in I} \lambda_i a_i$.	Soit M un K-module à gauche, et $(a_i)_{i\in I}$ une famille de vecteurs de M, $x \in M$ est **combinaison linéaire** des vecteurs a_i $(i \in I)$ si $\exists\,(\lambda_i)_{i\in I}$, une famille de scalaires presque tous nuls de K tel que $x = \sum_{i\in I} \lambda_i a_i$.

Espaces vectoriels (e.v.)	**Modules**
Définitions	
Soit E un e.v à gauche sur K, et $(a_i)_{i\in I}$ une famille de vecteurs de E,	Soit M un K-module à gauche, et $(a_i)_{i\in I}$ une famille de vecteurs de M,
- E est **engendré par les vecteurs** a_i $(i \in I)$ si E est l'ensemble des combinaisons linéaires de ces vecteurs	- M est **engendré par les vecteurs** a_i $(i \in I)$ si M est l'ensemble des combinaisons linéaires de ces vecteurs
- un e.v. qui est engendré par un nombre fini de vecteurs est appelé **e.v. de dimension finie.** Ces vecteurs forment un système de générateurs de E.	- Un module qui est engendré par un nombre fini de vecteurs est appelé **module libre de type fini.** Ces vecteurs forment un système de générateurs de M.
- les vecteurs a_i $(i \in I)$ sont **linéairement indépendants** ou la famille $(a_i)_{i\in I}$ est **libre** si, $\sum_{i\in I} \lambda_i a_i = 0 \Rightarrow \forall\, i \in I,\ \lambda_i = 0$, $\forall$ $(\lambda_i)_{i\in I}$ famille de scalaires presque tous nuls de K.	- les vecteurs a_i $(i \in I)$ sont **linéairement indépendants** ou la famille $(a_i)_{i\in I}$ est **libre** si, $\sum_{i\in I} \lambda_i a_i = 0 \Rightarrow \forall\, i \in I,\ \lambda_i = 0$, $\forall$ $(\lambda_i)_{i\in I}$ famille de scalaires presque tous nuls de K.

La première différence entre modules et espaces vectoriels est donnée par le théorème 3.1.1, qui nécessite que K soit un corps pour être démontré.

Espaces vectoriels (e.v.)	**Modules**
Dire que des vecteurs non nuls sont linéairement dépendants...	
... implique que l'on peut toujours écrire l'un d'eux comme combinaison linéaire des autres. Proposition 3.1.1	... n'implique pas obligatoirement qu'un de ces vecteurs soit combinaison linéaire des autres Illustration : exemple 3.1.4

Le théorème 3.1.4 ainsi que ses deux corollaires (3.1.2 et 3.1.3) ne nécessitent pas que K soit un corps pour être démontrés. Ils sont donc valables aussi bien dans les modules que dans les espaces vectoriels. Nous ne présentons ici que le théorème 3.1.4.

Théorème 3.1.4

Soient M un K-module à gauche libre et de type fini ou un espace vectoriel à gauche sur K de dimension finie ainsi que $(a_i)_{i=1}^n$ une base de M.

Soient N un K-module à gauche quelconque et $c_1, \ldots, c_n$ des éléments de N.

Alors, il existe une et une seule application linéaire de M dans N qui vérifie $f(a_i) = c_i, \quad 1 \leq i \leq n$.

De plus, on a les équivalences suivantes :

f est injective $\iff$ Les vecteurs $c_1, \ldots, c_n$ sont linéairement indépendants

f est surjective $\iff$ Les vecteurs $c_1, \ldots, c_n$ engendrent N.

Les théorèmes d'existence et de caractérisation des bases nous permettent de différencier davantage les espaces vectoriels des modules. Un autre critère de dissimilitude important entre ces deux concepts est le nombre de vecteurs dans une base.

Espaces vectoriels (e.v.)	**Modules**
Existence de base	
Tout espace vectoriel admet une base. Théorème 3.2.1	Certains modules n'admettent pas de base. Illustration : exemple 3.2.1
Un ensemble de vecteurs linéairement indépendants...	
...peut toujours être complété pour former une base Corollaire 3.2.1	...peut ne pas faire partie d'une base Illustration : exemple 3.3.2
Théorème 3.3.1 : Nombre de vecteurs dans une base	
Théorème 3.3.1 : Deux bases d'un même e.v. contiennent toujours le même nombre de vecteurs	Le théorème 3.3.1 n'a pas d'équivalent dans les modules
La **dimension d'un e.v.** est le nombre de vecteurs d'une base de cet e.v.	——

Conclusion

Dans ce mémoire, nous avons réalisé une production didactique à destination des étudiants en cours de première année universitaire en mathématiques. Un des objectifs de ce mémoire est de les conscientiser à l'existence d'un cadre plus large que celui des espaces vectoriels de dimension finie dans lesquels ils ont l'habitude de travailler : celui des modules. Ceci nous a conduits à mettre progressivement en évidence les conséquences de cet élargissement de cadre.
La lecture de quelques ouvrages nous a permis de réfléchir à une structure didactique à mettre en place pour faciliter la compréhension en profondeur de ces concepts.

Après avoir rédigé un premier chapitre de rappels sur les structures algébriques de groupe, d'anneau et de corps, nous avons introduit, dans un deuxième chapitre, la notion de module ainsi que quelques résultats importants. Le troisième chapitre, consacré aux bases dans un module, nous a permis de distinguer davantage les modules des espaces vectoriels et d'étayer la comparaison entre ces deux objets mathématiques, notamment grâce aux théorèmes d'existence et de caractérisation des bases.
Ces différences, pouvant aller à l'encontre des conceptions des étudiants, ont été mises en lumière par divers exemples tout au long du travail.
Néanmoins, faute de temps, certaines différences n'ont pas été suffisament illustrées et investiguées, comme par exemple, le questionnement concernant le nombre de vecteurs constituant deux bases distinctes d'un même module. Elaborer des exercices supplémentaires serait un premier prolongement possible. Une autre pespective serait de prolonger la comparaison en travaillant, dans le cadre des modules puis dans celui des espaces vectoriels, d'autres notions comme la représentation matricielle d'un homomorphisme ou encore la dualité. Enfin, il serait intéressant de proposer cette production aux étudiants et d'analyser leurs difficultés et leurs erreurs, dans les exercices notamment, afin de l'adapter et de l'améliorer.

Bibliographie

[1] Adkins William A., Weintraub Steven H., *Algebra - An Approach via Module Theory*, Springer, United States of America, 1999.

[2] Colson B., Jancart S., Lemaitre A., *Recueil d'exercices d'Algèbre pour les premiers baccalauréats en Sciences mathématiques et physiques*, Librairie des Sciences, Namur, 2004-2005.

[3] Godement R., *Cours d'algèbre*, 3ème édition, Hermann, Toulouse, 1978.

[4] Mersch J., *Algèbre - Première candidature en Sciences Mathématiques*, Librairie des Sciences, Namur, 1989.

[5] Mersch J., Duchâteau C., Thiry S., *Recueil d'exercices d'Algèbre pour les premières candidatures en Sciences mathématiques*, Librairie des Sciences, Namur, 1978.

[6] Schumacher C., *Chapter Zero / Fundamental Notions of Abstract Mathematics* , Addison-Wesley Publishing Company, United States of America, 1996.

[7] Thiry S., *Algèbre supérieure (compléments) - Deuxièmes baccalauréats en Sciences mathématiques*, Librairie des Sciences, Namur, 2005-2006.

[8] Toint P., *Algèbre - Premièrs baccalauréats en Sciences mathématiques et physiques*, Librairie des Sciences, Namur, 2004-2005.