COLLECTION ENSEIGNEMENT SUP //// Mathématiques

L3M1M2

Algèbre II

ANNEAUX, MODULES ET ALGÈBRE MULTILINÉAIRE

$$\Lambda(M) = \bigoplus_p \Lambda^p(M) \qquad M \otimes_A N$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \arrow[d, "\pi'"] \\ A/I \arrow[r, "\overline{f}"'] & B/J \end{tikzcd}$$

$$A \longrightarrow S^{-1}A \qquad \mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

Daniel Guin

edp sciences

ALGÈBRE

Tome 2

ANNEAUX, MODULES ET ALGÈBRE MULTILINÉAIRE

Daniel Guin

edp sciences

17, avenue du Hoggar
Parc d'activités de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

Illustration de couverture :

Imprimé en France

ISBN : 978-2-7598-1001-7

TABLE DES MATIÈRES

AVANT-PROPOS

Cet ouvrage fait suite à celui intitulé « Algèbre I » (écrit en collaboration avec Thomas Hausberger) dont je reprends ici une partie de l'avant-propos.

La très longue histoire de l'étude des nombres, puis des équations, a permis de remarquer des analogies entre certaines propriétés vérifiées par des objets mathématiques de natures différentes, par exemple les nombres et les polynômes. Cela a conduit les mathématiciens, en particulier au XIX^{e} siècle, à tenter de dégager une axiomatique qui rende compte des raisons profondes de ces analogies. Il est alors apparu que ces objets, de natures différentes, possédaient les mêmes *structures algébriques*, par exemple groupe, espace vectoriel, anneau, etc.

Il devint évident qu'il était plus efficace d'étudier ces structures pour elles-mêmes, indépendamment de leurs réalisations concrètes, puis d'appliquer les résultats obtenus dans les divers domaines que l'on considérait antérieurement.

L'algèbre abstraite était née.

C'est l'étude des équations algébriques qui est à l'origine de la création et du développement de l'algèbre, dont le nom provient du titre d'un traité d'Al-Khowarizmi. D'abord exclusivement dévolue au calcul, à l'introduction des outils (nombres négatifs, extraction de racines, nombres complexes) et à l'élaboration des règles d'utilisation de ces objets, l'algèbre a évolué vers ce qu'elle est maintenant, l'étude des structures.

L'étude des nombres entiers remonte à la plus Haute Antiquité, mais c'est l'étude des *nombres algébriques*, au XIX^{e} siècle, qui a conduit aux notions d'***anneau*** et de ***corps***.

L'étude de la divisibilité dans les nombres entiers est basée sur la propriété fondamentale suivante : tout nombre entier s'écrit, de manière unique, comme produit de nombres premiers. Comme pour toutes les structures algébriques importantes, la structure d'anneau apparaît dans de nombreuses situations dans lesquelles les éléments ne sont plus des nombres entiers. C'est en particulier le cas des polynômes. Il est donc utile, en étudiant la notion de divisibilité dans des anneaux généraux, de voir si l'analogue de la décomposition en produit de nombres premiers existe : on l'appelle alors décomposition en produit d'éléments irréductibles. Cela conduit à la notion d'anneau ***factoriel*** qui généralise les notions d'anneau ***euclidien*** ou ***principal*** (chapitre II). On étudie ensuite cette décomposition dans le cas des anneaux de polynômes (chapitre III).

L'idée essentielle a été l'introduction de la notion d'idéal : celle-ci permet de généraliser des énoncés portant sur les propriétés usuelles de la divisibilité des nombres entiers. En particulier, la généralisation aux idéaux de la propriété de décomposition en produit d'irréductibles, associée à la notion d'extension de corps, a permis de faire de très grands progrès en arithmétique, notamment avec l'étude des anneaux de ***Dedekind*** (chapitre VI).

La structure d'espace vectoriel (sur un corps), qui est l'une des plus fécondes des mathématiques, a des applications très nombreuses, non seulement en mathématique, mais également en physique, chimie, biologie et sciences humaines. C'est la raison pour laquelle l'***algèbre linéaire*** est un domaine fondamental et son étude cruciale.

Si l'on remplace le corps de base par un anneau, la définition de la structure d'espace vectoriel garde tout son sens et, pour la différencier de la notion précédente, on parle de structure de ***module*** (sur un anneau) (chapitre IV). Cette structure de module possède beaucoup de propriétés des espaces vectoriels, mais elle est plus subtile et certains résultats fondamentaux des espaces vectoriels ne sont plus valables : par exemple, un module ne possède pas nécessairement une base. Néanmoins, cette structure algébrique est d'une grande richesse – en particulier si l'anneau de base est principal (chapitre V) et relativement à la ***dualité*** (chapitre VII) – et intervient naturellement dans de nombreux contextes mathématiques ou autres.

On sait que les ***applications linéaires*** sont au cœur de l'algèbre linéaire, mais de nombreux problèmes font apparaître des applications de plusieurs variables, linéaires en chaque variable, les applications ***multilinéaires***. Pour en simplifier l'étude, l'on se ramène à des applications linéaires en utilisant le ***produit tensoriel*** (chapitre VIII) ou le ***produit extérieur*** (chapitre IX). Cela conduit aux notions d'***algèbre tensorielle*** ou ***algèbre extérieure***, qui sont des outils très puissants en algèbre et géométrie.

Comme dans le cas des groupes, la structure d'anneau a donné naissance à une approche algébrique de la géométrie, en particulier des courbes et des surfaces : la géométrie algébrique. Cette démarche « algébrique » a été également appliquée, de manière très efficace, en analyse – groupes topologiques, espaces vectoriels normés, algèbres de Banach.

Par le programme couvert, ces deux ouvrages Algèbre I – Groupes, Corps et Théorie de Galois et Algèbre II – Anneaux, Modules et Algèbre Multilinéaire s'adressent aux étudiants de L3 et master et leur contenu fait partie de la culture normale d'un candidat à l'agrégation de mathématiques.

This page intentionally left blank

REMERCIEMENTS

Ce texte doit beaucoup à la relecture de Jean-Michel Oudom. Il a résolu tous les exercices et TR, ce qui a conduit, dans bien des cas, à une amélioration notable de leurs énoncés.

Qu'il trouve ici l'expression de mon amicale reconnaissance.

This page intentionally left blank

AVERTISSEMENT

Depuis plusieurs années, l'enseignement de l'algèbre en L1–L2 se limite généralement à l'algèbre linéaire. Cet ouvrage, en deux volumes, donne une présentation des thèmes d'un enseignement d'algèbre générale – groupes, anneaux, corps – et donne une introduction à l'algèbre multilinéaire, sans connaissance préalable nécessaire de ces domaines. On s'est volontairement limité à un exposé simple des concepts fondamentaux qui trouvent leurs places dans un enseignement de L3 et M1.

Chaque chapitre comporte, dans le cours du texte, des exemples et des exercices qui illustrent les notions développées, au fur et à mesure qu'elles apparaissent. Les exercices signalés par le symbole ¶ sont plus difficiles que les autres.

À la fin de chacun des chapitres, on trouvera des thèmes de réflexion (TR) (et des travaux pratiques (TP) pour « *Algèbre I* »).

Les TR se présentent sous forme de questions, dont l'énoncé contient la réponse, qui guident le lecteur dans l'étude d'un objet ou d'une notion particulière – illustration, complément ou approfondissement du cours. Ils sont de trois types :

– ceux qui sont signalés par le symbole ♡ doivent être considérés comme du cours et doivent être étudiés comme tel. Ils sont utilisés sans rappel dans les chapitres suivants ;

– ceux qui sont signalés par le symbole ♣ sont des problèmes d'application qui utilisent des notions développées dans le chapitre concerné ou dans ceux qui précèdent ;

– ceux qui sont signalés par le symbole ♠ sont des approfondissements plutôt destinés aux étudiants préparant l'agrégation.

Certains de ces TR sont repris dans plusieurs chapitres : on peut ainsi constater comment l'enrichissement de la théorie permet d'étudier, de façon de plus en plus fine, un même objet.

Les exercices et les TR de ce tome 2 représentent près de 300 questions, dont la résolution permettra au lecteur d'acquérir une bonne maîtrise des concepts de base concernant les anneaux (euclidiens, principaux, factoriels, de Dedekind), l'arithmétique (éléments entiers), les modules et l'algèbre multilinéaire.

Les démonstrations intègrent de fréquentes références à des résultats contenus dans ce livre. Celles qui commencent par un chiffre romain, renvoient à un résultat contenu dans le chapitre correspondant à ce chiffre. Les autres renvoient à un résultat contenu dans le chapitre en cours. Le symbole $\diamondsuit$ indique la fin, ou l'absence, d'une démonstration.

Première partie

Anneaux et modules

This page intentionally left blank

I

GÉNÉRALITÉS SUR LES ANNEAUX

1. Définitions – Exemples

Rappelons qu'un groupe est la donnée d'un ensemble non vide G **et** d'une loi de composition interne

$$G \times G \longrightarrow G$$
$$(x, y) \longmapsto x * y$$

vérifiant les propriétés suivantes :

(i) $\forall\, x, y, z \in G,\ (x * y) * z = x * (y * z)$,
(ii) $\exists\, e \in G$, tel que $\forall\, x \in G, x * e = e * x = x$,
(iii) $\forall\, x \in G, \exists\, \overline{x} \in G$ tel que $x * \overline{x} = \overline{x} * x = e$.

Si, de plus, la propriété suivante est vérifiée :

$$\forall\, (x, y) \in G \times G,\ x * y = y * x,$$

le groupe G est dit commutatif ou abélien.

Définitions 1.1.

a) Un **anneau** est la donnée d'un ensemble non vide A **et** de deux lois de composition interne, notées $+$ et $.$ (appelées respectivement addition et multiplication), telles que :

(i) $(A, +)$ est un groupe abélien (on notera 0 son élément neutre),
(ii) $\forall\, (a, b, c) \in A \times A \times A,\ (a.b).c = a.(b.c)$,
(iii) $\exists\, 1 \in A,\ \ \forall\, a \in A\ \ a.1 = 1.a = a$,
(iv) $\forall\, (a, b, c) \in A \times A \times A,\ \ a.(b + c) = a.b + a.c$ et $(b + c).a = b.a + c.a$.

Si, de plus, la propriété suivante est vérifiée :

$$\forall\,(a,b) \in A \times A,\ a.b = b.a,$$

l'anneau A est dit **commutatif**.

b) Un **corps** est un anneau A non réduit à $\{0\}$ tel que $(A \setminus \{0\}, .)$ soit un groupe.

La propriété (ii) est **l'associativité** de la multiplication ; l'élément 1, dont l'existence est assurée par la propriété (iii), est l'élément neutre de la multiplication et est appelé **l'unité** de l'anneau A ; la propriété (iv) est la **distributivité** de la multiplication par rapport à l'addition.

Remarques 1.2.

a) Dans un anneau A, on a les relations

$$\forall\, a \in A,\ 0.a = a.0 = 0 \quad \text{et} \quad (-1).a = -a.$$

En effet, on a

$$0.a + a = (0+1).a = 1.a = a,\ \text{ d'où }\ 0.a = 0,$$

et de même pour $a.0 = 0$. De plus,

$$(-1).a + a = (-1).a + 1.a = (-1+1).a = 0.a = 0,\ \text{ d'où }\ (-1).a = -a.$$

b) Si $1 = 0$, alors A est réduit à $\{0\}$, car on a alors

$$\forall\, a \in A,\ \ a = 1.a = 0.a = 0.$$

c) De la même manière que ci-dessus, on a

$$\forall\,(a,b) \in A \times A, \quad -(a.b) = (-a).b = a.(-b) \quad \text{et} \quad (-a).(-b) = a.b.$$

Dans la suite, on notera la multiplication dans A par ab, en omettant le point. Bien entendu, les mots « addition » et « multiplication » sont des noms donnés aux opérations définissant la structure d'anneau et ne correspondent pas forcément aux opérations que l'on désigne usuellement par ces termes, cf. E1.2 ci-après.

Exemples 1.3.

a) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, est un anneau commutatif.

b) Les ensembles $\mathbb{Q}$ des nombres rationnels, $\mathbb{R}$ des nombres réels et $\mathbb{C}$ des nombres complexes, munis des opérations usuelles, sont des corps.

c) L'ensemble $M_n(k)$ des matrices (n, n) à coefficients dans un anneau commutatif k, muni de l'addition et de la multiplication des matrices, est un anneau, non commutatif pour $n \geqslant 2$.

d) Soit G un groupe abélien (noté additivement), alors $\mathrm{End}(G)$ muni de l'addition et de la composition des morphismes de groupes est un anneau (en général non commutatif).

e) Pour tout entier $n > 0$, le groupe abélien $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication définie par $cl(p)cl(q) = cl(pq)$ est un anneau commutatif, dont l'unité est $cl(1)$, où $cl(x)$ désigne la classe dans $\mathbb{Z}/n\mathbb{Z}$ de l'élément x de $\mathbb{Z}$.

f) L'ensemble $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$, muni de l'addition et de la multiplication des polynômes, est un anneau commutatif.

Exercice E1.

1. *Soient X un ensemble non vide et A un anneau. On note $\mathcal{F}(X, A)$ l'ensemble des applications de X dans A. Montrer que $\mathcal{F}(X, A)$ muni des opérations définies par*

$$\forall\, f \in \mathcal{F}(X, A),\ \ \forall\, g \in \mathcal{F}(X, A),\ \ \forall\, x \in X,\ \ (f + g)(x) = f(x) + g(x)$$
$$\forall\, f \in \mathcal{F}(X, A),\ \ \forall\, g \in \mathcal{F}(X, A),\ \ \forall\, x \in X,\ \ (fg)(x) = f(x)g(x)$$

est un anneau (commutatif si et seulement si A est commutatif).

2. *Soient X un ensemble et $\mathcal{P}(X)$ l'ensemble des parties de X. Pour deux éléments A et B de $\mathcal{P}(X)$, on pose*

$$A\Delta B = (A \cap (X \setminus B)) \cup (B \cap (X \setminus A)),$$

que l'on appelle ***différence symétrique*** *de A et B. Montrer que $\mathcal{P}(X)$ muni des opérations*

$$\forall A \in \mathcal{P}(X),\ \ \forall B \in \mathcal{P}(X),\ \ (A, B) \mapsto A\Delta B$$
$$\forall A \in \mathcal{P}(X),\ \ \forall B \in \mathcal{P}(X),\ \ (A, B) \mapsto A \cap B$$

est un anneau commutatif.