



SCIENCES SUP

Cours et exercices corrigés

Licence 3 • CAPES • Agrégation

ALGÈBRE POUR LA LICENCE 3

Groupes, anneaux, corps

*Jean-Jacques Risler
Pascal Boyer*

DUNOD

ALGÈBRE POUR LA LICENCE 3

Groupes, anneaux, corps

Jean-Jacques Risler

Professeur à l'université Paris 6
Pierre-et-Marie-Curie

Pascal Boyer

Maître de conférences à l'université Paris 6
Pierre-et-Marie-Curie

DUNOD

Consultez nos catalogues sur le Web



www.dunod.com

Conseiller éditorial : Sinnou David

Illustration de couverture : DigitalVision®

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements



d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).

© Dunod, Paris, 2006

ISBN 2 10 049498 8

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

INTRODUCTION	V
CHAPITRE 1 • L'ANNEAU $\mathbb{Z}$	
1.1 Définitions de base	1
1.2 L'anneau $\mathbb{Z}$. Division euclidienne	7
1.3 Algorithme d'Euclide	8
1.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$	10
Exercices	19
CHAPITRE 2 • MODULES DE TYPE FINI	
2.1 Le langage des modules	25
2.2 Calcul matriciel sur un anneau principal	29
2.3 Modules libres de type fini	35
2.4 Modules de type fini sur un anneau principal	38
2.5 Modules indécomposables	41
Exercices	46
CHAPITRE 3 • RÉDUCTION DES ENDOMORPHISMES	
3.1 L'anneau $K[X]$	49
3.2 Polynôme minimal	50
3.3 Espaces cycliques	52
3.4 Invariants de similitude	53
3.5 Forme réduite de Jordan	55
Exercices	60

CHAPITRE 4 • GROUPES

4.1 Généralités	65
4.2 Le groupe symétrique	68
4.3 Opération d'un groupe sur un ensemble	71
4.4 Quelques exemples liés à la géométrie	78
Exercices	89

CHAPITRE 5 • RACINES DES POLYNÔMES

5.1 Généralités, irréductibilité	97
5.2 Les racines réelles	101
5.3 Résultant et discriminant	106
5.4 *Fonctions symétriques des racines	111
Exercices	115

CHAPITRE 6 • THÉORIE DES CORPS

6.1 Caractéristique	123
6.2 Groupe multiplicatif	124
6.3 Extensions	124
6.4 Corps de rupture	127
6.5 Corps finis	129
6.6 *Compléments	134
Exercices	141

SOLUTIONS DES EXERCICES ET DES PROBLÈMES

Chapitre 1	147
Chapitre 2	160
Chapitre 3	171
Chapitre 4	177
Chapitre 5	187
Chapitre 6	200

RÉFÉRENCES BIBLIOGRAPHIQUES	208
------------------------------------	-----

INDEX	209
--------------	-----

Introduction

Ce livre correspond au cours fondamental d'algèbre professé à l'université Pierre et Marie Curie dans le cadre de la troisième année de la licence de mathématiques (niveau L3 du nouveau cursus LMD).

Le cours correspond à 12 ECTS (quatre heures de cours et six heures de travaux dirigés sur douze semaines).

Le parti pris pédagogique de cet ouvrage est l'inverse de celui habituellement adopté par les cours de mathématiques ; il va du « particulier au général », ce qui implique quelquefois des redites (par exemple les groupes commutatifs (chapitre 2) sont traités avant les groupes généraux (chapitre 4) et certains résultats valables dans les deux cas sont énoncés deux fois). De plus de nombreux résultats sont présentés sous forme d'algorithmes (en particulier les théorèmes du chapitre II).

D'autre part ce livre comprend après chaque chapitre un grand nombre d'exercices et problèmes classés par thèmes et tous corrigés.

Enfin certains développements sont marqués d'une astérisque ; ils concernent des notions un peu plus élaborées, plutôt à notre avis du programme de maîtrise que de licence, et ne sont donc pas enseignés dans le cours dont il a été question plus haut. Cependant ces questions sont classiques et bien à leur place dans le cadre de cet ouvrage.

Le livre comprend six chapitres (plus une dernière partie consacrée à la correction des exercices) largement indépendants les uns des autres et qui exposent les notions fondamentales d'algèbre que tout professionnel des mathématiques (chercheur, enseignant, ingénieur mathématicien) se doit de connaître.

Le premier chapitre débute par une sorte de petit lexique dans lequel sont rassemblées toutes les définitions de base auxquelles le lecteur peut ainsi aisément se reporter ; il traite ensuite de l'arithmétique classique.

Le deuxième chapitre est consacré aux groupes abéliens de type fini et aux modules de type fini sur l'anneau de polynômes $k[X]$; la méthode consiste à utiliser le calcul matriciel à coefficients entiers présenté sous forme algorithmique.

Le chapitre suivant consiste en l'application classique des résultats du chapitre 2 à la réduction des endomorphismes d'un espace vectoriel de dimension finie (forme réduite de Jordan, décomposition de Dunford, etc.).

Le chapitre 4 traite des groupes généraux en évitant le plus possible les notions abstraites conformément au parti pris de ce livre. Il traite essentiellement deux exemples fondamentaux ; le groupe symétrique et le groupe orthogonal en dimension 2 et 3.

Le chapitre 5 s'occupe des racines des polynômes à une variable ; toute la partie sur les racines réelles, pourtant fondamentale, n'est en général pas traitée dans les ouvrages d'enseignement et constitue une des originalités de ce livre.

Enfin le chapitre 6 est une introduction à la théorie des corps, en insistant sur les corps finis.

Chapitre 1

L'anneau $\mathbb{Z}$

Ce chapitre, après une section qui rassemble les définitions de base, traite de l'arithmétique classique : factoriabilité de $\mathbb{Z}$, groupes cycliques, petit théorème de Fermat, lemme chinois, etc.

1.1 DÉFINITIONS DE BASE

Cette section est conçue comme une sorte de lexique dans lequel sont répertoriées les définitions de base (groupes, sous-groupes, anneaux, morphismes, quotients, etc.) utilisées tout au long du livre, de façon à ce que le lecteur puisse s'y référer commodément.

1.1.1. Notations, conventions

- Un objet mathématique (par exemple une application entre deux ensembles, ou un morphisme de groupes) est dit *canonique* si sa définition ne nécessite pas de choix arbitraire (elle ne dépend que des données).
- La notation : « $:=$ » au cours de la description d'un algorithme doit être lue comme « doit être remplacé par ».
- Le symbole : ■ signifie la fin d'une démonstration.
- Certains paragraphes sont précédés d'une astérisque ; ces astérisques indiquent des résultats qui, bien que traitant de questions classiques qui s'insèrent naturellement dans les développements de ce livre, nous semblent dépasser le programme de Licence de mathématiques, et peuvent donc être omis en première lecture.

1.1.2. Généralités

Définition 1.1. Un groupe $(G, *)$ est un ensemble G muni d'une loi de composition interne $G \times G \longrightarrow G, (a, b) \mapsto a * b$, telle que :

1. il existe un élément neutre e , i.e. tel que pour tout $a \in G$, $e * a = a * e = a$;
2. la loi est associative : pour tous $a, b, c \in G$, on a $a * (b * c) = (a * b) * c$;
3. tout élément $a \in G$ a un inverse a' tel que $a * a' = a' * a = e$.

La notation $(G, *)$ pour un groupe précise que la loi de groupe est notée $*$. Si la loi de groupe est notée multiplicativement, le groupe est noté $(G, \times)$ ou simplement G car on omet en général le symbole $\times$. L'élément neutre se note alors 1, et l'inverse de a se note a^{-1} . Pour un groupe $(G, +)$ l'élément neutre se note 0, et l'inverse d'un élément a se note $-a$; par convention, la notation additive est réservée aux groupes commutatifs (cf. la définition ci-dessous).

Définition 1.2.

- Soient G et H deux groupes. On dit d'une application $\phi : G \longrightarrow H$ qu'elle est un morphisme de groupes si elle est compatible avec les lois de groupes (notées ici multiplicativement), i.e. pour tous x et y dans G , $\phi(xy) = \phi(x)\phi(y)$. Cela entraîne que $\phi(1) = 1$ et $\phi(x^{-1}) = (\phi(x))^{-1}$. S'il n'y a pas d'ambiguïté possible, on dira simplement morphisme au lieu de morphisme de groupes.
- Si G est un groupe fini, le cardinal de G , noté $|G|$, s'appelle l'ordre de G .
- Si pour tous $a, b \in G$ on a $ab = ba$, on dit que le groupe est commutatif ou abélien.
- Un sous-groupe d'un groupe G est un sous-ensemble qui contient l'unité et qui est stable pour la loi de groupe et pour l'opération de passage à l'inverse, autrement dit, un sous-ensemble $H \subset G$ d'un groupe G est un sous-groupe si et seulement si $1 \in H$ et $\forall x, y \in H, xy^{-1} \in H$.
- Soient $x_i, (i \in I)$ des éléments d'un groupe G noté multiplicativement. Le sous-groupe engendré par les éléments x_i est l'ensemble des produits finis $x_{i_1}^{\lambda_{i_1}} \dots x_{i_k}^{\lambda_{i_k}}$, les λ_{i_j} parcourant $\mathbb{Z}$. Ce sous-groupe est noté $\langle (x_i)_{i \in I} \rangle$.

Si $\phi : G \rightarrow H$ est un morphisme, il est immédiat de voir que l'image de ϕ (notée $\text{Im } \phi$) est un sous-groupe de H , et que le noyau $\phi^{-1}(e)$ de ϕ (noté $\ker \phi$) est un sous-groupe de G .

Définition 1.3. Soit G un groupe, $g \in G$. L'ordre de g , noté $\text{ord}(g)$, est le cardinal $|\langle g \rangle|$ du groupe $\langle g \rangle$ si $|\langle g \rangle|$ est fini, sinon $\text{ord}(g) = +\infty$ (cf. le lemme 1.34 plus bas).

Définition 1.4.

- Un anneau (commutatif et unitaire) A est un groupe commutatif $(A, +)$ muni d'une deuxième loi de composition interne (notée multiplicativement et appelée multiplication) vérifiant les conditions suivantes :

1. la multiplication est associative, commutative, et possède un élément neutre noté 1 ;
2. la multiplication est distributive par rapport à l'addition, i.e. pour tous $a, b, c \in A$ on a :

$$a(b + c) = ab + bc.$$

- Si A et B sont deux anneaux (commutatifs et unitaires), une application

$$\phi : A \longrightarrow B$$

est un morphisme d'anneaux si elle est compatible avec les opérations des deux anneaux, i.e. si :

1. ϕ est un morphisme des groupes additifs $(A, +)$ et $(B, +)$;
2. $\phi(1) = 1$ et pour tous $a, b \in A$, $\phi(ab) = \phi(a)\phi(b)$.

Dans tout le livre, « anneau » signifiera « anneau commutatif unitaire » (un anneau non commutatif est tel que sa multiplication ne soit pas commutative ; l'addition est toujours commutative).

Définition 1.5. Un corps (commutatif) K est un anneau tel que tout élément non nul soit inversible pour la multiplication.

Remarque 1.6. Soient A et B deux groupes (resp. deux anneaux). Il existe une structure naturelle de groupe (resp. d'anneau) sur le produit cartésien $A \times B$ en définissant les opérations coordonnées par coordonnées. En revanche, si A et B sont des corps commutatifs, l'anneau produit $A \times B$ n'est pas un corps (par exemple les éléments $(1, 0)$ et $(0, 1)$ ne sont pas inversibles pour la multiplication).

Définition 1.7. Un idéal I d'un anneau A est un sous-groupe de $(A, +)$ tel que I soit stable par la multiplication par les éléments de A , i.e. $x \in I$ et $\lambda \in A \implies \lambda x \in I$.

Il est immédiat de voir que le noyau d'un morphisme d'anneaux $\phi : A \rightarrow B$ est un idéal de A . Réciproquement, nous verrons au chapitre suivant (définition 2.3 et remarque 2.9) que tout idéal est le noyau d'un morphisme d'anneaux.

Définition 1.8. Soient x_i ($i \in I$) des éléments d'un anneau A (resp. d'un groupe abélien $(G, +)$). L'ensemble des combinaisons linéaires $\sum_{j=1}^{n_j} \lambda_{i_j} x_{i_j}$, $i_j \in I$, $\lambda_{i_j} \in A$ (resp. $\lambda_{i_j} \in \mathbf{Z}$) est un idéal de A (resp. un sous-groupe de G). On dit que c'est l'idéal (ou le sous-groupe) engendré par les x_i ; c'est aussi le plus petit idéal de A (resp. sous-groupe de G) contenant les x_i .

Si $x_i \in A$ ($i \in I$), on note $((x_i)_{i \in I})$ l'idéal engendré par les éléments x_i . Cet idéal est aussi l'intersection de tous les idéaux de A contenant tous les x_i . Si $\phi : A \rightarrow B$ est un morphisme d'anneaux et $I \subset B$ un idéal, $\phi^{-1}(I)$ est un idéal de A .

Le cas des groupes non commutatifs sera traité au chapitre 4.

Exemple 1.9. Un sous-ensemble $I \subset \mathbf{Z}$ est un idéal de $\mathbf{Z}$ si et seulement si c'est un sous-groupe de $(\mathbf{Z}, +)$.