

ERRATA

Page	Ligne	Erreur
8	19	$d = \text{ppcm}(a, b)$
13	6	divise divise
23	18	...qu'en...
30	12	...l'image l'image...
35	22	..., diverse...
40	24	...par Rapport...
49	27	sont deux comparables
55	14	$f \leq g \iff f(x) \leq g(x), \forall x$
60	19	...entier...
67	5	$f \leq g \iff f(x) \leq g(x), \forall x \in$
78	10	pm $\frac{a}{b}$
82	39	...injective...
91	13	quils
132	27	précédent
137	39	un élément de du g
138	6	[Exercices 3 & ??]
142	29	[Exercice??]
143	1	théorème
145	31	anneaux ! unitaire
147	14	pour la
149	21	[Exercice??]

Table des Matières

Avant Propos

CHAPITRE I. ARITHMÉTIQUE	1
Introduction	1
I.1. Entiers naturels	2
I.2. Divisibilité dans $\mathbb{Z}$	4
I.3. Pgcd, Ppcm	6
I.4. Unique décomposition	9
I.5. Congruences	10
Exercices	14
CHAPITRE II. ENSEMBLES ET APPLICATIONS	21
Introduction	21
II.1. Ensembles	22
II.2. Opérations sur les parties	25
II.3. Applications	27
II.4. Injection, surjection, bijection	30
II.5. Catégories	34
Exercices	40
CHAPITRE III. QUOTIENTS	49
Introduction	49
III.1. Ensemble quotient	50
III.2. Ensemble ordonné	53
III.3. Bornes	56
III.4. Appendice A (Lemme de Zorn)	60
III.5. Appendice B (Construction de $\mathbb{R}$)	61
Exercices	63
CHAPITRE IV. CARDINAUX	71
Introduction	71
IV.1. Ensembles finis	72
IV.2. Cardinaux	75
IV.3. Puissance du dénombrable, puissance du continu	77
IV.4. Opérations sur les cardinaux	80
IV.5. Appendice (Démonstration du théorème de Cantor-Bernstein)	82
Exercices	83

TABLE DES MATIÈRES

CHAPITRE V. GROUPES	89
Introduction	89
V.1. Permutations	90
V.2. Loi de composition, monoïde	96
V.3. Morphismes et sous-groupes	100
V.4. Groupe $\mathbb{Z}$ des entiers relatifs	104
Exercices	105
CHAPITRE VI. LAGRANGE	111
Introduction	111
VI.1. Groupe cyclique	112
VI.2. Théorème de Lagrange	115
VI.3. Indicateur d'Euler	118
VI.4. Groupe quotient	121
Exercices	126
CHAPITRE VII. ANNEAUX	135
Introduction	135
VII.1. Propriétés multiplicatives de $\mathbb{Z}/n\mathbb{Z}$	137
VII.2. Structures d'anneaux et de corps	140
VII.3. Morphismes et sous-anneaux	145
VII.4. Idéaux et anneaux quotients	149
Exercices	152
Index Terminologique	157
Index des Noms Propres	161

CHAPITRE I

ARITHMÉTIQUE

1. Entiers naturels
2. Divisibilité dans $\mathbb{Z}$
3. Pgcd, Ppcm
4. Unique décomposition
5. Congruences

Introduction

Certains entiers naturels peuvent se décomposer en produit de facteurs, ainsi $6 = 2 \times 3$, $1728 = 26 \times 33$, d'autres au contraire sont indécomposables, on dit qu'ils sont premiers. On peut en commencer la liste

2, 3, 5, 7, 13, 17, 19, 23, 29, 31, ...

(on convient que 1 n'est pas premier).

Les notions de divisibilité d'entiers, nombres premiers, Pgcd, Ppcm, décomposition en produit de facteurs premiers, etc., remontent à l'Antiquité et les principaux résultats d'arithmétique que nous énonçons ici se trouvent dans les *Éléments* d'Euclide.

A la différence des Grecs qui ne connaissaient que les nombres positifs, nous avons avantage à considérer l'ensemble $\mathbb{Z}$ des entiers relatifs (c'est à dire positifs, négatifs ou nuls). Les démonstrations s'en trouvent simplifiées, notamment par la considération des idéaux de $\mathbb{Z}$.

La notion de congruence, introduite par Gauss dans les *Disquisitiones Arithmeticae* en 1801, est en fait également très ancienne et les résultats que nous exposons ici, comme la preuve par 9 ou divers critères de divisibilité étaient connus de mathématiciens arabes tels qu'Al Khawarizmi ou Al Kharkhi. Enfin, la considération de l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$, plus moderne mais de définition par ailleurs très simple, nous permet de donner, dès le début de cet ouvrage, un exemple concret de groupe et d'anneau ayant n éléments.

L'arithmétique connut une renaissance au XVII^{ème} siècle, notamment avec Fermat, dont nous exposons ici le "Petit théorème" :

Soit p un nombre premier. Alors p divise $n^p - n$ pour tout entier n . Fermat énonçait ce résultat sans démonstration dans une lettre en 1640, Euler fut le premier à en donner une preuve, un siècle plus tard (et la démonstration que nous exposons ici fut publiée par Dirichlet en 1828).