

# Table des matières

<b>Introduction</b>	<b>VII</b>
<b>1 L'ensemble <math>\mathbb{N}</math> des entiers naturels</b>	<b>1</b>
1.1 Le principe de récurrence . . . . .	1
1.1.1 Démonstration par récurrence . . . . .	2
1.2 La propriété fondamentale de $\mathbb{N}$ . . . . .	4
1.3 Ensembles finis . . . . .	5
1.4 Éléments de combinatoire . . . . .	9
<b>2 La division euclidienne dans l'anneau <math>\mathbb{Z}</math></b>	<b>13</b>
2.1 Construction de l'anneau $\mathbb{Z}$ . . . . .	13
2.2 La division euclidienne . . . . .	14
2.3 Les sous-groupes de $\mathbb{Z}$ . . . . .	15
2.4 Diviseurs, nombres premiers . . . . .	16
2.5 Plus grand commun diviseur ou pgcd . . . . .	18
2.6 Algorithme d'Euclide . . . . .	21
2.7 Lemme de Gauss . . . . .	22
2.8 Plus petit commun multiple ou ppcm . . . . .	23
2.9 Décomposition d'un entier en facteurs premiers . . . . .	24
<b>3 Groupes finis</b>	<b>29</b>
3.1 Généralités sur les groupes finis . . . . .	29
3.2 Les groupes quotients $\mathbb{Z}/n\mathbb{Z}$ . . . . .	33
3.3 Groupes cycliques et indicatrice d'Euler . . . . .	34
<b>4 Arithmétique des congruences</b>	<b>41</b>
4.1 Les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$ . . . . .	41
4.2 Théorèmes de Fermat et d'Euler . . . . .	43
4.3 Systèmes de congruences. Théorème chinois . . . . .	44
4.4 Application à la cryptographie . . . . .	49
4.4.1 L'algorithme à clé publique RSA . . . . .	50

<b>5</b>	<b>La division euclidienne dans <math>\mathbb{K}[X]</math> et ses conséquences</b>	<b>55</b>
5.1	Généralités . . . . .	55
5.2	Les idéaux de $\mathbb{K}[X]$ . . . . .	59
5.3	Polynômes irréductibles . . . . .	60
5.4	Pgcd de deux polynômes . . . . .	61
5.5	Décomposition d'un polynôme en facteurs irréductibles . . . . .	62
5.6	L'algèbre quotient $\mathbb{K}[X]/\langle P \rangle$ . . . . .	62
5.7	Représentation de l'algèbre $\mathbb{K}[X]/\langle P \rangle$ . . . . .	64
5.8	Règles de calculs dans l'algèbre $\mathbb{K}[X]/\langle P \rangle$ . . . . .	65
<b>6</b>	<b>Corps finis</b>	<b>67</b>
6.1	Construction des corps finis . . . . .	68
6.2	Éléments primitifs . . . . .	69
6.3	Caractéristique d'un corps fini . . . . .	70
6.4	Calculs dans un corps fini. Logarithme discret . . . . .	73
6.5	Application à la cryptographie . . . . .	78
6.5.1	Protocole d'échange de clés de Diffie-Hellman . . . . .	78
6.5.2	Algorithme de chiffrement à clé publique d'El Gamal . . . . .	79
6.6	Compléments sur les corps finis . . . . .	81
6.6.1	Structure générale d'un corps fini . . . . .	81
6.6.2	Polynôme minimal . . . . .	83
6.6.3	Automorphismes . . . . .	86
6.6.4	Existence de corps finis . . . . .	87
<b>7</b>	<b>Codes correcteurs d'erreurs</b>	<b>91</b>
7.1	Généralités . . . . .	91
7.1.1	Exemples élémentaires . . . . .	91
7.1.2	Définitions . . . . .	92
7.1.3	Distance entre les mots, la distance de Hamming . . . . .	93
7.1.4	Stratégie du maximum de vraisemblance . . . . .	94
7.1.5	Capacité de correction . . . . .	95
7.1.6	Codes parfaits . . . . .	96
7.2	Codes linéaires . . . . .	96
7.2.1	Encodage des codes linéaires – Matrices génératrices . . . . .	99
7.2.2	Codes systématiques . . . . .	101
7.2.3	Décodage des codes linéaires – Matrices de contrôle . . . . .	102
7.3	Codes cycliques . . . . .	108
7.3.1	Polynôme générateur . . . . .	110
7.3.2	Matrice génératrice associée au polynôme générateur . . . . .	115
7.3.3	Polynôme de contrôle et matrice de contrôle associée . . . . .	116
7.3.4	Codes binaires de Hamming de longueur $(2^s - 1)$ . . . . .	117
7.3.5	Codes de Reed-Solomon . . . . .	119

<b>Les règles du jeu</b>	<b>123</b>
<b>A Logique mathématique élémentaire</b>	<b>125</b>
1.1 Pour commencer . . . . .	125
1.2 Construction des énoncés, les opérations logiques . . . . .	125
1.3 Les quantificateurs . . . . .	129
1.4 Les différents types de démonstrations . . . . .	130
<b>B Les ensembles</b>	<b>133</b>
2.1 Le symbole d'appartenance $\in$ . . . . .	133
2.2 La relation d'inclusion $\subseteq$ . . . . .	134
2.3 Le schéma de compréhension . . . . .	135
2.4 Opérations sur les ensembles . . . . .	135
2.5 Fonctions et applications . . . . .	138
2.6 Relation d'ordre . . . . .	142
2.7 Relation d'équivalence . . . . .	145
<b>C Structures algébriques de base</b>	<b>147</b>
3.1 Opérations . . . . .	147
3.2 Groupes . . . . .	149
3.2.1 Sous-groupes . . . . .	152
3.2.2 Classes modulo un sous-groupe . . . . .	155
3.2.3 Groupes quotients . . . . .	156
3.3 Anneaux et corps . . . . .	157
3.4 Espaces vectoriels et algèbres . . . . .	160
3.4.1 L'espace vectoriel $\mathbb{K}^n$ . . . . .	165
3.4.2 Algèbres . . . . .	166
3.5 Calcul matriciel . . . . .	166
3.5.1 Méthode du pivot de Gauss . . . . .	168
3.5.2 Réduction d'une matrice par la méthode du pivot de Gauss . . . . .	169
3.6 L'anneau des polynômes $\mathcal{A}[X]$ . . . . .	171
<b>D Corrigés des exercices</b>	<b>173</b>
<b>Index</b>	<b>203</b>