

collection informatique dirigée par Jean-Charles Pomerol

Algèbre et protection de l'information

Alain Poli
Philippe Guillot

 **hermes**

Lavoisier

Table des matières

Introduction	15
Chapitre 1. Éléments d'algèbre	19
1.1. Ensembles	19
1.1.1. Ensembles finis ou infinis	20
1.1.2. Parties d'un ensemble, ensemble des parties d'un ensemble	20
1.1.3. Construction d'ensembles à partir d'ensembles, de parties à partir de parties	21
1.1.3.1. Construction d'ensembles à partir d'ensembles	21
1.1.3.2. Constructions de parties à partir de parties	21
1.1.3.3. Recouvrement et partition	22
1.2. Ordre et équivalence	22
1.2.1. Relation d'ordre	22
1.2.2. Relation d'équivalence	23
1.3. Applications	23
1.3.1. Parties et applications	23
1.3.2. Composée d'applications	24
1.3.3. Propriétés possibles pour une application	24
1.3.3.1. Propriétés	24
1.3.3.2. Applications importantes	24
1.4. Enrichissement des ensembles : lois de composition	25
1.4.1. Les lois de composition	25
1.4.1.1. Loi de composition interne	25
1.4.1.2. Loi de composition externe	26
1.4.2. Propriétés possibles pour les lois internes	26
1.4.2.1. Loi produit	26
1.4.3. Table cartésienne d'une loi interne	26
1.5. Enrichissement des applications : les morphismes	27
1.5.1. Propriétés d'un morphisme	27

1.6. Ensembles structurés	28
1.6.1. Groupes, sous-groupes, morphismes de groupes	28
1.6.1.1. Groupes	28
1.6.1.2. Sous-groupes	28
1.6.1.3. Morphismes	29
1.6.2. Anneaux, sous-anneaux, idéaux, morphismes d'anneaux	29
1.6.2.1. Anneaux	29
1.6.2.2. Sous-anneaux, idéaux	30
1.6.2.3. Morphismes	30
1.6.3. Corps, sous-corps, morphismes de corps	31
1.6.3.1. Corps	31
1.6.3.2. Sous-corps	31
1.6.3.3. Morphismes	31
1.6.4. Espaces vectoriels, sous-espaces vectoriels, applications linéaires	32
1.6.4.1. Espaces vectoriels	32
1.6.4.2. Sous-espace vectoriel	32
1.6.4.3. Applications linéaires	33
1.6.5. Classes latérales d'une sous-structure	33
1.6.5.1. Sous-structures et classes latérales	33
1.6.5.2. Classes latérales du noyau de f et résolution d'équations	34
1.6.5.3. Classes latérales et structures quotients	34
1.7. Anneaux et corps importants	35
1.7.1. Anneaux importants : $\mathbb{Z}$ et $K[X]$	35
1.7.1.1. Les deux ordres, PGCD et PPCM	35
1.7.1.2. Nombres premiers, polynômes irréductibles	36
1.7.1.3. L'indicateur d'Euler : $\varphi(n)$	36
1.7.1.4. Une « bonne » application	37
1.7.1.5. Égalité d'Euclide	37
1.7.1.6. Anneau principal	37
1.7.1.7. Égalité de Bezout	37
1.7.1.8. La décomposition primaire	38
1.7.1.9. Calculs de PGCD	38
1.7.2. Corps importants	40
1.7.2.1. Racines de polynômes	40
1.7.2.2. Irréductibles sur $\mathbb{R}$ ou sur un corps fini F_q	40
1.8. Algèbre Linéaire	41
1.8.1. Quelques propriétés de base	41
1.8.1.1. Indépendance linéaire et dépendance linéaire de r vecteurs	41
1.8.1.2. Systèmes de générateurs	42
1.8.1.3. Système minimal de générateurs	42
1.8.1.4. Base de E , dimension de E	42
1.8.1.5. Compléter une base d'un sous-espace vectoriel	43
1.8.1.6. Somme de sous-espaces vectoriels	44

1.8.1.7. Somme directe de sous-espaces vectoriels, supplémentaire	44
1.8.2. Représentation	45
1.8.2.1. Représentation d'un vecteur	45
1.8.2.2. Représentation d'une application linéaire, et représentation de l'image d'un vecteur	45
1.8.2.3. Représentation d'une somme de deux applications linéaires	47
1.8.2.4. Représentation d'une composée de deux applications linéaires	47
1.8.3. Changement de représentation	48
1.8.3.1. Vecteur de E	48
1.8.3.2. Application linéaire f de E dans F	49
1.8.4. Anneaux importants en Algèbre Linéaire	50
1.8.4.1. $\text{End}(E)$	50
1.8.4.2. $K[h]$	50
1.8.4.3. M_n	50
1.8.4.4. $M_n[X]$	50
1.8.5. Calcul matriciel	51
1.8.5.1. Manipulations élémentaires	51
1.8.5.2. Expressions matricielles des manipulations élémentaires	51
1.8.5.3. Algorithme de Gauss	52
1.8.5.4. Recherche de l'inverse d'une matrice M carrée, d'ordre n	53
1.8.5.5. Recherche de noyau	54
1.8.5.6. Résolution de systèmes linéaires	55
1.9. Plus loin en Algèbre Linéaire	56
1.9.1. Déterminant	56
1.9.1.1. Autres développements d'un déterminant	57
1.9.1.2. Propriétés d'un déterminant	58
1.9.1.3. Déterminant et algorithme de Gauss	59
1.9.1.4. Le produit d'une matrice et de son adjointe (vers le théorème de Cayley-Hamilton)	60
1.9.1.5. Le déterminant d'un produit de deux matrices carrées	61
1.9.2. Vecteurs et valeurs propres	63
1.9.2.1. Recherche de λ et d'une base de F_λ	64
1.9.2.2. Propriétés des sous-espaces propres	64
1.9.3. Polynômes remarquables associés à un endomorphisme	65
1.9.3.1. Une propriété générale	65
1.9.3.2. Polynôme caractéristique	65
1.9.3.3. Polynôme caractéristique d'une matrice compagne	66
1.9.3.4. Polynôme minimum	67
1.9.3.5. Polynôme minimum d'une matrice compagne	67
1.9.3.6. Polynôme minimum d'un élément x de E	68
1.9.3.7. Calcul de $\text{PMIN}_h(X)$, $\text{pmin}_x(X)$ et $\text{PCAR}_h(X)$	68
1.9.4. Première décomposition de E en somme directe	68

1.9.4.1. Le cas particulier de $\text{Ker}(p^k(h))$	69
1.9.4.2. Le cas général	73
1.9.5. Raffinement de la décomposition en somme directe	75
1.9.5.1. Construction de ce raffinement de la décomposition en somme directe	77
1.9.6. Le fin du fin : la diagonalisation de A	77

Chapitre 2. Structures algébriques finies 79

2.1. Groupes finis	79
2.1.1. Théorème de Lagrange	79
2.1.2. Sous-groupe d'un groupe cyclique fini	79
2.1.3. Groupe des permutations	80
2.1.3.1. Propriétés générales des permutations	80
2.1.3.2. La signature	82
2.2. Corps finis : $\mathbb{Z}/(p)$ et $F_2[X]/(p(X))$	84
2.2.1. Les lois de composition internes	84
2.2.1.1. Les lois dans $\mathbb{Z}/(p)$	84
2.2.1.2. Les lois dans $F_2[X]/(p(X))$	85
2.2.1.3. Inverses et opposés	86
2.2.2. $\mathbb{Z}/(p)$ et $F_2[X]/(p(X))$ sont des corps	87
2.2.3. Ordre d'un élément, primitifs, nombre de primitifs	87
2.2.3.1. Ordre d'un élément	87
2.2.3.2. Primitifs, nombre de primitifs	88
2.2.3.3. Primitifs et logarithmes discrets	89
2.2.4. Circuits électroniques et calculs polynomiaux	90
2.2.4.1. Eléments de base	90
2.2.4.2. Indexation des bascules et des fils	90
2.2.4.3. Fonctionnement général	91
2.2.4.4. Circuit multiplicateur par X	93
2.2.4.5. Circuit diviseur	93
2.2.4.6. Circuit multiplicateur	94
2.2.4.7. Circuit multiplicateur-diviseur	94
2.2.4.8. Codeur d'un code cyclique	95
2.2.5. Le groupe des racines n -ièmes de l'unité	95
2.2.6. Classes cyclotomiques dans $F_2[X]/(p(X))$	95
2.2.6.1. Les classes cyclotomiques	96
2.2.6.2. Polynôme minimum d'un élément	97
2.2.6.3. Racines de polynômes	98
2.2.7. Quelques polynômes irréductibles sur F_2 et sur F_3	99
2.3. Anneaux finis : $\mathbb{Z}/(n)$ et $F_2[X]/(a(X))$	99
2.3.1. Les lois de composition internes	99
2.3.2. Ordre et inverse	100
2.3.3. Résoudre une équation $aX + b = 0$ dans $\mathbb{Z}/(n)$	101

2.3.4. Les trois problèmes en Arithmétique	101
2.3.4.1. Enoncés de ces problèmes	101
2.3.4.2. Résolution de ces problèmes	102
2.3.5. Les idéaux	104
2.4. Décomposition de $\mathbb{Z}/(n)$ et de $F_2[X]/(a(X))$	105
2.4.1. Décomposition en produit direct	105
2.4.1.1. Cas de $\mathbb{Z}/(n)$	105
2.4.1.2. Cas de $F_2[X]/(a(X))$	106
2.4.2. Décomposition en somme directe	107
2.4.2.1. Cas de $\mathbb{Z}/(n)$	107
2.4.2.2. Cas de $F_2[X]/(a(X))$	108
2.4.3. Les idempotents primitifs	109
2.4.3.1. Cas de $\mathbb{Z}/(n)$	109
2.4.3.2. Cas de $F_2[X]/(a(X))$	109
2.4.4. Les deux décompositions sont isomorphes	110
2.4.4.1. Un isomorphisme particulier	110
2.4.4.2. L'isomorphisme du produit cartésien sur $\mathbb{Z}/(n)$	110
2.4.4.3. L'isomorphisme du produit cartésien sur $F_2[X]/(a(X))$	111
2.5. Factorisation de polynômes	111
2.5.1. Algorithme de factorisation de E. Berlekamp	111
2.5.2. Comment obtenir $p(X)$ à partir de $p^i(X)$	113
2.6. Quelques complexités d'algorithmes	113
2.6.1. Calcul d'un PGCD (Euclide)	114
2.6.2. Expression d'un PGCD (Bezout)	114
2.6.3. Calcul de x^m	115
2.6.4. Inverse de x modulo n (quand il existe)	115
2.6.5. Inverse d'une matrice carrée d'ordre n	115
2.6.6. Recherche du noyau d'une $m \times n$ matrice ($m < n$)	116
2.6.7. Méthode de E. Berlekamp : factoriser $f(X)$ sous la forme $f_1(X)f_2(X)$	116
2.6.8. Calcul d'un déterminant	116
2.6.9. Calcul de $\text{PMIN}_h(X)$	116
2.6.10. Calcul de $\text{PCAR}_h(X)$	116
2.6.11. Calcul de $\text{pmin}_x(X)$	117
2.7. Fractions continues	117
2.7.1. De l'algorithme d'Euclide à certaines fractions	117
2.7.2. Des fractions particulières	117
2.7.3. Fraction continue associée à un réel positif	118
2.7.4. Réduite d'une fraction continue	119
2.7.5. Approximation d'un réel positif par une réduite	120
2.7.5.1. Cas d'un irrationnel	120
2.7.5.2. Cas d'un rationnel	120
2.7.5.3. Fraction continue et Cryptographie	121

Chapitre 3. Cryptographie	123
3.1. Introduction	123
3.1.1. Cryptologie	123
3.1.1.1. Système cryptographique	123
3.1.2. Sécurité inconditionnelle	124
3.1.3. Cryptographie symétrique	125
3.1.4. Cryptographie asymétrique	125
3.1.5. Modèles d'attaque	126
3.1.6. Services de sécurité	126
3.2. Chiffrements traditionnels	127
3.2.1. Transposition	127
3.2.1.1. La Scytale (Sparte, 400 avant J.C.)	127
3.2.1.2. La grille tournante	127
3.2.2. Substitution simple	128
3.2.2.1. Chiffre de César	128
3.2.2.2. Rot13	128
3.2.2.3. Chiffre de Wolseley	128
3.2.2.4. Cryptanalyse des substitutions simples	129
3.2.3. Substitutions polygrammiques	129
3.2.3.1. Chiffre de Playfair	129
3.2.3.2. Chiffre de Hill	129
3.2.4. Le carré de Vigenère (1586)	130
3.3. Chiffrement symétrique moderne	131
3.3.1. Le chiffrement à flot (<i>stream cipher</i>)	131
3.3.1.1. Le masque jetable (Vernam, 1917)	132
3.3.1.2. Générateur pseudo-aléatoire	132
3.3.1.3. Le registre filtré	133
3.3.1.4. Attaque par corrélation	134
3.3.2. Le chiffrement par blocs	135
3.3.2.1. Définition	135
3.3.2.2. Architecture d'un calcul par bloc	136
3.3.2.3. Schéma de Feistel (1973)	136
3.3.2.4. Réseaux substitutions-permutations	137
3.3.3. Le DES	137
3.3.3.1. Architecture générale du DES	137
3.3.3.2. Cadencement de clé	138
3.3.3.3. Déchiffrement	138
3.3.3.4. Clés faibles	138
3.3.3.5. Le triple DES	138
3.3.3.6. La cryptanalyse différentielle du DES (Biham et Shamir, 1990)	139
3.3.3.7. La cryptanalyse linéaire du DES (Matsui, 1993)	140
3.3.4. L'AES	141

3.3.4.1. Le corps $\mathbb{F}_{256}$	141
3.3.4.2. La fonction de diffusion	141
3.3.4.3. La boîte-S	142
3.3.4.4. La fonction de tour	142
3.3.4.5. Le cadencement de clé	143
3.3.4.6. Le déchiffrement	143
3.4. Cryptographie à clés publiques	143
3.4.1. Le protocole Diffie-Hellman	143
3.4.1.1. Fonctions à sens unique	143
3.4.1.2. La négociation de clé Diffie-Hellman (1976)	144
3.4.1.3. L'exponentiation et le logarithme discret	144
3.4.1.4. L'attaque de l' <i>homme au milieu</i>	145
3.4.1.5. Le chiffrement ElGamal	145
3.4.1.6. Algorithmes de calcul du logarithme discret	145
3.4.2. Le cryptosystème de Rabin	147
3.4.2.1. Calcul de la racine carrée modulo n	147
3.4.2.2. Fonction à sens unique avec porte dérobée (<i>trapdoor</i>)	149
3.4.2.3. Définition du système de Rabin	149
3.4.2.4. Sécurité du système de Rabin	150
3.4.2.5. Factoriser les grands entiers.	150
3.4.3. Le RSA.	152
3.4.3.1. Description du système RSA	152
3.4.3.2. La sécurité du RSA	153
3.4.4. Signature numérique	155
3.4.4.1. Définition d'un schéma de signature	156
3.4.4.2. Fonctions de hachage	156
3.4.4.3. La signature RSA	157
3.4.4.4. La signature ElGamal (1985)	157
Chapitre 4. Les codes correcteurs	159
4.1. Un peu d'histoire	159
4.2. Le bruit, les erreurs, probabilité d'entrée et probabilité résiduelle	160
4.3. Codes sans structure	160
4.3.1. Les paramètres d'un code C	161
4.3.2. Codage, mot émis, mot reçu, mot d'erreurs, décodage	161
4.3.3. Schéma général du décodage à maximum de vraisemblance	162
4.3.4. Bornes des paramètres d'un code	163
4.3.5. Construire un code sans structure	163
4.4. Codes linéaires	164
4.4.1. Propriétés des codes linéaires	164
4.4.1.1. Distance minimale et poids minimum	164
4.4.1.2. Base, base sous forme systématique, codage	164
4.4.2. Code dual	165

4.4.3. Les classes latérales d'un code linéaire C	165
4.4.4. Les syndromes	166
4.4.5. Décodage et syndromes	166
4.4.6. Matrice de test et poids minimum de code	167
4.4.7. Quelques codes linéaires	168
4.4.8. Décodage des codes linéaires	168
4.5. Codes cycliques	168
4.5.1. Propriétés d'un code cyclique	169
4.5.2. Base d'un code cyclique ($g(X)$)	170
4.5.3. Annulateur d'un code cyclique C	171
4.5.4. Puissance de correction d'un code cyclique : les racines de $g(X)$	171
4.5.5. Théorème de BCH	171
4.5.6. Codage	172
4.5.7. Syndromes	173
4.5.8. Codes tronqués, et codes étendus	173
4.5.8.1. Codes tronqués	173
4.5.8.2. Codes étendus	173
4.6. Quelques codes cycliques	174
4.6.1. Codes de Hamming	174
4.6.2. Codes BCH	174
4.6.3. Codes RM	175
4.6.4. Codes RS	175
4.6.5. Codes à distance vraie supérieure à leur distance BCH	176
4.7. Existence et construction de codes cycliques	176
4.7.1. Existence	176
4.7.2. Construction	177
4.7.2.1. Utilisation des classes de $Z/(n)$	177
4.7.2.2. Utilisation de la factorisation de $X^n - 1$	177
4.7.3. Cahier des charges	178
4.7.4. Comment chercher un code cyclique	178
4.7.5. Exemple d'une telle recherche	179
4.7.6. Comment chercher un code cyclique tronqué	180
4.8. Applications des codes	180
4.9. Codes et cryptographie	181
4.9.1. Utilisation d'un code correcteur en cryptographie	181
4.9.2. Une première attaque	181
4.9.3. Une première contre-attaque	181
4.9.4. Une seconde attaque	181
4.9.5. La parade	181

Chapitre 5. Exercices et problèmes	183
I. Enoncés	183
5.1. Chapitre 1	183
5.1.1. Exercices de compréhension	183
5.1.2. Exercices de réflexion	184
5.1.3. Problèmes	186
5.2. Chapitre 2	189
5.2.1. Exercices de compréhension	189
5.2.2. Exercices de réflexion	191
5.2.3. Problèmes	193
5.3. Chapitre 3	197
5.3.1. Exercices de compréhension	197
5.3.2. Exercices de réflexion	198
5.3.3. Problèmes	202
5.4. Chapitre 4	205
5.4.1. Exercices de compréhension	205
5.4.2. Exercices de réflexion	206
5.4.3. Problèmes	207
II. Solutions	211
5.5. Chapitre 1	211
5.5.1. Exercices de compréhension	211
5.5.2. Exercices de réflexion	212
5.5.3. Problèmes	215
5.6. Chapitre 2	221
5.6.1. Exercices de compréhension	221
5.6.2. Exercices de réflexion	225
5.6.3. Problèmes	229
5.7. Chapitre 3	234
5.7.1. Exercices de compréhension	234
5.7.2. Exercices de réflexion	236
5.7.3. Problèmes	239
5.8. Chapitre 4	241
5.8.1. Exercices de compréhension	241
5.8.2. Exercices de réflexion	243
5.8.3. Problèmes	244
Bibliographie	249
Index	251

Cet ouvrage couvre l'algèbre classique et l'algèbre discrète ainsi que ses applications à la cryptographie et aux codes correcteurs d'erreurs.

Partant de la théorie des ensembles, il aboutit à la diagonalisation des matrices. Les structures finies sont étudiées, ainsi que certains circuits électroniques utilisés dans la pratique pour effectuer les calculs. Des exemples de complexité d'algorithmes sont donnés.

Ce livre introduit les principales techniques de protection des informations contre les attaques éventuelles. De nombreuses constructions sont proposées. Un exemple concret précède chaque preuve délicate. Plus de cent cinquante exercices et problèmes, avec leurs corrigés complets, illustrent *Algèbre et protection de l'information*.

Les auteurs

Alain Poli, responsable de vingt contrats avec l'industrie, a créé en 1984 la conférence internationale AAECC (Algèbre Appliquée Et Codes Correcteurs). Docteur d'Etat ès Mathématiques, il est professeur à l'université Paul Sabatier de Toulouse où il enseigne l'algèbre et les codes correcteurs.

Philippe Guillot a été successivement responsable des départements de cryptographie de Thales et de Canal+ Technologies. Il est actuellement maître de conférences à l'université Paris 8 où il enseigne la cryptographie.

hermes
Science
— publications —

www.hermes-science.com

ISBN 2-7462-1068-1



9 782746 210684