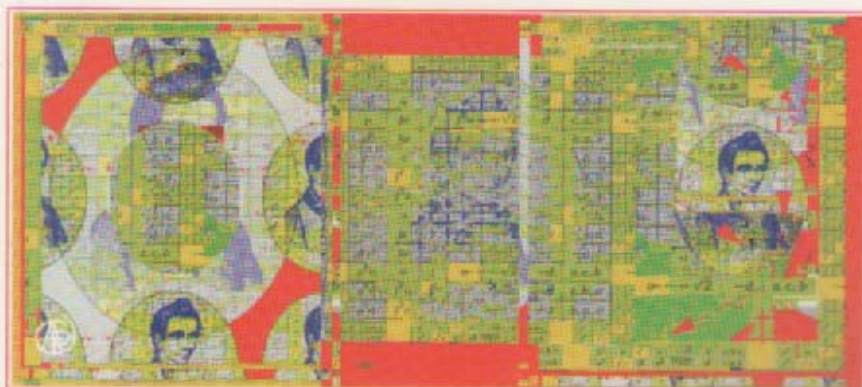


Jean-Pierre Escofier

2^e CYCLE

Théorie de Galois

Cours et exercices corrigés



2^e édition

DUNOD

Table des matières

AVANT-PROPOS	XV
CHAPITRE 1 • DIFFÉRENTS ASPECTS HISTORIQUES DE LA RÉOLUTION DES ÉQUATIONS ALGÈBRIQUES	
1.1 Calcul approché des racines d'une équation	1
1.2 Construction de solutions par intersections de courbes	2
1.3 Liens avec la trigonométrie	2
1.4 Problèmes de notation et de terminologie	2
1.5 Problème de la localisation des racines	4
1.6 Problème de l'existence des racines	4
1.7 Problème de la résolution algébrique des équations	5
CHAPITRE 2 • HISTOIRE DE LA RÉOLUTION DES ÉQUATIONS DE DEGRÉ 2, 3 OU 4 AVANT 1640	7
2.1 Équations du second degré	7
2.1.1 Les Babyloniens	7
2.1.2 Les Grecs	9
2.1.3 Les Arabes	9
2.1.4 Usage des nombres négatifs	10
2.2 Équations du troisième degré	10
2.2.1 Les Grecs	10
2.2.2 Omar Khayyam et Sharaf al Din al Tusi	11
2.2.3 Scipio del Ferro, Tartaglia, Cardan	11

2.2.4	Résolution algébrique de l'équation du troisième degré	12
2.2.5	Premiers calculs avec les complexes	13
2.2.6	Raffaele Bombelli	14
2.2.7	François Viète	15
2.3	Équations du quatrième degré	15
	EXERCICES	17
	SOLUTIONS	20
	CHAPITRE 3 • POLYNÔMES SYMÉTRIQUES	22
3.1	Polynômes symétriques	22
3.1.1	Rappel	22
3.1.2	Définitions	23
3.2	Polynômes symétriques élémentaires	24
3.2.1	Définition	24
3.2.2	Produit des $X - X_i$ et relations entre coefficients et racines	24
3.3	Polynômes symétriques et polynômes symétriques élémentaires	25
3.3.1	Théorème	25
3.3.2	Proposition	28
3.3.3	Proposition	28
3.4	Formules de Newton	28
3.5	Résultant de deux polynômes	31
3.5.1	Définition	31
3.5.2	Proposition	31
3.6	Discriminant d'un polynôme	33
3.6.1	Définition	33
3.6.2	Proposition	33
3.6.3	Formules	33
3.6.4	Polynômes à coefficients réels : racines réelles et signe du discriminant	34
	EXERCICES	35
	SOLUTIONS	39
	CHAPITRE 4 • EXTENSIONS DE CORPS	44
4.1	Extensions de corps	44
4.1.1	Définition	44
4.1.2	Proposition	45
4.1.3	Degré d'une extension	45
4.1.4	Tour de corps	45

4.2	Formule de multiplicativité des degrés	45
4.2.1	Proposition	45
4.3	Extension engendrée	47
4.3.1	Proposition	47
4.3.2	Définition	47
4.3.3	Proposition	47
4.4	Éléments algébriques	48
4.4.1	Définition	48
4.4.2	Nombres transcendants	48
4.4.3	Proposition	48
4.4.4	Polynôme minimal d'un élément algébrique	49
4.4.5	Propriétés du polynôme minimal	49
4.4.6	Lien entre l'irréductibilité dans $\mathbb{Z}[X]$ et l'irréductibilité dans $\mathbb{Q}[X]$	50
4.4.7	Méthodes pour prouver l'irréductibilité d'un polynôme de $\mathbb{Z}[X]$	50
4.5	Extensions algébriques	52
4.5.1	Extension engendrée par un élément algébrique	52
4.5.2	Propriétés de $K[a]$	52
4.5.3	Définition	53
4.5.4	Extensions de degré fini	53
4.5.5	Corollaire : tour d'extensions algébriques	53
4.6	Extensions algébriques par n éléments	53
4.6.1	Notation	53
4.6.2	Proposition	54
4.6.3	Corollaire	54
4.7	Construction d'une extension par adjonction de racine	54
4.7.1	Définition	55
4.7.2	Proposition	55
4.7.3	Corollaire	55
4.7.4	Propriété universelle de $\frac{K[X]}{(P)}$	56
	EXERCICES	57
	SOLUTIONS	61
	CHAPITRE 5 • CONSTRUCTIONS À LA RÈGLE ET AU COMPAS	69
5.1	Points constructibles	69
5.2	Exemples de constructions classiques	70
5.2.1	Projection d'un point sur une droite	70
5.2.2	Construction d'un repère orthonormé à partir de deux points	70
5.2.3	Construction de la parallèle à une droite passant par un point	71

5.3	Lemme	71
5.4	Coordonnées des points constructibles en une étape	72
5.5	Condition nécessaire de constructibilité	72
5.6	Deux problèmes vieux de plus de deux mille ans	73
5.6.1	Duplication du cube	73
5.6.2	Trisection de l'angle	73
5.7	Condition suffisante de constructibilité	74
EXERCICES		76
SOLUTIONS		79
CHAPITRE 6 • K -HOMOMORPHISMES		81
6.1	Nombres conjugués	81
6.2	K -homomorphismes	82
6.2.1	Définitions	82
6.2.2	Propriétés	82
6.3	Éléments algébriques et K -homomorphismes	83
6.3.1	Proposition	83
6.3.2	Exemple	84
6.4	Extensions de plongements dans $\mathbb{C}$	84
6.4.1	Définition	84
6.4.2	Proposition	84
6.4.3	Proposition	86
6.5	Théorème de l'élément primitif	87
6.5.1	Théorème et définition	87
6.5.2	Exemple	88
6.6	Indépendance linéaire des K -homomorphismes	88
6.6.1	Caractère	88
6.6.2	Théorème (Emil Artin)	88
6.6.3	Corollaire : théorème de Dedekind	89
EXERCICES		90
SOLUTIONS		91
CHAPITRE 7 • EXTENSIONS NORMALES		93
7.1	Corps de décomposition	93
7.1.1	Définition	93
7.1.2	Corps de décomposition d'un polynôme du troisième degré	94

7.2	Extensions normales	94
7.3	Extensions normales et K -homomorphismes	95
7.4	Corps de décomposition et extensions normales	95
7.4.1	Proposition	95
7.4.2	Réciproque	96
7.5	Extensions normales et extensions intermédiaires	96
7.6	Clôture normale	97
7.6.1	Définition	97
7.6.2	Proposition	97
7.6.3	Proposition	97
7.7	Corps de décomposition, cas général	97
EXERCICES		99
SOLUTIONS		101
CHAPITRE 8 • GROUPES DE GALOIS		103
8.1	Groupes de Galois	103
8.1.1	Groupe de Galois d'une extension	103
8.1.2	Ordre du groupe de Galois d'une extension normale de degré fini	103
8.1.3	Groupe de Galois d'un polynôme	104
8.1.4	Groupe de Galois comme sous-groupe d'un groupe de permutations	104
8.1.5	Petite histoire de la notion de groupe	105
8.2	Corps des invariants	106
8.2.1	Définition et proposition	106
8.2.2	Théorème (Emil Artin)	106
8.3	Exemple de $\mathbb{Q}[\sqrt[3]{2}, j]$, première partie	107
8.4	Groupes de Galois et extensions intermédiaires	109
8.5	La correspondance de Galois	110
8.6	Exemple de $\mathbb{Q}[\sqrt[3]{2}, j]$, seconde partie	111
8.7	Exemple de $X^4 + 2$	111
8.7.1	Groupes diédraux	111
8.7.2	Cas particulier de D_4	112
8.7.3	Groupe de Galois de $X^4 + 2$	113
8.7.4	Correspondance de Galois	114
8.7.5	Recherche de polynômes minimaux	115
EXERCICES		116
SOLUTIONS		120

CHAPITRE 9 • RACINES DE L'UNITÉ	128
9.1 Groupe $U(n)$ des unités de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$	128
9.1.1 Définition et rappel	128
9.1.2 Structure de $U(n)$	129
9.2 Fonction de Möbius	129
9.2.1 Fonction multiplicative	129
9.2.2 Fonction de Möbius	130
9.2.3 Proposition	130
9.2.4 Formule d'inversion de Möbius	130
9.3 Racines de l'unité	131
9.3.1 Racines n -ièmes de l'unité	131
9.3.2 Proposition	131
9.3.3 Racines primitives	131
9.3.4 Propriétés des racines primitives	131
9.4 Polynômes cyclotomiques	132
9.4.1 Définition	132
9.4.2 Propriétés du polynôme cyclotomique	132
9.5 Groupe de Galois sur $\mathbb{Q}$ d'une extension de $\mathbb{Q}$ par une racine de l'unité	134
EXERCICES	136
SOLUTIONS	141
CHAPITRE 10 • EXTENSIONS CYCLIQUES	153
10.1 Extensions cycliques et abéliennes	153
10.2 Extensions par une racine et extensions cycliques	153
10.3 Irréductibilité de $X^n - a$	154
10.4 Théorème 90 de Hilbert	155
10.4.1 Norme	155
10.4.2 Théorème 90 de Hilbert	155
10.5 Extensions par une racine et extensions cycliques : réciproque	156
10.6 Résolvantes de Lagrange	156
10.6.1 Définition	156
10.6.2 Propriétés	157
10.7 Résolution de l'équation du troisième degré	158
10.8 Résolution de l'équation du quatrième degré	159

10.9	Commentaire historique	161
EXERCICES		162
SOLUTIONS		164
CHAPITRE 11 • GROUPES RÉSOLUBLES		166
11.1	Première définition	166
11.2	Groupe dérivé ou groupe des commutateurs	167
11.3	Seconde définition	167
11.4	Exemples de groupes résolubles	168
11.5	Troisième définition	168
11.6	Simplicité de A_n pour $n \geq 5$	169
11.6.1	Théorème	169
11.6.2	A_n non résoluble pour $n \geq 5$, preuve directe	170
11.7	Des résultats récents	170
EXERCICES		171
SOLUTIONS		174
CHAPITRE 12 • RÉSOLUBILITÉ DES ÉQUATIONS PAR RADICAUX		177
12.1	Extensions radicales et polynômes résolubles par radicaux	177
12.1.1	Extensions radicales	177
12.1.2	Polynôme résoluble par radicaux	178
12.1.3	Première construction	178
12.1.4	Seconde construction	178
12.2	Si un polynôme est résoluble par radicaux, son groupe de Galois est résoluble	179
12.3	Exemple de polynôme non résoluble par radicaux	179
12.4	Réciproque du critère fondamental	180
12.5	Équation générale de degré n	180
12.5.1	Éléments algébriquement indépendants	180
12.5.2	Existence d'éléments algébriquement indépendants	180
12.5.3	Équation générale de degré n	181
12.5.4	Groupe de Galois d'une équation générale de degré n	182
EXERCICES		185
SOLUTIONS		185
CHAPITRE 13 • VIE D'ÉVARISTE GALOIS		187

CHAPITRE 14 • CORPS FINIS	193
14.1 Corps algébriquement clos	193
14.1.1 Définition	193
14.1.2 Clôture algébrique	194
14.1.3 Théorème (Steinitz, 1910)	194
14.2 Exemples de corps finis	195
14.3 Caractéristique d'un corps	195
14.3.1 Définition	195
14.3.2 Propriétés	195
14.4 Propriétés d'un corps fini	196
14.4.1 Proposition	196
14.4.2 Homomorphisme de Frobenius	197
14.5 Existence et unicité d'un corps fini à p^n éléments	197
14.5.1 Proposition	197
14.5.2 Corollaire	198
14.6 Extensions de corps finis	198
14.7 Normalité d'une extension finie de corps fini	199
14.8 Groupe de Galois d'une extension finie de corps fini	199
14.8.1 Proposition	199
14.8.2 Correspondance de Galois	200
14.8.3 Exemple	200
EXERCICES	201
SOLUTIONS	208
CHAPITRE 15 • EXTENSIONS SÉPARABLES	216
15.1 Séparabilité	216
15.2 Exemple d'élément inséparable	217
15.3 Critère de séparabilité	217
15.4 Corps parfaits	218
15.5 Corps parfaits et extensions séparables	218
15.6 Extensions galoisiennes	218
15.6.1 Définition	218
15.6.2 Proposition	218
15.6.3 Correspondance de Galois	219

CHAPITRE 16 • DEUX DÉVELOPPEMENTS RÉCENTS	220
16.1 Le problème inverse de la théorie de Galois	220
16.1.1 Le problème	220
16.1.2 Le cas abélien	220
16.1.3 Exemple	221
16.2 Calculs de groupes de Galois sur $\mathbb{Q}$ pour des polynômes de petit degré	221
16.2.1 Simplifications du problème	221
16.2.2 Problème de l'irréductibilité	222
16.2.3 Plongement de G dans S_n	222
16.2.4 Recherche de G parmi les sous-groupes transitifs de S_n	222
16.2.5 Sous-groupes transitifs de S_4	223
16.2.6 Étude de $\Phi(G) \subset A_n$	224
16.2.7 Étude de $\Phi(G) \subset D_4$	224
16.2.8 Étude de $\Phi(G) \subset \frac{\mathbb{Z}}{4\mathbb{Z}}$	225
16.2.9 Algorithme d'étude pour $n = 4$	226
BIBLIOGRAPHIE	229
INDEX	235

