

Table des matières

I. Arithmétique de $\mathbb{Z}$	
1. Les entiers relatifs	4
1.1. Discrétion	4
1.2. Divisibilité	4
1.3. Sous-groupes de $\mathbb{Z}$	6
1.4. Plus grand diviseur commun	8
1.5. Le groupe $\mathbb{Z}/n\mathbb{Z}$.– Congruences	11
1.6. L’anneau $\mathbb{Z}/n\mathbb{Z}$.– Petit théorème de Fermat	13
2. Quelques applications	16
2.1. Jouer à la marchande	16
2.2. Nombres pratiques	20
2.3. Fractions égyptiennes	24
2.4. Développement décimal de $1/p$, d’après J. Germoni	28
2.5. Contenu et lemme de Gauss	34
2.6. Polygones de Newton	35
3. Le joyau de l’arithmétique du XIX ^e siècle	42
3.1. Énoncé de la loi de réciprocité quadratique	43
3.2. Résidus quadratiques : applications	47
3.3. Preuve d’Eisenstein	49
3.4. Zolotarev revisité par Duke-Hopkins	50
3.5. Déterminant de Vandermonde et corps finis	54
3.6. Preuve utilisant les résultants	55
3.7. Une équation diophantienne	56
3.8. Sommes de Gauss	58
4. Histoires de carrés	61
4.1. Théorème des deux carrés	61
4.2. Quaternions et théorème des quatre carrés	64
4.3. Théorème (1, 2, 4, 8) de Hurwitz	67
4.4. Théorème de Pfister	70
4.5. Formes de Pfister et niveau d’un corps	73
5. Nombres réels	76

5.1. Quelques exemples de nombres irrationnels	76
5.2. Construction	80
5.3. Relation d'ordre total	82
5.4. Complétude	84
5.5. Borne supérieure et inférieure	86
5.6. Fractions continuées	87
5.7. Meilleures approximations	96
5.8. Nombres équivalents	100
5.9. Nombres de Markoff	103
6. Suites de Brocot	108
6.1. Fraction médiane ou l'addition des cancrs	108
6.2. L'arbre de Stern-Brocot	111
6.3. Suite diatomique de Stern	116
6.4. Arbre de Calkin-Wilf	120
6.5. Suites de Farey et cercles de Ford	123
7. Vers l'infini et au delà	125
7.1. Ordinaux	126
7.2. Cardinaux	130
7.3. Ensembles dénombrables	133
7.4. Le jeu de Nim	135
7.5. Introduction à la théorie des jeux	136
7.6. Le corps des nombres surréels	145
7.7. Exemples de nombres surréels	150
7.8. Forme normale d'un nombre surréel	156
8. Introduction aux nombres p -adiques	160
8.1. Nombres décadiques	160
8.2. Définition algébrique	164
8.3. Définition analytique	166
8.4. Théorème d'Ostrowski	169
9. Exercices	171

II. Nombres premiers

1. Quelques propriétés sur l'ensemble des nombres premiers	181
1.1. Retour sur le théorème d'Euclide	181
1.2. L'ensemble $\mathcal{P}$ des nombres premiers n'est pas algébrique . .	182
1.3. L'ensemble des nombres premiers est diophantien	184
1.4. Formules décrivant $\mathcal{P}$	187
1.5. Exemples de familles infinies	189
1.6. Trous dans l'ensemble des nombres premiers	192
1.7. Nombres premiers inévitables	195
2. Premiers représentés par une forme quadratique	197
2.1. Descente à la Fermat et réciprocité	197
2.2. Généralisation de la descente	198

2.3. Formes quadratiques réduites	201
2.4. Composition des formes quadratiques	205
2.5. Résolution du cas général via le corps de classes de Hilbert	206
3. Tests de primalité	208
3.1. Nombres de Fermat	208
3.2. Nombres de Mersenne	210
3.3. Autour du petit théorème de Fermat	212
3.4. AKS	214
4. Factorisation	219
4.1. Nombre et taille des facteurs premiers	219
4.2. L'algorithme de Fermat	220
4.3. Méthode de Gauss	221
4.4. Algorithme $p - 1$ de Pollard	221
4.5. Algorithme $p + 1$ de Williams	221
4.6. Algorithme ρ de Pollard	222
4.7. Méthode des factorielles	223
4.8. Crible linéaire de Dixon	224
4.9. Crible quadratique de Pomerance	225
4.10. Formes quadratiques et factorisation	226
4.11. Méthode de factorisation de Lenstra	230
4.12. Crible du corps de nombres	232
5. Introduction à la théorie analytique des nombres	233
5.1. Théorème de Tchébychev	233
5.2. La fonction zêta de Riemann	235
5.3. Preuve du théorème des nombres premiers	241
5.4. Séries de Dirichlet	244
5.5. Théorème de Dirichlet	248
5.6. Quelques conjectures en récente évolution	254
5.7. Une brève introduction au programme de Langlands	256
6. Exercices	259

III. Corps et théorie de Galois

1. Théorie des corps	264
1.1. Généralités sur les extensions	264
1.2. Extensions algébriques et transcendantes	266
1.3. Corps de rupture et corps de décomposition	270
2. Nombres algébriques ou transcendants	275
2.1. Mesure d'irrationalité	275
2.2. Nombres de Liouville	278
2.3. Transcendance de e	280
2.4. Transcendance de π	281
2.5. Quelques résultats sur la transcendance	283
2.6. Classification de Mahler des nombres transcendants	284

3. Corps finis	286
3.1. Théorème de Wedderburn	286
3.2. Propriétés générales	289
3.3. Existence et unicité des corps finis : preuves constructives	290
3.4. Factorisation des polynômes de $\mathbb{Q}[X]$	294
4. Théorie de Galois	300
4.1. Introduction	300
4.2. Extensions séparables	301
4.3. Extensions normales et galoisiennes	305
4.4. Correspondance de Galois	309
4.5. Extensions composées	312
5. Exemples de calculs de groupes de Galois	314
5.1. Groupe de Galois du polynôme $X^n - a$	314
5.2. Extensions résolubles	318
5.3. Extensions cyclotomiques	321
5.4. Retour sur $X^n - a$	328
5.5. Le groupe de Galois comme sous-groupe de $\mathfrak{S}_n$	332
5.6. Le théorème de Dedekind	336
5.7. Résolvantes	341
6. Localisation des racines d'un polynôme	343
6.1. Racines réelles : règle de Descartes et suites de Sturm	344
6.2. Matrices compagnon et valeurs propres	348
6.3. Théorème de Cauchy and co	350
6.4. Théorème de Rouché et applications	351
6.5. Localisation des racines de P'	356
7. Corps de fonctions	360
7.1. L'extension $k(t)/k$	360
7.2. Polynômes de Carlitz	362
7.3. Module de Carlitz	364
7.4. Extensions de Carlitz de $\mathbb{F}_p(T)$	367
7.5. Loi de réciprocité quadratique	368
8. Compléments autour de la théorie de Galois	371
8.1. Extensions d'Artin-Schreier	371
8.2. Théorème d'Artin-Schreier	374
8.3. Lemme de Hensel	376
8.4. Théorème de Puiseux	380
8.5. Théorème d'irréductibilité de Hilbert	382
8.6. Problème de Galois inverse	391
9. Exercices	393

IV. Théorie des nombres

1. Entiers algébriques	406
1.1. Théorème de Minkowski	406
1.2. Normes, traces, discriminant	411
1.3. Anneaux des entiers d'un corps de nombres	413
1.4. Deux exemples	416
1.5. Unités d'un corps de nombres	417
2. Idéaux d'un corps de nombres	422
2.1. Anneaux de Dedekind	422
2.2. Idéaux fractionnaires	423
2.3. Groupes de classes d'idéaux	424
2.4. Décomposition des idéaux premiers dans une extension	428
2.5. Nombre de classes de $\mathbb{Q}[\sqrt[3]{17}]$	431
2.6. Application : une équation diophantienne	433
3. Corps quadratiques, ordres et formes quadratiques	435
3.1. Entiers et ordres	435
3.2. Idéaux et formes quadratiques	437
3.3. Composition des formes quadratiques	442
3.4. Formes réduites de discriminant $D > 0$	445
3.5. Étude de $\mathbb{Q}(\sqrt{-23})$	448
4. Lois de réciprocité supérieures	449
4.1. Loi de réciprocité cubique	450
4.2. Loi de réciprocité quartique	454
4.3. Loi de réciprocité abélienne : théorie du corps de classe	455
5. Exercices	461

V. Équations diophantiennes

1. Quelques techniques élémentaires	466
1.1. Le cas linéaire	466
1.2. Congruences	468
1.3. Méthode géométrique	468
1.4. Méthode de descente	469
1.5. Problème de Waring	469
1.6. Factorisation dans une extension	470
1.7. Méthode de Strassmann	471
2. Équations possédant un nombre infini de solutions	472
2.1. Équation de Pell-Fermat	472
2.2. Équation de Markoff	474
2.3. Équations d'Hurwitz	476
2.4. Courbes elliptiques	479
2.5. Équations de Thue	480
2.6. Principe de Hasse	480
3. Équations diophantiennes exponentielles	484

3.1. Équation de Lebesgue	484
3.2. Équation de Ramanujan-Nagell	485
3.3. Équation de Fermat	486
3.4. Équation de Catalan	487
4. Équations diophantiennes sur $\mathbb{C}[X]$	487
4.1. Grand théorème de Fermat	488
4.2. Théorème de Mason et ses corollaires	488
4.3. Problème de Waring	490
5. Équations diophantiennes sur les corps finis	491
5.1. Sommes de Gauss	491
5.2. Équations diophantiennes modulo p	493
5.3. Sommes de Jacobi	494
5.4. Généralisations à plus de deux variables	496
5.5. Fonction zêta	499
6. Exercices	502

VI. Cryptographie

1. Une brève histoire de la cryptographie	509
1.1. Scytale	509
1.2. Les codes de César	510
1.3. Code de Hill	512
1.4. Code de Vigenère	512
1.5. Enigma et VIC : deux codes du XX ^e siècle	514
1.6. Notions élémentaires de complexité	519
2. Registres à décalage	521
2.1. Codes de Vernam	522
2.2. LFSR	522
2.3. Propriétés	524
2.9. Cryptanalyse	525
3. Chiffrement symétrique : AES	527
4. Chiffrement asymétrique : RSA	529
4.1. Présentation	529
4.2. Authentification et signature	530
4.3. Cryptanalyse	532
5. Logarithme discret	534
5.1. El Gamal	534
5.2. Signature	535
5.3. Sécurité	536
6. La méthode du sac à dos	538
7. Quelques protocoles	539
7.1. Fonctions de hachage	539
7.3. Mots de passe	543
7.4. Signature	543

7.5. Échange de clefs	547
7.6. Jouer à pile ou face au téléphone	549
7.7. Preuve sans transfert de connaissance	549
7.8. Transfert inconscient	550
8. Codes correcteurs	551
8.1. Mise en place	551
8.2. Codes linéaires	553
8.3. Codes linéaires cycliques	555
8.4. Codes BCH	557
9. Exercices	564

VII. Indications de solutions

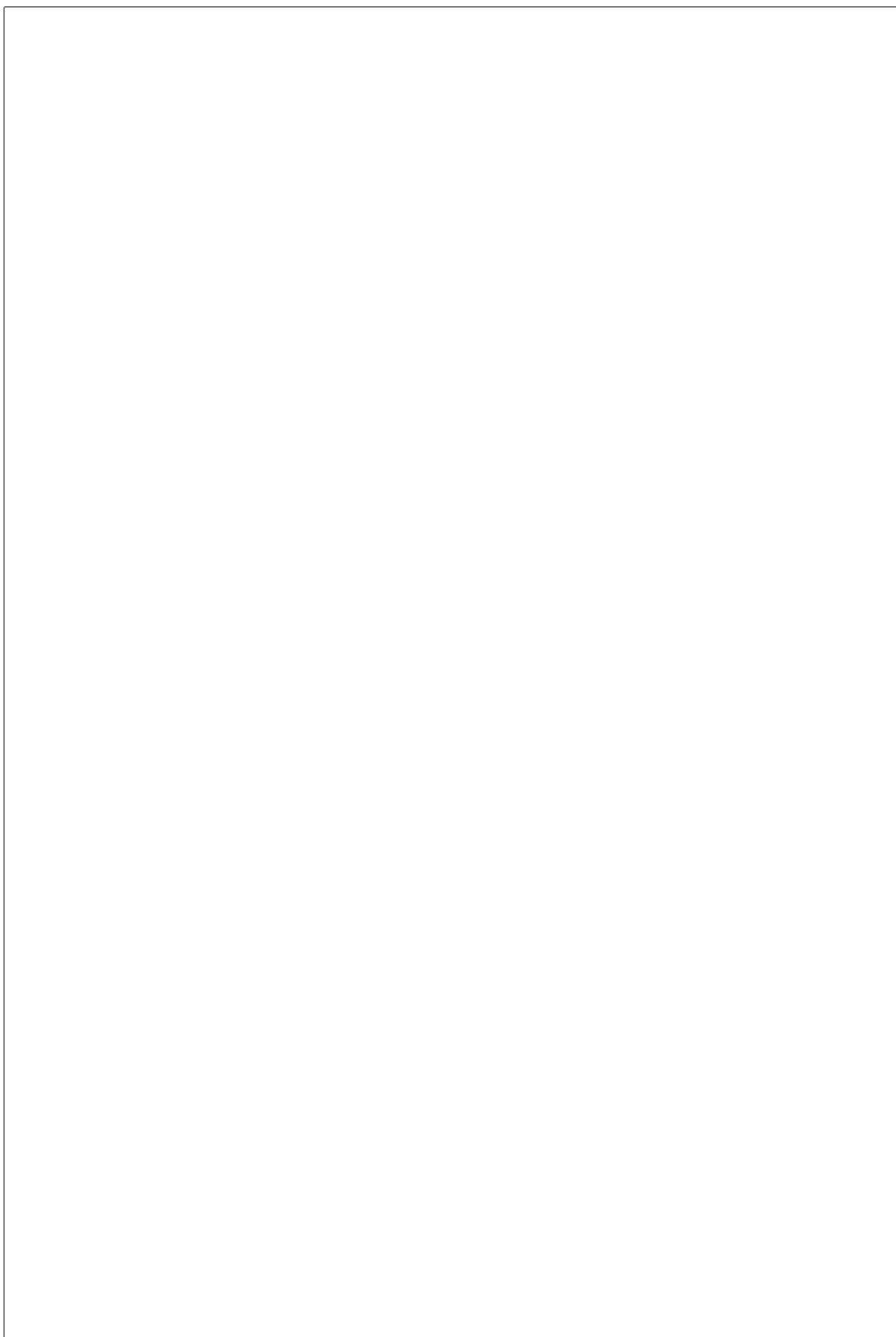
Bibliographie	637
Notations	639
Index	643

|

|

—

—



—

—

|

|

Avant-propos

Au delà du découpage en chapitres, ce livre se déroule en trois temps autour de l'étude

- ▷ tout d'abord de l'arithmétique classique sur les entiers relatifs, autour des nombres premiers et quelques-unes de leurs applications ;
- ▷ on introduit ensuite le lecteur à la théorie des corps, avec les nombres algébriques, les corps finis et la théorie de Galois ;
- ▷ on donne enfin des applications en étudiant les équations diophantiennes, la cryptographie et la théorie des codes correcteurs.

1) Le joyau de l'arithmétique ou le théorème d'or comme l'appelait Gauss est *la loi de réciprocité quadratique*, donnée dans le premier chapitre. Il existe plus de deux cent cinquante preuves différentes de ce résultat, et nous en présentons six, dont la plus ancienne est due à Gauss, une relativement récente reposant sur des idées de V.A. Lebesgue et deux autres illustrant parfaitement l'idée selon laquelle toute formule avec un signe doit permettre de démontrer la loi de réciprocité quadratique. Enfin, une autre preuve utilisant la théorie de Galois et les corps cyclotomiques sera donnée en section §III-5.6, laquelle conduira naturellement aux *lois de réciprocité supérieure*.

Dans le premier chapitre, on s'intéresse essentiellement aux nombres rationnels et à l'approximation des nombres réels par des rationnels.

- ▷ Au delà de la construction abstraite des nombres réels, une vision intuitive d'un nombre réel est donnée par son *développement décimal illimité*, qui consiste à répéter les opérations suivantes : enlever la partie entière et multiplier le résultat par 10.
- ▷ Une autre stratégie voisine et « plus efficace », consiste à enlever la partie entière et à prendre l'inverse du résultat : on arrive ainsi à la notion de *fractions continues* du §I-5.6, qui permettent de construire les « meilleures approximations » d'un nombre réel par un nombre rationnel du §I-5.7. On présente sur ce thème le remarquable travail de Markoff avec la description explicite du *spectre de Lagrange* à l'aide des solutions de *l'équation diophantienne de Markoff* du chapitre IV.

- ▷ Une autre façon d’approcher les nombres réels, longtemps utilisée en horlogerie, est d’utiliser, suivant Brocot, *l’addition des cancrs*

$$\frac{x}{y} \oplus \frac{x'}{y'} = \frac{x+x'}{y+y'}.$$

À l’aide de cette loi, on construit une numérotation étonnante des nombres rationnels via l’arbre de Stern-Brocot, qui révèle des curiosités mathématiques remarquables, cf. le §I-6.

Ce premier chapitre d’arithmétique est aussi l’occasion d’aborder des thématiques intrigantes sur, par exemple, *les fractions égyptiennes*, les *identités remarquables* autour des sommes de carrés avec les travaux d’Hurwitz et Pfister, les fameux *nombres p-adiques* ainsi que les surprenants *nombres surréels* de Conway.

Les nombres premiers apparaissent bien évidemment tout au long de ce livre avec par exemple la non-finitude de l’ensemble $\mathcal{P}$ des nombres premiers ou l’étude du développement décimal de $\frac{1}{p}$.

Dans le deuxième chapitre, nous avons rassemblé quelques faits spectaculaires sur l’ensemble $\mathcal{P}$: par exemple, il semble évident que $\mathcal{P}$ *n’est pas algébrique*, i.e. n’est pas décrit par un polynôme serait-ce en plusieurs variables ; en revanche, le lecteur sera certainement surpris que $\mathcal{P}$ soit *dio-phantien*, i.e. contrôlé par les valeurs positives d’un polynôme explicite, ou même qu’il existe des formules relativement simples donnant le n -ième nombre premier. Les liens entre $\mathcal{P}$ et les formes quadratiques sont aussi très intéressants, et nous en donnons quelques aspects au §II-2.

Les besoins cryptographiques de la technologie actuelle, avec par exemple *le cryptosystème RSA* cf. le §VI-4, stimulent la recherche mathématique autour des questions de primalité et de factorisation. En 2002, trois mathématiciens indiens ont proposé *un nouvel algorithme*, appelé *AKS* des trois initiales des noms de ses découvreurs (voir le §II-3.4), pour tester la primalité d’un entier *en temps polynomial* : le résultat est d’autant plus surprenant que l’algorithme est très simple, reposant sur le fait que n est premier si, et seulement si, la congruence

$$(X+a)^n \equiv X^n + a \pmod{n}$$

est vérifiée pour un a premier avec n . Dans les faits, leur algorithme n’est pas utilisé et on lui préfère *le test probabiliste dit de Rabin-Miller*, que nous présentons au §II-3.3 et qui fournit des nombres n qui sont premiers à 99,9999% de chance, où le nombre de 9 peut être aussi grand qu’on le souhaite, et cela de manière extrêmement rapide : avec les erreurs de transmission, une telle probabilité est largement suffisante pour les besoins.

Symétriquement, la sécurité de RSA repose sur l'impossibilité pratique de factoriser un entier n relativement grand, de quelques centaines de chiffres : au §II-4, on passe en revue quelques-uns des *meilleurs algorithmes de factorisation*.

Enfin, on conclut notre promenade dans l'arithmétique dite classique, par un très rapide aperçu de la théorie analytique des nombres, avec *le théorème des nombres premiers* et le théorème de *progression arithmétique de Dirichlet*.

2) On aborde ensuite la théorie des nombres en commençant par introduire le vocabulaire autour des extensions de corps, algébriques ou transcendentes, corps de rupture et de décomposition. On donne ensuite quelques exemples de *nombres transcendants*, avec bien entendu celui de π qui clôt par la négative la fameuse *quadrature du cercle*. Les *corps finis* sont présentés au §III-3 sous le point de vue constructif, i.e. en justifiant l'existence d'un polynôme irréductible de degré n à coefficients dans $\mathbb{F}_p$. La factorisation modulo p d'un polynôme unitaire de $\mathbb{Z}[X]$ abordée au §III-3.4 sera utilisée intensivement via le théorème de Dedekind III-5.6.4, pour le calcul des groupes de Galois.

La théorie de Galois est le cœur du chapitre ; elle consiste en « un pont » entre d'un côté des questions sur les extensions de corps et de l'autre la théorie des groupes. Dans ce livre, excepté au §III-7.1, nous nous restreindrons aux extensions finies, et donc aux groupes finis. L'énoncé et la preuve du théorème de Galois sont relativement simples et tout le sel consiste à essayer de calculer explicitement des groupes de Galois. Au §III-5, on donne deux familles de tels calculs, les extensions *cyclotomiques* et celles de *Kummer*. Ces dernières permettent en particulier de répondre à la question pour laquelle la théorie de Galois a été inventée, i.e. de répondre par la négative à la question de savoir si étant donnée une équation quelconque de degré ≥ 5 , il est possible d'écrire ses racines en utilisant les symboles $\pm, \times, \sqrt[n]{}$. Pour autant, le mathématicien ne rend pas les armes, et le lecteur trouvera au §III-6 des moyens de localiser les racines d'un polynôme de degré quelconque.

On fait ensuite, au §III-7, une incursion sur les corps de fonctions avec notamment *les polynômes de Carlitz*, qui fournissent une généralisation en caractéristique p des extensions cyclotomiques. Cette construction de Carlitz vers 1930, a connu depuis les travaux de Lubin-Tate et de Drinfeld vers 1970, des succès spectaculaires dans *le programme de Langlands*, dont un des objectifs est de comprendre les représentations des groupes de Galois $\text{Gal}(F^{\text{sep}}/F)$, où F est un corps quelconque et F^{sep} sa clôture séparable ; voir la fin du §IV-4.3. On termine ce rapide tour d'horizon de la théorie de Galois par quelques applications importantes : le théorème

d'Artin-Schreier, qui détermine quels sont les corps F tels que $\bar{F}/F$ est finie, le *théorème d'irréductibilité de Hilbert*, dont une des applications est la construction d'extensions dont le groupe de Galois est $\mathfrak{S}_n$ et nous évoquons le problème de Galois inverse. Enfin, au §IV-4, on revient sur la notion de loi de réciprocité afin de généraliser celle d'Euler dans le cas quadratique.

Les §IV-1 et IV-2 sont une très courte introduction à *la théorie algébrique des nombres*. L'idée est de généraliser l'inclusion $\mathbb{Z} \subset \mathbb{Q}$ avec la distinction entre entiers et nombres. Le contexte général est celui des anneaux de Dedekind, où les idéaux se comportent « idéalement », d'où leur nom, au sens où ils prennent le relais des entiers dans la factoriabilité : je m'explique, en général, les anneaux d'entiers ne sont pas factoriels ce qui est un problème important, par exemple pour généraliser l'approche pour $n = 2$ de l'équation de Fermat, en revanche dans les anneaux de Dedekind, tout idéal s'écrit de manière unique comme un produit d'idéaux dits premiers. Le défaut de factoriabilité de l'anneau des entiers se mesure alors à l'aide *du groupe fini des classes d'idéaux*. Cette théorie a été utilisée par Kummer pour démontrer des cas nouveaux du théorème de Fermat, ceux où le groupe de classe de l'extension cyclotomique $\mathbb{Q}(\zeta_p)$ est premier avec p .

3) En première approximation, *une équation diophantienne* est un polynôme en plusieurs variables à coefficients dans $\mathbb{Z}$ dont on cherche les solutions dans $\mathbb{Z}$. D'un point de vue logique, il serait déraisonnable d'espérer disposer d'une théorie générale traitant du sujet, et l'on se contentera d'un corpus de techniques. Le sujet est vaste et très complexe et va bien au delà des outils introduits dans ce livre. Signalons que la fin du XX^e siècle a connu enfin la résolution de la plus fameuse de ces équations, i.e. celle de Fermat par des techniques très élaborées et astucieuses. Dans notre présentation de ce sujet, nous avons mis l'accent sur quelques-unes des plus célèbres équations possédant une infinité de solutions (Pell-Fermat, Markoff, courbes elliptiques...) avec un détour vers $\mathbb{C}[X]$ et les corps finis.

On termine le livre sur un dernier chapitre consacré à *la cryptographie*. Après une introduction historique rapide, on étudie les registres à décalage, le chiffrement symétrique AES et le système à clefs publiques RSA. Plus que l'aspect mathématique théorique de ces cryptosystèmes, ce qui est réellement intéressant est leur mise en œuvre, que nous étudions à travers quelques protocoles. Enfin, nous abordons les codes correcteurs d'erreurs et plus particulièrement ceux liés aux corps finis, les codes BCH utilisés en particulier dans la lecture des CD.