HAL
open science

Les groupes abéliens et leurs anneaux d'endomorphismes

Gentiana Danila, Jean Denis-Eiden, Rached Mneimne

To cite this version:

Gentiana Danila, Jean Denis-Eiden, Rached Mneimne. Les groupes abéliens et leurs anneaux d'endomorphismes. Calvage&Mounet. Algèbre éclectique, Calvage&Mounet, pp.39-79, 2021, 978-2-91-635290-9. hal-03927390

HAL Id: hal-03927390

https://hal.science/hal-03927390v1

Submitted on 11 Feb 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MATHÉMATIQUES EN DEVENIR

Mathématiques en devenir

102. — Patrice Tauvel. *Corps commutatifs et théorie de Galois*

104. — Clément de Seguins Pazzis. *Invitation aux formes quadratiques*

105. — Bruno Ingrao. *Coniques projectives, affines et métriques*

107. — Henri Lombardi & Claude Quitté. *Algèbre commutative. Méthodes constructives.* Nouvelle édition revue et augmentée

109. — Grégory Berhuy. *Modules : théorie, pratique... et un peu d'arithmétique.* Nouvelle édition

112. — Gema-Maria Díaz-Toca, Henri Lombardi & Claude Quitté. *Modules sur les anneaux commutatifs*

114. — Alain Debreil. *Groupes finis et treillis de leurs sous-groupes*

117. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome premier* (Nouveau tirage)

119. — Alain Debreil, Jean-Denis Eiden, Rached Mneimné et Tuong-Huy NGuyen. *Formes quadratiques et géométrie*

120. — Christian Leruste. *Topologie algébrique – Une introduction, et au-delà*

121. — Grégory Berhuy. *Algèbre : le grand combat.* Nouvelle édition

122. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome second*

125. — Pascal Boyer. *Petit compagnon des nombres et de leurs applications*

129. — Gentiana Danila, Jean-Denis Eiden et Rached Mneimné. *Algèbre éclectique*

Gentiana Danila, Jean-Denis Eiden
Rached Mneimné

Algèbre éclectique

Un bouquet de thèmes et d'exercices pour le M1

Calvage & Mounet

Gentiana DANILA et Rached MNEIMNÉ sont maîtres de conférences à l'université Paris Diderot.
Jean-Denis Eiden est professeur honoraire de chaire supérieure au lycée Fabert à Metz.

Mathematics Subject Classification (2000) :

14-XX Algebraic geometry
14H-XX Curves
14.20 Algebraic curves, surfaces and special varieties
51-XX Geometry
51F-XX Metric geometry
51N-XX Analytic and descriptive geometry
51N10 Affine analytic geometry
51N15 Projective analytic geometry
51N20 Euclidean analytic geometry
51N25 Analytic geometry with other transformation groups
51N30 Geometry of classical groups
51A05 General theory and projective geometries

ISBN 978-2-91-635290-9

♾ Imprimé sur papier permanent

© Calvage & Mounet, Paris, 2021

Nous nous rendons compte que ce que nous accomplissons n'est qu'une goutte dans l'océan. Mais si cette goutte n'existait pas dans l'océan, elle manquerait.

Mère Teresa

Table des matières

Préface
1. Préface et/ou propos liminaires 1
2. Pourquoi ce livre ? 1
3. Un lieu propice à l'imagination 2
4. Rédiger une preuve ou une solution : un art en soi 2
5. Le travail commence donc après la conquête 3
6. Mouvement du corps et mouvement de l'esprit 3
7. Exigence morale 4
8. Bourbaki est-il vraiment mort ? 5
9. Et l'ordinateur dans tout ça ? 6
10. Le mélange, ici, c'est bien 6
11. Le vague à l'âme, et le beau temps après la pluie 7
12. Les treize chapitres 8
12.1. L'anneau des endomorphismes d'un groupe abélien 8
12.2. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ 8
12.3. Les anneaux généraux 9
12.4. Un problème d'examen 10
12.5. Les polynômes symétriques 10
12.6. Anneaux en théorie des nombres 10
12.7. Modules de type fini sur un anneau principal 11
12.8. Un zeste d'algèbre linéaire 11
12.9. Les algèbres semi-simples 11
12.10. Corps finis 12
12.11. Botanique fine de petits groupes 12
12.12. La correspondance de Galois 12
12.13. Problèmes d'examen 13
13. Les treize chapitres qui manquent 13
13.1. Géométrie supérieure 13
13.2. Rudiments d'algèbre commutative et de géométrie algébrique 13
13.3. Arithmétique et réseaux 13
13.4. Formes quadratiques et algèbres de Clifford 13

13.5. Groupes de lie classiques 14
13.6. Algèbres de Lie semi-simples complexes 14
13.7. Corps généraux 14
13.8. Algèbres de polynômes en plusieurs variables 14
13.9. Compléments en théorie de Galois 14
13.10. Algèbre homologique 14
13.11. Algèbres de groupes et représentations 14
13.12. Représentations de carquois 14
13.13. Introduction au programme de Langlands 14
14. Créances 14
15. Pour finir 15
15.1. Considérations générales 15
15.2. Finition et pagination 15

Avant-propos
1. Applications et Cie 17
1.1. Les notations $\to$, $\to\to$, $\hookrightarrow$, $\rightsquigarrow$ 17
1.2. Restriction, application induite, passage au quotient 18
1.3. Corestriction 19
1.4. Fibres 19
1.5. Sections ensemblistes et sections morphiques 20
1.6. Suites exactes courtes scindables et/ou scindées 21
2. Notations dans les structures algébriques 21
2.1. Groupes monogènes, groupes cycliques 21
2.2. Sous-groupe dérivé, sous-groupe de Frattini, p-Sylow . . . 22
2.3. Anneaux, corps, algèbres 23
2.4. Idéaux 23
2.5. Polynômes et séries formelles 24
2.6. Extensions de corps 24
2.7. Les notations $\subseteq$ et $\subset$, a posteriori 25
3. Le langage des groupes opérant. Rappels 25
3.1. Treillis des sous-groupes d'un groupe 28
4. Groupe opérant sur un autre. Les produits semi-directs 29
5. Structure des groupes abéliens finis et de type fini. Rappels . . . 30
5.1. Groupes abéliens finis 30
5.2. Le groupe $(\mathbb{Z}^n, +)$ 30
6. Modules de type fini sur un anneau principal. Rappels 32
7. Hérédité dans le cas des anneaux de polynômes 32
8. Les relations d'équivalence matricielle 33
8.1. Cas d'un corps 33
8.2. Cas d'un anneau principal 33
9. De la réduction des endomorphismes 34
9.1. Diverses multiplicités d'une valeur propre 34

9.2. Dimension du commutant 35
9.3. Théorème de Weyr 35
9.4. Matrices normales 35
10. Notations matricielles 36
11. Corps parfaits 36
12. Familles et systèmes 37
13. Théorème de Maschke et lemme de Schur 37
14. Des géométries affine et affine euclidienne 38

I. Les groupes abéliens et leurs anneaux d'endomorphismes
1. Introduction 39
2. L'anneau $\big(\mathrm{End}(G,+),+,\circ\big)$ 40
2.1. Énoncé 40
2.2. Corrigé 40
2.3. Commentaires 47
3. Les anneaux d'endomorphismes ? Cela sert à quoi ? 50
3.1. Énoncé 51
3.2. Commentaires 52
4. Détermination des anneaux de cardinal p^2 52
4.1. Énoncé 52
4.2. Corrigé 53
4.3. Commentaires 57
5. L'anneau $\mathbb{Z}_p$ des entiers p-adiques 58
5.1. Énoncé 60
5.2. Corrigé 60
5.3. Commentaires 66
6. L'anneau $\mathbb{Z}_p$ revisité 67
6.1. Mise au point 67
6.2. Énoncé 68
6.3. Corrigé 69
7. Deux problèmes pour finir 76
7.1. Les groupes divisibles 76
7.2. L'anneau des endomorphismes du groupe $G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 78

II. Aimer $\mathbb{Z}/n\mathbb{Z}$
1. Préliminaires 81
2. Premières caresses 82
2.4. Deux treillis côte à côte 85
2.5. One floor one flat 85
3. Le théorème des restes chinois et ses applications 89
4. Des restes chinois au Kamasutra indien 93
4.9. Les idempotents de $\mathbb{Z}/60\mathbb{Z}$ 99
5. Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ 100

6. Sortir des eaux calmes ou les tumultes de l'amour 111
6.2. Exemple*.– Un groupe d'ordre 72 aux 2-Sylow cycliques . . 113
6.3. Un cardinal incompatible avec la simplicité 115
6.4. Quand les 2-Sylow sont cycliques 115
7. Reliquat 118
7.1. Les idéaux minimaux de $\mathbb{Z}/n\mathbb{Z}$ 118
7.2. Vu à l'oral de l'agrégation interne 118
7.3. Un treillis à quatre sous-groupes 118
7.4. Diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$ 119
7.5. Les sous-groupes de $\mathrm{Frat}(\mathbb{Z}/n\mathbb{Z})$ 119
7.6. Une question piège 120
7.7. L'isomorphie $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \{\bar{x} \in \mathbb{Z}/n\mathbb{Z}, m\bar{x} = \bar{0}\}$. 121
7.8. Théorème du treillis-quotient et groupes cycliques 121
7.9. Les 2-groupes cycliques 122
7.10. Représentations irréductibles et centre 122
7.11. Les cycliques parmi les abéliens 122
7.12. Produits semi-directs $\mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ et 2-Sylow de $\mathrm{GL}(2, \mathbb{F}_3)$ 124
7.13. Anybody got a match ? 127
7.14. Groupe abéliens finis et dualité 127
7.15. Groupe dérivé et produits pleins 127

III. Anneaux généraux
1. Apéro 130
1.1. Matrices nilpotentes dans $\mathbb{Z}/n\mathbb{Z}$ 130
1.2. Résoudre de tête 130
2. Des radicaux 133
3. Idéaux à gauche de $\mathrm{M}(n, \mathbb{C})$ 139
4. Idempotents 140
5. Anneaux artiniens commutatifs 142
5.4. Vrai ou Faux ? 148
5.5. Pourquoi « artinien $\Rightarrow$ noethérien » et pourquoi pas l'inverse ? 151
6. Le spectre premier d'un anneau commutatif 151
6.1. Idéaux premiers dans $\mathbb{Z}[X]$ 152
6.6. Vrai ou Faux ? 160
7. Algèbres de groupes 161
8. Quelques condiments de plus 163
9. L'anneau des entiers de Gauss et le théorème des deux carrés . . 166

IV. Examen, premier semestre du L2
1. Énoncé, avec entête 171
2. Corrigé 173
3. Deux exercices d'oral en bonus 181

V. Polynômes symétriques, ou presque
1. L'algèbre polynomiale $K[\sigma_1, \ldots, \sigma_n]$ 183
1.2. L'action de $\mathfrak{S}_n$ sur $\mathscr{R}_n = K[X_1, \ldots, X_n]$ 183
1.4. Un projecteur qui symétrise 184
1.9. La construction inverse 190
2. Théorème de structure 191
2.3. Exemples introductifs 191
2.4. Une preuve constructive d'existence 192
2.8. Unicité du polynôme Q 193
2.10. La méthode des poids 194
3. Fonctions symétriques des racines d'un polynôme 198
4. Les sommes de Newton 200
4.1. La première grande famille 201
4.2. La seconde grande famille 201
5. Les polynômes de Vandermonde et de Schur 205
5.1. Le déterminant de Vandermonde 206
5.4. Les déterminants de Vandermonde incomplets 208
5.7. Les déterminants de Schur 209
5.12. La seconde formule de Jacobi-Trudy 215
5.13. Des décompositions $L \cdot U$ 216
6. Les polynômes symétriques de degré 7 en trois variables 218
6.1. La base formée des monômes H_λ en les polynômes symétriques complets H_d, de degré d 218
6.2. La base formée des polynômes monomiaux M_λ, associés à la partition λ 218
6.3. La base (E_μ) issue des polynômes symétriques élémentaires σ_ℓ 219
6.4. La base (S_λ) des polynômes de Schur 219
6.5. Les Schur en fonction des σ_ℓ 220

VI. Anneaux en théorie des nombres
1. Rappels 224
1.7. Au sujet des réseaux 226
2. Groupes abéliens de type fini en arithmétique. First encounter . 230
3. Résidus quadratiques 233
4. Entiers d'un corps de nombres 234
4.1. Entiers algébriques 234
4.10. Norme et trace 237
5. Les unités d'un corps de nombres 258
5.7. L'exemple d'un corps cubique 260
6. L'anneau de Dedekind $\mathcal{O}_K$ 263
7. Finitude du monoïde des classes d'idéaux 267
7.1. Le monoïde $\mathrm{Cl}(A)$ 267
7.2. La constante de Minkowski 268

8. Exemples et exercices 269
9. En guise de conclusion 281
10. Annexe.– La loi de réciprocité quadratique 282

VII. Modules de type fini sur un anneau principal
1. Introduction 293
2. Tableaux de Young et réduction de Jordan 294
3. Panorama succinct de la réduction sous l'angle des $\mathbb{K}[X]$-modules 297
4. Vocabulaire des R-modules, pour R anneau commutatif 300
4.1. Premiers vocables 300
4.2. Complètement réductible $\Leftrightarrow$ semi-simple 301
5. Cas où M est le $\mathbb{K}[X]$-module E_u 302
5.1. Les cycliques 302
5.2. Les simples 302
5.3. Les indécomposables 303
5.4. Détermination du radical de E_u 305
5.5. Retour sur les cycliques 307
5.6. Commutant dans le cas d'une matrice compagnon 307
5.7. Les semi-simples 308
6. Réduction d'une matrice particulière 308
6.1. Les tableaux de Young de M_A 308
6.2. La matrice M_A sous l'angle des $\mathbb{K}[X]$-modules 311
6.3. Le secours de la forme normale de Smith 315
7. Matrices dont le cube est deux fois l'identité 316
8. Annexe. Restriction et extension des scalaires 326
9. Fourre-tout 332
9.1. Énoncé 332
9.2. Corrigé 332
9.3. Un exercice pour taupins, et au-delà 333
9.4. Corrigé 333
9.5. Une variante en $\natural\flat$ majeur de l'exercice précédent 334
9.6. Corrigé 334
9.7. Des nilpotents, encore et encore 334
9.8. Corrigé 335

VIII. Un zeste d'algèbre linéaire
1. L'algèbre $\mathbb{K}[u]$ des polynômes en l'endomorphisme u 337
1.2. Les nilpotents de $\mathbb{C}[M]$ 339
1.3. Projecteurs sur les sous-espaces caractéristiques 340
1.4. Pour en finir avec le lemme des noyaux 341
1.5. Décomposition de Dunford 341
2. Variations autour de la décomposition de Dunford 342
2.1. Quand le polynôme caractéristique vaut $(X^2-1)^n$ 342

2.2. Une généralisation immédiate 351
2.3. Deux derniers exemples 352
2.4. Énoncé 354
2.5. Corrigé 354
2.6. Énoncé 355
2.7. Corrigé 355
3. In the loop ou les matrices croisées 358
3.1. Deux matrices croisées ont (presque) même polynôme caractéristique 359
3.2. Matrices croisées nilpotentes 359
3.3. Cas général. Classes de similitude croisées 365
3.4. Un cas particulier 369
4. Matrices régulières versus matrices génériques 369
5. Sous-espaces vectoriels de $\mathrm{M}(n, \mathbb{C})$ stables par similitude 370
6. Représentations de Steinitz et de Jordan 373
6.1. Représentations irréductibles d'un produit 374
6.2. Idéaux à gauche de $\mathrm{M}(n, \mathbb{K})$ 378
7. Cardinal du cône nilpotent sur un corps fini 378
7.1. Le secours du lemme de Fitting 379
7.2. L'agrégat cellulaire nilpotent. Faits et bienfaits 380
8. Fourre-tout 382
8.1. Énoncé 382
8.2. Énoncé 383
9. Ampoules et interrupteurs 386
9.1. Le problème des interrupteurs 386
9.2. Un problème sur les intersections de sous-ensembles 388
9.3. Les groupes $\mathrm{O}(4, \mathbb{F}_2)$ et $\mathrm{O}(5, \mathbb{F}_2)$ 391
10. Sur les ordres des sous-groupes finis de $\mathrm{SL}(n, \mathbb{Z})$ *(ENS-2006, extrait)* 393
11. Trois derniers exercices (faciles) pour la route 395

IX. Algèbres semi-simples
1. Introduction 399
1.1. Voter à droite ou à gauche ? 404
2. Définitions et premières propriétés 405
2.1. Exercice 408
2.2. Corrigé 409
3. Finitude du nombre de représentations irréductibles 411
4. Automorphismes de l'algèbre (associative) des matrices $\mathrm{M}(n, \mathbb{K})$ 412
5. Théorème de Burnside 412
6. Théorème de Burnside – Autre approche 414
7. Théorème de Wedderburn 416
8. Anneaux semi-simples. Anneaux artiniens 418

X. Corps finis

1. Deux corps à seize éléments 420
1.1. Une situation classique 420
1.2. Commentaire 421
1.3. Énoncé.– 421
1.4. Corrigé.– 421
1.5. Morale 429
2. Interrogation écrite 429
3. Polynômes irréductibles de degré 2 dans $\mathbb{F}_4[X]$ 431
4. Deux corps à vingt-cinq éléments 433
5. Décomposition en facteurs irréductibles dans l'anneau $\mathbb{F}_3[X]$ . . 436
6. Un polynôme irréductible de degré 8 sur $\mathbb{F}_2$ 437
6.1. Irréductiblité de P 437
6.2. Super-primitivité des racines de P 439
7. Réduction des endomorphismes dans $\mathbb{F}_{16}$: le cas du Frobenius . 441
7.1. Énoncé 441
7.2. Corrigé.– 441
7.3. Remarque 444
7.4. Morale 444
7.5. Remarques annexes 445
8. L'étoile kellerienne 448
8.1. Énoncé 448
8.2. Corrigé.– 449
8.3. Commentaires 457
9. Devoir sur table impliquant des calculs dans $\mathbb{F}_{64}$ 461
10. Une liane infinie de corps 463
10.1. Premier énoncé 464
10.2. Corrigé du premier énoncé 464
10.3. Second énoncé 467
10.4. Corrigé du second énoncé 467
11. Sous-espaces vectoriels formés de matrices non inversibles 471
11.1. Énoncé 472
11.2. Corrigé.– 472
11.3. Morale 475
11.4. Remarque annexe 476
12. Le groupe $\mathrm{SO}(2, \mathbb{F}_q)$ 477
12.1. Énoncé 477
12.2. Corrigé.– 478
12.3. Conclusion.– 481
13. Racines de l'unité et cyclotomie dans $\mathbb{F}_p$ 486
14. Petit exercice de révision 491
15. Devoir sur table 492

XI. Botanique fine de petits groupes

1. Le procédé de binarisation 497
1.1. Les binaires parmi les groupes d'ordre 12, 20 et 24 497
1.2. Binaires de groupes d'ordre 8, et au delà 498
1.3. Un cas où l'on ne peut binariser 498
1.4. La binarisation pour elle-même 498
2. Les cinq groupes d'ordre 12 500
3. Les trois groupes non commutatifs d'ordre 20 502
4. Les cinq groupes d'ordre 24 à involution unique 504
5. Les groupes dicycliques 506
6. Deux groupes d'ordre 16 ayant les mêmes treillis 509
7. Des quotients simultanés impossibles 510
8. Conjugaison dans $\mathfrak{A}_4$ et dans $\mathfrak{S}_4 \times C_2$ 512
9. Exercice inspiré par le précédent 513
10. Un concentré de $\mathrm{GL}(3, \mathbb{F}_2)$ 514
11. Pas de C_6 dans $\mathrm{GL}(3, \mathbb{F}_2)$ 516
12. Y a-t-il des $\mathfrak{S}_3$ dans $\mathfrak{A}_4 \times C_2$? 517
13. Une caractérisation de $\mathrm{SL}(2, \mathbb{F}_3)$ 517
14. Une caractérisation de $\mathfrak{S}_4$ 518
15. Une autre caractérisation de $\mathfrak{S}_4$ 520
16. Groupes d'ordre 24 avec des C_2^3 pour 2-Sylow 520
17. Des distingués en quantité dans $\mathrm{T}(2, \mathbb{F}_5)$ 521
17.1. Distinction des sous-groupes d'indice 4 et 8 521
17.2. Intermède 521
17.3. Les sept sous-groupes d'ordre 20 de $\mathrm{T}(2, \mathbb{F}_5)$ 521
18. Des groupes rares, sertis dans $\mathrm{SL}(2, \mathbb{F}_5)$ 523
19. Un groupe d'ordre 32 bien particulier 523
20. Pas d'épimorphismes sur C_6 *et* $\mathfrak{S}_3$ depuis un groupe d'ordre 24 524
21. Les quatre sous-groupes $\mathbb{H}_8$ du groupe de Dedekind $\mathbb{H}_8 \times C_2$ . . 525
22. Automorphismes d'ordre 2 dans un 2-groupe 526
23. Les sous-groupes d'indice 6 de $\mathfrak{A}_6$ 527
24. Une autre caractérisation de $\mathfrak{A}_5$ 529
25. Le treillis de $\mathcal{D}_{10}$. Autre accoutrement 531
26. Classes de conjugaison des sous-groupes de $\mathfrak{A}_5$ 531
27. Les $\mathfrak{S}_4$ de $\mathfrak{S}_5$ 535
28. Les $\mathfrak{S}_4$ de $\mathfrak{A}_6$ 535
29. AntiDote60 536
29.1. Produits directs d'ordre 60 536
29.2. Intermède 537
29.3. Un groupe d'ordre 60 sans nom 538
29.4. Treillis de Dic_{15} 538
29.5. Treillis du produit semi-direct $G{=}C_{15} \rtimes_u C_4$, où $u : x \mapsto x^2$ 539
29.6. Treillis du groupe dicyclique $\mathrm{Dic}_{15} = \widetilde{\mathcal{D}_{15}}$ 541

30. Les 2-Sylow de $\mathfrak{S}_6$ 542
30.1. Isométries d'un carré dans l'espace 542
30.2. Le treillis de $\mathcal{D}_4 \times C_2$ 543
31. Théorème de Scorza et isométries du cube 545
31.1. La preuve du théorème de Scorza 545
31.2. Autre preuve (Alain Debreil) 548
31.3. Cas du cube 549
31.4. Le cube coloré et son patron 557
31.5. Le treillis de $\mathfrak{A}_4 \times C_2$ 558
31.6. Fleurs à cinq ou sept pétales 559
32. Le groupe du cube comme produit en couronne 559
33. Tiges et racines des sous-groupes d'un p-groupe 561
34. Sous-groupes finis du groupe spécial unitaire SU(2) 565
35. Le groupe de Heisenberg d'ordre 27 et son grand frère 565
35.1. Prérequis 565
35.2. Énoncé 566
35.3. Corrigé 566
35.4. Une caractérisation de $\mathrm{H}(3, \mathbb{F}_3)$ 568
35.5. Énoncé, suite et fin 568
35.6. Corrigé, suite et fin 569
35.7. Un automorphisme explicite d'ordre 8 de $\mathrm{H}(3, \mathbb{F}_3)$ 570
35.8. Remarques de culture générale 572
36. Vérifier que cet exo n'est pas à sa bonne place 572
37. Le groupe spécial linéaire $\mathrm{SL}(2, \mathbb{Z})$ 573
37.1. Deux générateurs particuliers de $G = \mathrm{SL}(2, \mathbb{Z})$ 573
37.2. Cyclicité de l'abélianisé de $\mathrm{SL}(2, \mathbb{Z})$ 575
37.3. L'indice du groupe dérivé de $\mathrm{SL}(2, \mathbb{Z})$ 575
37.4. Un lemme dû à Serre 583
37.5. La torsion dans $\mathrm{SL}(2, \mathbb{Z})$ 584

XII. La correspondance de Galois
1. Introduction 589
2. Qu'est-ce donc que la correspondance de Galois ? 589
3. Côté « Groupes » dans la correspondance de Galois 591
4. Côté « Corps » de la correspondance de Galois 594
5. L'énoncé complet de la correspondance 596
6. Corps de décomposition de $X^6 - 2$ et son groupe de Galois . . . 597
7. Le groupe $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comme groupe de Galois 601
7.1. Un premier exemple 601
7.2. Un deuxième exemple 603
7.5. Un troisième exemple 605
7.6. Un bonus en cadeau 605
8. Deux corps jumeaux non isomorphes 614

9. Quelques exercices de plus 615
9.1. Là où Eisenstein n'est d'aucun secours 615
9.2. Comment montrer que $\cos\left(\frac{2\pi}{9}\right)$ est irrationnel 616
9.3. Deux extensions de degré 2 ne constituent pas à elles seules une fratrie 617
9.4. Les constructibles et $\mathfrak{A}_4$ 617
10. L'extension galoisienne de $\mathbb{Q}$ engendrée par $\sqrt{\sqrt{3}+1}$ 618
11. Quand $\mathrm{Gal}(\mathbb{K},\mathbb{Q}) \simeq \mathfrak{S}_4$ 620
12. Une combinaison linéaire nulle en 1, $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{5}$ 621
13. L'équation $X^2-60=0$ dans $\mathbb{Q}(\sqrt{10},\sqrt{42})$ 621
14. L'extension galoisienne de $\mathbb{Q}$ engendrée par $\sqrt{\sqrt{2}+\sqrt{3}}$ 621
15. Un groupe de Galois $\mathbb{H}_8$ 631
16. Le groupe $\mathrm{HoT}(2,\mathbb{F}_3)$ comme groupe de Galois 635
17. Le groupe de Galois inédit de X^8-2 652
18. Considérations finales 652

XIII. Sujets d'examen

Bibliographie **717**
Index **719**

« À trente ans, une femme doit choisir entre le groupe et l'anneau. »
Proverbe tzigane

« J'ai mis toute ma vie à savoir dessiner comme un enfant. »
Pablo Picasso

Chapitre I

Les groupes abéliens et leurs anneaux d'endomorphismes

1. Introduction

Un groupe abélien A devrait être toujours accompagné de son anneau d'endomorphismes, ou du moins l'on devrait toujours s'inquiéter de savoir quel en est l'anneau d'endomorphismes. Si l'on ne fait pas toujours cela, c'est parce que l'anneau $\mathrm{End}(A)$ est parfois bien difficile à « calculer » [1]. L'objet de ce premier chapitre est de familiariser le lecteur avec ces anneaux-là et de montrer à quoi ils servent en priorité. *C'est l'occasion de comprendre ce qu'est un R-module M, pour un anneau R.* Contrairement à beaucoup d'auteurs qui disent pour introduire les R-modules qu'il s'agit d'espaces vectoriels sur l'anneau R, propos qui ne fait rien comprendre à l'idée de modules, nous insistons sur le fait qu'un R-module M est une façon de donner vie aux éléments de l'anneau R en en faisant des endomorphismes du groupe abélien sous-jacent à M. Autrement dit, un R-module M est la donnée d'un morphisme (d'anneaux unitaires) de R dans l'anneau des endomorphismes $\big(\mathrm{End}(M,+),+,\circ\big)$ d'un groupe abélien M, un élément quelconque de R agissant de la sorte sur les éléments de $(M,+)$, comme font exactement les endomorphismes.

1. Parmi les groupes abéliens finis, seuls les groupes cycliques et les groupes abéliens élémentaires ont des anneaux d'endomorphismes abordables pour un débutant. En dehors de deux ou trois exemples de groupes abéliens infinis $\big($tels les groupes abéliens libres de type fini $\mathbb{Z}^n$, ou bien $(\mathbb{Q},+)\big)$, la détermination de $\mathrm{End}(A)$ peut s'avérer bien compliquée ; on tombe ainsi sur l'anneau $\mathbb{Z}_p$ des entiers p-adiques quand on part avec le groupe $\mathbb{U}_{p^\infty}$ de toutes les racines p^k-ièmes de l'unité, avec k quelconque !

2. L'anneau $\big(\mathbf{End}(G,+),+,\circ\big)$

Soit $(G,+)$ un groupe abélien, noté additivement. On appelle endomorphisme de G un homomorphisme de groupes $G \to G$. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G.

2.1. Énoncé

1. *On pose* $(\phi_1+\phi_2)(g)=\phi_1(g)+\phi_2(g)$, *pour* $\phi_1,\phi_2\in\mathrm{End}(G)$ *et* $g\in G$. *Vérifier que l'on définit ainsi sur* $\mathrm{End}(G)$ *une loi de composition interne notée* $+$. *Montrer alors que* $\big(\mathrm{End}(G),+,\circ\big)$ *est un anneau. Pointer le ou les endroit(s) où la commutativité de la loi sur* G *est indispensable.*
2. *Établir que le groupe des éléments inversibles de l'anneau* $\big(\mathrm{End}(G),+,\circ\big)$ *des endomorphismes du groupe abélien* G *coïncide avec le groupe* $\big(\mathrm{Aut}(G),\circ\big)$ *des automorphismes de* G.
3. *Montrer que l'anneau* $\mathrm{End}(\mathbb{Z})$ *est isomorphe à* $\mathbb{Z}$.
4. *Quel est l'anneau des endomorphismes du groupe additif* $(\mathbb{Z}/n\mathbb{Z},+)$ *?*
5. *Donner, pour* $n\geqslant 1$, *une version matricielle de l'anneau* $\big(\mathrm{End}(\mathbb{Z}^n),+,\circ\big)$. *Vérifier qu'il existe beaucoup d'endomorphismes nilpotents sur le groupe additif* $\mathbb{Z}^2$. *En déduire que les groupes additifs* $\mathbb{Z}$ *et* $\mathbb{Z}^2$ *ne sont pas isomorphes.*
6. *Donner au moins trois autres arguments qui montrent que les groupes additifs* $(\mathbb{Z},+)$ *et* $(\mathbb{Z}^2,+)$ *ne sont pas isomorphes.*
7. *Déterminer le groupe des automorphismes du groupe additif* $\mathbb{Z}$ *ainsi que celui du groupe additif* $\mathbb{Z}^n$. *Déterminer également les automorphismes du groupe additif* $\mathbb{Z}/n\mathbb{Z}$.
8. *Calculer le cardinal de* $\mathrm{End}(\mathbb{Z}/36\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z},+)$.
9. (*) *Montrer que l'anneau des endomorphismes du groupe additif* $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ *contient trente-deux éléments et en déterminer le groupe des éléments inversibles.*

2.2. Corrigé

1. Vérifions déjà que la somme de deux endomorphismes est bien un endomorphisme :

$$(\phi_1+\phi_2)(g+h)=\phi_1(g+h)+\phi_2(g+h)=\phi_1(g)+\phi_1(h)+\phi_2(g)+\phi_2(h),$$

qui, en vertu de la commutativité, nous donne bien le résultat :

$$\begin{aligned}\phi_1(g)+\phi_1(h)+\phi_2(g)+\phi_2(h)&=\phi_1(g)+\phi_2(g)+\phi_1(h)+\phi_2(h)\\&=(\phi_1+\phi_2)(g)+(\phi_1+\phi_2)(h).\end{aligned}$$

Cela définit une loi de composition interne sur $\mathrm{End}(G)$, candidate à être l'addition dans le futur anneau. Il s'agit maintenant de vérifier que

cette loi est bien commutative. On a

$$(\phi_1+\phi_2)(g)=\phi_1(g)+\phi_2(g)=\phi_2(g)+\phi_1(g)=(\phi_2+\phi_1)(g),$$

de nouveau par commutativité de la loi $+$ dans G.

Le reste des axiomes de la structure d'anneau se vérifie aisément. On retient qu'il y a deux endroits où la commutativité de G a été sollicitée. Retenons aussi que l'endomorphisme nul est donné par $g\mapsto 0_G$ et l'endomorphisme unité par $\mathrm{Id}_G : g\mapsto g$.

2. Dire que f est inversible dans $\mathrm{End}(G)$, c'est dire qu'il existe $g\in\mathrm{End}(G)$ tel que $g\circ f=f\circ g=\mathrm{Id}_G$. Alors, f est bijectif, et est donc un élément de $\mathrm{Aut}(G)$. Inversement, si f est un automorphisme de G, f^{-1} est encore un morphisme, et f^{-1} est l'inverse de f dans $\mathrm{End}(G)$.
3. Le groupe additif $\mathbb{Z}$ est monogène, engendré par 1 ou -1. Un endomorphisme ϕ de $\mathbb{Z}$ est déterminé, par exemple, par l'image $\phi(1)$ de 1. Or, pour deux tels endomorphismes ϕ_1 et ϕ_2,

$$(\phi_1\circ\phi_2)(1)=\phi_1\big(\phi_2(1)\big)=\phi_2(1)\phi_1(1)=\phi_1(1)\phi_2(1).$$

L'application $\Psi:\mathrm{End}(\mathbb{Z})\to\mathbb{Z}$ définie par $\Psi(\phi)=\phi(1)$ est à la fois additive et multiplicative. En outre, et c'est important de ne pas l'oublier [2],

$$\Psi(1)=\Psi(\mathrm{Id}_{\mathbb{Z}})=\mathrm{Id}_{\mathbb{Z}}(1)=1.$$

L'application Ψ (par ailleurs clairement bijective) réalise ainsi un isomorphisme entre l'anneau $\big(\mathrm{End}(\mathbb{Z},+),+,\circ\big)$ et l'*anneau* $(\mathbb{Z},+,\cdot)$.

Il y a autant d'isomorphismes entre ces deux anneaux que d'automorphismes de l'anneau $\mathbb{Z}$, c'est-à-dire un seul ! En effet, un endomorphisme de l'*anneau* $\mathbb{Z}$, appliquant forcément 1 sur 1, est l'identité. L'isomorphisme Ψ est donc unique.

4. Le cas $n=0$ vient d'être traité. Le cas $n=1$ nous conduit au groupe trivial, dont l'anneau des endomorphismes est l'anneau nul $(0=1)$.

Pour $n\geqslant 2$, on procède de manière analogue au cas de $\mathbb{Z}$, car le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré, par exemple, par la classe $\overline{1}$ de 1. On a par conséquent l'isomorphisme d'anneaux (unique)

$$\big(\mathrm{End}(\mathbb{Z}/n\mathbb{Z},+),+,\circ\big)\simeq(\mathbb{Z}/n\mathbb{Z},+,\cdot),$$

qui associe à l'endomorphisme ϕ sa valeur en $\overline{1}$.

5. Le cas $n=1$ ayant déjà été traité, regardons le cas $n=2$ pour commencer . Un endomorphisme du groupe additif $\mathbb{Z}^2$ est entièrement par ses valeurs sur $e_1=(1,0)$ et $e_2=(0,1)$. Si ϕ_1 et ϕ_2 sont deux tels

2. Un morphisme d'anneaux doit, rappelons-le, appliquer élément unité sur élément unité. Si l'on avait posé $\Psi(\phi)=\phi(-1)$, cette condition aurait été en défaut. L'application Ψ présente donc moins de flexibilité que l'on aurait pu le soupçonner.

endomorphismes, on pose

$$\begin{array}{rl} & \phi_1(e_1) = a_1e_1 + b_1e_2, \quad \phi_1(e_2) = c_1e_1 + d_1e_2, \\ \text{et} & \phi_2(e_1) = a_2e_1 + b_2e_2, \quad \phi_2(e_2) = c_2e_1 + d_2e_2, \end{array}$$

où les coefficients a_i et b_i sont de simples entiers.

On a alors $(\phi_1 + \phi_2)(e_1) = (a_1 + a_2)e_1 + (b_1 + b_2)e_2$ et idem pour $(\phi_1 + \phi_2)(e_2)$, alors que

$$\begin{array}{rcl} \phi_1 \circ \phi_2(e_1) & = & \phi_1(a_2e_1 + b_2e_2) \;=\; a_2\phi_1(e_1) + b_2\phi_1(e_2) \\ & = & a_2(a_1e_1 + b_1e_2) + b_2(c_1e_1 + d_1e_2) \\ & = & (a_1a_2 + c_1b_2)e_1 + (b_1a_2 + d_1b_2)e_2, \end{array}$$

et, de même,

$$\phi_1 \circ \phi_2(e_2) = (a_1c_2 + c_1d_2)e_1 + (b_1c_2 + d_1d_2)e_2.$$

Si l'addition semble aller de source, la composition apparaît relever, en revanche, de règles de calcul autrement plus sophistiquées pour le regard innocent. Quant à l'œil averti, il discernera, bien sûr, une vieille connaissance, en l'occurrence la multiplication des matrices 2×2 :

$$\begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + c_1b_2 & a_1c_2 + c_1d_2 \\ b_1a_2 + d_1b_2 & b_1c_2 + d_1d_2 \end{bmatrix}.$$

Cette question offre donc l'occasion de réinventer ou redécouvrir le produit matriciel.

Passons au cas général et ayons les coudées franches. Le groupe additif $\mathbb{Z}^n$, muni de sa base canonique $(e_1, e_2, \ldots, e_n)$, est un groupe libre. Ses endomorphismes sont déterminés entièrement par leurs valeurs sur les vecteurs de cette base. Si ϕ est un tel endomorphisme, on disposera les composantes de chaque vecteur $\phi(e_j)$ comme j-ième colonne d'un tableau T_ϕ de taille $n \times n$.

L'addition des endomorphismes se propage en une addition terme à terme des coefficients des tableaux correspondants, alors que la composition des endomorphismes se propage à son tour en la multiplication des matrices carrées. L'anneau $\big(\mathrm{End}(\mathbb{Z}^n, +), +, \circ\big)$ est donc isomorphe à l'anneau $\big(\mathrm{M}(n, \mathbb{Z}), +, \cdot\big)$ des matrices carrées à coefficients entiers [3]. Le cas $n = 1$ se retrouve dans cette optique, une fois que l'on identifie les entiers aux matrices de taille 1×1, à coefficients dans $\mathbb{Z}$.

Les endomorphismes nilpotents du groupe additif $\mathbb{Z}^2$ sont associés aux matrices nilpotentes de l'anneau $\mathrm{M}(2, \mathbb{Z})$, c'est-à-dire aux matrices M de taille 2×2 à coefficients dans $\mathbb{Z}$ telles que $\det(M) = 0$ et $\mathrm{tr}(M) = 0$.

3. Pour $n \geqslant 2$, la matrice unité n'est surtout pas celle qui comporte partout des 1, mais bien celle qui n'a des 1 que sur sa diagonale principale, et des 0 partout ailleurs.

Ainsi, $(x,y)\in\mathbb{Z}^2\mapsto(ny,0)$, avec $n\in\mathbb{Z}$, ou bien

$$(x,y)\in\mathbb{Z}^2\mapsto(mx+y,-m^2x-my),\quad \text{avec } m\in\mathbb{Z},$$

fournissent deux familles infinies d'endomorphismes nilpotents de $\mathbb{Z}^2$, parmi bien d'autres.

L'anneau des endomorphismes du groupe additif $\mathbb{Z}$ étant intègre, le seul endomorphisme nilpotent de $(\mathbb{Z},+)$ est l'endomorphisme nul. Or, deux groupes abéliens isomorphes ont leurs anneaux d'endomorphismes également isomorphes. D'où un premier argument, pas des plus simples, pour nier l'isomorphisme des groupes additifs $\mathbb{Z}$ et $\mathbb{Z}^2$.

6. a) Le groupe $\mathbb{Z}$ est le modèle par excellence des groupes monogènes infinis. Le premier réflexe consiste donc à montrer que $(\mathbb{Z}^2,+)$ n'admet pas de générateur. Donnons de cela, à cet effet, trois arguments.

   (i) Supposons, par l'absurde, que (a,b) soit un tel générateur. On en déduirait l'existence de deux entiers non nuls k_1 et k_2 tels que $(1,0)=k_1(a,b)$ et $(0,1)=k_2(a,b)$, d'où $a=b=0$. L'élément $(0,0)$ engendrerait alors $\mathbb{Z}^2$. On a là une contradiction.

   (ii) Si α était un générateur du groupe additif $\mathbb{Z}^2$, tout $M\in\mathbb{Z}^2$ serait dans la droite rationnelle $\mathscr{D}$ et le sous-espace vectoriel de $\mathbb{Q}^2$ engendré par $\mathbb{Z}^2$, en l'occurrence $\mathbb{Q}^2$, serait encore dans $\mathscr{D}$, et donc $\dim_{\mathbb{Q}}(\mathbb{Q}^2)\leqslant 1$. Contradiction à nouveau.

   (iii) La propriété « α divise β » [4] se transmet par isomorphisme de groupes additifs. Les éléments (a,b) de $\mathbb{Z}^2$ qui n'ont que deux diviseurs sont tels que $a\wedge b=1$. Il en existe une infinité dans $\mathbb{Z}^2$, et seulement deux dans $\mathbb{Z}$.

   b) Tous les sous-groupes de $\mathbb{Z}$ sont d'indice fini, sauf le sous-groupe trivial $\{0\}$, alors que $\mathbb{Z}\times\{0\}$ et $\{0\}\times\mathbb{Z}$ sont deux sous-groupes de $\mathbb{Z}^2$ (parmi tant d'autres) qui sont d'indice infini.

   c) Si G est un groupe abélien, l'évaluation en 1 établit une correspondance bijective entre l'ensemble $\mathrm{Hom}(\mathbb{Z},G)$ et G. Or [5],

$$\mathrm{Hom}(\mathbb{Z}\oplus\mathbb{Z},G)\simeq\mathrm{Hom}(\mathbb{Z},G)\oplus\mathrm{Hom}(\mathbb{Z},G)\simeq G\oplus G.$$

   Un isomorphisme éventuel entre $\mathbb{Z}$ et $\mathbb{Z}^2$ fournirait par composition à droite une correspondance bijective entre $\mathrm{Hom}(\mathbb{Z}^2,G)$ et $\mathrm{Hom}(\mathbb{Z},G)$. On aurait $\mathrm{Card}(G)=\mathrm{Card}(G\times G)$, ce qui est évidemment faux pour peu que G soit fini, non trivial.

4. Autrement dit, β est un multiple (entier) de α.
5. Additivité du foncteur Hom.

D'autres arguments niant l'existence d'un isomorphisme entre $\mathbb{Z}$ et $\mathbb{Z}^2$ viendront dans la suite de l'ouvrage s'ajouter aux cinq déclinés antécédemment [6].

7. a) Les automorphismes de $(\mathbb{Z},+)$ sont les inversibles de l'anneau $\mathrm{End}(\mathbb{Z})$, c'est-à-dire de l'anneau $\mathbb{Z}$: ils sont en nombre de 2, en l'occurence les automorphismes $x \mapsto x$ et $x \mapsto -x$. On a donc

$$\big(\mathrm{Aut}(\mathbb{Z},+),\circ\big) \;\simeq\; (\{\pm 1\},\cdot).$$

b) Les automorphismes du groupe $(\mathbb{Z}^n,+)$ sont les inversibles de l'anneau des matrices $\mathrm{M}(n,\mathbb{Z})$, c'est-à-dire les éléments du groupe multiplicatif $\mathrm{GL}(n,\mathbb{Z})$. Une matrice M de $\mathrm{M}(n,\mathbb{Z})$ est inversible si, et seulement si, $\det(M)=\pm 1$. D'une part, l'égalité $MN = I_n$ entraîne que $\det(M) \in \mathbb{Z}^\times = \{\pm 1\}$.
D'autre part, comme $M\widetilde{M} = \widetilde{M}M = \det(M)I_n$, où $\widetilde{M}$ est la transposé de la matrice des cofacteurs, la condition $\det(M) = \pm 1$ implique M inversible dans $\mathrm{M}(n,\mathbb{Z})$. On a ainsi

$$\big(\mathrm{Aut}(\mathbb{Z}^n,+),\circ\big) \;\simeq\; \big(\mathrm{GL}(n,\mathbb{Z}),\cdot\big).$$

c) En suivant la même démarche, on a

$$\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z},+),\circ\big) \;\simeq\; (\mathbb{Z}/n\mathbb{Z}^\times,\cdot),$$

et $\overline{m} \mapsto k\overline{m}$, où $k \wedge n = 1$, est le modèle typique des automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

8. Le théorème des restes chinois [7] nous donne l'isomorphisme de groupes suivant : $\mathbb{Z}/36\mathbb{Z} \;\simeq\; \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.
Par fonctorialité bi-additive, un élément f de

$$\mathrm{End}(\mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z},+) = \mathrm{End}(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z},+)$$

s'identifie à un tableau

$$\begin{bmatrix} \alpha & \alpha_{12} & \alpha_{13} \\ \beta_{21} & \beta & \beta_{23} \\ \gamma_{31} & \gamma_{32} & \gamma \end{bmatrix},$$

où α, β et γ sont des endomorphismes de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/27\mathbb{Z}$ respectivement, où $\alpha_{12} \in \mathrm{Hom}(\mathbb{Z}/9\mathbb{Z},\mathbb{Z}/4\mathbb{Z})$, ... et $\gamma_{32} \in \mathrm{Hom}(\mathbb{Z}/9\mathbb{Z},\mathbb{Z}/27\mathbb{Z})$.

6. L'alinéa suivant nous en fournit d'ailleurs un de plus : le groupe additif $\mathbb{Z}$ n'admet que les deux automorphismes $x \mapsto \pm x$, alors que le groupe $\mathbb{Z}^2$ en admet déjà quatre évidents, en l'occurrence les automorphismes $(x,y) \mapsto (\pm x, \pm y)$.

7. Pour en savoir plus au sujet de ce célèbre résultat, se reporter au chapitre II, pages 90.

Or, on a

$$\mathrm{Hom}(\mathbb{Z}/p^m\mathbb{Z},\mathbb{Z}/q^n\mathbb{Z})=\{0\},\quad \text{si } p \text{ et } q \text{ sont premiers distincts,}$$

et

$$\mathrm{Hom}(\mathbb{Z}/p^m\mathbb{Z},\mathbb{Z}/p^n\mathbb{Z}) \;\simeq\; \mathbb{Z}/p^n\mathbb{Z},\quad \text{si } m\geqslant n,$$

et enfin

$$\mathrm{Hom}(\mathbb{Z}/p^m\mathbb{Z},\mathbb{Z}/p^n\mathbb{Z}) \;\simeq\; \mathbb{Z}/p^m\mathbb{Z},\quad \text{si } m< n.$$

En effet, tout cela se justifie par l'argument suivant. Le groupe au départ $\mathbb{Z}/p^m\mathbb{Z}$ est engendré par l'élément $\bar{1}$, lequel est annulé par p^m. L'image de $\bar{1}$ par un morphisme défini sur $\mathbb{Z}/p^m\mathbb{Z}$ doit encore être annulé par p^m. Or, le sous-groupe Z annulé par p^m dans le groupe à l'arrivée est nul dans le premier cas, et vaut $\mathbb{Z}/p^{\inf(m,n)}\mathbb{Z}$ dans les deux autres cas. Cela puisque p^m engendre $\mathbb{Z}/q^n\mathbb{Z}$, si q est premier distinct de p, et que lorsque $m\geqslant n$, p^m annule tout le monde, et enfin que, pour $m<n$, l'élément p^{n-m}, qui engendre Z, est d'ordre p^m.

Aussi f s'identifie-t-il à un tableau de morphismes appartenant à

$$\begin{bmatrix} \mathbb{Z}/4\mathbb{Z} & \{0\} & \{0\} \\ \{0\} & \mathbb{Z}/9\mathbb{Z} & \mathbb{Z}/9\mathbb{Z} \\ \{0\} & 3\mathbb{Z}/27\mathbb{Z} & \mathbb{Z}/27\mathbb{Z} \end{bmatrix},$$

et l'on a $4\times 9^3\times 27$ choix possibles pour f.

9. Le décompte des éléments suit la recette de la question précédente, et

$$\mathrm{Card}\Big(\begin{bmatrix} \mathbb{Z}/4\mathbb{Z} & 2(\mathbb{Z}/4\mathbb{Z}) \\ \mathbb{Z}/2\mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \end{bmatrix}\Big)=32,$$

car, comme expliqué plus haut, $2(\mathbb{Z}/4\mathbb{Z})$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$.

Comment se passe la multiplication ? Pour répondre, nous reprenons la démarche décrite au début du corrigé. Mais on a là des matrices dont les coefficients sont cette fois-ci des morphismes, au lieu d'être des entiers. Leur multiplication s'avère possible, car lorsque l'on effectue le produit matriciel, comme d'usage, deux morphismes α et β censés se multiplier pour donner $\alpha\circ\beta$, sont tels que l'espace d'arrivée de α est égal, comme il se doit, à l'espace de départ de β. Cela donne ici, après vérification laissée au bon soin des lecteurs,

$$\begin{bmatrix} \bar{\bar{a}} & 2\bar{\bar{b}} \\ \bar{c} & \bar{d} \end{bmatrix}\begin{bmatrix} \bar{\bar{x}} & 2\bar{\bar{y}} \\ \bar{z} & \bar{t} \end{bmatrix}=\begin{bmatrix} \overline{\overline{ax+2bz}} & 2\,\overline{\overline{ay+bt}} \\ \overline{cx+dz} & \overline{dt} \end{bmatrix},$$

où la simple-barre réfère à une classe modulo 2, et la double-barre à une classe modulo 4.

L'étude de cet anneau peu familier, que l'on notera par convenance $\mathscr{R}$, n'est point banale. L'application [8]

$$\mu : \begin{bmatrix} \bar{\bar{a}} & 2\bar{\bar{b}} \\ \bar{c} & \bar{d} \end{bmatrix} \mapsto \begin{bmatrix} \bar{a} & \bar{0} \\ \bar{c} & \bar{d} \end{bmatrix},$$

(bien) définie sur $\mathscr{R}$ à valeurs dans $\mathrm{M}(2, \mathbb{F}_2)$, est manifestement un morphisme d'anneaux [9]. L'idéal bilatère $\ker(\mu)$ est formé par les quatre matrices suivantes [10] :

$$\begin{bmatrix} \bar{\bar{0}} & \bar{\bar{0}} \\ \bar{0} & \bar{0} \end{bmatrix}, \quad \begin{bmatrix} \bar{\bar{2}} & \bar{\bar{0}} \\ \bar{0} & \bar{0} \end{bmatrix}, \quad \begin{bmatrix} \bar{\bar{0}} & \bar{\bar{2}} \\ \bar{0} & \bar{0} \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} \bar{\bar{2}} & \bar{\bar{2}} \\ \bar{0} & \bar{0} \end{bmatrix},$$

alors que $\mathrm{Im}(\mu)$ s'identifie à l'anneau $\mathscr{T}(2, \mathbb{F}_2)$ des matrices triangulaires inférieures. Le groupe multiplicatif $\mathscr{R}^\times$ se trouve donc au milieu de la suite exacte courte suivante :

$$I_2 + \ker(\mu) \hookrightarrow \mathscr{R}^\times \twoheadrightarrow \mathscr{T}(2, \mathbb{F}_2)^\times,$$

la surjectivité de la flèche à droite provenant du lemme ci-après [11].

Lemme. *Si le noyau* $\ker(\mu)$ *d'un morphisme d'anneaux* $\mu : R_1 \twoheadrightarrow R_2$, *supposé surjectif, est formé d'éléments nilpotents, l'homomorphisme naturel* $\mu^\times : R_1^\times \to R_2^\times$ *entre leurs groupes multiplicatifs est également surjectif, et son noyau coïncide avec* $1 + \ker(\mu)$.

Si $a_2 b_2 = b_2 a_2 = 1$ dans R_2, et si a_1 et b_1 relèvent respectivement a_2 et b_2 dans R_1, les produits $a_1 b_1$ et $b_1 a_1$ sont inversibles dans R_1, car ils s'écrivent chacun sous la forme $1 + \nu$, avec ν nilpotent [12]. L'élément a_1 est de ce fait à son tour inversible (car il l'est à à droite et à gauche).♡

Le groupe $\mathscr{T}(2, \mathbb{F}_2)^\times$ est formé de deux matrices : I_2 et $\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}$. On trouve donc huit éléments dans $\mathscr{R}^\times$. Il n'est pas inutile alors de remarquer que $M = \begin{bmatrix} \bar{\bar{a}} & 2\bar{\bar{b}} \\ \bar{c} & \bar{d} \end{bmatrix}$ dans $\mathscr{R}$ est inversible si, et seulement si, $\det\big(\mu(M)\big) = \overline{ad}$ est non nul dans $\mathbb{F}_2$, c'est-à-dire $\bar{a} = \bar{d} = \bar{1}$, ou

8. Sortie du chapeau, mais sait-on comment ? ! En fait, tout endomorphisme de notre groupe $A = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ laisse invariant le sous-groupe C engendré par $(\bar{2}, \bar{0})$ et induit donc un endomorphisme du quotient $A/C \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, si bien que nous disposons d'un morphisme $\mathrm{End}(A) \to \mathrm{End}(A/C)$, qui n'est autre que notre μ magique.

9. On aura noté que l'élément unité de l'anneau $\mathscr{R}$ est donné par la matrice $\begin{bmatrix} \bar{\bar{1}} & \bar{\bar{0}} \\ \bar{0} & \bar{1} \end{bmatrix}$.

10. Ces matrices sont toutes de carré nul. Cela nous servira par la suite.

11. Le noyau du morphisme de groupes multiplicatifs $\mathscr{R}^\times \twoheadrightarrow \mathscr{T}(2, \mathbb{F}_2)^\times$ induit par le morphisme d'anneaux μ est a priori l'intersection de la fibre de μ au dessus de 1 avec $\mathscr{R}^\times$, c'est-à-dire $\big(I_2 + \ker(\mu)\big) \cap \mathscr{R}^\times$, mais comme les éléments de $\ker(\mu)$ sont nilpotents, les éléments de la forme $I_2 + M$, pour $M \in \ker(\mu)$, sont tous inversibles (voir la note de bas de page rattachée au lemme suivant).

12. Si $\nu^k = 0$, l'inverse de $1 + \nu$ est donné par $1 + \nu + \cdots + \nu^{k-1}$.

encore $\bar{\bar{a}} = \pm\bar{\bar{1}}$ et $\bar{d} = \bar{1}$. On pourrait retrouver ainsi les huit éléments de $\mathscr{R}^\times$. Pour toute $M \in \ker(\mu)$, on a $(I_2+M)^2 = I_2+2M = I_2$. Le sous-groupe $I_2+\ker(\mu)$ de $\mathscr{R}^\times$ est donc isomorphe à $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$. Pour peu que l'on établisse que le groupe $\mathscr{R}^\times$ (d'ordre 8) est non commutatif, on aura la preuve [13] que

$$\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+) \;\simeq\; \mathcal{D}_4.$$

Les deux matrices $\begin{bmatrix} \bar{\bar{1}} & \bar{\bar{0}} \\ \bar{1} & \bar{1} \end{bmatrix}$ et $\begin{bmatrix} \bar{\bar{1}} & 2\cdot\bar{\bar{1}} \\ \bar{0} & \bar{1} \end{bmatrix}$ ne commutant pas, le groupe est bien non abélien [14].

2.3. Commentaires

1. La loi de multiplication dans $\mathbb{Z}$ se lit dans l'anneau des endomorphismes du groupe additif $(\mathbb{Z},+)$.

   Quand, en propédeutique, on préfère le groupe $(\mathbf{U}_n,\cdot)$ des racines n-ièmes de l'unité au groupe additif $\mathbb{Z}/n\mathbb{Z}$ comme modèle du groupe cyclique à n éléments, il semble que l'on perde a priori au change la multiplication, que l'on a sur les congruences. Il est cependant possible de la retrouver dans l'anneau des endomorphismes du groupe $(\mathbf{U}_n,\cdot)$.

2. L'existence d'un isomorphisme entre les groupes additifs $\mathbb{Z}^m$ et $\mathbb{Z}^n$ entraîne que $m = n$. L'argument utilisé plus haut s'applique encore, puisque $\mathrm{Hom}(\mathbb{Z}^k,\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^k$.

   Variante : une extension des scalaires au corps $\mathbb{F}_2$, qui s'obtient en tensorisant par $\mathbb{Z}/2\mathbb{Z}$, montre que le $\mathbb{F}_2$-espace vectoriel $\mathbb{Z}^k\otimes_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$ est isomorphe à $(\mathbb{F}_2)^k$. On peut aussi étendre les scalaires à $\mathbb{Q}$, et invoquer, en place d'un argument de cardinalité, un argument de dimension sur $\mathbb{Q}$ (ce qui est évidemment plus coûteux) : $\mathbb{Z}^k\otimes_{\mathbb{Z}}\mathbb{Q} \overset{e.v.}{\simeq} \mathbb{Q}^k$.

   L'exercice examine le cas des groupes $\mathbb{Z}$ et $\mathbb{Z}^2$, car il se prête à maintes approches. D'ailleurs, l'évocation de l'anneau des endomorphismes des groupes $\mathbb{Z}$ et $\mathbb{Z}^2$ peut être mise à profit d'une manière plus simple que celle suggérée par l'énoncé. Les anneaux $\mathbb{Z}$ et $\mathrm{M}(2,\mathbb{Z})$ refusent aussi d'être isomorphes, car l'un est commutatif et l'autre non, ou bien car le groupe des inversibles de l'un est $(\{\pm1\},\cdot)$ et celui de l'autre est le groupe multiplicatif $\mathrm{GL}(2,\mathbb{Z})$ des matrices à coefficients entiers de déterminant ±1.

13. Les groupes non commutatifs d'ordre 8 sont, à isomorphisme près, le groupe diédral $\mathcal{D}_4$ des isométries du carré et le groupe quaternionique $\mathbb{H}_8$. Le groupe $\mathcal{D}_4$ possède deux sous-groupes $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, alors que $\mathbb{H}_8$ n'en possède aucun.

14. Ces deux matrices, qui ne commutent pas, sont de surcroît d'ordre 2. Cela suffit pour détecter le groupe $\mathcal{D}_4$, qui, en effet, est le seul groupe d'ordre 8 possédant deux involutions qui ne commutent pas.

Maintenant, remarquons que si $\mathbb{Z}^m$ est isomorphe à $\mathbb{Z}^n$, alors il en est de même de leurs anneaux d'endomorphismes [15]. Or, on peut lire l'entier n dans l'anneau $\mathrm{End}(\mathbb{Z}^n)$, par exemple comme le plus grand indice de nilpotence de ses éléments, entier qui est invariant évidemment par isomorphisme d'anneaux : il s'ensuit donc que $m = n$.

3. L'énoncé de l'exercice manque de poser une question naturelle : *quelle est la caractéristique de l'anneau* $\mathrm{End}(G)$ *?* Il s'agit de déterminer l'idéal de l'anneau $\mathbb{Z}$ formé des entiers n tels que $n \cdot \mathrm{Id}_G = 0$, où 0 désigne l'endomorphisme nul de G. L'existence d'un tel entier n non nul équivaut donc à dire que G est d'exposant [16] fini, auquel cas *l'exposant du groupe abélien G coïncide avec la caractéristique de l'anneau* $\mathrm{End}(G)$ *de ses endomorphismes* [17]. Si G n'est pas d'exposant fini, $\mathrm{End}(G)$ est de caractéristique nulle. Ainsi, $\mathrm{End}(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, +)$ est de caractéristique 4 et $\mathrm{End}(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}, +)$ est de caractéristique nulle.

4. Posons-nous la question de savoir quand est-ce que $\mathrm{End}(G)$ est un corps.
   ▷ Les groupes $\mathbb{Z}/p\mathbb{Z}$ (avec p premier quelconque) sont des exemples évidents de groupes ayant des anneaux d'endomorphismes qui soient des corps. Nous nous contenterons de répondre pleinement à la question posée au début du présent alinéa lorsque le groupe G est fini [18]. On va montrer que *les seuls groupes abéliens finis dont l'anneau des endomorphismes est un corps sont les groupes simples* $\mathbb{Z}/p\mathbb{Z}$.

---

15. Si $\phi : G_1 \xrightarrow{\simeq} G_2$ est un isomorphisme de groupes abéliens, alors $\Phi : f \mapsto \phi \circ f \circ \phi^{-1}$ réalise un isomorphisme entre les anneaux $\mathrm{End}(G_1)$ et $\mathrm{End}(G_2)$. Noter cependant que la correspondance $G \rightsquigarrow \mathrm{End}(G)$ n'est pas fonctorielle (pas plus d'ailleurs que la correspondance $G \rightsquigarrow \mathrm{Aut}(G)$), puisqu'un morphisme entre les groupes abéliens G_1 et G_2 ne donne pas un morphisme entre les anneaux $\mathrm{End}(G_1)$ et $\mathrm{End}(G_2)$ (et pas davantage entre les groupes d'automorphismes $\mathrm{Aut}(G_1)$ et $\mathrm{Aut}(G_2)$).

16. Le groupe G est dit d'*exposant fini* s'il existe un entier $n > 0$ tel que $n \cdot x = 0_G$, pour tout $x \in G$ (ou bien $x^n = e_G$ si la loi dans G, d'élément neutre e_G, est notée multiplicativement), notion qui a encore un sens pour un groupe pas nécessairement commutatif. Sous cette hypothèse, l'ensemble des entiers $n \in \mathbb{Z}$ tel que $n \cdot x = 0_G$ (ou $x^n = e_G$), pour tout $x \in G$, est un sous-groupe additif non nul de $\mathbb{Z}$, et son générateur strictement positif s'appelle l'*exposant* de G. Quand G est fini, son exposant est fini et divise son cardinal.

17. Rappelons que la caractéristique d'un anneau est le générateur positif ou nul du sous-groupe de $\mathbb{Z}$ formé des entiers k tels que $k \cdot 1 = 0$, autrement dit si la caractéristique d'un anneau $(R, +, \cdot)$ est non nulle, c'est l'ordre de l'élément unité 1 dans le groupe additif $(R, +)$ sous-jacent à R. Si cette caractéristique est égale à $n \neq 0$, alors

$$n \cdot x = x + \cdots + x = (1 + \cdots + 1)x = (n \cdot 1)x = 0 \cdot x = 0,$$

si bien que la caractéristique de l'anneau R coïncide dans ce cas avec l'exposant du groupe additif sous-jacent à R. Noter enfin que, lorsque G est abélien, l'exposant du groupe additif $(\mathrm{End}(G), +)$ est égal à celui de G.

18. Le raisonnement qui suit demande quelques rudiments sur les groupes abéliens finis, qui apparaîtront comme bien innocents, une fois que l'on aura abordé le chapitre VII.

Si G est un groupe abélien fini de cardinal n et si p premier divise n, la p-torsion $T_p(G)$ de G (définie comme le sous-groupe des $x \in G$ tels que $p{\cdot}x = 0$) apparaît comme le noyau de l'*endomorphisme* $\pi_p : x \mapsto p{\cdot}x$ de G. Le noyau de π_p étant non nul (puisqu'il existe dans G des éléments d'ordre p), le morphisme π_p ne peut être un automorphisme : il est donc nul. Cela se traduit par le fait que G est un p-groupe abélien élémentaire, c'est-à-dire une somme directe de n copies de $\mathbb{Z}/p\mathbb{Z}$, avec $n \geqslant 1$. L'anneau des endomorphismes d'un tel groupe est $\mathrm{M}(n,\mathbb{F}_p)$ et son groupe d'automorphismes est $\mathrm{GL}(n,\mathbb{F}_p)$. Demander donc que tout endomorphisme soit un automorphisme impose que $n = 1$ (penser à $E_{1,1}$). Le lecteur perspicace choisira, en usant de l'alinéa précédent, de commencer plutôt par faire appel à la caractéristique, sachant que celle d'un corps fini est un nombre premier p : l'hypothèse que $\mathrm{End}(G)$ est un corps (fini) implique alors que G est aussitôt d'exposant un nombre premier p, si bien qu'étant abélien c'est un p-groupe abélien élémentaire[19], et la preuve se termine comme précédemment.

▷ En général, le cas des groupes abéliens infinis est nettement plus compliqué. Nous disposons au moins d'un exemple simple où l'anneau des endomorphismes est un corps, à savoir le groupe additif $\mathbb{Q}$.
En effet, un endomorphisme f de $(\mathbb{Q},+)$ est déterminé par sa valeur en 1 : si $f(1) = a$, alors

$$qf\big(\frac{p}{q}\big) = f(p) = pf(1) = pa \quad \text{et donc} \quad f\big(\frac{p}{q}\big) = \frac{p}{q}a.$$

Il s'ensuit que l'anneau des endomorphismes du groupe additif $(\mathbb{Q},+)$ est le corps $\mathbb{Q}$:

$$\big(\mathrm{End}(\mathbb{Q},+),+,\circ\big) \simeq (\mathbb{Q},+,\cdot).$$

La clef de l'argument qui précède est que le groupe additif $(\mathbb{Q},+)$ est *divisible*[20] :

$$\begin{tikzcd}
\{0\} \arrow[r] & \mathbb{Z} \arrow[r] \arrow[d, "f"'] & \mathbb{Q} \arrow[dl, dotted, "\tilde{f}\in\mathrm{End}(\mathbb{Q})"] \\
f : 1 \mapsto a & \mathbb{Q}\,. &
\end{tikzcd}$$

19. Le groupe des matrices unipotentes supérieures à coefficients dans $\mathbb{F}_p$ est d'exposant p et n'est pas commutatif dès que $p \geqslant 3$.

20. Rappelons qu'un groupe $(G,+)$ est divisible si pour tout $n > 0$, $nG = G$. Cela revient à dire que le $\mathbb{Z}$-module G est injectif. Un R-module I est injectif si tout morphisme f défini sur le sous-module N d'un R-module M quelconque à valeurs dans I

$$\begin{tikzcd}
\{0\} \arrow[r] & N \arrow[r] \arrow[d, "f"'] & M \arrow[dl, dotted, "\tilde{f}"] \\
& I &
\end{tikzcd}$$

peut être prolongé à M.

Le fait que les endomorphismes de $(\mathbb{Q},+)$ forment un corps implique que le groupe $\mathbb{Q}$ est *indécomposable*, autrement dit si $\mathbb{Q} = M_1 \oplus M_2$, l'une des composantes M_1 ou M_2 est nulle [21]. En effet, si par exemple M_1 est non nul, la projection sur M_1 parallèlement à M_2 est un endomorphisme non nul. Il est donc inversible, c'est-à-dire bijectif, et son noyau M_2 est donc nul. En particulier, le sous-groupe $\mathbb{Z}$ n'est pas *facteur direct* dans $\mathbb{Q}$:

$$\nexists S, \quad \mathbb{Q} = \mathbb{Z} \oplus S\,.$$

La morale de cela est que si l'anneau des endomorphismes de $(G,+)$ est un corps, il est nécessaire que G soit indécomposable [22].

Le groupe additif $\mathbb{Q}/\mathbb{Z}$, qui joue un rôle important parmi les groupes abéliens non triviaux [23], est isomorphe au groupe $\mathbf{U}_\infty$ de toutes les racines n-ièmes de l'unité, comme il résulte clairement de la suite exacte courte [24] :

$$(\mathbb{Z},+) \hookrightarrow (\mathbb{Q},+) \overset{\varepsilon}{\twoheadrightarrow} (\mathbf{U}_\infty,\cdot),$$

où $\varepsilon : x \mapsto \exp(2\mathrm{i}\pi x)$.

Ce groupe est divisible (en tant qu'image d'un groupe divisible), mais n'est pas indécomposable, puisqu'il est la somme directe (infinie) de tous les $\mathbf{U}_{p^\infty}$, où p décrit l'ensemble $\mathscr{P}$ des nombres premiers :

$$\mathbf{U}_\infty = \bigoplus_{p\in\mathscr{P}} \mathbf{U}_{p^\infty}\,.$$

On verra un peu plus loin (cf. problème 5, en page 58) que le groupe multiplicatif $\mathbf{U}_{p^\infty}$ est, en revanche, indécomposable. On verra également que ce groupe abélien est divisible et admet l'anneau local $\mathbb{Z}_p$ comme anneau d'endomorphismes.

3. Les anneaux d'endomorphismes ? Cela sert à quoi ?

Nous avons rencontré, dans l'exercice précédent, quelques exemples plus ou moins naturels d'anneaux d'endomorphismes de groupes abéliens. Un tel anneau est considéré communément comme un anneau heureux.

21. Le groupe $(\mathbb{Z},+)$ fournit un exemple bien plus simple de groupe indécomposable infini, puisque deux sous-groupes non nuls $a\mathbb{Z}$ et $b\mathbb{Z}$ de $\mathbb{Z}$ ont toujours une intersection non nulle (penser au PGCD de a et b).

22. On démontrera que si le groupe abélien G est injectif et indécomposable, alors l'anneau $\mathrm{End}(G)$ n'est pas très loin d'être un corps, car il sera sous ces conditions un *anneau local*, c'est-à-dire qu'il a un idéal (bilatère) maximal unique.

23. On entend ici par trivial un groupe abélien qui est de type fini, c'est-à-dire isomorphe à $\mathbb{Z}^r \oplus F$, où F est (abélien) fini et $r \in \mathbb{N}$. Le sous-groupe de torsion d'un tel groupe est en particulier fini, ce qui n'est pas le cas de $\mathbb{Q}/\mathbb{Z}$, dont tous les éléments sont d'ordre fini.

24. Que d'aucuns écriraient tout aussi efficacement $\{0\} \to \mathbb{Z} \to \mathbb{Q} \xrightarrow{\varepsilon} \mathbf{U}_\infty \to \{1\}$.

Expliquons-nous. L'apprenti mathématicien se heurte de nos jours aux structures algébriques avant même d'en avoir des exemples concrets. Jadis, Abel, Lagrange ou Galois usaient de la notion de groupe sans en formuler pour autant une définition abstraite. Les groupes étaient pour eux des collections de permutations d'ensembles de racines d'équations, et pour ceux de leurs confrères qui firent plus tard de la géométrie, ces groupes-là furent remplacés par des groupes de transformations. À présent, on procède à rebrousse-poil. Une fois que l'on a défini ce qu'est un groupe G, on cherche à en étudier des réalisations diverses et variées en le laissant agir de tout côté sur des ensembles adéquats. On est encore plus satisfait si nos actions sont linéaires, c'est-à-dire que l'on a réussi à réaliser le groupe G, ou un de ses quotients, comme sous-groupe d'un groupe linéaire. Il en de même pour les anneaux. On est cette fois d'autant plus content que notre anneau R est réalisé comme sous-anneau d'un anneau d'endomorphismes de groupe abélien. On touche là à la théorie des R-modules ! Pour conforter davantage notre propos, signalons que l'on est conduit pareillement dans le cas d'une algèbre de Lie $\mathfrak{g}$ sur le corps $\mathbb{K}$ à en chercher les représentations, c'est-à-dire les morphismes $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$, où $\mathfrak{gl}(V)$ est l'algèbre de Lie des endomorphismes du $\mathbb{K}$-espace vectoriel V.

Cet exercice sera donc pour nous l'occasion de s'approprier la notion de R-module, mais aussi d'apprécier les degrés de liberté dont dispose un groupe abélien qui veut devenir anneau.

3.1. Énoncé

Soit $(R, +, \cdot)$ un anneau, supposé évidemment unitaire, mais pas nécessairement commutatif.

1. *Rappeler la définition d'un R-module M et celle d'un morphisme de R-modules $f : M \to N$. Traduire les axiomes de définition en termes de l'anneau R et de l'anneau des endomorphismes du groupe abélien $(M, +)$ sous-jacent à M. Examiner le cas particulier des $\mathbb{K}$-espaces vectoriels et interpréter dans ce cas et dans le cas général ce qu'est la « multiplication » par un scalaire.*
2. *On s'intéresse dans cette question à l'anneau des endomorphismes du groupe abélien $(R, +)$ sous-jacent à l'anneau R. Pour $a \in R$, on définit l'application $m_a : R \to R$, $x \mapsto a \cdot x$. Montrer que m_a est un endomorphisme du groupe abélien $(R, +)$, puis que l'application $a \mapsto m_a$ est un homomorphisme d'anneaux de R dans $\mathrm{End}(R)$. Montrer que cet homomorphisme est injectif, puis que $\mathrm{End}(R)$ possède un sous-anneau isomorphe à R. Donner ensuite un exemple où ce sous-anneau est distinct de $\mathrm{End}(R)$.*

3. *Réaliser l'anneau* $\mathbb{Z}[\mathrm{i}]$ *des entiers de Gauss et l'anneau* $\mathbb{Z}[\mathrm{j}]$ *comme sous-anneaux de* $\mathrm{M}(2,\mathbb{Z})$. *Quelles sont toutes les structures d'anneaux ayant* $(\mathbb{Z}^2,+)$ *comme groupe abélien sous-jacent ?*
4. *Déterminer ce qu'est un* $\mathbb{Z}$*-module, un* $\mathbb{Z}[\mathrm{j}]$*-module, un* $\mathbb{K}[X]$*-module, un* $\mathbb{K}[X]/(X^3)$*-module, un* $\mathbb{K}[X,Y]$*-module, où* $\mathbb{K}$ *est bien sûr un corps, et enfin ce qu'est un* $\mathscr{T}(2,\mathbb{K})$*-module, où* $\mathscr{T}(2,\mathbb{K})$ *désigne l'anneau des matrices triangulaires* 2×2 *à coefficients dans* $\mathbb{K}$.
5. *Déterminer la catégorie des* $\mathrm{M}(n,\mathbb{K})$*-modules en prenant le soin de rappeler brièvement le vocabulaire propre à ce contexte.*
6. *Reprendre la question précédente en remplaçant l'anneau* $\mathrm{M}(n,\mathbb{K})$ *par l'anneau* $\mathrm{End}(\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z},+)$.

3.2. Commentaires

Rappeler également la définition d'une application $f : X \to Y$ qui est G-équivariante.

4. Détermination des anneaux de cardinal p^2

Le groupe additif sous-jacent à un anneau de cardinal p^2, étant abélien et fini, a une structure bien connue. Un tel groupe est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou bien à $\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$.
Faire de ces groupes des anneaux revient à mettre en évidence, *grâce à la représentation régulière*, des sous-anneaux de cardinal p^2 de leurs anneaux d'endomorphismes respectifs, à savoir l'anneau $\mathbb{Z}/p^2\mathbb{Z}$ et l'anneau $\mathrm{M}(2,\mathbb{F}_p)$. Cela ne nous laisse pas beaucoup de choix dans le premier cas. En revanche, en examinant l'autre cas, nous rencontrerons trois possibilités en tout et pour tout.

4.1. Énoncé

1. *Rappeler comment un anneau* $(R,+,\cdot)$ *se réalise comme sous-anneau de l'anneau des endomorphismes* $\big(\mathrm{End}(R,+),+,\circ\big)$ *de son groupe additif.*
2. *Rappeler comment l'on établit que* $\big(\mathrm{End}(\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z},+),+,\circ\big)$ *est isomorphe à l'anneau* $\big(\mathrm{M}(2,\mathbb{F}_p),+,\cdot\big)$.
3. *Soit* $M\in\mathrm{M}(2,\mathbb{K})$. *Montrer que le sous-anneau engendré par* M *apparaît comme un quotient de* $\mathbb{Z}[X]$. *Est-ce un quotient de* $\mathbb{K}[X]$ *?*
4. *Dresser la liste des quatre anneaux d'ordre* p^2 *et donner divers arguments pour montrer que ces anneaux ne sont pas isomorphes.*

4.2. Corrigé

1. L'application $L : R \to \mathrm{End}(R)$ définie par $L(a)(x) = ax$ est clairement un homomorphisme d'anneaux. Son noyau est réduit à $\{0\}$, car l'anneau est unitaire. Cela permet de réaliser les éléments de l'anneau abstrait $(R, +, \cdot)$ comme endomorphismes d'un groupe abélien, en l'occurrence $(R, +)$. D'ailleurs, pour ceux qui ne l'ont pas encore remarqué, c'est simplement la prise de conscience que R est un R-module à gauche.
2. Un endomorphisme du groupe additif $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ est un endomorphisme du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^2$, puisque tout élément est annulé par p (un A-module M devient un $A/\mathfrak{m}$-espace vectoriel si les éléments de M sont annulés par les éléments de l'idéal maximal $\mathfrak{m}$). Par ailleurs, il est bien connu que les anneaux $\mathrm{End}_{\mathbb{F}_p}(\mathbb{F}_p^n)$ et $\mathrm{M}(n, \mathbb{F}_p)$ sont canoniquement isomorphes.
3. Un quotient de l'anneau $\mathbb{Z}[X]$ est l'image homomorphique de $\mathbb{Z}[X]$ par un morphisme d'anneaux. Or, définir un morphisme sur l'anneau $\mathbb{Z}[X]$ revient à se donner l'image de l'indéterminée X. L'anneau engendré par M est de ce fait isomorphe au quotient de $\mathbb{Z}[X]$ par l'idéal des polynômes $P \in \mathbb{Z}[X]$ tels que $P(M) = 0$. Le sous-anneau engendré par M est une sous-algèbre de $\mathrm{M}(2, \mathbb{K})$ si le sous-anneau engendré par 1 s'identifie à $\mathbb{K}$. Cette dernière condition n'est satisfaite que si $\mathbb{K} = \mathbb{F}_p$.
4. D'après la première question et l'introduction, notre anneau (de cardinal p^2) est un sous-anneau de $\mathbb{Z}/p^2\mathbb{Z}$ ou de $\mathrm{M}(2, \mathbb{F}_p)$. Dans le premier cas c'est donc $\mathbb{Z}/p^2\mathbb{Z}$ lui-même, et dans le second, il contient (au vu de la question précédente) une sous-algèbre de la forme $\mathbb{F}_p[M]$, où M est une matrice forcément *non scalaire*. Dans ce cas, la matrice M admet pour polynôme minimal son polynôme caractéristique χ_M (de degré 2). Notre anneau coïncide alors avec l'algèbre $\mathbb{F}_p[M] \simeq \mathbb{F}_p[X]/(\chi_M)$, qui est de cardinal p^2. Ces algèbres-quotient se répartissent en trois classes d'isomorphie, selon que le polynôme χ_M a deux racines distinctes, une racine double ou, enfin, est irréductible dans $\mathbb{F}_p$. On a donc ici, à isomorphisme près, trois anneaux de cardinal p^2 possibles : l'anneau $\mathbb{F}_p \times \mathbb{F}_p$, l'anneau $\mathbb{F}_p[X]/(X^2)$ et le corps à p^2 éléments $\mathbb{F}_{p^2}$. Cette affirmation demande quelques éclaircissements. Elle suppose entre autres qu'il n'y a, à isomorphisme près, qu'un seul corps [25] de cardinal p^2, mais elle sous-entend aussi que les quatre anneaux sus-cités ne sont pas isomorphes.

25. Autrement dit, la classe d'isomorphie du corps $\mathbb{F}_p[X]/\big(p(X)\big)$, où $p(X)$ est un polynôme irréductible de degré 2, ne dépend pas de p. Cela résulte élémentairement de deux remarques :

▷ une extension de degré 2 sur un corps $\mathbb{K}$ s'écrit toujours $\mathbb{K}(\sqrt{\alpha})$, où $\alpha \notin \mathbb{K}^2$. Pour s'en convaincre, établir pour commencer que $\mathbb{Q}(\mathrm{j}) = \mathbb{Q}[X]/(X^2 + X + 1) = \mathbb{Q}(\sqrt{-3})$, puis penser à la mise sous forme canonique et au discriminant d'une équation du second degré pour le cas général ;

▷ deux non-carrés de $\mathbb{F}_p$ diffèrent multiplicativement d'un carré, puisque $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ est d'ordre 2.

Les explications qui suivent nous aideront à clarifier tout cela.

(a) Si Φ est un automorphisme d'un anneau R, et si $\mathfrak{a}$ est un idéal de R, alors les anneaux-quotient $R/\mathfrak{a}$ et $R/\Phi(\mathfrak{a})$ sont isomorphes. L'homomorphisme d'anneaux $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$, qui applique X sur le polynôme $X - \alpha$, est un tel automorphisme Φ (dont l'automorphisme réciproque applique X sur $X + \alpha$).

(b) L'anneau $\mathbb{F}_p[X]/\big(X(X-1)\big)$, tout comme $\mathbb{F}_p[X]/\big((X-\alpha)(X-\beta)\big)$ pour $\alpha \neq \beta$ dans $\mathbb{F}_p$, est isomorphe, d'après le théorème des restes chinois, à l'anneau $\mathbb{F}_p \times \mathbb{F}_p$. On aura noté que $\mathbb{F}_p[X]/(X) \simeq \mathbb{F}_p$.

(c) L'anneau $\mathbb{F}_p[X]/(X^2)$ est isomorphe à $\mathbb{F}_p[X]/(X-\alpha)^2$, pour tout scalaire $\alpha \in \mathbb{F}_p$.

(d) Seul $\mathbb{Z}/p^2\mathbb{Z}$ parmi les quatre anneaux trouvés est de caractéristique p^2, les trois autres étant de caractéristique p.

(e) On appelle *diviseur de zéro* dans l'anneau commutatif[26] R un élément *a non nul* tel qu'il existe $b \neq 0$ avec $ab = 0$. Un anneau *intègre* est un anneau commutatif sans diviseurs de zéro. Dans un tel anneau, le seul élément nilpotent est 0. Un anneau est dit *réduit* si 0 en est le seul élément nilpotent. Un produit de deux ou plusieurs corps fournit un exemple d'un anneau réduit mais non intègre. L'ensemble $\mathrm{Nil}(R)$ des éléments nilpotents de l'anneau *commutatif* R est un idéal de R, appelé *nilradical* de R. Notons maintenant $\mathrm{Div}_0(R)$ l'ensemble des diviseurs de zéro de R.

Si $R = \mathbb{Z}/n\mathbb{Z}$, avec $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$, le nilradical est l'idéal engendré par la classe de $p_1 \times p_2 \times \cdots \times p_k$, alors que $\mathrm{Div}_0(R)$ est l'ensemble des éléments non inversibles. Les deux ensembles coïncident si, et seulement si, l'anneau $R = \mathbb{Z}/n\mathbb{Z}$ est local, c'est-à-dire $n = p^\alpha$, avec p premier.

Les mêmes commentaires s'appliquent mutatis mutandis au cas de l'anneau quotient $\mathbb{K}[X]/\big(P(X)\big)$, où

$$P(X) = P_1(X)^{\alpha_1} \times P_2(X)^{\alpha_2} \times \cdots \times P_k(X)^{\alpha_k}$$

est la décomposition du polynôme P appartenant à l'anneau principal $\mathbb{K}[X]$ en facteurs irréductibles.

26. Dans le cadre non commutatif, on a, bien sûr, la notion de *diviseur de zéro à gauche*, *diviseur de zéro à droite* ou *diviseur de zéro bilatère*.
Dans le cas de $\mathrm{M}(n, \mathbb{K})$, les trois notions coïncident avec la non-inversibilité à gauche (ou à droite), une fois la matrice nulle écartée : si A est non inversible de rang $0 < r < n$, alors A est rg-équivalente à la matrice $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, c'est-à-dire $A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q^{-1}$, avec P et Q inversibles. La matrice $B = Q \begin{bmatrix} 0 & 0 \\ 0 & I_{n-r} \end{bmatrix} P^{-1}$ est non nulle et vérifie la double-égalité $AB = BA = 0$.

Dans l'anneau $R = \mathbb{F}_p[X]/(X^n)$, le nilradical est l'idéal maximal (X) et l'anneau-quotient $R/\mathrm{nil}(R)$ est isomorphe au corps $\mathbb{F}_p$: il y a par conséquent p^{n-1} éléments nilpotents [27]. On notera que lorsque $n = 2$, l'idéal engendré par (X) est égal au groupe additif engendré par X.

(f) Le théorème des restes chinois dévisse l'anneau $R = \mathbb{Z}/n\mathbb{Z}$ en un produit d'anneaux locaux ou l'algèbre $R = \mathbb{K}[X]/(P)$ en un produit d'algèbres locales. Cela rend plus aisé l'étude du groupe des éléments inversibles $R^\times$, du nilradical et de l'anneau de Boole $\mathrm{Idemp}(R)$ des éléments idempotents [28] de l'anneau commutatif R. Cela ne nous est pas d'une grande utilité ici, puisque nos deux anneaux $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{F}_p[X]/(X^2)$ sont locaux.

(g) Le groupe multiplicatif $(\mathbb{Z}/p^n\mathbb{Z})^\times$ $(n \geqslant 2)$ est un groupe de cardinal $\varphi(p^n) = p^n - p^{n-1}$, qui est cyclique si p est premier impair, et produit direct de $\mathbb{Z}/2\mathbb{Z}$ par un groupe cyclique, lequel est obligatoirement de cardinal 2^{n-2} si $p = 2$. (Voir les propositions II-5.2 et II-5.4, en pages 101 et 106.)

(h) Les éléments inversibles de l'anneau local $\mathbb{F}_p[X]/(X^2)$ sont, au vu de ce qui précède, les éléments de la forme $aX+b$, avec $b \neq 0$. Leur nombre est donc égal à $p(p-1)$. Or, si J_2 est la matrice $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ (de polynôme minimal X^2), l'anneau $\mathbb{F}_p[X]/(X^2)$ est isomorphe à l'anneau $\mathbb{F}_p[\mathrm{J}_2]$ des polynômes en J_2, c'est-à-dire l'anneau des matrices de la forme $\begin{bmatrix} b & a \\ 0 & b \end{bmatrix}$, avec $a, b \in \mathbb{F}_p$. Le groupe G des éléments inversibles de cet anneau est formé des matrices $\begin{bmatrix} b & a \\ 0 & b \end{bmatrix}$, avec $b \neq 0$.

27. La $\mathbb{F}_p$-algèbre $\mathbb{F}_p[X]/(P)$, où P est un polynôme de degré d, est de dimension d, ayant $(1, X, \ldots, X^{d-1})$ pour base. En effet, une division euclidienne par P montre que la famille est génératrice. Pour établir que la famille est libre on utilise qu'un multiple de P est ou bien nul, ou bien de degré supérieur ou égal à d. Par conséquent le cardinal de $\mathbb{F}_p[X]/(P)$ est p^d.

Les idéaux d'un quotient R/I sont de la forme J/I, où J est un idéal de l'anneau R contenant l'idéal I. Pour calculer le cardinal c de J/I on peut calculer le cardinal q du quotient $(R/I)/(J/I) \simeq R/J$. Pour un anneau fini R de cardinal r il ne reste plus qu'a écrire $c = \dfrac{r}{q}\cdot$

28. Un élément e d'un anneau R est dit *idempotent* s'il vérifie $e^2 = e$. Quand R est commutatif, l'ensemble des idempotents $\mathrm{Idemp}(R)$ est stable par produit et par l'opération Δ, où $e\Delta f = e + f - 2ef$, ce qui fait de $(\mathrm{Idemp}(R), \Delta, \cdot)$ un anneau de Boole, c'est-à-dire un anneau dans lequel tout élément est idempotent. Un tel anneau est de caractéristique 2 et est nécessairement commutatif. Il possède par conséquent une structure de $\mathbb{F}_2$-espace vectoriel. S'il est fini, il est donc de cardinal une puissance de 2.

On dispose de la suite exacte naturellement scindée

$$\begin{array}{ccccc} (\mathbb{Z}/p\mathbb{Z},+) & \hookrightarrow & (G,\cdot) & \twoheadrightarrow & (\mathbb{F}_p^\times,\cdot)\simeq(\mathbb{Z}/(p-1)\mathbb{Z},+) \\ & & \begin{bmatrix} b & a \\ 0 & b \end{bmatrix} & \mapsto & b\,. \end{array}$$

D'ailleurs, l'application $(\mathbb{Z}/p\mathbb{Z},+)\oplus(\mathbb{F}_p^\times,\cdot)\to(G,\cdot)$ qui associe au couple (c,d) la matrice $\begin{bmatrix} d & cd \\ 0 & d \end{bmatrix}$ de G est un isomorphisme.

(i) Les éléments idempotents d'un anneau local sont triviaux. En effet, si $e(1-e)=0$, l'un des facteurs est inversible [29] et l'autre, de ce fait, nul. Autrement dit, $e=0$ ou $e=1$.

Les anneaux de la liste, à l'exception de $\mathbb{F}_p\times\mathbb{F}_p$, sont locaux.

Les idempotents d'un produit d'anneaux $R=R_1\times R_2$ sont les couples $e=(e_1,e_2)$ tels que e_1 et e_2 soient idempotents.

Ces considérations permettent de remplir la ligne $|\mathrm{Idemp}(R)|$ du tableau ci-dessous.

(j) Cherchons l'ensemble $\mathscr{S}(R,+)$ des sous-groupes du groupe $(R,+)$. Le groupe $\mathbb{Z}/p^2\mathbb{Z}$ est cyclique de cardinal p^2. Ses sous-groupes sont en correspondance bijective avec les diviseurs de son cardinal. Il y en a donc 3, les deux triviaux et le sous-groupe engendré par $\bar{p}$.

Par ailleurs, les sous-groupes d'un p-groupe abélien élémentaire [30], de cardinal p^n, sont exactement les sous-espaces vectoriels du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$, et on se retrouve ainsi en terrain familier. Dans le cas $n=2$, on a, outre les deux sous-espaces triviaux, toutes les droites de $\mathbb{F}_p^2$, c'est-à-dire les $p+1$ points de la droite projective $\mathbb{P}_1(\mathbb{F}_p)$ (la droite projective est la réunion d'un point à l'infini et d'une droite affine).

(k) Les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ ne sont pas moins nombreux que les sous-groupes du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Les idéaux d'un corps sont en nombre de deux.

Les idéaux d'un produit de k corps sont en nombre de 2^k. En général, les idéaux d'une somme directe d'anneaux $R=\oplus_{i=1}^k R_i$ se décomposent bien (suivant la somme directe). Autrement dit, tout idéal $\mathfrak{I}$ de R est somme directe $\mathfrak{I}=\oplus_{i=1}^k(\mathfrak{I}\cap R_i)$. En effet, si l'on note e_i l'élément unité de R_i, on a $1=e_1+\cdots+e_k$, et si $x\in\mathfrak{I}$, $x=x\cdot 1=\sum_{i=1}^k x\cdot e_i$ et il est clair que $xe_i\in(\mathfrak{I}\cap R_i)$.

29. Si e et $1-e$ étaient tous deux non inversibles, leur somme serait non inversible, ce qui est évidemment faux.

30. On appelle ainsi les p-groupes abéliens annulés par p, c'est-à-dire les groupes abéliens somme directe d'un nombre fini de groupes $\mathbb{Z}/p\mathbb{Z}$.

Les idéaux d'un quotient $R/\mathfrak{I}$ sont en correspondance bijective avec les idéaux de R contenant $\mathfrak{I}$. Les idéaux de $\mathbb{F}_p[X]/(X^2)$ sont en correspondance avec les idéaux (de l'anneau principal $\mathbb{F}_p[X]$) contenant l'idéal (X^2), c'est-à-dire avec les trois diviseurs unitaires du polynôme X^2.

(l) Les notations habituelles $\mathrm{Idéaux}(R)$, $\mathrm{Princ}(R)$, $\mathrm{Spec}(R)$ et $\mathrm{Max}(R)$, que l'on voit apparaître dans le tableau *infra*, désignent respectivement l'ensemble des idéaux, des idéaux principaux, des idéaux premiers et des idéaux maximaux de l'anneau R. Le lecteur vérifiera sans peine la validité des lignes de ce tableau correspondant aux cardinaux de ces différents ensembles [31].

anneau R	$\mathbb{Z}/p^2\mathbb{Z}$	$\mathbb{F}_p\times\mathbb{F}_p$	$\mathbb{F}_p[X]/(X^2)$	$\mathbb{F}_{p^2}$
caractéristique	p^2	p	p	p
commutativité	oui	oui	oui	oui
intégrité	non	non	non	oui
$\lvert\mathrm{Div}_0(R)\rvert$	$p-1$	$2(p-1)$	$p-1$	0
$\lvert\mathrm{nil}(R)\rvert$	p	1	p	1
$R^\times$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/(p-1)\mathbb{Z}$	$\big(\mathbb{Z}/(p-1)\mathbb{Z}\big)^2$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/(p-1)\mathbb{Z}$	$\mathbb{Z}/(p^2-1)\mathbb{Z}$
$\lvert R^\times\rvert$	$p(p-1)$	$(p-1)^2$	$p(p-1)$	p^2-1
$\lvert\mathrm{Idemp}(R)\rvert$	2	4	2	2
$(R,+)$	$\mathbb{Z}/p^2\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$
$\lvert\mathscr{S}(R,+)\rvert$	3	$p+3$	$p+3$	$p+3$
$\mathrm{End}(R,+)$	$\mathbb{Z}/p^2\mathbb{Z}$	$\mathrm{M}(2,\mathbb{F}_p)$	$\mathrm{M}(2,\mathbb{F}_p)$	$\mathrm{M}(2,\mathbb{F}_p)$
$\mathrm{Aut}(R,+)$	$\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/(p-1)\mathbb{Z}$	$\mathrm{GL}(2,\mathbb{F}_p)$	$\mathrm{GL}(2,\mathbb{F}_p)$	$\mathrm{GL}(2,\mathbb{F}_p)$
$\lvert\mathrm{Idéaux}(R)\rvert$	3	4	3	2
$\lvert\mathrm{Princ}(R)\rvert$	3	4	3	2
$\lvert\mathrm{Spec}(R)\rvert$	1	2	1	1
$\lvert\mathrm{Max}(R)\rvert$	1	2	1	1

4.3. Commentaires

1. Il est frappant de constater qu'aucune ligne du tableau ci-dessus ne suffit à elle seule à distinguer ces quatre anneaux les uns des autres. On trouvera cependant un même trait, spécifique de chacune de ces

31. On notera au passage que les idéaux de nos trois premiers anneaux

$$\mathbb{Z}/p^2\mathbb{Z},\quad \mathbb{F}_p\times\mathbb{F}_p \quad\text{et}\quad \mathbb{F}_p[X]/(X^2)$$

sont tous principaux, mais nos anneaux ne le sont point, faute d'être intègres.

familles, en regardant pour chacun de ces anneaux R la catégorie des R-modules correspondante [32].

2. Un sous-produit de la discussion qui précède montre que tout anneau de cardinal p^2 est commutatif. Cela cesse d'être le cas à partir du cardinal p^3. L'exemple classique est celui de l'algèbre des matrices triangulaires supérieures $\mathscr{T}(2,\mathbb{F}_p) \subset \mathrm{M}(2,\mathbb{F}_p)$: les deux matrices $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ et $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ ne commutent pas, car toute matrice qui commute avec la seconde est, comme elle, diagonale.

5. L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Le groupe additif $\mathbb{Q}/\mathbb{Z}$ mérite toute l'attention qu'on lui témoigne communément. Pour en maîtriser les premières propriétés, il est souvent bon de l'observer tel quel ou dans sa version multiplicative comme le groupe $\mathbf{U}_\infty$ de toutes les racines de l'unité dans $\mathbb{C}$. L'une de ses vertus est de posséder pour chaque entier n une copie et une seule du groupe cyclique C_n de cardinal n. Cette copie est détectée dans la version multiplicative comme le sous-groupe $\mathbf{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}$. Sa version dans $\mathbb{Q}/\mathbb{Z}$ est le sous-groupe $\big(\mathbb{Z}\cdot\frac{1}{n}\big)/\mathbb{Z}$, où $\mathbb{Z}\cdot\frac{1}{n}$ est le sous-groupe de $(\mathbb{Q},+)$ engendré par $\frac{1}{n}$. La suite exacte courte

$$\begin{array}{ccccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}\cdot\dfrac{1}{n} & \twoheadrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & & \dfrac{k}{n} & \mapsto & \bar{k} \end{array}$$

réalise le groupe quotient $\big(\mathbb{Z}\cdot\frac{1}{n}\big)/\mathbb{Z}$ comme $\mathbb{Z}/n\mathbb{Z}$. Le graphe du treillis des sous-groupes de $\mathbf{U}_\infty$ est évidemment assez compliqué : si le nombre de « racines » émanant de $\mathbf{U}_n \subset \mathbf{U}_\infty$ est relativement facile, le nombre de « tiges » qui lui arrivent dessus est infini [33]. Des lianes infinies se détachent cependant dans ce paysage quelque peu inextricable : il s'agit des lianes correspondant aux divers sous-groupes $\mathbf{U}_{p^\infty}$, pour p décrivant l'ensemble $\mathscr{P}$ de tous les nombres premiers [34].

32. La catégorie des R_i-modules est en effet :
(a) celle des groupes abéliens annulés par p^2, pour $R_1 = \mathbb{Z}/p^2\mathbb{Z}$;
(b) celle des $\mathbb{F}_p$-espaces vectoriels munis d'une somme directe, pour $R_2 = \mathbb{F}_p \times \mathbb{F}_p$ (autrement dit des espaces vectoriels munis d'un projecteur) ;
(c) celle des $\mathbb{F}_p$-espaces vectoriels muni d'un endomorphisme nilpotent de carré nul, pour $R_3 = \mathbb{F}_p[X]/(X^2)$;
(d) celle, enfin, des $\mathbb{F}_{p^2}$-espaces vectoriels, pour $R_4 = \mathbb{F}_{p^2}$.

33. Les sous-groupes maximaux du groupe $\mathbb{Z}/n\mathbb{Z}$ sont en correspondance bijective avec les nombres premiers divisant n. De l'autre côté, le sous-groupe $\mathbf{U}_n$ est maximal dans tous les $\mathbf{U}_{pn}$, où p est un nombre premier quelconque.

34. Le sous-groupe $\mathbf{U}_{p^\infty}$ est la composante p-primaire de $\mathbf{U}_\infty$, c'est-à-dire
$$\mathbf{U}_{p^\infty} = \big\{x \in \mathbb{U}_\infty \mid \exists\, k \in \mathbb{N},\ x^{p^k} = 1\big\}.$$

Le groupe multiplicatif $\mathbf{U}_{p^\infty}$ a un treillis infini des plus simples :

$$\{1\} \subset \mathbf{U}_p \subset \mathbf{U}_{p^2} \subset \cdots \subset \mathbf{U}_{p^k} \subset \ldots, \tag{1}$$

liane qui aboutit en $\mathbf{U}_{p^\infty}$ lui-même [35]. Ce groupe est infini, alors que, remarquablement, tous ses sous-groupes propres sont finis ! Notons également que tous ses quotients non triviaux lui sont isomorphes :

$$\begin{array}{ccccc} \mathbf{U}_{p^k} & \hookrightarrow & \mathbf{U}_{p^\infty} & \twoheadrightarrow & \mathbf{U}_{p^\infty} \\ & & x & \mapsto & x^{p^k}, \end{array}$$

ce qui est prévisible au vu du treillis [36].

L'anneau $\mathbb{Z}_p$ des entiers p-adiques est présenté dans cet exercice comme l'anneau des endomorphismes [37] *du groupe abélien $\mathbf{U}_{p^\infty}$.*

Pour aller de l'avant, nous introduisons le vocable *élément-liane* pour parler d'une suite infinie $X = (x_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbf{U}_{p^\infty}$, telle que pour tout entier $k \geqslant 0$, $x_k \in \mathbf{U}_{p^k}$, et pour tout $k > 0$, $x_k^p = x_{k-1}$. Attention, les éléments-lianes ne sont pas des éléments de $\mathbf{U}_{p^\infty}$. On découvrira sous peu tout leur intérêt ; contentons-nous pour l'instant de la justification sommaire qui suit. L'accès aux endomorphismes d'un espace vectoriel E est facilité par l'introduction d'une base de E. Les éléments-lianes $X = (x_k)_{k\in\mathbb{N}}$ tels que $x_1 \neq 1$ rendront ici les mêmes services que rendent les bases d'un espace vectoriel [38]. Nous leur attribuerons le nom d'*éléments-lianes basiques*.

35. On se doit quand même de démontrer que tout sous-groupe propre de $\mathbf{U}_{p^\infty}$ est l'un des $\mathbf{U}_{p^k}$. Cela résulte de la constatation générale suivante : si $(X_n)_n \nearrow X$, autrement dit si l'ensemble X est réunion croissante d'une suite $(X_n)_{n\in\mathbb{N}}$ de parties $X_n \subset X$, alors une sous-réunion finie de ces parties est l'une d'elles, et une sous-réunion infinie est X tout entier. (On se sert ici du fait que tout partie infinie P de $\mathbb{N}$ est *cofinale*, c'est-à-dire que tout élément de $\mathbb{N}$ est dépassé par au moins un élément de P. Par exemple, l'ensemble dénombrable $\{0,1\} \times \mathbb{N}$, totalement ordonné par l'ordre lexicographique, ne vérifie pas cette propriété.) Or, tout sous-groupe H est réunion des sous-groupes engendrés par ses éléments, $H = \cup_{x\in H}\langle x\rangle = \cup_{x\in H}\mathbf{U}_{p^{v(x)}}$, où $v(x) = v_p\big(o(x)\big)$ est la valuation relativement au nombre premier p de l'ordre $o(x)$ de x. Le lecteur troublé dans les dédales de l'infini, pourra remplacer l'argument qui précède par le suivant. Si H est un sous-groupe strict et $x_0 \notin H$ alors $H \subset \langle x_0\rangle$. Soit, à cet effet, $x \in H$. Deux racines p^k-ièmes de l'unité sont toujours telles que l'une est puissance de l'autre, donc telles que l'une est contenue dans le sous-groupe engendré par l'autre. Comme $x_0 \notin \langle x\rangle$, c'est que $x \in \langle x_0\rangle$.

36. Se rappeler que le graphe du treillis du groupe G/H, quotient du groupe G par le sous-groupe distingué H, s'obtient en gommant dans le graphe du treillis de G tous les sous-groupes ne contenant pas H.

37. Cette approche inédite apparaîtra au spécialiste, qui ne connaît que trop les nombres p-adiques, comme un exercice de contorsion. Elle est pourtant en parfaite harmonie avec le sujet de ce chapitre. Le jeu consiste à faire découvrir au lecteur candide ces nombres — considérés naguère comme exotiques —, pour l'emmener ensuite, petit à petit, vers les présentations plus familières de cet objet truculent qu'est l'anneau $\mathbb{Z}_p$.

38. La condition $x_1 \neq 1$ revient à dire que x_1 est un générateur de $\mathbf{U}_p$, mais alors la condition $x_2^p = x_1 \neq 1$ fait de x_2 un générateur de $\mathbf{U}_{p^2}$ et il en est de même la condition $x_k^{p^{k-1}} = x_1 \neq 1$ qui fait de x_k un générateur de $\mathbf{U}_{p^k}$, car $x_k \in \mathbf{U}_{p^k} \setminus \mathbf{U}_{p^{k-1}}$.

5.1. Énoncé

1. *Déterminer le quotient du groupe multiplicatif* $\mathbb{C}^*$ *par* $\mathbf{U}_n$.
2. *Montrer avec le moins de savoir possible*[39] *qu'il n'y a pas d'épimorphisme du groupe abélien libre* $\mathbb{Z}^n$ *sur le groupe additif* $\mathbb{Q}/\mathbb{Z}$*, autrement dit que le groupe* $(\mathbb{Q}/\mathbb{Z}, +)$ *n'est pas de type fini.*
3. *Quelle est la version dans* $\mathbb{Q}/\mathbb{Z}$ *de l'inclusion* $\mathbf{U}_{p^\infty} \subset \mathbf{U}_\infty$ *?*
4. *Montrer que le groupe* $\mathbf{U}_{p^\infty}$ *est indécomposable, divisible et pas de type fini. De quelle façon l'endomorphisme* $x \mapsto x^p$ *du groupe* $\mathbf{U}_{p^\infty}$ *agit-il sur le treillis de ses sous-groupes ?*
5. *Déterminer l'anneau des endomorphismes du groupe abélien* $(\mathbf{U}_{p^\infty}, \cdot)$. *On pourra, à cet effet, privilégier un élément parmi tous les éléments-lianes basiques et examiner l'effet d'un endomorphisme sur chacune de ses composantes.*
6. *Déterminer le groupe des automorphismes du groupe* $\mathbf{U}_{p^\infty}$.

5.2. Corrigé

1. La suite exacte courte suivante donne la réponse :
$$\begin{array}{ccccc} \mathbf{U}_n & \hookrightarrow & \mathbb{C}^* & \twoheadrightarrow & \mathbb{C}^* \\ & & x & \mapsto & x^n. \end{array} \tag{2}$$
Le quotient $\mathbb{C}^*/\mathbf{U}_n$ est ainsi isomorphe à $\mathbb{C}^*$.
2. Nous allons montrer que tout sous-groupe de type fini H est strictement inclus dans $\mathbb{Q}/\mathbb{Z}$. En effet, soit $H = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_k$, où pour tout entier $i \in [\![1, k]\!]$, x_i est la classe dans $\mathbb{Q}/\mathbb{Z}$ du rationnel $\dfrac{m_i}{n_i}$; tous les éléments de H sont annulés par $N = n_1 \times n_2 \times \cdots \times n_k$, alors que la classe de $\dfrac{1}{N+1}$ dans $\mathbb{Q}/\mathbb{Z}$ ne l'est pas. L'inclusion $H \subset \mathbb{Q}/\mathbb{Z}$ est donc stricte.
3. Il s'agit de remonter en une suite exacte le sous-groupe $\mathbf{U}_{p^\infty}$ de $\mathbf{U}_\infty$:
$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] & \mathbb{Q} \arrow[r, two heads, "\varepsilon"] & \mathbf{U}_\infty \\ & & \mathbf{U}_{p^\infty}. \arrow[u, hook] \end{tikzcd}$$
Le sous-groupe préimage $\varepsilon^{-1}\big(\mathbf{U}_{p^\infty}\big)$ est formé des rationnels dont le multiple par p^n, pour un $n \in \mathbb{N}$, est dans $\mathbb{Z}$. Nous noterons $\mathbb{Z}\big[\frac{1}{p}\big]$ ce

39. Le résultat est immédiat si l'on fait appel au théorème de structure des groupes abéliens de type fini, cf. note en bas de la page 50.

sous-groupe [40] de sorte que

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] & \mathbb{Q} \arrow[r, two heads, "\varepsilon"] & \mathbf{U}_\infty \\ \mathbb{Z} \arrow[r, hook] & \mathbb{Z}[\frac{1}{p}] \arrow[r, two heads, "\varepsilon"] & \mathbf{U}_{p^\infty} \arrow[u, hook] \end{tikzcd}.$$

De la suite exacte qui aboutit ainsi en $\mathbf{U}_{p^\infty}$ on déduit que

$$\big(\mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}, +\big) \;\simeq\; \big(\mathbf{U}_{p^\infty}, \cdot\big).$$

Notons au passage que la version additive du treillis (1), rencontré en page 59, s'écrit :

$$\{0\} \subset \big(\mathbb{Z}\cdot\frac{1}{p}\big)/\mathbb{Z} \subset \big(\mathbb{Z}\cdot\frac{1}{p^2}\big)/\mathbb{Z} \subset \cdots \subset \big(\mathbb{Z}\cdot\frac{1}{p^n}\big)/\mathbb{Z} \subset \ldots \qquad (3)$$

4. Un coup d'œil furtif sur le treillis de $\mathbf{U}_{p^\infty}$ nous convainc qu'aucun sous-groupe non trivial n'admet de complément : le groupe abélien $(\mathbf{U}_{p^\infty}, \cdot)$ est donc indécomposable.
   Comme tout entier admet une factorisation en produit de nombres premiers, un groupe abélien $(G, +)$ qui vérifie $qG = G$, pour tout q premier, vérifiera $nG = G$, pour tout $n \in \mathbb{N}$. Or, la multiplication par un entier k, premier avec p, est un automorphisme dans tous les $\mathbb{Z}/p^i\mathbb{Z}$. Il s'ensuit que $x \mapsto x^k$ est un automorphisme de $\mathbf{U}_{p^\infty}$. Il nous reste, pour établir que $\mathbf{U}_{p^\infty}$ est divisible, à montrer que $\pi : x \mapsto x^p$ est un endomorphisme surjectif de $\mathbf{U}_{p^\infty}$. Regardons pour cela l'effet de cet endomorphisme sur le treillis des sous-groupes. On a :

$$\mathbf{U}_{p^n} \xrightarrow{\pi_n} \mathbf{U}_{p^{n-1}},$$

   où π_n est la restriction $\pi_{|\mathbf{U}_{p^n}}$ à $\mathbf{U}_{p^n}$. La liane infinie descend d'un cran, mais reste (pour notre bonheur et celui de Tarzan) infinie.
   Comme $(\mathbf{U}_{p^k})_k \nearrow \mathbf{U}_{p^\infty}$, tout sous-ensemble fini de $\mathbf{U}_{p^\infty}$ se retrouvera dans un des sous-groupes $\mathbf{U}_{p^k}$, et ne peut donc engendrer $\mathbf{U}_{p^\infty}$. Ce dernier n'est donc pas un groupe de type fini [41].

---

40. La notation $\mathbb{Z}[\frac{1}{p}]$ désigne habituellement l'anneau image directe de $\mathbb{Z}[X]$ par le morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Q}$, qui applique X sur $1/p$. Le noyau de ce morphisme s'avère égal à l'idéal $(pX-1)$, de sorte que le groupe $\big(\mathbb{Z}[\frac{1}{p}], +\big)$ est isomorphe au groupe additif sous-jacent à l'anneau quotient $\mathbb{Z}[X]/(pX-1)$. En tout cas, l'ensemble $\mathbb{Z}[\frac{1}{p}]$ est constitué des rationnels de la forme m/p^n, avec $m \in \mathbb{Z}$ et $n \in \mathbb{N}$. C'est donc aussi l'ensemble sous-jacent au localisé de $\mathbb{Z}$ par rapport à la partie multiplicative S engendrée par l'entier p. Par exemple, l'anneau $\mathbb{Z}[\frac{1}{10}]$ n'est autre que l'anneau des nombres décimaux (pour d'autres précisions, se téléporter à l'exemple 3 de la page 152).

41. Cela prouve aussi, mais de manière moins élémentaire que précédemment, que $\mathbb{Q}/\mathbb{Z}$ n'est pas type fini.

5. Un endomorphisme f de $\mathbf{U}_{p^\infty}$ doit en premier lieu commuter avec l'endomorphisme π. Par ailleurs, l'endomorphisme f laisse clairement stable chacun des sous-groupes de notre treillis et induit donc un endomorphisme sur $\mathbf{U}_{p^n}$, noté f_n. Le diagramme suivant éclaire notre perception de la situation :

$$\begin{tikzcd}
\{1\} \arrow[loop above, "f_0"] \arrow[loop below] & \mathbf{U}_p \arrow[l, bend right, "\pi_1"'] \arrow[loop above, "f_1"] \arrow[r, hook, bend right] & \mathbf{U}_{p^2} \arrow[l, bend right, "\pi_2"'] \arrow[loop above, "f_2"] \arrow[r, hook] & \cdots \arrow[r, hook] & \mathbf{U}_{p^{n-1}} \arrow[loop above, "f_{n-1}"] \arrow[r, hook, bend right] & \mathbf{U}_{p^n} \arrow[l, bend right, "\pi_n"'] \arrow[loop above, "f_n"] \arrow[r, hook] & \cdots \mathbf{U}_{p^\infty}, \arrow[loop above, "f"] \arrow[loop below, "\pi"]
\end{tikzcd}$$

où l'on a
$$\forall\, n\,, \quad \pi_n \circ f_n = f_{n-1} \circ \pi_n\,. \tag{4}$$

Or, nous connaissons les endomorphismes du groupe cyclique $\mathbf{U}_{p^n}$. Ils sont déterminés par l'image d'un générateur. Aussi allons-nous nous précipiter pour fixer en chacun des $\mathbf{U}_{p^n}$ un générateur, en prenant soin que ces générateurs restent compatibles avec les projections π_n. L'élément-liane

$$X_1 = \big(1, e^{2\mathrm{i}\pi/p}, e^{2\mathrm{i}\pi/p^2}, \dots, e^{2\mathrm{i}\pi/p^{n-1}}, e^{2\mathrm{i}\pi/p^n}, \dots\big),$$

qui est clairement basique, sera notre élément privilégié, et ses composantes vérifient, comme on s'y attend (cf. note (38) du bas de la page 59), la condition souhaitée. Un endomorphisme f de $\mathbf{U}_{p^\infty}$ est déterminé par les images des composantes de X_1, lesquelles à leur tour s'enchaînent pour définir un élément-liane, vu les relations de compatibilité (4), ci-dessus. On en conclut qu'une fois fixé l'élément-liane privilégié X_1, les endomorphismes du groupe abélien $\mathbf{U}_{p^\infty}$ s'identifient aux éléments-lianes qui se profilent le long du treillis des sous-groupes de $\mathbf{U}_{p^\infty}$. L'élément-liane X_1 correspond alors à l'endomorphisme identité et l'élément-liane

$$X_0 = \big(1, 1, 1, \dots, 1, 1, \dots\big),$$

à l'endomorphisme trivial.

Une fois les endomorphismes cernés, il s'agit maintenant de comprendre les lois de l'anneau qu'ils définissent. C'est l'occasion pour nous de constater combien il est inconfortable de décrire les lois de l'anneau des endomorphismes d'un groupe abélien $(G, \cdot)$ noté multiplicativement, car ici l'« addition » des endomorphismes f et g devrait se noter $f \cdot g$ (avec $(f \cdot g)(x) = f(x) \cdot g(x)$), et l'« opposé » de f s'appelant du même coup l'« inverse » ! Les automorphismes de G seront les éléments inversibles de l'anneau $\big(\mathrm{End}(G), \cdot, \circ\big)$ et auront deux « inverses »(un pour chacune des deux lois), rarement égaux[42], mais désignés et notés de

42. C'est le cas des anti-involutions, c'est-à-dire, quand le groupe est noté additivement, les endomorphismes tels que $f^2 + Id_G = 0$, ou encore $-f = f^{-1}$.

la même façon. Aussi, nous ne resterons pas longtemps dans ce cadre, mais avant de le déserter faisons-en une description sommaire.

Remarquons d'abord que l'élément-liane X_0 est l'endomorphisme « nul » et l'élément-liane X_1 est l'« unité », dont l'« opposé » est fourni par l'élément-liane $X_{-1} = \big(1, e^{-2i\pi/p}, e^{-2i\pi/p^2}, \dots, e^{-2i\pi/p^{n-1}}, e^{-2i\pi/p^n}, \dots\big)$. L'« addition » de deux éléments-lianes se fait en multipliant leurs composantes respectives dans $\mathbb{C}$. Quant à la multiplication, elle est aussi déplaisante à détailler que la structure de l'anneau $\mathrm{End}(\mathbf{U}_p)$ des endomorphismes du groupe des racines p-ièmes de l'unité [43], mais tout son secret se résume dans le fait que les différentes applications de passage à l'induit $\rho_k : f \mapsto f_k$ sont toutes des homomorphismes d'anneaux de $\mathrm{End}(\mathbf{U}_{p^\infty})$ dans $\mathrm{End}(\mathbf{U}_{p^k})$.

Voyons cela dans le cadre additif. On se reporte donc au treillis (3), en page 61. Les morphismes π_k deviennent ici les multiplications par p, soit

$$\pi_k(\overline{x_k}) = p \cdot \overline{x_k} = \overline{px_k},$$

et les éléments-lianes des chaînes $X = (\overline{x_k})_{k\in\mathbb{N}}$, où, pour tout $k \in \mathbb{N}$, on a $\overline{x_k} \in \big(\mathbb{Z} \cdot \dfrac{1}{p^k}\big)/\mathbb{Z}$, et $\pi_k(\overline{x_k}) = \overline{x_{k-1}}$. Les guillemets récurrents rencontrés plus haut n'ont plus de raison d'être, l'addition et la multiplication dans $\mathrm{End}\big(\mathbb{Z}\big[\dfrac{1}{p}\big]/\mathbb{Z}\big)$ sont, composante par composante, de vraies additions et multiplications de rationnels, modulo $\mathbb{Z}$. L'endomorphisme nul correspond à la liane constante $X_0 = (\bar{0}, \bar{0}, \dots)$ et l'endomorphisme unité à $X_1 = \Big(\bar{0}, \overline{\dfrac{1}{p}}, \overline{\dfrac{1}{p^2}}, \dots\Big)$, dont l'opposé est

$$X_{-1} = \Big(\bar{0}, \overline{-\frac{1}{p}}, \overline{-\frac{1}{p^2}}, \dots\Big) = \Big(\bar{0}, \overline{\frac{p-1}{p}}, \overline{\frac{p^2-1}{p^2}}, \dots\Big).$$

Cette version, déjà plus maniable, peut être encore allégée. Les sous-groupes $\big(\mathbb{Z} \cdot \dfrac{1}{p^k}\big)/\mathbb{Z}$ sont, après tout, de braves $\mathbb{Z}/p^k\mathbb{Z}$ et dans ce nouveau déguisement π_k devient $x \pmod{p^k} \mapsto x \pmod{p^{k-1}}$.

Ce que l'on perd au change est l'inévitable disparition des inclusions canoniques $\mathbf{U}_{p^{k-1}} \hookrightarrow \mathbf{U}_{p^k}$ et avec elles l'image mentale d'un élément-liane « inscrit » dans le treillis. Ce déguisement des éléments de l'anneau $\mathbb{Z}_p$ des entiers p-adiques est leur attirail le plus chic.

Un entier p-adique est donc une suite $X = (x_k)_{k\in\mathbb{N}}$, que l'on continuera à appeler élément-liane, avec $x_k \in \mathbb{Z}/p^k\mathbb{Z}$ et $\pi_k(x_k) = x_{k-1}$. L'ensemble

43. Prenons à titre d'exemple $p = 5$ et $\omega = e^{2i\pi/5} \in \mathbf{U}_5$. La composée de l'endomorphisme φ_2 défini par $\omega \mapsto \omega^2$ et de l'endomorphisme φ_3 défini par $\omega \mapsto \omega^3$ est φ_6 défini par $\omega \mapsto \omega^6$, de sorte que φ_2 et φ_3 sont inverses l'un de l'autre. La notation $\omega^2 \circ \omega^3 = \omega^6$ éclaire la situation.

de ces éléments-lianes est appelé dans la littérature *limite inverse* (ou *limite projective*) des ensembles $\mathbb{Z}/p^k\mathbb{Z}$, et noté $\varprojlim \mathbb{Z}/p^k\mathbb{Z}$. Dans ce contexte, $X_0 = (0, 0, \ldots)$, où les zéros successifs représentent les classes de 0 modulo les $\mathbb{Z}/p^k\mathbb{Z}$ et, attention, ne sont pas égaux les uns aux autres (une classe modulo p n'est pas égale à une classe modulo p^2). De même, on constate que l'élément unité est $X_1 = (0, 1, 1, \ldots)$, avec la même remarque concernant les 1 successifs et l'élément $X_{-1} = -X_1$ est égal à $(0, -1, -1, \ldots) = (0, p-1, p^2-1, \ldots)$.

Un élément-liane se présente en général comme une suite

$$X = (0, a, a + bp, a + bp + cp^2, \ldots),$$

avec $a, b, c, \ldots$ des entiers de $[\![0, p-1]\!]$. Dans cette écriture, la quatrième composante $a+bp+cp^2$, par exemple, doit être pensée comme une classe modulo p^3 dont le représentant est dans l'intervalle $[\![0, p^3-1]\!]$. On est alors trop tenté de remplacer cette suite par la suite des coefficients significatifs a, b, c, etc., suite représentée dans la littérature par la notation $abc\ldots$, ou bien par $\ldots cba$ ou encore par la « série »

$$a + bp + cp^2 + \ldots,$$

les additions et les multiplications se faisant alors comme d'habitude avec des retenues. On retrouve là une non moins célèbre écriture des nombres p-adiques, et peut-être même la plus commune, et que l'on appellera *écriture p-adique*.

Traitons un ou deux exemples de calcul avec $p = 3$. L'élément écrit sous la forme $X = \ldots 212121$ correspond à l'élément-liane (additif)

$$(0,1,1+2\cdot 3,1+2\cdot 3+1\cdot 3^2,1+2\cdot 3+1\cdot 3^2+2\cdot 3^3,\ldots)=(0,1,7,16,70,\ldots)_3.$$

L'opposé $-X$ de X correspond à l'élément-liane

$$(0, -1, -7, -16, -70, \ldots)_3 = (0, 2, 2, 11, 11, \ldots)_3 = \ldots 0102\,,$$

et plus précisément

$$-X = \ldots 01010102 = (0, 2, 2, 11, 11, 92, 92, 821, 821 \ldots)_3\,.$$

Expliquons notre démarche. Si $X = (0, \alpha, \beta, \gamma, \ldots)_p$ où $\alpha, \beta, \gamma, \ldots,$ vérifient $\alpha \in [\![0, p-1]\!]$, $\beta \in [\![0, p^2-1]\!]$, $\gamma \in [\![0, p^3-1]\!]$, $\ldots$, les divers coefficients $a, b, c, \ldots$ correspondants s'obtiennent à partir des égalités

$$a = \alpha, \quad a + bp = \beta, \quad a + bp + cp^2 = \gamma, \ \ldots,$$

d'où $b = \dfrac{\beta - \alpha}{p}$, $c = \dfrac{\gamma - \beta}{p^2}$, $\ldots$, et l'on a donc

$$X = (0, a, a + bp, a + bp + cp^2, \ldots) = \ldots cba.$$

L'élément s'avère inversible [44] et son inverse est

$$X^{-1}=(0,1,7^{-1},16^{-1},70^{-1},151^{-1},\ldots)_3=(0,1,4,22,22,103,\ldots)_3=\ldots 10211.$$

Ces chiffres ne sortent pas du chapeau du magicien. Que l'on trouve 22 pour inverse de 16 dans $\mathbb{Z}/3^3\mathbb{Z}$ est encore accessible à la main : on dresse pour cela la liste des éléments inversibles et on les réunit deux par deux, x à x^{-1}, après avoir noté que l'inverse de 1 est 1 et l'inverse de $26 = -1$ est encore lui-même. On prend soin de remplacer dans la liste ci-dessus les éléments 14, 16, 17, 19, 20, 22, 23 et 25 par les éléments -13, -11, -10, -8, -7, -5, -4 et -2. On unit facilement 2 et $14 = -13$ (donc aussi $-2 = 25$ et 13), 4 et 7 (donc $-4 = 23$ et $-7 = 20$), 5 et 11 (donc $-5 = 22$ et $-11 = 16$, ouf !). En revanche, il est plus ardu de détecter que l'inverse de 70 dans $\mathbb{Z}/3^4\mathbb{Z}$ est 22, et encore davantage que l'inverse de $151 = 70 + 1 \cdot 3^4$ est 103 dans $\mathbb{Z}/3^5\mathbb{Z}$. Pour les trouver nous mimons la multiplication avec retenue, supposée acquise avant l'entrée au collège [45] :

$$\begin{array}{cccccccc}
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
\times & \cdots & \star & \star & \star & 2 & 1 & 1 \\
\hline
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
 & \cdots & 1 & 2 & 1 & 2 & 1 & \\
 & \cdots & 2 & 0 & 1 & 2 & & \\
 & \cdots & \star & \star & \star & & & \\
 & \cdots & \star & \star & & & & \\
\hline
 & \cdots & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
\quad \rightsquigarrow \quad
\begin{array}{cccccccc}
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
\times & \cdots & \star & 1 & 0 & 2 & 1 & 1 \\
\hline
 & \cdots & 2 & 1 & 2 & 1 & 2 & 1 \\
 & \cdots & 1 & 2 & 1 & 2 & 1 & \\
 & \cdots & 2 & 0 & 1 & 2 & & \\
 & \cdots & 0 & 0 & 0 & & & \\
 & \cdots & 2 & 1 & & & & \\
\hline
 & \cdots & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

La première multiplication reproduit les inverses déjà trouvés (de 1 dans $\mathbb{Z}/3\mathbb{Z}$, de 7 dans $\mathbb{Z}/3^2\mathbb{Z}$ et de 16 dans $\mathbb{Z}/3^3\mathbb{Z}$), mais elle peut aider à les retrouver. La deuxième multiplication va plus loin, puisqu'elle nous permet, entre autres, de déterminer l'inverse de 70 dans $\mathbb{Z}/3^4\mathbb{Z}$ et de 151 dans $\mathbb{Z}/3^5\mathbb{Z}$. On obtient pour inverse de ce dernier

$$1 + 1 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 = 22 + 1 \cdot 3^4 = 103.$$

Quand le nombre premier est petit, comme dans le cas précédent (où l'on avait $p = 3$), une manière peut-être un peu plus rapide consiste à utiliser le caractère « liane » de l'inverse. Plus précisément, l'inverse de X s'écrit $(0, 1, 4, x_3, x_4, x_5, \ldots)$, avec trois possibilités pour x_3 (à savoir $x_3 = 4$ ou $x_3 = 4 + 1 \cdot 3^2$ ou $x_3 = 4 + 2 \cdot 3^2$) et trois possibilités pour x_4 une fois x_3 déterminé, et ainsi de suite. Cela nous donne à choisir pour inverse de 16 entre 4, 13 ou 22, et l'on vérifie que $x_3 = 22$ seul convient. Pour l'inverse de 70, on a à choisir entre 22, $22 + 1 \cdot 3^4$

44. Cf. question suivante. Le lecteur s'est sûrement rendu compte déjà que les automorphismes de $\mathbf{U}_{p^\infty}$ correspondent aux éléments-lianes basiques X (i.e. dont le terme $x_1 \neq 1$ en notation multiplicative, et $x_1 \neq 0$ en notation additive).

45. À ne pas confondre avec le "college" de nos amis d'outre-Manche.

ou $22+2\cdot 3^4$. On tombe aussitôt sur $x_4 = 22$. On fait de même avec 151 et l'on trouve $x_5 = 103$. Continuons au-delà pour trouver l'inverse de $151+2\cdot 3^5 = 637$ parmi 103, $103+1\cdot 3^5$ ou $103+2\cdot 3^5$. Là aussi, le premier essai est réussi : l'inverse de 637 dans l'anneau $\mathbb{Z}/3^6\mathbb{Z}$ est 103, puisque $637\cdot 103 = 3^6\cdot 90+1$. On deviendra, à l'issue de l'exercice suivant, encore plus familier avec les calculs dans l'anneau $\mathbb{Z}_p$.

Résumons maintenant la longue investigation qui précède. L'anneau des endomorphismes du groupe abélien $(\mathbf{U}_{p^\infty},\cdot)$ s'avère être pour l'initié l'anneau des entiers p-adiques, et pour le débutant une façon de découvrir ce dernier. Quant à nous, qui jouons les deux rôles à la fois, nous ferons en sorte, quand cela est intéressant, de donner d'une même propriété concernant les éléments de l'anneau $\mathbb{Z}_p$ les traductions possibles dans l'un ou l'autre de ses quatre accoutrements rencontrés plus haut : éléments-lianes dans le treillis de $(\mathbf{U}_{p^\infty},\cdot)$, éléments-lianes dans le treillis de $\big(\mathbb{Z}[\frac{1}{p}]/\mathbb{Z},+\big)$, éléments $(x_k)_k \in \varprojlim \mathbb{Z}/p^k\mathbb{Z}$ et enfin comme nombres en les deux écritures p-adiques $\ldots cba$ ou $a+bp+cp^2+\ldots$

6. Traitons en premier la version multiplicative $\mathbf{U}_{p^\infty}$. Si $X=(x_k)_k$ est un élément-liane basique dans le treillis de $\mathbf{U}_{p^\infty}$, alors pour tout k la composante x_k engendre le groupe multiplicatif $\mathbf{U}_{p^k}$, et cela a lieu si, et seulement si, x_1 engendre $\mathbf{U}_p$, c'est-à-dire $x_1\neq 1$. Un automorphisme de $\mathbf{U}_{p^\infty}$ est un endomorphisme bijectif : il envoie donc l'élément-liane privilégié X_1 sur un élément-liane basique[46], ce qui établit une correspondance bijective entre l'ensemble pointé en X_1 des éléments-lianes basiques et l'ensemble pointé sous-jacent au groupe $\big(\mathrm{Aut}(\mathbf{U}_{p^\infty}),\circ\big)$. Dans les versions additives, les automorphismes sont en correspondance bijective avec les éléments dont la composante $x_1=a$ est non nulle.

   Ce groupe est noté comme il se doit $\big(\mathrm{Aut}(\mathbf{U}_{p^\infty}),\circ\big)$ dans la version multiplicative ou $(\mathbb{Z}_p^\times,\cdot)$ dans les autres.

5.3. Commentaires

1. La suite exacte (2) en page 60 n'est pas scindable, puisque $\mathbb{C}^*$ n'a pas de sous-groupe d'indice fini >1. En effet, si $f:\mathbb{C}^*\twoheadrightarrow G$ est un morphisme surjectif à valeurs dans le groupe fini $(G,\cdot)$, de cardinal n, on a $f(z^n)=f(z)^n=e_G$ (d'après le théorème de Lagrange). Comme tout élément de $\mathbb{C}^*$ est une puissance n-ième, f est donc constant, et par conséquent $G=\{e_G\}$.

46. Autrement dit, le groupe $\big(\mathrm{Aut}(\mathbf{U}_{p^\infty}),\circ\big)$ agit simplement transitivement sur l'ensemble des éléments-lianes basiques, tout comme le groupe linéaire $\mathrm{GL}(E)$ agit simplement transitivement sur l'ensemble des bases de l'espace vectoriel E.

2. Pour $n \in \mathbb{Z}$, l'endomorphisme $z \mapsto z^n$ de $\mathbf{U}_{p^\infty}$ correspond à l'élément-liane X_n dont les composantes sont les puissances n-ièmes dans $\mathbb{C}$ des composantes de X_1. La caractéristique de l'anneau $\mathbb{Z}_p$ des entiers p-adiques, vu comme $\mathrm{End}(\mathbf{U}_{p^\infty})$, est bien nulle, puisque l'élément-liane X_n, pour $n \geqslant 1$, n'aura jamais toutes ses composantes égales à 1, même pour $n = p^k$ assez grand.

6. L'anneau $\mathbb{Z}_p$ revisité

6.1. Mise au point

Nous avons introduit l'anneau $\mathbb{Z}_p$ dans l'exercice précédent comme l'anneau des endomorphismes du groupe abélien $(\mathbf{U}_{p^\infty}, \cdot)$. Cette approche est cohérente avec le titre du présent chapitre, mais ne se prête pas systématiquement, comme on vient de le voir, aux calculs que l'on est amené à effectuer avec les nombes p-adiques.

Nous allons mettre en évidence quelques-unes des propriétés les plus immédiates de l'anneau $\mathbb{Z}_p$, notamment le fait que c'est un anneau intègre [47] et local. Rappelons que pour établir que l'anneau des polynômes à coefficients dans $\mathbb{Z}$ est intègre, le degré joue un rôle primordial ; pour établir l'intégrité de $\mathbb{Z}_p$ la notion fondamentale de *valuation p-adique* viendra nous porter secours.

Auparavant, arrêtons-nous devant quelques mystères, qui ne sont pas des mystères pour tout le monde, de l'écriture décimale d'un nombre entier, tel que 8352, par exemple. Tout le monde s'accorde que l'on y lit 2 comme chiffre des unités, 5 comme celui des dizaines, 3 celui des centaines et enfin 8 celui des milliers. Il y a déjà moins de monde qui reconnaisse les chiffres qui compose ce nombre comme des restes de division par 10. En effet,

$$\begin{aligned} 8352 &= 835 \cdot 10 + 2, & 835 &= 83 \cdot 10 + 5, \\ 83 &= 8 \cdot 10 + 3, & 8 &= 0 \cdot 10 + 8. \end{aligned}$$

Et peu de monde, sans doute, remarquerait qu'à ce nombre est associé l'élément-liane suivant

$$(0, 2, 52, 352, 8352, 8352, 8352, \ldots)_{10} \in \varprojlim \mathbb{Z}/10^k\mathbb{Z}.$$

47. Sous-entendre commutatif et sans diviseurs de zéro. On laisse le soin au lecteur de détecter le vrai moment où l'anneau $\mathbb{Z}_p$ lui est paru commutatif.

Cet élément-liane redonne les chiffres de l'écriture 8352 comme quotients :

$$\begin{aligned} 2 &= \frac{2-0}{10^0}\,, \\ 5 &= \frac{52-2}{10^1}\,, \\ 3 &= \frac{352-52}{10^2}\,, \\ 8 &= \frac{8352-352}{10^3}\,, \\ 0 &= \frac{8352-8352}{10^4}\,, \ldots \end{aligned}$$

Ces quelques remarques naïves s'adaptent littéralement au cas p-adique, avec p premier, et nous aideront à mieux passer d'une écriture à une autre d'un même élément de $\mathbb{Z}_p$.

Posons-nous pour finir cette introduction la question de savoir lequel des deux nombres 7992 ou 1952 est plus « proche » de notre 8352 ? Si l'on est sur la droite numérique, il n'y a pas de doute que c'est 7992, mais pour le joueur de tiercé, c'est 1952 qui remporte la mise [48]. Cette question servira à mieux comprendre l'écriture d'un nombre p-adique comme série formelle.

6.2. Énoncé

1. *Partant de l'écriture p-adique des éléments a et b de $\mathbb{Z}_p$ comme « séries formelles » $a = \sum_{k\geqslant 0} a_k p^k$ et $b = \sum_{k\geqslant 0} b_k p^k$, donner l'expression exacte des k-ièmes composantes de $a+b$ et $a\cdot b$ (on introduira avec bénéfice une suite de retenues et une suite de restes).*
2. *Expliquer comment $\mathbb{Z}$ se plonge dans $\mathbb{Z}_p$ et en déduire que la caractéristique de $\mathbb{Z}_p$ est nulle.*
3. *Que signifie l'intégrité de $\mathbb{Z}_p$ vu comme l'anneau des endomorphismes du groupe abélien $\mathbf{U}_{p^\infty}$? Si $a = \sum_{k\geqslant 0} a_k p^k$, on pose $v_p(a)$ le premier rang pour lequel a_k est non nul et l'on convient que la valuation de 0 est $+\infty$. Démontrer l'intégrité de $\mathbb{Z}_p$ en utilisant la valuation.*
4. *On note $\mathbb{Q}_p$ le corps des fractions de l'anneau intègre $\mathbb{Z}_p$. Montrer que, dans $\mathbb{Q}_p$, on a*
$$\mathbb{Q}\cap\mathbb{Z}_p = \mathbb{Z}_p^{per} = \mathbb{Z}_{(p)},$$
où $\mathbb{Z}_p^{per}$ est le sous-anneau de $\mathbb{Z}_p$ formé des entiers p-adiques ayant un développement périodique (sous-entendu, à partir d'un certain rang)

48. Mettons en garde le lecteur passionné de courses de ne pas pousser l'analogie plus loin.

et $\mathbb{Z}_{(p)}$ est le sous-anneau de $\mathbb{Q}$ formé des rationnels $\dfrac{a}{b}$ tels que $a \wedge b = 1$ et $p \wedge b = 1$. (Ce dernier anneau est le localisé de $\mathbb{Z}$ relativement à l'idéal premier $\mathfrak{p} = (p)$ engendré par p.)

5. *Montrer que l'anneau $\mathbb{Z}_p$ est un anneau local, et en déterminer le corps résiduel. Montrer que $\mathbb{Z}_p$ est principal.*
6. *Déterminer les carrés dans $\mathbb{Z}_p$. En déduire que $\mathbb{Z}_p$ ne peut pas être muni d'une relation d'ordre qui en fasse un* anneau ordonné.

6.3. Corrigé

1. Nous allons définir deux suites $(r_k)_{k\in\mathbb{N}}$ et $(q_k)_{k\in\mathbb{N}}$, pas après pas, à partir des divisions euclidiennes successives ci-après :

$$\begin{aligned} a_0 + b_0 &= q_0 p + r_0 \\ a_1 + b_1 + q_0 &= q_1 p + r_1 \\ a_2 + b_2 + q_1 &= q_2 p + r_2, \ \ldots, \end{aligned}$$

où les $r_k \in [\![0, p-1]\!]$ définissent la suite des restes, et les $q_k \geqslant 0$ la suite des retenues. Nous affirmons que la somme $a + b$ admet pour écriture p-adique en série

$$a + b = \sum_{k\geqslant 0} a_k p^k + \sum_{k\geqslant 0} b_k p^k = \sum_{k\geqslant 0} r_k p^k.$$

ll s'agit donc de prouver que les composantes des éléments-lianes correspondant dans $\varprojlim \mathbb{Z}/p^k\mathbb{Z}$ sont les mêmes, c'est-à-dire prouver que

$$\forall N \in \mathbb{N}, \quad \sum_{k=0}^{N} a_k p^k + \sum_{k=0}^{N} b_k p^k \ = \ \sum_{k=0}^{N} r_k p^k \quad \big(\bmod p^{N+1}\big).$$

Il n'y a pas récurrence sous roche, mais plutôt un calcul direct :

$$\begin{aligned} \sum_{k=0}^{N}(a_k + b_k)p^k - \sum_{k=0}^{N} r_k p^k &= \sum_{k=0}^{N}(a_k + b_k - r_k)p^k \\ &= a_0 + b_0 - r_0 + \sum_{k=1}^{N}(q_k p - q_{k-1})p^k \\ &= q_0 p + \sum_{k=1}^{N} q_k p^{k+1} - \sum_{k=1}^{N} q_{k-1} p^k \\ &= q_0 p + \sum_{k=1}^{N} q_k p^{k+1} - \sum_{k=0}^{N-1} q_k p^{k+1} \\ &= q_0 p + q_N p^{N+1} - q_0 p \\ &= 0 \quad \big(\bmod p^{N+1}\big). \end{aligned}$$

Afin de multiplier a par b, nous allons procéder de manière analogue, en définissant deux nouvelles suites, une suite de restes et une autre de retenues, $(R_k)_{k\in\mathbb{N}}$ et $(Q_k)_{k\in\mathbb{N}}$, à partir des divisions euclidiennes suivantes :

$$\begin{aligned} a_0\cdot b_0 &= Q_0p+R_0\\ a_0\cdot b_1+a_1\cdot b_0+Q_0 &= Q_1p+R_1\\ a_0\cdot b_2+a_1\cdot b_1+a_2\cdot b_0+Q_1 &= Q_2p+R_2\\ &\cdots, \end{aligned}$$

avec $R_k\in[\![0,p-1]\!]$ et $Q_k\geqslant 0$.
De nouveau, nous affirmons que le produit $a\cdot b$ admet pour écriture p-adique en série

$$a\cdot b=\Big(\sum_{k\geqslant 0}a_kp^k\Big)\cdot\Big(\sum_{k\geqslant 0}b_kp^k\Big)=\sum_{k\geqslant 0}R_kp^k,$$

ce qui revient à démontrer que

$$\forall N\in\mathbb{N},\quad \sum_{k=0}^{N}\Big(\sum_{i=0}^{k}a_ib_{k-i}\Big)p^k \;=\; \sum_{k=0}^{N}R_kp^k \pmod{p^{N+1}},$$

pour les mêmes raisons qu'auparavant. Un calcul similaire s'applique :

$$\begin{aligned} \sum_{k=0}^{N}\Big(\Big(\sum_{i=0}^{k}a_ib_{k-i}\Big)-R_k\Big)p^k &= a_0\cdot b_0-r_0+\sum_{k=1}^{N}(Q_kp-Q_{k-1})p^k\\ &= Q_0p+\sum_{k=1}^{N}Q_kp^{k+1}-\sum_{k=1}^{N}Q_{k-1}p^k\\ &= Q_0p+\sum_{k=1}^{N}Q_kp^{k+1}-\sum_{k=0}^{N-1}Q_kp^{k+1}\\ &= Q_0p+Q_Np^{N+1}-Q_0p\\ &= 0 \pmod{p^{N+1}}. \end{aligned}$$

Ces formules doivent être accompagnées de « travaux pratiques », et ne sauraient suffire pour une bonne maîtrise des règles de calcul (tout comme à l'école primaire).
Retrouvons ainsi l'opposé -1 de 1. On a clairement

$$-1=p-1+(p-1)p+(p-1)p^2+\ldots,$$

et l'exemple de $p=5$, où $-1=\cdots 44444=(0,4,24,124,624,1249,\ldots)_5$ rend cette écriture encore plus manifeste :

$$\begin{array}{cccccc} & \cdots & 0 & 0 & 0 & 0 & 1\\ + & \cdots & 4 & 4 & 4 & 4 & 4\\ \hline & \cdots & 0 & 0 & 0 & 0 & 0 \end{array}$$

L'autre manière (mécanique) de procéder serait d'écrire

$$\begin{aligned}
-1 &= -(0,1,1,1,1,,\ldots)_p \\
&= (0,-1,-1,-1,-1,\ldots)_p \\
&= (0,p-1,p^2-1,p^3-1,p^4-1,\ldots)_p \\
&= \frac{p-1}{p^0} + \frac{(p^2-1)-(p-1)}{p^1}p + \frac{(p^3-1)-(p^2-1)}{p^2}p^2 + \ldots \\
&= p-1+(p-1)p+(p-1)p^2+\ldots
\end{aligned}$$

Le lecteur vérifiera, en utilisant les deux manières fournies, que si $p=3$, alors $-21 = \ldots 22202$, et que si $p=5$, alors $\ldots 333341$ est l'opposé de $\ldots 111104$ et $\ldots 44440322$ est l'opposé du nombre entier $\ldots 00004123$. Tout cela pour dire que pour p premier quelconque, les entiers négatifs auront une écriture p-adique infinie [49] et avec une période de longueur 1, où figure $p-1$.

Quel est maintenant l'entier dont l'écriture 5-adique est $\ldots 000444444$ (obtenue en ne gardant que les six premiers [50] chiffres du développement 5-adique de -1) ? La réponse est

$$4(1+5+5^2+5^3+5^4+5^5) = 4\frac{5^6-1}{5-1} = 5^6-1.$$

Plus généralement, si l'on ne garde que les k premiers chiffres du développement p-adique de -1, on tombe sur l'entier p^k-1, dont on déduit aussitôt l'écriture en base p. L'écriture p-adique de l'entier négatif $1-p^k$ en découle : dans l'exemple ci-dessus, on a $1-5^6 = \ldots 444000001$, et l'on peut donc, dans le cas général, écrire [51]

$$1-p^k = \ldots (p-1)(p-1)00\ldots 001,$$

où figurent $k-1$ zéros entre le terme périodique $p-1$ et le premier chiffre 1. L'inverse de ce nombre se calcule aisément à partir de l'identité remarquable

$$\frac{1}{1-p^k} = 1+p^k+p^{2k}+p^{3k}+\ldots = \cdots 00100\cdots 00100\cdots 001, \qquad (5)$$

49. Le désarroi face aux nombres négatifs n'est-il pas davantage justifié ici que l'angoisse des Anciens face à ces « quantités plus petites que rien », et qui leur semblaient le « comble de l'aberration humaine » ?

50. Les chiffres étant comptés de droite à gauche.

51. Les parenthèses qui apparaissent dans l'écriture que l'on donne de $1-p^k$ sont fictives. Elles servent juste comme délimitateurs : dans la pratique, on attribue p symboles aux nombres allant de 0 à $p-1$.
Par exemple, si $p=13$, on pourra prendre : 0, 1, …, 9, A, B et C.

que l'on peut traduire pour notre contexte par

$$\begin{aligned}(1-p^k)\cdot(1+p^k+p^{2k}+p^{3k}+\dots) &= 1+p^k+p^{2k}+p^{3k}+p^{4k}+\cdots \\ &\qquad -p^k\cdot(1+p^k+p^{2k}+p^{3k}+\dots) \\ &= 1+p^k\cdot(1+p^k+p^{2k}+p^{3k}+\dots) \\ &\qquad -p^k\cdot(1+p^k+p^{2k}+p^{3k}+\dots) \\ &= 1\,,\end{aligned}$$

l'égalité $p^k + p^{2k} + p^{3k} + p^{4k} + \dots = p^k \cdot (1 + p^k + p^{2k} + p^{3k} + \dots)$ résultant de la règle de calcul du produit de deux nombres p-adiques écrits sous forme de séries. Le produit $p^k \cdot (1+p^k+p^{2k}+p^{3k}+\dots)$ est égal aussi à la somme p^k fois de $1+p^k+p^{2k}+p^{3k}+\dots$, cf. la note de bas de page 407.

2. Soit $n \in \mathbb{N}$. Déterminons l'écriture p-adique de

$$n \cdot 1 = \underbrace{1+1+\cdots+1}_{n \text{ fois}}\,, \tag{6}$$

où 1 est l'élément unité de l'anneau $\mathbb{Z}_p$. Nos règles de calcul montrent facilement que $n \cdot 1 = \dots 00 r_k r_{k-1} \dots r_1 r_0$, où la suite de restes $(r_k)_k$ est obtenue à partir des divisions euclidiennes

$$\begin{aligned} n &= q_0 \cdot p + r_0, \\ q_0 &= q_1 \cdot p + r_1, \\ q_1 &= q_2 \cdot p + r_2, \\ &\dots \end{aligned}$$

Bien sûr, $\forall k$, $r_k \in [\![0, p-1]\!]$ et $q_k \geqslant 0$. Nous venons d'effectuer l'algorithme de l'écriture de l'entier n en base p, comme l'on s'y attendait [52].

Dire que $n \cdot 1 = 0$, où 0 est le zéro de l'anneau $\mathbb{Z}_p$, revient à dire que n est nul dans $\mathbb{N}$. La caractéristique de l'anneau $\mathbb{Z}_p$ est donc nulle [53]. Le lecteur a déjà compris sur les exemples que les entiers strictement négatifs exigent un petit effort, et sont exactement ceux dont l'écriture p-adique est périodique de période 1 faisant intervenir le symbole correspondant à $p-1$. S'il en souhaite la preuve formelle, la voici.

Prenons un nombre p-adique z dont l'écriture en série est celle annoncée.

52. Lorsque $n = p^k$, nous obtenons que $p^k \cdot 1$ est la série p^k, ce qui justifie en particulier la notation apparaissant dans (6).
53. Ce que l'on savait déjà, depuis les commentaires en page 67.

On a

$$\begin{aligned} z &= \dots(p-1)(p-1)z_{k-1}z_{k-2}\dots z_1z_0 \\ &= z_0 + z_1p + \dots + z_{k-1}p^{k-1} + (p-1)p^k + (p-1)p^{k+1} + \dots \\ &= x + (p-1)p^k(1+p+p^2+\dots) \\ &= x + (p-1)p^k\frac{1}{1-p} \\ &= x - p^k, \end{aligned}$$

où la « partie pré-période » [54] $x = z_0+z_1p+\dots+z_{k-1}p^{k-1}$ sera montrée inférieure à p^k et où l'on a utilisé le développement p-adique de $\dfrac{1}{1-p}$ déjà explicité. Puisque pour tout $i \in [\![0, k-1]\!]$ on a $z_i \leqslant p-1$, on en déduit que $x \leqslant (p-1)(1+p+p^2+\dots+p^{k-1}) = p^k - 1 < p^k$, ce qui implique de suite que z représente un entier strictement négatif. Réciproquement, si z est un entier strictement négatif, soit p^k une puissance [55] de p telle que $p^k \geqslant -z = |z|$. Alors, si l'on note $x = z+p^k \in \mathbb{N}$, on a $x < p^k$, et donc l'écriture en base p de x admet au maximum k chiffres (éventuellement nuls) : $x = z_0 + z_1p + \dots + z_{k-1}p^{k-1}$. On en déduit aussitôt l'écriture p-adique de z :

$$\begin{aligned} z &= x - p^k \\ &= x + (p-1)p^k\frac{1}{1-p} \\ &= x + (p-1)p^k(1+p+p^2+\dots) \\ &= z_0 + z_1p + \dots + z_{k-1}p^{k-1} + (p-1)p^k + (p-1)p^{k+1} + \dots \\ &= \dots(p-1)(p-1)z_{k-1}z_{k-2}\dots z_1z_0\,, \end{aligned}$$

qui est bien de la forme annoncée.

3. L'énoncé suggère de commencer par regarder l'endomorphisme composé de deux endomorphismes de $\mathbf{U}_{p^\infty}$, c'est-à-dire d'examiner l'intégrité au niveau des éléments-lianes. Autant aller aussitôt à $\varprojlim \mathbb{Z}/p^k\mathbb{Z}$, où les calculs sont relativement faciles. Pour avoir un soupçon de ce qui se passe, effectuons le produit des deux éléments-lianes x et y non nuls suivants,

54. Il n'est pas indispensable de prendre exactement pour x la pré-période de z, car on comprend dans la suite que z_{k-1} peut être égal à $p-1$. Le processus de la pensée tend tout de même vers une certaine économie.

55. Si l'on veut récupérer tout de suite le morceau pré-période de z, il vaut mieux considérer ici la plus petite puissance k-ième de p vérifiant $p^k \geqslant -z$.

$$\begin{aligned} x &= (0,0,p^2,p^2+p^3,p^2+p^3+p^4,\dots)_p \\ &= \dots 11100 \\ y &= (0,0,0,p^3,p^3+p^4,\dots)_p \\ &= \dots 11000 \end{aligned}$$

que l'on écrit dans $\varprojlim \mathbb{Z}/p^k\mathbb{Z}$, où le produit se fait composante par composante :

	$\mathbb{Z}/p\mathbb{Z}$	$\leftarrow$	$\mathbb{Z}/p^2\mathbb{Z}$	$\leftarrow$	$\mathbb{Z}/p^3\mathbb{Z}$	$\leftarrow$	$\mathbb{Z}/p^4\mathbb{Z}$	$\leftarrow$	$\mathbb{Z}/p^5\mathbb{Z}$	$\leftarrow$	$\mathbb{Z}/p^6\mathbb{Z}$	$\cdots$
x	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	p^2	$\leftarrow\!\shortmid$	p^2+p^3	$\leftarrow\!\shortmid$	$p^2+p^3+p^4$	$\leftarrow\!\shortmid$	$p^2+p^3+p^4+p^5$	$\cdots$
y	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	p^3	$\leftarrow\!\shortmid$	p^3+p^4	$\leftarrow\!\shortmid$	$p^3+p^4+p^5$	$\cdots$
$x\cdot y$	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	0	$\leftarrow\!\shortmid$	p^5	$\cdots$

Il importe de relever que les quatrième et cinquième composantes de $x\cdot y$ sont nulles, alors que x_4, x_5, y_4 et y_5 ne le sont pas. En revanche, les composantes $(x\cdot y)_k$ sont toutes non nulles à partir de $k=6$. L'idée maîtresse se révèle dans l'écriture p-adique et s'incarne, comme suggéré par l'énoncé, dans la valuation p-adique.
On a $x = p^2(1+p+\dots)$ (donc $v_p(x)=2$) et $y = p^3(1+p+\dots)$ $\big($et donc $v_p(y)=3\big)$, d'où $x\cdot y = p^5(1+\dots)\neq 0$, avec $v_p(x\cdot y) = 5 = 2+3$.
En toute généralité, la valuation p-adique d'un produit $x\cdot y$ est la somme des valuations p-adiques respectives de x et de y :

$$v_p(x\cdot y) = v_p(x) + v_p(y).$$

Ainsi, le produit de deux éléments non nuls est non nul.

4. Regardons l'entier 3-adique $r = \dots 202020$ dont l'écriture présente la période 20 de longueur 2. On a

$$\begin{aligned} r &= 0 + 2\cdot 3 + 0\cdot 3^2 + 2\cdot 3^3 + \dots \\ &= 2\cdot 3(1+3^2+3^4+3^6+\dots) \\ &= 6\times\frac{1}{(1-3^2)} = \frac{6}{-8} = -\frac{3}{4} \in \mathbb{Q}\,, \end{aligned}$$

ce qui se vérifie en écrivant

$$\begin{aligned} -4r &= (-1)\cdot(\dots 00011)\cdot r \\ &= (\dots 22222)\cdot(\dots 00011)\cdot r \\ &= (\dots 22212)\cdot(\dots 202020) = \dots 000010 = 3\ . \end{aligned}$$

Adoptons à ce stade une convention utile dans l'écriture des nombres p-adiques périodiques, en enveloppant la période [56] entre crochets. L'élé-

56. On devrait parler plutôt de « la » période, tant que l'on n'a pas défini soigneusement la notion de période. Cela alourdirait notre propos et n'apporterait aucun bénéfice pour la suite.

ment r s'écrit alors $r = [20]$, et l'élément $1 + r = \ldots 202021 = [02]1$. Noter que r s'écrit aussi $r = [02]0$.

Passons maintenant à la démonstration, en établissant les quatre inclusions suivantes : $\mathbb{Z}_p^{per} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q} \cap \mathbb{Z}_p \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p^{per}$.

(a) *L'inclusion* $\mathbb{Z}_p^{per} \subseteq \mathbb{Z}_{(p)}$. Un élément $z \in \mathbb{Z}_p$ dont l'écriture p-adique présente une périodicité s'écrit [57]

$$\begin{aligned} z &= [y_l \ldots y_1] z_k \ldots z_0 \\ &= z_0 + z_1 p + \cdots + z_k p^k + p^{k+1}(y_1 + y_2 p + \cdots + y_l p^{l-1})(1 + p^l + p^{2l} + \ldots) \\ &= x + y p^{k+1} \frac{1}{1-p^l} \in \mathbb{Z}_{(p)} \ , \end{aligned}$$

où x et y sont, respectivement, les entiers $z_0 + z_1 p + \cdots + z_k p^k$ et $y_1 + y_2 p + \cdots + y_l p^{l-1}$.

Par convention, si l'élément z ne présente à priori pas de partie pré-période $x = z_k \ldots z_0$, on va lui en attribuer une de force, comme dans le cas $z = [4] = [4]4$, de façon à ce que x ne soit jamais nul.

(b) *L'inclusion* $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. On aura besoin pour cela du résultat préliminaire suivant : *si $b \in \mathbb{N}^*$ est premier avec p, alors il existe $n \in \mathbb{N}^*$ tel que $b \mid p^n - 1$.* En effet, $\bar{p}$ est, vu l'hypothèse, inversible dans l'anneau $\mathbb{Z}/b\mathbb{Z}$, et appartient donc au groupe $(\mathbb{Z}/b\mathbb{Z})^\times$, qui est de cardinal $\varphi(b)$; il s'ensuit que $p^{\varphi(b)} = 1 \pmod b$, ou encore $b \mid p^n - 1$ avec $n = \varphi(b)$.

Soit maintenant $\dfrac{a}{b} \in \mathbb{Z}_{(p)}$, tel que $a \wedge b = 1$, $p \wedge b = 1$, et $b \in \mathbb{N}^*$. D'après l'assertion ci-dessus, il existe $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que

$$\frac{a}{b} = \frac{ma}{p^n - 1} = -ma \frac{1}{1 - p^n} = -ma(1 + p^n + \ldots) \in \mathbb{Z}_p \, .$$

(c) *L'inclusion* $\mathbb{Q} \cap \mathbb{Z}_p \subseteq \mathbb{Z}_{(p)}$. Si $\dfrac{a}{b} \in \mathbb{Z}_p$, avec $a \wedge b = 1$. Si $p \wedge b = 1$, c'est fait, et si par l'absurde $p \mid b$, c'est que $a \in \mathbb{Z}_p$ est inversible, si bien que $a^{-1} \dfrac{a}{b} = \dfrac{1}{b} \in \mathbb{Z}_p$, soit b inversible, d'où contradiction.

(d) *L'inclusion* $\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p^{per}$. Nous allons procéder comme nous l'avons fait pour l'inclusion $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$, en écrivant un élément $\dfrac{a}{b} \in \mathbb{Z}_{(p)}$ (tel que $a \wedge b = 1$, $p \wedge b = 1$, et $b \in \mathbb{N}^*$) sous la forme

$$\frac{a}{b} = \frac{ma}{p^n - 1} = -ma \frac{1}{1 - p^n} = -ma(1 + p^n + p^{2n} + \ldots) \, ,$$

pour $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ (dont l'existence a été déjà prouvée). Puisque $1 + p^n + p^{2n} + \ldots \in \mathbb{Z}_p^{per}$, il reste à prouver que la somme

57. Cf. l'identité remarquable (5), en page 71.

de deux éléments de $\mathbb{Z}_p^{per}$ est périodique (ce que nous laisserons aux bons soins du lecteur), et que l'opposé d'un élément de $\mathbb{Z}_p^{per}$ est périodique.

Pour ce qui concerne l'opposé, écrivons, comme pour la preuve de l'inclusion $\mathbb{Z}_p^{per} \subset \mathbb{Z}_{(p)}$, la forme générale d'un élément $z \in \mathbb{Z}_p^{per}$:

$$\begin{aligned} z &= [y_l \ldots y_1] z_k \ldots z_0 \\ &= z_0 + z_1 p + \cdots + z_k p^k + p^{k+1}(y_1 + y_2 p + \cdots + y_l p^{l-1})(1 + p^l + p^{2l} + \ldots) \\ &= x + y p^{k+1} \frac{1}{1-p^l} \in \mathbb{Z}_{(p)}, \end{aligned}$$

avec les mêmes conventions quant aux entiers naturels x et y. Alors,

$$-z \;=\; -x - y p^{k+1} \frac{1}{1-p^l} \;=\; X + Y p^{k+1} \frac{1}{1-p^l}\,,$$

avec $X = p^{k+1} - x$ et $Y = p^l - 1 - y$. Comme $0 < x < p^{k+1}$, on a bien $0 < X < p^{k+1}$, si bien que X admet une écriture en base p d'au plus $k+1$ chiffres : $X = Z_0 + Z_1 p + \cdots + Z_k p^k$ et constitue la future pré-période de $-z$.

De même, $0 \leqslant y \leqslant p^l - 1$, d'où $0 \leqslant Y \leqslant p^l - 1$, et Y admet une écriture en base p d'au plus l chiffres : $Y = Y_1 + Y_2 p + \cdots + Y_l p^{l-1}$ et constitue la future « partie périodique » de $-z$. Cela prouve bien que $-z \in \mathbb{Z}_p^{per}$.

5. Le groupe $\mathbb{Z}_p^\times$ est formé des éléments de valuation nulle. Son complémentaire dans $\mathbb{Z}_p$ est $p\mathbb{Z}_p$, l'unique idéal maximal, noyau de la projection naturelle $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$, si bien que le corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p$ est isomorphe au corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

   On fait comme pour $\mathbb{K}[[X]]$, et l'on montre que tout idéal de $\mathbb{Z}_p$ est de la forme $p^k\mathbb{Z}_p$, pour $k \in \mathbb{N}$.

6. La solution de cette question est laissée au lecteur.

7. Deux problèmes pour finir

7.1. Les groupes divisibles

1. *Montrer que le groupe additif $G = \mathbb{Z}^{(\mathbb{Z})}$ est isomorphe à $G \times G$ et de même $H = \mathbb{Z}/2\mathbb{Z}^{(\mathbb{Z})}$ est isomorphe à $H \times H$.*

2. *Montrer que les groupes $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont isomorphes.*

   Réponse.– On montre avec l'axiome du choix que $\mathbb{R}$ et $\mathbb{C}$ sont des $\mathbb{Q}$-espaces vectoriels isomorphes, car ayant des bases de même cardinal, de sorte que leurs groupes additifs sous-jacents sont aussi isomorphes.

3. *Quels sont les sous-groupes maximaux du groupe additif $\mathbb{Q}$? Montrer en fait que $\mathbb{Q}$ n'a pas de sous-groupe maximal, car il est divisible.*

Réponse.–

▷ Supposons qu'il existe H sous-groupe maximal. Alors, le groupe quotient $\mathbb{Q}/H$ ne peut avoir de sous-groupe non trivial, c'est donc un $\mathbb{Z}/p\mathbb{Z}$, avec p premier.

Il s'ensuit que $p\,\mathbb{Q} \subseteq H$. Mais, $p\,\mathbb{Q} = \mathbb{Q}$, car $\mathbb{Q}$ est divisible. On vient d'établir que $H = \mathbb{Q}$, d'où contradiction.

▷ Une variante consiste à démontrer que H est lui aussi divisible et qu'il contient 1 : il est donc égal à $\mathbb{Q}$. Soit à cet effet $H \leqslant \mathbb{Q}$ un sous-groupe maximal.

a) On remarque d'abord que H est divisible : si $h \in H$, $n \geqslant 1$ et si $\frac{1}{n}h \notin H$, alors $\langle H, \frac{1}{n}h\rangle$ est un sous-groupe propre de $\mathbb{Q}$ (puisque si $\frac{1}{n^2}h \in \langle H, \frac{1}{n}h\rangle$, alors $\frac{1}{n}h \in \langle H, h\rangle = H$) contenant strictement H, une contradiction. (Un sous-groupe maximal d'un groupe divisible est lui aussi divisible.)

b) Ensuite, $1 \in H$: si $\frac{m}{n} \in H$ (avec $m \neq 0$), alors $m = n\frac{m}{n} \in H$ puis $1 = \frac{1}{m}m \in H$ puisque H est divisible.

c) On en déduit que $H = \mathbb{Q}$: si $\frac{m}{n} \in \mathbb{Q}\backslash\{0\}$, alors $m = m \cdot 1 \in H$ puis par divisibilité $\frac{m}{n} = \frac{1}{n}m \in H$.

Remarque.– Nous allons examiner la réciproque. Mais, auparavant, montrons que si $(G, +)$ est divisible, alors G est infini.

Voici le bon argument. Si G est fini, il existe n tel que $nG = \{0\}$, où l'on peut prendre pour n, par exemple, le cardinal de G. Mais, par divisibilité, $nG = G$; il s'ensuit que G est trivial. On vient de démontrer qu'*un groupe divisible est ou bien infini ou bien est le groupe trivial.*

Ensuite, on montre sans peine que si G est divisible selon tout p premier, il est divisible selon tout n.

Maintenant, montrons que si $(G, +)$ n'a pas de sous-groupes maximaux, c'est qu'il est divisible.

Procédons par l'absurde. Si $x \mapsto px$ n'est pas surjective pour un certain p premier, alors le quotient G/pG est non réduit à $\{0\}$, mais il est par ailleurs annulé par p, c'est donc un $\mathbb{F}_p$-espace vectoriel non nul. Il admet donc (axiome du choix) un hyperplan, soit $\overline{H}$. L'image réciproque H de $\overline{H}$ par $\pi : G \to G/pG$ est un sous-groupe maximal de G puisque l'on a

$$G/H \simeq (G/pG)/(H/pG) = (G/pG)/\overline{H} \simeq \mathbb{Z}/p\mathbb{Z}.$$

4. *Soit G un groupe tel que* $\mathrm{D}(G)/\mathrm{D}\big(\mathrm{D}(G)\big)$ *et* $\mathrm{D}\big(\mathrm{D}(G)\big)$ *sont cycliques. Alors,* $\mathrm{D}(G)$ *est cyclique !*
5. *Montrer que le groupe* $(\mathbb{Q}/\mathbb{Z},+)$ *ne peut être le groupe additif sous-jacent à un quelconque anneau*[58].

   Réponse.– Si tel est le cas, notons tout simplement « $\cdot$ » la loi produit et désignons par e l'élément unité d'un tel anneau, que nous supposerons égal à $\mathbb{Q}/\mathbb{Z}$, pour ne pas ajouter encore une notation de plus. Appelons n l'ordre de e comme élément du groupe additif $\mathbb{Q}/\mathbb{Z}$. Comme ce groupe est divisible, il existe $x \in \mathbb{Q}/\mathbb{Z}$ tel que $e = nx$. On écrit alors

   $$e{=}e{\cdot}e{=}(nx)e{=}(x{+}\cdots{+}x)e{=}xe{+}xe{+}\cdots{+}xe{=}x(e{+}\cdots{+}e){=}x(ne){=}x{\cdot}0{=}0.$$

   Mais, si $e = 0$, tout z de $\mathbb{Q}/\mathbb{Z}$ serait nul aussi, car $z = z \cdot e = z \cdot 0 = 0$, et cela est absurde.

7.2. L'anneau des endomorphismes du groupe $G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

On invite le lecteur à reprendre l'exercice traité dans le texte (voir page 40). En particulier, il établira que l'anneau $\mathrm{End}(G)$ est d'ordre 64 et que son groupe des unités, qui est $\mathrm{Aut}(G)$, est d'ordre 16.

On indique dans la suite comment démontrer que *ce groupe d'automorphismes est isomorphe au produit direct* $\mathcal{D}_4 \times C_2$.

En effet, ce groupe d'automorphismes est *non commutatif* (pourquoi ?) ; en le plaçant au milieu d'une suite exacte *scindable* ayant à gauche un sous-groupe $(\mathbb{Z}/2\mathbb{Z})^3$, on constatera qu'il est isomorphe à un produit semi-direct externe $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/2\mathbb{Z}$ non trivial. Comme les éléments d'ordre 2 de $\mathrm{Aut}\big((\mathbb{Z}/2\mathbb{Z})^3\big) = \mathrm{GL}(3,\mathbb{F}_2)$ sont tous conjugués[59], le groupe $\mathrm{Aut}(G)$ est isomorphe à $\mathcal{D}_4 \times C_2$, ce dernier étant lui-même aussi, par ailleurs, un produit semi-direct interne $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/2\mathbb{Z}$ non trivial[60].

Indications.–

1. Commencer par dessiner le treillis de notre groupe G, en y plaçant de plus les éléments (le voir par exemple dans le treillis apparaissant en page 108).
2. Un endomorphisme de ce groupe s'apparente à une matrice 2×2 de la forme $M = \begin{bmatrix} a & 4b \\ c & d \end{bmatrix}$, où a et b sont des classes modulo 8, et c et d

58. Plus simplement, on ne peut faire de $\mathbb{Q}/\mathbb{Z}$ un anneau.

59. À la matrice $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, par exemple.

60. Le groupe $\mathcal{D}_4 \times C_2$ contient un (et même deux) C_2^3 manifestes, forcément distingués, et contient en outre onze éléments d'ordre 2. (Voir la sous-section XI-30.2 ou la section XII-14.)

des classes modulo 2. La composition des endomorphismes se traduit au niveau de nos matrices par le produit, que nous effectuons, tête baissée, comme si leurs coefficients appartenaient à un même anneau.

3. Les endomorphismes laissent stable le sous-groupe cyclique H d'ordre 4 de G donné par l'image $\mathrm{Im}(x \mapsto 2x)$ de l'endomorphisme $x \mapsto 2x$ (avec lequel ils commutent) [61].
4. Il en découle [62] un morphisme d'anneaux $\mu : \mathrm{End}(G) \to \mathrm{End}(G/H)$, dont le noyau s'avère être formé d'éléments nilpotents, au nombre de huit [63], et l'image s'avère coïncider avec l'anneau des matrices triangulaires inférieures de $\mathrm{M}(2, \mathbb{F}_2)$.
5. On applique alors le lemme en page 46, et l'on finit en usant gracieusement des propos figurant avant la présente liste d'indications.

Commentaire.– Il est remarquable de constater que, tout comme le produit direct $C_8 \times C_2$, les deux produits semi-directs $C_8 \rtimes_{x \mapsto 3x} C_2$ et $C_8 \rtimes_{x \mapsto 5x} C_2$ ont eux aussi $\mathcal{D}_4 \times C_2$ pour groupe d'automorphismes [64]. En revanche, le groupe des automorphismes du groupe diédral $\mathcal{D}_8 \simeq C_8 \rtimes_{x \mapsto -x} C_2$ est plus compliqué (voir [12], page 523).

61. Comme $G/H \simeq C_2 \times C_2$, cela permet de repérer H dans le treillis de G.
62. C'est peut-être ici l'occasion de relever qu'un morphisme entre deux groupes abéliens n'induit pas en général un morphisme au niveau de leurs algèbres d'endomorphismes $\big($i.e. la correspondance $A \rightsquigarrow \mathrm{End}(A)$ n'est pas fonctorielle…$\big)$.
63. Que l'on prendra le soin d'énumérer.
64. Le groupe $C_8 \rtimes_{x \mapsto 3x} C_2$ est le modèle des 2-Sylow de $\mathrm{GL}(2, \mathbb{F}_3)$… Voir plus loin dans le livre, notamment la sous-section II-7.12, en page 124 et suivantes.

Bibliographie

[1] Arnaudiès Jean-Marie et José Bertin, ? ?XXX, Ellipses.

[2] Arnaudiès Jean-Marie et Delezoïde Pierre, Nombres (2,3)-constructibles, Advances in Mathematics, 158, 2001.

[3] Atiyah Michael and MacDonald Irving, *Introduction to Commutative Algebra*, (Addison-Wesley 1969).

[4] Berhuy Grégory, *Modules : théorie et pratique..., et un peu d'arithmétique*, (deuxième édition, Calvage & Mounet, 2020).

[5] Berhuy Grégory, *Algèbre : le grand combat*, (deuxième édition, Calvage & Mounet, 2020 ? ? ?).

[6] Bordellès Olivier and Bordellès Véronique, *Arithmetic Tales,* (Springer Universitext, 2012).

[7] Caldero Philippe et Germoni Jérôme *nouvelles histoires ? ? 1*, (Calvage & Mounet, 20 ? ?).

[8] Caldero Philippe et Germoni Jérôme, *Histoires hédonistes de groupes et de géométries*, Tome second, (Calvage & Mounet, 2015).

[9] Chambert-Loir Antoine, *A Field Guide to Algebra*, (Springer 2010)

[10] Cox David, Galois Theory, (Wiley 2012).

[11] Curtis Charles and Reiner Irving, *Methods of Representation Theory : With Applications to Finite Groups and Orders*, (John Wiley & Sons, 1987).

[12] Debreil Alain, *Groupes et treillis de leurs sous-groupes*, (Calvage & Mounet, 2016).

[13] Debreil Alain et Mneimné Rached, *Le groupe symétrique* $\mathfrak{S}_4$ *et ses métamorphoses*, (Calvage & Mounet, 2020).

[14] Debreil Alain et Mneimné Rached, *Le groupe unimodulaire* $\mathrm{SL}(2,\mathbb{Z})$ *chez les groupes finis*, (à paraître chez Calvage & Mounet).

[15] Diaz-Toca Gema-Maria, Lombardi Henri et Quitté Claude *LaTeX Modules sur les anneaux commutatifs*, (Calvage & Mounet, 2014).

[16] Diller Antoni, *LaTeX Line by Line : Tips and Techniques for Document Processing,* (New York : J. Wiley, 1993).

[17] Eiden Jean-Denis, *Espaces vectoriels euclidiens, avec une ouverture vers les espaces préhilbertiens réels* (Calvage & Mounet, 2020).

[18] Goossens Michel, *The LaTeX Companion,* (New York : Addison, 1994).

[19] Gurari Eitan, *TeX and LaTeX : Drawing and Literate Programming,* (New York : McGraw-Hill, 1994).

[20] Hernandez David et Laszlo, Yves. ? ? ?

[21] Hindry Marc, *Arithmétique,* (Calvage & Mounet, 2008).

[22] Kopka Helmut, *A Guide to LaTeX : Document Preparation for Beginners and Advanced Users,* (New York : Addison-Wesley Pub. Co., 1993).

[23] Kouris Éric, *Une année de colles en MPSI,* (Calvage & Mounet, 2018). ? ? ?

[24] Lamport Leslie, *LaTeX : a Document Preparation System : User's Guide and Reference Manual,* (New York : Addison-Wesley Pub. Co., 1994).

[25] Lang Serge, *Algebra,* (GTM 211, Springer, 2002).

[26] Mansuy Roger et Mneimné Rached, *Algèbre linéaire. Réduction des endomorphismes,* (deuxième édition, Vuibert, 20 ? ?).

[27] Mneimné Rached, *Éléments de géométrie. Actions de Groupes,* (Cassini, 1997).

[28] Mneimné Rached, *Réduction des endomorphismes,* (Calvage & Mounet, 2007).

[29] Mneimné Rached et Frédéric Testard *Introduction à la théorie des groupes de Lie classiques* (Hermann, 2006).

[30] Naudin Pierre et Quitté Claude, *Algorithmique algébrique, avec exercices corrigés,* (Elsevier, Masson 1997).

[31] Neumann Peter, Stoy Gabrielle et Edward Thompson, *Groups and Geometry,* (Oxford University Press, 1988).

[32] Perrin Daniel, *Algèbre, ENS,* (Ellipses, ? ?).

[33] Perrin-Riou Bernadette, *Algèbre, arithmétique et Maple,* (Cassini, 2000).

[34] Roman Steven, *Field Theory*, Springer 2005.

[35] Rotman Joseph J., *Advanced Modern Algebra,* (AMS, 2010).

[36] Samuel Pierre *Théorie algébrique des nombres,* (Hermann, ? ? ?XX).

[37] Skandalis Georges, *Agrégation interne.– Algèbre générale, algèbre linéaire et un peu de géométrie*, Calvage & Mounet 2019.

[38] Shultis J. Kenneth, *LaTeX Notes : Practical Tips for Preparing Technical Documents,* (New York : PTR Prentice Hall, 1994).

[39] Sternberg Shlomo, *Group Theory and Physics* (Cambridge University Press, 1994).

[40] Tauvel Patrice, *Corps commutatifs et théorie de Galois*, (Calvage & Mounet 2021).

[41] Testard Frédéric, *Analyse mathématique. La maîtrise de l'implicite*, (Calvage & Mounet ? ?).

Index

Abélianisé, 575
action
  de groupe, 25
  simplement transitive, 27, 28
  transitive, 27
anneau
  d'endomorphismes, 39, 40, 47, 50, 51, 59, 60, 66, 68, 78
  de Dedekind, 249
  factoriel, 32
  intégralement clos, 237
artinien
  module, 144, 148, 149, 305

base adaptée, 232

cône nilpotent, 378
cœur, 355, 367, 368, 379
centralisateur, 26
classe de conjugaison, 26
Commutateur, 575
corps
  de nombres, 223
corps cubique, 248
corps cyclotomique, 247
cyclique
  groupe, 39, 41, 55, 58, 62, 78, 79

degré
  d'une extension, 223
divisible (groupe), 49

entier algébrique, 235
équivariant
  voir G-équivariante, 25, 26, 52, 357, 366, 378, 379, 385, 564, 590, 591, 597

factoriel (anneau), 32
fleur des 2-Sylow
  de SL(2, Z/4Z), 582
Frattini (sous-groupe de), 496, 525

G-équivariante, 25, 26, 52, 357, 366, 378, 379, 385, 564, 590, 591, 597
G-ensemble, 25
G-équivariante (application), 26
G-homogène (espace), 26
G-orbite d'un élément, 25
Groupe
  dérivé, 575
groupe
  abélien de type fini, 31, 227
  abélien libre de type fini, 31, 226
  agissant sur un ensemble, 25
  cyclique, 39, 41, 55, 58, 62, 78, 79, 429
  monogène, 41, 43

habitant, 85
holomorphe (d'un groupe), 29, 112

idéal, 32, 57, 61, 84, 97, 99, 100, 133, 134, 146, 150, 223, 232, 236, 242, 320
  éployé, 158
  à droite, 138, 139, 405–407, 409, 413, 414
  à gauche, 138–140, 142, 400, 409, 416
  à roite, 400
  annulateur, 163
  bilatère, 23, 46, 50, 141, 400
  idéal, 224
  maximal, 50, 53, 55, 76, 93, 101, 106, 132, 134, 135, 138, 139, 142–144, 154, 160, 165, 281, 301, 411
  minimal, 118, 119, 161
  monogène, 406
  premier, 69, 93, 119, 130, 133–135, 143, 151, 157, 158, 160, 164, 246, 251, 266, 274, 279

principal, 152, 165, 175, 236, 239, 257, 264, 268, 270, 271, 328, 337, 339, 349, 446
produit, 132, 232, 263
idéaux étrangers, 132, 232

liane, 58–67, 73, 102, 150, 463, 465
localisé, 281

module
artinien, 144, 148, 149, 305
injectif, 49, 50
monoïde, 268
monogène
groupe, 41, 43
morphisme
de G-ensembles, 25
mou (élément), 22
multiplicité
algébrique, 34, 131, 340, 369
géométrique, 34, 130, 340
minimale, 34, 340

nœthérien, 249
nilespace, 355, 357, 358, 366, 368, 369, 379
nilpotent
cône, 378
élément, 46, 54, 79
endomorphisme, 40, 42, 58, 79
matrice, 42
nilradical (ou radical nilpotent), 93
normalisateur, 27
norme, 237
norme d'un idéal, 263

orbite
d'un élément, 25

plongements d'un corps de nombres, 242
Polynôme cyclotomique, 486
Polynôme primitif, 491
Polynôme symétrique complet, 210
produit semi-direct, 29, 78, 79, 109, 115, 116, 124, 125, 496, 499, 504, 505, 508, 511, 517, 518, 538, 539, 553, 558–560, 568–570, 572, 622, 630
projecteur, 140

résidu quadratique, 233
racine (émanant), 28
Racine primitive, 491
radical
nilpotent, 93
représentation
de Steinitz associée, 373

section (ensembliste ou morphique), 20, 21, 226
simplement transitive (action), 27
singleton, 20
socle, 93
sous-espace
caractéristique, 34, 131, 141, 304, 307, 338, 340, 341, 355, 358, 371
propre, 34, 122, 340, 377, 444
sous-groupe
distingué, 26, 27
stabilisateur
d'un élément, 25–28
d'un sous-groupe, 26
Steinitz (représentation de), 373
super-primitif (élément), 423
symbole de Legendre, 233

tautologique (action), 25
théorème
de la base adaptée, 11, 31, 34, 91–93, 226, 232, 293
de la bijection équivariante, 26
des restes chinois, 44, 54, 55, 89, 93, 96, 101, 132, 146, 174, 232, 274, 302, 340, 432, 505, 607
tige (émanant), 28
torsion, 30, 31, 49, 50, 82, 83, 97, 226, 231, 256, 327, 328, 341, 478, 606

trace, 237
transitive (action), 27
transporteur, 27, 28, 382, 457, 459
treillis
de $\mathfrak{A}_4$, 177, 500
de $\mathfrak{A}_4 \times C_2$, 558
de $\mathfrak{A}_5$, 532
de C_{12}, 500
de $C_{12} \times C_2$, 178, 179
de $C_{15} \rtimes_u C_4$, 539, 540
de C_{24}, 504
de $C_4 \times C_2$, 176
de $C_6 \times C_2$, 177, 500
de $C_6 \times C_4$, 178, 179
de C_8, 176
de $C_8 \rtimes_3 C_2$, 126
de $C_8 \times C_2$, 510
de $\mathcal{D}_6$, 500
de $\mathcal{D}_{10}$, 503
de $\mathcal{D}_3 \times C_4$, 502
de $\mathcal{D}_4$, 177
de $\mathcal{D}_4 \times C_2$, 544
de $\mathcal{D}_4 \times C_3$, 564
de $\widetilde{\mathcal{D}_5}$, 503
de $\widetilde{\mathcal{D}_6}$, 506
de Dic_{15}, 541
de $\mathbf{F}_{20}$, 503
de F9, 114
de $\mathrm{H}(3, \mathbb{F}_3)$, 568
de $\mathbb{H}_8$, 177
de $\mathbb{H}_8 \times C_2$, 526
de $\mathbb{H}_8 \times C_3$, 505
de $\widetilde{\mathfrak{S}_3}$, 500
de $\widetilde{\widetilde{\mathfrak{S}_3}}$, 506
de $\mathfrak{S}_3 \times \mathfrak{S}_3$, 704, 710
de $\mathfrak{S}_4$, 650, 651
de $\mathrm{SL}(2, \mathbb{F}_3)$, 505, 517
de $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 510
partiel de $C_2 \times C_2 \times C_2$, 451

unité, 259
fondamentale, 259

valuation –adique, 281

Weyr (théorème, 35, 336

Imprimé en Belgique sur les presses de SNEL Grafics, à Liège
Dépôt légal Septembre 2021