Sous la direction de Jean-Pierre Ramis et André Warusfel
Xavier Buff · Emmanuel Halberstadt · François Moulin · Monique Ramis · Jacques Sauloy

Mathématiques

Tout-en-un pour la Licence 2

4e édition

DUNOD

Jean-Pierre Ramis, ancien élève de l'École Normale Supérieure de la rue d'Ulm, membre de l'Institut (Académie des Sciences), membre de l'Institut Universitaire de France, membre de l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse, professeur émérite à l'Institut de Mathématiques de Toulouse (Université Paul Sabatier), a été directeur de l'Institut de Recherches Mathématiques Avancées de Strasbourg et de l'Institut de Mathématiques de Toulouse.

André Warusfel, ancien élève de l'École Normale Supérieure de la rue d'Ulm, a été professeur de mathématiques spéciales au Lycée Louis-le-Grand à Paris et inspecteur général de Mathématiques.

Xavier Buff, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur à l'Institut de Mathématiques de Toulouse, ancien directeur de l'Institut de Recherches sur l'Enseignement des Mathématiques de Toulouse.

Emmanuel Halberstadt, a été maître de conférences à l'Université Paris 6 Pierre et Marie Curie, ancien chargé de cours d'agrégation aux Écoles Normales Supérieures d'Ulm et de Cachan.

François Moulin, ancien élève de l'École Normale Supérieure de la rue d'Ulm, professeur de chaires supérieures au Lycée sainte-Geneviève (spéciales MP*).

Monique Ramis, ancienne élève de l'École Normale Supérieure de Sèvres, a été professeur de chaires supérieures (à Paris, Strasbourg, Toulouse).

Jacques Sauloy, ancien élève de l'École Normale Supérieure de Saint-Cloud, a été maître de conférences à l'Institut de Mathématiques de Toulouse.

Les éditions Dunod remercient Jean-Marie Monier, professeur de mathématiques en classes préparatoires au lycée La Martinière-Monplaisir (Lyon), pour sa relecture attentive de l'ouvrage.

© Dunod, Paris, 2007, 2014, 2020 , 2023
ISBN 978-2-10-085947-4
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

Préface

Les mathématiques constituent l'ossature de la science moderne et sont une source intarissable de concepts nouveaux d'une efficacité incroyable pour la compréhension de la réalité matérielle qui nous entoure. Ainsi l'apprentissage des mathématiques est devenu indispensable pour la compréhension du monde par la science. Les nouveaux concepts eux-mêmes sont le résultat d'un long processus de distillation dans l'alambic de la pensée. Essayer de justifier les mathématiques par leurs applications pratiques n'a guère de sens, tant ce processus de création est sous-tendu par la soif de connaître et non l'intérêt immédiat.
Les mathématiques restent l'un des domaines dans lequel la France excelle et ceci malgré la mutilation des programmes dans le secondaire et l'influence néfaste d'un pédagogisme dont l'effet principal est de compliquer les choses simples.
Vues de loin les mathématiques apparaissent comme la réunion de sujets distincts comme la géométrie, qui a pour objet la compréhension du concept d'espace, l'algèbre, art de manipuler les symboles, l'analyse, science de l'infini et du continu, la théorie des nombres etc. Cette division ne rend pas justice à l'un des traits essentiels des mathématiques qui est leur unité profonde de sorte qu'il est impossible d'en isoler une partie sans la priver de son essence. En ce sens les mathématiques ressemblent à un être biologique qui ne peut survivre que comme un tout et serait condamné à périr si on le découpait en morceaux en oubliant son unité fondamentale.
L'une des caractéristiques de l'apprentissage des mathématiques, c'est la possibilité donnée à tout étudiant de devenir son propre maître et en ce sens il n'y a pas d'autorité en mathématiques. Seules la preuve et la rigueur y font la loi. L'étudiant peut atteindre par le travail une maîtrise suffisante pour pouvoir s'il le faut tenir tête au maître. La rigueur, c'est être sûr de soi, et à l'âge où l'on construit sa personnalité, se confronter au monde mathématique est le moyen le plus sûr de construire sur un terrain solide. Il faut, si l'on veut avancer, respecter un équilibre entre les connaissances qui sont indispensables et le « savoir-faire » qui l'est autant. On apprend les maths en faisant des exercices, en apprenant à calculer sans l'aide de l'ordinateur, en se posant des questions et en ne lâchant pas prise facilement devant la difficulté. Seule la confrontation réelle à la difficulté a une valeur formatrice, en rupture avec ce pédagogisme qui complique les choses simples et mélange l'abstraction mathématique avec le jeu qui n'a vraiment rien à voir. Non, les mathématiques ne sont pas un jeu et l'on n'apprend pas les mathématiques en s'amusant.
L'ouvrage qui suit est un cours soigné et complet idéal pour apprendre toutes les Mathématiques qui sont indispensables au niveau de la Licence. Il regorge d'exercices (700) qui

incitent le lecteur à réfléchir et ne sont pas de simples applications de recettes, et respecte parfaitement l'équilibre nécessaire entre connaissances et savoir-faire, permettant à l'étudiant de construire des images mentales allant bien au-delà de simples connaissances mémorisées. Il s'agit d'un ouvrage de référence pour la Licence, non seulement pour les étudiants en mathématiques mais aussi pour tous ceux qui s'orientent vers d'autres disciplines scientifiques. Il insiste sur la rigueur et la précision et va au fond des notions fondamentales les plus importantes sans mollir devant la difficulté et en respectant constamment l'unité des mathématiques qui interdit tout cloisonnement artificiel. Il répond à une demande de tant de nos collègues d'un ouvrage qui les aide à « redresser la barre », mais sera aussi un atout merveilleux pour l'étudiant travaillant seul par la cohérence et la richesse de son contenu.
Il est l'œuvre d'une équipe qui rassemble des mathématiciens de tout premier plan ayant une véritable passion pour l'enseignement. Il était grand temps !

Alain Connes,
Médaille Fields 1982,
Professeur au Collège de France.

Table des matières

Préface iii

Avant-propos xiii

I Algèbre

I.1 Compléments d'algèbre 3

1 Quotients . . . 3
1.1 Quotient d'un ensemble par une relation d'équivalence . . . 3
1.2 Passage au quotient d'une loi de composition interne . . . 6
1.3 Groupes quotients . . . 9
1.4 Anneaux quotients . . . 14
1.5 Espaces vectoriels quotients . . . 16
2 Anneaux commutatifs . . . 18
2.1 Idéaux . . . 18
2.2 Polynômes sur un anneau commutatif . . . 22
3 Algèbres sur un corps commutatif . . . 26
4 Séries formelles . . . 30
4.1 La K-algèbre des séries formelles . . . 31
4.2 Convergence dans le corps $K((X))$ . . . 39

I.2 Actions de groupes 57

1 Généralités . . . 58
1.1 Définitions et exemples . . . 58
1.2 Espaces affines et actions de groupes . . . 62
2 Orbites, stabilisateurs . . . 65
2.1 Orbites . . . 65
2.2 Points fixes, stabilisateur . . . 69
2.3 Classes modulo un sous-groupe . . . 72
3 Quelques applications des actions de groupes . . . 75
3.1 Problèmes de classification . . . 75
3.2 Groupes de symétries . . . 76
3.3 Applications au groupe symétrique . . . 79
3.4 Applications aux groupes finis . . . 83
3.5 Une application à la combinatoire . . . 86

I.3 Algèbre bilinéaire 95

1 Dualité . . . 96
1.1 Formes linéaires et hyperplans . . . 96
1.2 Orthogonalité . . . 98
1.3 Transposition . . . 100
1.4 Dualité en dimension finie . . . 101
2 Applications multilinéaires . . . 106
2.1 Définitions et exemples . . . 106
2.2 Retour sur le déterminant . . . 108
2.3 Formes bilinéaires . . . 111
2.4 Formes bilinéaires symétriques, antisymétriques . . . 115
3 Formes quadratiques . . . 123
3.1 Généralités sur les formes quadratiques . . . 123
3.2 Décomposition LU, décomposition de Gauß . . . 141
4 Formes quadratiques sur un espace vectoriel réel . . . 161
4.1 Formes positives, définies positives — inégalité de Cauchy-Schwarz . . . 162
4.2 Signature d'une forme quadratique réelle, théorème d'inertie de Sylvester . . . 164
4.3 Matrices symétriques réelles définies positives, décomposition de Cholesky . 167

I.4 Espaces préhilbertiens 181

1 Espaces vectoriels préhilbertiens réels Espaces euclidiens . . . 182
1.1 Produit scalaire, norme euclidienne . . . 182
1.2 Orthogonalité, projecteurs orthogonaux, symétries orthogonales . . . 185
1.3 Distance d'un point à un sous-espace vectoriel de dimension finie, inégalité de Bessel . . . 193
1.4 Orthogonalisation de Gram-Schmidt . . . 196
1.5 Adjoint d'un endomorphisme d'un espace préhilbertien réel . . . 205
1.6 Groupe orthogonal . . . 213
1.7 Endomorphismes symétriques et applications . . . 217
2 Formes sesquilinéaires — Formes hermitiennes . . . 250
2.1 Formes sesquilinéaires . . . 251
2.2 Formes hermitiennes . . . 255
3 Espaces vectoriels préhilbertiens complexes, espaces hermitiens . . . 260
3.1 Produit scalaire, norme hermitienne . . . 260
3.2 Orthogonalité, distance d'un point à un sous-espace de dimension finie, inégalité de Bessel . . . 261
3.3 Adjonction, groupe unitaire, endomorphismes hermitiens . . . 263
3.4 Réduction d'un endomorphisme normal, applications . . . 269

I.5 Réduction des matrices 287

1 Rappels et compléments . . . 287
1.1 Sommes directes de sous-espaces vectoriels . . . 287
1.2 Calculs matriciels par blocs . . . 291
1.3 Polynômes d'endomorphismes . . . 294
1.4 Trace d'une matrice carrée, d'un endomorphisme . . . 296
2 Diagonalisabilité — Trigonalisabilité . . . 298
2.1 Sous-espaces propres, sous-espaces stables . . . 298
2.2 Théorème de Cayley-Hamilton . . . 304

2.3 Endomorphismes et matrices diagonalisables 305
2.4 Endomorphismes et matrices trigonalisables 312
3 Réduction : résultats généraux 316
3.1 Sous-espaces caractéristiques 316
3.2 Endomorphismes nilpotents, matrices nilpotentes 320
3.3 Décomposition de Dunford 323
3.4 Réduction de Jordan 327

I.6 Groupes classiques 335

1 Le groupe linéaire $GL_n(K)$ 335
1.1 Propriétés algébriques 336
1.2 Propriétés géométriques 339
1.3 Propriétés topologiques et différentielles 346
2 Groupe orthogonal, groupe unitaire 354
2.1 Propriétés algébriques 355
2.2 Propriétés géométriques 358
2.3 Propriétés topologiques et différentielles 361
2.4 Les groupes $O_3(\mathbb{R})$ et $SO_3(\mathbb{R})$ 363
3 Homographies 372
3.1 Le groupe projectif et la droite projective 372
3.2 Le groupe spécial projectif réel et le demi-plan de Poincaré 375

I.7 Polynômes à plusieurs indéterminées 387

1 Calcul dans $K[X_1, \ldots, X_n]$ 387
1.1 Construction de $K[X_1, \ldots, X_n]$ 387
1.2 Règles de calcul 392
1.3 Dérivations 397
1.4 Polynômes symétriques 403
2 Fonctions polynomiales 409
2.1 Prolongement des identités algébriques 409
2.2 Résultant et discriminant 412

I.8 Structures discrètes et récursivité 427

1 Mots et langages 427
1.1 L'algèbre des mots 429
1.2 Langages 431
2 Graphes 436
2.1 Graphes non orientés 437
2.2 Graphes orientés 441
2.3 Arbres 446
3 Récursion 449
3.1 Exemples expliqués 450
3.2 Analyse d'algorithmes récursifs 454
3.3 Récursion et induction structurelle 456

II Analyse

II.1 Espaces vectoriels normés 467

1 Espaces vectoriels normés, espaces métriques . . . 467
1.1 Normes . . . 468
1.2 Espaces métriques . . . 470
1.3 Limites de suites dans un espace métrique . . . 475
1.4 Parties ouvertes, parties fermées . . . 477
1.5 Applications continues . . . 483
1.6 Applications (multi)linéaires continues . . . 490
1.7 Normes équivalentes . . . 495
1.8 Métriques et topologies . . . 497
2 Espaces métriques complets . . . 498
2.1 Suites de Cauchy — Espaces complets . . . 498
2.2 Théorème du point fixe . . . 502
2.3 Séries dans un espace vectoriel normé . . . 504
3 Espaces métriques compacts . . . 508
3.1 Définition et premières propriétés . . . 508
3.2 Fonctions continues sur un compact . . . 512
4 Espaces vectoriels normés de dimension finie . . . 516
4.1 Théorèmes fondamentaux . . . 516
4.2 Normes matricielles . . . 519
5 Connexité, convexité . . . 520
5.1 Parties convexes . . . 520
5.2 Espaces connexes . . . 524
5.3 Fonctions convexes . . . 528
5.4 Inégalités de convexité . . . 533
6 Espaces de Hilbert . . . 535
6.1 Théorème de projection . . . 536
6.2 Bases hilbertiennes . . . 538

II.2 Suites et séries de fonctions 551

1 Suites de fonctions . . . 551
1.1 Convergence simple, convergence uniforme . . . 551
1.2 Convergence uniforme et continuité . . . 555
1.3 Intégration et dérivation . . . 559
1.4 Théorème d'approximation de Weierstraß . . . 563
2 Séries de fonctions . . . 565
2.1 Passage des suites de fonctions aux séries de fonctions . . . 565
2.2 Convergence normale . . . 568
3 Séries entières . . . 576
3.1 Domaine de convergence . . . 577
3.2 Opérations algébriques sur les séries entières . . . 585
3.3 Dérivation terme à terme d'une série entière . . . 590
3.4 Fonctions développables en série entière . . . 598
3.5 Exponentielle d'une matrice carrée . . . 606

II.3 Intégration 619

1 Intégrale de Riemann d'une fonction réelle sur un segment 625
1.1 Subdivisions d'un segment 625
1.2 Applications en escalier à valeurs dans un espace vectoriel 626
1.3 Fonctions intégrables, définition de l'intégrale et propriétés 628
2 Sommes de Darboux et de Riemann 646
2.1 Sommes de Darboux 646
2.2 Sommes de Riemann d'une fonction 653
3 Intégrale de Riemann d'une application à valeurs dans un espace vectoriel de dimension finie 656
3.1 Définitions 656
3.2 Propriétés 657
3.3 Sommes de Riemann 658
4 Intégrale de Riemann d'une application à valeurs dans un espace de Banach 660
4.1 Applications en escalier 660
4.2 Applications intégrables au sens de Riemann 661
4.3 Intégrale d'une application intégrable 661
4.4 Sommes de Riemann d'une application à valeurs dans un espace de Banach . 666
5 Applications réglées 666
5.1 Définition et premières propriétés 666
5.2 Intégrabilité des fonctions réglées 670
5.3 Caractérisation des fonctions intégrables au sens de Riemann 672
6 Propriétés de l'intégrale fonction de sa borne supérieure 675
6.1 Compléments sur la dérivation 675
6.2 L'application intégrale 677
6.3 Le théorème des accroissements finis 678
6.4 Primitives et théorème fondamental 681
6.5 Changement de variable, intégration par parties 684
7 Intégration sur un intervalle quelconque 687
7.1 Intégrales impropres au sens de Riemann 687
7.2 Changement de variable, intégration par parties 699
7.3 Intégration des relations de comparaison 701
8 Théorèmes de convergence 703
8.1 Interversion des limites et des intégrales 703
8.2 Continuité et dérivabilité des fonctions définies par une intégrale 720

II.4 Séries de Fourier 737

1 Coefficients de Fourier 738
1.1 La famille des exponentielles 739
1.2 La famille des sinus et cosinus 742
1.3 Propriétés des coefficients de Fourier 743
1.4 Taille des coefficients de Fourier 744
1.5 Problème inverse 746
2 Convergence de la série de Fourier d'une fonction continue 747
2.1 Produit de convolution 748
2.2 Formule de Parseval 750
2.3 Théorème de Dirichlet 752

2.4 Théorème de Féjer . . . 755
2.5 Une fonction continue qui n'est pas la somme de sa série de Fourier . . . 757
3 Série de Fourier d'une fonction réglée . . . 759
3.1 Coefficients de Fourier, formule de Parseval . . . 759
3.2 Théorèmes de Dirichlet et de Féjer . . . 763
3.3 Phénomène de Gibbs . . . 766
4 Quelques applications . . . 768
4.1 Équation de la chaleur . . . 768
4.2 Théorème ergodique . . . 772
4.3 Inégalité isopérimétrique . . . 773
4.4 Séries lacunaires . . . 775

II.5 Fonctions de plusieurs variables 783

1 Théorème d'inversion locale – Théorème des fonctions implicites . . . 784
1.1 Rappels . . . 784
1.2 Énoncés des théorèmes . . . 785
1.3 Exemples . . . 789
1.4 Démonstrations des théorèmes . . . 794
2 Sous-variétés de $\mathbb{R}^n$ . . . 798
2.1 Définition et exemples . . . 798
2.2 Sous-variétés paramétrées . . . 801
2.3 Espaces tangents . . . 804
3 Développement de Taylor . . . 808
3.1 Fonctions de classe $\mathcal{C}^k$ . . . 810
3.2 Les formules de Taylor . . . 815
3.3 Classification des points critiques d'une fonction . . . 819
4 Calcul différentiel . . . 823
4.1 Intégrales curvilignes . . . 823
4.2 Dérivée d'une forme différentielle de degré 1 . . . 827
4.3 Formule de Green-Riemann . . . 830
4.4 Quelques explications . . . 834

II.6 Fonctions analytiques 841

1 Définition et premières propriétés . . . 841
1.1 Retour sur les séries entières . . . 842
1.2 Fonctions analytiques . . . 846
2 Principe du prolongement analytique $-$ Principe des zéros isolés . . . 848
2.1 Principe du prolongement analytique . . . 849
2.2 Principe des zéros isolés . . . 851
3 Logarithme complexe et racines . . . 854
3.1 Logarithme complexe . . . 854
3.2 Racines $k^{èmes}$ . . . 857
3.3 Théorème d'inversion locale . . . 859
3.4 Analyticité du logarithme complexe et des racines $k^{èmes}$ . . . 861
4 Séries entières et séries de Fourier . . . 863
4.1 Formule de Cauchy pour un cercle . . . 863
4.2 Analyticité des fonctions holomorphes . . . 865
4.3 Inégalités de Cauchy . . . 867
4.4 Principe du maximum . . . 869
4.5 Suites de fonctions analytiques . . . 870

II.7 Équations différentielles 879

1 Équations différentielles linéaires sur $\mathbb{R}$ . . . 880
1.1 Généralités . . . 884
1.2 Équations à coefficients constants . . . 891
1.3 Vectorialisation et existence des solutions globales . . . 899
2 Existence et comportement des solutions . . . 906
2.1 Le théorème de Cauchy-Lipschitz linéaire . . . 906
2.2 Aspects qualitatifs . . . 916
2.3 Équations à coefficients périodiques . . . 926
3 Équations différentielles non linéaires . . . 930
3.1 Généralités . . . 930
3.2 Existence et comportement des solutions . . . 939
3.3 Systèmes différentiels autonomes[2] . . . 945

II.8 Méthodes numériques 961

1 Calcul numérique . . . 961
1.1 Rappels et compléments sur le calcul en base b . . . 962
1.2 Calcul en représentation flottante . . . 964
1.3 Performances des méthodes itératives . . . 969
1.4 La formule de Stirling . . . 970
2 Résolution approchée de l'équation $f(x) = 0$ . . . 972
2.1 Principes généraux . . . 972
2.2 Les principales méthodes . . . 978
3 Interpolation et approximation polynomiales . . . 985
3.1 Interpolation polynomiale . . . 985
3.2 Approximation polynomiale . . . 989
4 Calcul approché d'intégrales . . . 994
4.1 Première approche . . . 996
4.2 Méthodes de quadratures . . . 999
4.3 Méthode de Gauß . . . 1009
5 Analyse matricielle . . . 1011
5.1 Méthodes directes . . . 1012
5.2 Méthodes itératives . . . 1021

Bibliographie 1035

Indications 1036

Index 1069

Avant-propos

Cet ouvrage est le deuxième d'une série de trois, conçue pour couvrir les programmes de mathématiques de la plupart des Licences scientifiques.
Dans cette nouvelle édition nous avons, pour certains sujets (en particulier l'intégration), choisi une pédagogie plus progressive. Nous avons ainsi tenu compte, d'une part, de la mise en place des nouveaux programmes de l'enseignement secondaire et des modifications corrélatives des enseignements universitaires et, d'autre part, des remarques de nos lecteurs et de nos collègues enseignants. Cette présentation étant plus détaillée, certains sujets habituellement enseignés au niveau de la deuxième année de licence sont maintenant traités dans le troisième volume de la série, qui couvre par ailleurs un « tronc commun » des programmes de mathématiques au niveau de la troisième année.

Ce cours est illustré d'exemples et applications, il propose de plus au fil du texte de nombreux exercices corrigés qui permettront à l'étudiant de s'entraîner au fur et à mesure de son apprentissage, des notices historiques et un index très complet. On trouvera aussi à la fin de chaque « module » des exercices supplémentaires[3] avec des indications de solutions. Une correction détaillée d'une grande partie de ces exercices est accessible sur le site de l'éditeur.

Nos livres sont conçus comme une aide à l'enseignement oral dispensé par nos collègues dans les cours et travaux dirigés. L'ordre de lecture n'est pas complètement imposé et chaque étudiant peut se concentrer sur tel ou tel aspect en fonction de son programme et de son travail personnel.
Ce livre peut aussi être utilisé par un enseignant comme ouvrage de base pour son cours, dans l'esprit d'une pédagogie encore peu utilisée en France, mais qui a largement fait ses preuves ailleurs. Nous avons aussi pensé à l'étudiant travaillant seul, sans appui d'un corps professoral.

Dans les mathématiques d'aujourd'hui, un certain nombre de théories puissantes sont au premier plan. Leur maniement, au moins à un certain niveau dépendant de la filière choisie, devra évidemment être acquis par l'étudiant à la fin de ses années de licence. Mais celui-ci devra aussi avoir appris à calculer, sans s'appuyer exagérément sur les ordinateurs et les logiciels, à « se débrouiller » devant un problème abstrait ou issu des applications. Nous avons, à cette fin, mis en place une approche adaptée. Nous insistons aussi sur les exigences de rigueur (définitions précises, démonstrations rigoureuses), mais les choses sont mises

[3] Les plus difficiles sont marqués d'une ou deux étoiles.

en place de façon progressive et pragmatique, et nous proposons des exemples riches, dont l'étude met souvent en œuvre des approches multiples. Nous aidons progressivement le lecteur à acquérir le maniement d'un outillage abstrait puissant, sans jamais nous complaire dans l'abstraction pour elle même, ni un formalisme sec et gratuit : le cœur des mathématiques n'est sans doute pas un corpus de théories, si profondes et efficaces soient-elles, mais un certain nombre de problèmes dans toute leur complexité, souvent issus d'une réflexion sur le monde qui nous entoure.

Historiquement, les mathématiques se sont développées pendant des siècles en relation avec les autres sciences. De nos jours, leurs interactions se poursuivent vigoureusement (avec la physique, l'informatique, la mécanique, la chimie, la biologie, l'économie...). Nous souhaitons accompagner ce mouvement au niveau de l'enseignement des premières années d'université et aider à la mise en place, ici ou là, de filières scientifiques pluridisciplinaires contenant une composante mathématique pure ou appliquée. En particulier nous avons introduit de solides initiations aux probabilités et statistique ainsi qu'à l'algorithmique.

Malgré tout le soin apporté à cet ouvrage il est inévitable que quelques erreurs subsistent. Nous prions le lecteur, qui pourra les signaler à l'éditeur ou à l'un d'entre nous pour correction lors d'un nouveau tirage, de nous en excuser.

Jean-Pierre Ramis, André Warusfel

Vous pouvez accéder aux corrigés des exercices supplémentaires à partir de la page de présentation de l'ouvrage sur le site de l'éditeur `www.dunod.com`*. Les corrigés sont au format pdf et permettent une recherche classique par mots clef. Ils peuvent être lus, enregistrés ou imprimés en partie comme en totalité.*

Algèbre

Partie I

L'algèbre au sens moderne a deux visages : d'une part l'étude des structures indépendamment de leurs réalisations concrètes et d'autre part celle d'algorithmes performants permettant des calculs effectifs sur ordinateur.
Elle est issue de l'arithmétique, déjà bien présente chez les anciens Grecs (notamment Euclide), qui a connu de grands développements au XVII^{e} siècle (Fermat), au XVIII^{e} (Euler) et au XIX^{e} (Gauß, Hermite), et joue toujours un rôle très important, central dans un certain nombre de conjectures très célèbres comme celle de Riemann. Vers le milieu du XX^{e} siècle, l'algèbre a permis d'unifier arithmétique et géométrie algébrique, et d'établir aujourd'hui de fascinantes convergences entre arithmétique et physique théorique. Algèbre et arithmétique ont aussi d'importantes applications (cryptographie, codes correcteurs d'erreurs, secret bancaire, communications).
Les « recettes » pour équations du premier et du second degré remontent à une lointaine antiquité : à Babylone (vers 1800 avant Jésus-Christ), en Grèce grâce à Euclide et Diophante, suivis au Moyen Âge par des mathématiciens de langue arabe. Il faudra attendre le XVI^{e} siècle italien pour connaître les formules de résolution par radicaux des équations de degré trois et quatre (Del Ferro, Cardan, Ferrari). Un siècle plus tard, Viète et Descartes essaieront de dépasser ce stade, ce qui conduira ce dernier à inventer au passage la géométrie analytique. Au début du XIX^{e}, Gauß, Abel puis surtout Galois mettront un terme aux recherches vaines de leurs prédécesseurs : « il n'y a plus de formule » à partir du degré cinq. Après avoir joué un très grand rôle dans la construction des mathématiques, le sujet perdait presque tout intérêt ; toutefois les outils inventés pour le clore (groupes, théorie de Galois) restaient centraux dans les mathématiques et certaines de leurs applications.
Dans une perspective plus appliquée, Gauß, au XIX^{e} siècle, a développé des techniques « effectives » d'algèbre linéaire pour l'astronomie (trajectoire de Ceres en 1801). Au XX^{e} les groupes et l'algèbre linéaire interviennent de manière centrale en mécanique quantique et en chimie (cristallographie, chimie quantique). L'algèbre linéaire est aujourd'hui également omniprésente dans de nombreux problèmes industriels (contrôle, optimisation, robotique...).
Ce cours de seconde année approndit nettement deux aspects fondamentaux de l'algèbre, d'une part l'algèbre générale en systématisant les structures quotients (par exemple à propos des anneaux et des polynômes), et d'autre part en traitant l'algèbre linéaire et bilinéaire qui constitue le fonds classique d'une seconde année d'université. Il faut également signaler un important module consacré à la récursivité, complétant l'initiation à l'algorithmique du premier volume.

Compléments d'algèbre

I.1

Nous approfondissons ici, en vue d'applications dans ce volume, les notions d'algèbre de base de [L1] concernant les groupes, les anneaux, les espaces vectoriels et les polynômes.

1 Quotients

Cette section fait appel au vocabulaire de la section « Relations d'équivalence » du module « Fondements » de [L1], qu'il est donc nécessaire de bien maîtriser.

1.1 Quotient d'un ensemble par une relation d'équivalence

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On notera indifféremment $x\mathcal{R}y$ ou $x \equiv y \pmod{\mathcal{R}}$, ou encore, pour alléger l'écriture, $x \sim y$. Pour certains raisonnements ou calculs portant sur les éléments de E, il n'y a pas lieu de distinguer entre deux éléments équivalents, le résultat obtenu (ou les propriétés étudiées) ne dépendant pas du choix d'un élément particulier dans une classe d'équivalence donnée. Le but de cette section est de se donner des moyens (vocabulaire et méthodes) de raisonner et de calculer sur des objets considérés *à équivalence près*.

Exemple. Pour « vérifier » l'opération $54\,321 \times 6\,789 = 368\,785\,269$, on considère chaque entier naturel n comme « équivalent » à la somme $s(n)$ de ses chiffres. Ainsi, $54\,321 \sim 15 \sim 6$ et $6\,789 \sim 30 \sim 3$. On effectue le calcul sur les équivalents plus simples : $6 \times 3 = 18 \sim 9$. Par ailleurs, $368\,785\,269 \sim 54 \sim 9$. On estime alors que le résultat est plausible : il n'a pas été réfuté par le test dit de la « preuve par neuf ». L'idée sous-jacente est qu'il existe une relation d'équivalence $\sim$ telle que, d'une part, $\forall n \in \mathbb{N}\ ,\ n \sim s(n)$ et que, d'autre part, $a \sim a'$ et $b \sim b' \Rightarrow aa' \sim bb'$. Alors $54\,321 \sim 6$ et $6\,789 \sim 3 \Rightarrow 54\,321 \times 6\,789 \sim 6 \times 3 = 18 \sim 9$. C'est, bien entendu, la relation $\equiv_9$ de congruence modulo 9 qui convient.

Théorème et définition 1. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$, également notée $\sim$. Il existe alors un ensemble $\overline{E}$ et, pour chaque élément x de E, un élément $\overline{x}$ de $\overline{E}$ de telle sorte que l'application $\pi : x \mapsto \overline{x}$ soit surjective de E sur $\overline{E}$ et que l'on ait l'équivalence suivante : $\forall x, y \in E\ ,\ \pi(x) = \pi(y) \Leftrightarrow x \sim y$.
L'ensemble $\overline{E}$ est appelé *ensemble quotient de E par la relation d'équivalence $\mathcal{R}$*, et il est noté $E/\mathcal{R}$. L'application π est appelée *projection canonique* de E sur $\overline{E}$. L'élément $\overline{x}$ de $\overline{E}$ est appelé *classe de x* (dans $\overline{E}$) ; on dit que l'élément x est un *représentant* de $\overline{x}$ (dans E).

Autrement dit, on demande que soient vérifiés les axiomes suivants :

- Deux éléments quelconques de E ont la même classe si, et seulement s'ils sont équivalents : $\forall x, y \in E\ ,\ \overline{x} = \overline{y} \Longleftrightarrow x \sim y$.
- Tout élément de $\overline{E}$ est la classe d'un élément de E ; noter cependant que l'on ne requiert *pas* l'unicité du représentant $x \in E$ de $\overline{x} \in \overline{E}$.

Remarquons d'ailleurs qu'en toute rigueur, c'est l'ensemble $\overline{E}$ *muni de la projection canonique* π que l'on devrait appeler le quotient.

Démonstration. Il y a aux moins deux méthodes pour construire l'ensemble quotient $\overline{E} = E/\mathcal{R}$ et la projection canonique $\pi : E \to \overline{E}$. Dans la première méthode, on choisit, dans chaque classe d'équivalence, un élément arbitraire que l'on note $\overline{x}$. C'est possible grâce à l'axiome du choix (module « Fondements » de [L1]). L'ensemble $\overline{E} := \{\overline{x} \mid x \in E\}$ est donc, dans ce cas, un *ensemble de représentants.*
Dans la deuxième méthode, on pose $\overline{x} := \mathrm{cl}(x)$. L'objet $\overline{x}$ est donc *l'ensemble des éléments de E équivalents à x*, donc un sous-ensemble de E, et un représentant de $\overline{x}$ en est un élément. Dans ce cas : $\overline{E} = E/\mathcal{R} := \{\mathrm{cl}(x) \mid x \in E\} \subset \mathcal{P}(E)$. Pour chacune de ces deux constructions, le lecteur vérifiera sans peine que l'application $\pi : E \to \overline{E}$ est surjective et que $\pi(x) = \pi(y) \Leftrightarrow x \sim y$. ∎

L'avantage de la première construction est que les symboles $\overline{x}$ désignent des objets « concrets ». L'avantage de la deuxième construction est qu'elle ne fait pas jouer un rôle privilégié à un élément particulier de $\mathrm{cl}(x)$, ceux-ci sont vraiment équivalents ! L'inconvénient (surtout psychologique) est que le symbole $\overline{x}$ peut être parfois vu comme désignant un *élément* de $\overline{E}$, parfois comme désignant un *sous-ensemble* de E.

Corollaire 2. Soient $a \in \overline{E}$ et $x \in \pi^{-1}(a)$ un représentant de a dans E. Alors l'ensemble $\pi^{-1}(a)$ de tous les représentants de a dans E est la classe d'équivalence $\mathrm{cl}(x)$.

Démonstration. Notons que x existe bien puisque π est surjective. De plus, on a les équivalences logiques : $y \in \pi^{-1}(a) \Leftrightarrow \pi(y) = a = \pi(x) \Leftrightarrow y \sim x$, de sorte que, par définition de la classe d'équivalence de x, $\pi^{-1}(a) = \{y \in E \mid y \sim x\} = \mathrm{cl}(x)$. ∎

Exemple. Pour la relation $\equiv_9$, on a $\overline{E} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}$. Selon la première construction, on prend, par exemple, $\overline{n} := n \mod 9$ (reste de la division euclidienne) ; dans ce cas, $\overline{E} = [\![0, 8]\!]$ et $\overline{54321} = 6$. Selon la seconde construction, $\overline{n}$ est l'ensemble $\{n + 9k \mid k \in \mathbb{Z}\}$. Ainsi, $\overline{54321} = \overline{15} = \overline{6}$ est-il à la fois une sorte de nombre et une partie de $\mathbb{Z}$.

1.1.1 Passage au quotient d'une application

On reprend les notations précédentes E, $\mathcal{R}$, $\sim$ et $\pi : E \to \overline{E}$. Soit de plus $f : E \to F$ une application dont l'ensemble d'arrivée F est quelconque.

Théorème et définition 3 (Théorème de factorisation pour les applications).
Les assertions suivantes sont équivalentes :
(i) Deux éléments équivalents de E ont même image par f :

$$x \sim y \Rightarrow f(x) = f(y).$$

De manière équivalente, l'application f est constante sur chaque classe $\mathrm{cl}(x)$.
(ii) Il existe $\overline{f} : \overline{E} \to F$ telle que $\overline{f} \circ \pi = f$, c'est-à-dire : $\forall x \in E\ ,\ \overline{f}(\overline{x}) = f(x)$.
L'application $\overline{f}$ est alors unique. Nous dirons que la relation $\mathcal{R}$ est *compatible* avec l'application f, et que l'application $\overline{f}$ a été obtenue à partir de l'application f par *passage au quotient* par la relation $\mathcal{R}$.

Démonstration. S'il existe une application $\overline{f}$ satisfaisant (ii), on a les implications logiques : $x \sim y \Rightarrow \overline{x} = \overline{y} \Rightarrow f(x) = \overline{f}(\overline{x}) = \overline{f}(\overline{y}) = f(y)$.
Supposons réciproquement (i) vérifiée. On définit alors l'application $\overline{f}$ de la manière suivante. Pour tout $a \in \overline{E}$, on choisit un représentant arbitraire $x \in E$ de a et l'on est obligé (pour respecter la condition requise) de poser $\overline{f}(a) = f(x)$, ce qui entraîne d'ailleurs l'unicité de $\overline{f}$. Le point crucial est que *cette définition ne dépend pas du choix du représentant* : pour tout autre représentant y, on a $\overline{x} = a = \overline{y}$, donc $x \sim y$, donc $f(x) = f(y)$.
Par construction, on a alors bien $\forall x \in E\ ,\ \overline{f}(\overline{x}) = f(x)$, autrement dit, $\overline{f} \circ \pi = f$. ∎

Pratiquement, on procède comme suit : soit $a \in \overline{E}$. Pour définir $\overline{f}(a)$, on choisit tout d'abord un représentant arbitraire $x \in E$ de a et l'on pose $\overline{f}(a) := f(x) \in F$; dans un deuxième temps, *il faut vérifier que $f(x)$ ne dépend pas du représentant x choisi.*

Corollaire 4. On suppose E et F respectivement munis des relations d'équivalence $\mathcal{R}$ et $\mathcal{S}$, abrégées en $\sim$ et en $\equiv$. Soit $f : E \to F$ une application telle que deux éléments équivalents de E ont des images équivalentes : $x \sim y \Rightarrow f(x) \equiv f(y)$.
Il existe alors une unique application $\overline{f} : \overline{E} := E/\mathcal{R} \to \overline{F} := F/\mathcal{S}$ telle que :

$$\forall x \in E\ ,\ \overline{f}(\overline{x}) = \overline{f(x)}.$$

Démonstration. On applique le théorème à l'application $x \mapsto \overline{f(x)}$ de E dans $\overline{F}$. ∎

Exemple. Prenons $E = \mathbb{R}$ muni de la relation $\equiv_{2\pi}$ de congruence modulo 2π ; l'ensemble quotient est alors noté $\mathbb{R}/2\pi\mathbb{Z}$ (module sur les nombres complexes de [L1]).
La relation $\equiv_{2\pi}$ est compatible avec l'application $\theta \mapsto \mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$ de $\mathbb{R}$ dans $\mathbb{C}$, car les fonctions cosinus et sinus sont 2π-périodiques. On peut donc en déduire, par passage au quotient, une application $\overline{\theta} \mapsto \mathrm{e}^{\mathrm{i}\theta}$ de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{C}$. En revanche, l'application $\theta \mapsto \mathrm{e}^{\mathrm{i}\theta/2}$ ne passe pas au quotient et l'application $\overline{\theta} \mapsto \mathrm{e}^{\mathrm{i}\theta/2}$ de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{C}$ *n'est pas définie* : on ne saurait en effet décider si $\overline{0} = \overline{2\pi}$ a pour image $\mathrm{e}^{\mathrm{i}0/2} = 1$ ou $\mathrm{e}^{\mathrm{i}2\pi/2} = -1$ (voir également l'exercice I.1.1 de la page 50).

Exercice 1.
Soit $f : E \to F$ une application. On définit sur E la relation $x \sim y \Leftrightarrow f(x) = f(y)$. Démontrer que c'est une relation d'équivalence compatible avec l'application f et que l'application $\overline{f} : \overline{E} \to F$ est injective. Elle induit donc une bijection de $\overline{E}$ sur $\mathrm{Im}\, f$.
Solution. On a vu dans [L1] que $\sim$ est une relation d'équivalence dont les classes d'équivalence sont exactement les ensembles de la forme $f^{-1}(y)$, où $y \in F$. Selon la deuxième construction de $\overline{E}$, on peut identifier l'élément $\overline{x}$ de $\overline{E}$ à $f^{-1}(y)$, où $y = f(x)$; on a alors $\overline{f}(\overline{x}) = y$. L'unique antécédent de y par $\overline{f}$ est donc la classe $\overline{x}$ de n'importe quel antécédent x de y par f.

1.2 Passage au quotient d'une loi de composition interne

On reprend les notations précédentes E, $\mathcal{R}$, $\sim$ et $\pi : E \to \overline{E}$. Soit de plus $\star$ une loi de composition interne sur E. On souhaite munir $\overline{E}$ d'une loi de composition interne $\diamond$ telle que π soit un morphisme, autrement dit : $\forall x, y \in E\ ,\ \overline{x} \diamond \overline{y} = \overline{x \star y}$. Pour que cela soit possible, il est évidemment *nécessaire* que $\overline{x \star y}$ ne change pas si l'on remplace x, y par x', y' tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$.

Définition 1. On dit que la relation $\sim$ est *compatible avec la loi* $\star$, ou encore que c'est une *congruence* si : $\forall x, y, x', y' \in E\ ,\ x \sim x'$ et $y \sim y' \Longrightarrow x \star y \sim x' \star y'$.

Il suffit en fait de vérifier séparément deux propriétés un peu plus faibles, la *compatibilité à gauche* : $y \sim y' \Rightarrow x \star y \sim x \star y'$, et la *compatibilité à droite* : $x \sim x' \Rightarrow x \star y \sim x' \star y$. En effet, des hypothèses $x \sim x'$ et $y \sim y'$, on peut alors déduire respectivement $x \star y \sim x' \star y$ et $x' \star y \sim x' \star y'$, d'où, par transitivité, $x \star y \sim x' \star y'$. Si la loi $\star$ est commutative, ces deux compatibilités partielles sont bien sûr équivalentes.

Proposition et définition 5. Si la relation $\sim$ est compatible avec la loi $\star$, l'ensemble quotient $\overline{E}$ peut être muni d'une unique loi de composition interne $\diamond$ telle que la projection canonique π est un morphisme de $(E, \star)$ dans $(\overline{E}, \diamond)$. La loi $\diamond$ est appelée *loi quotient* (de la loi $\star$ par la relation d'équivalence $\sim$).

Notons que la conclusion traduit l'équation $\overline{x} \diamond \overline{y} = \overline{x \star y}$.

Démonstration. Soient $a, b \in \overline{E}$ et soient $x, y \in E$ des représentants respectifs de a, b. Pour que π soit un morphisme, $\diamond$ doit être définie par la formule $a \diamond b = \overline{x \star y}$, d'où l'unicité de la loi $\diamond$. Il reste à voir que cette définition en est bien une, c'est-à-dire qu'elle ne dépend pas du choix des représentants. Si $a = \overline{x} = \overline{x'}$ et $b = \overline{y} = \overline{y'}$, on a $x \sim x'$ et $y \sim y'$, d'où, par hypothèse, $x \star y \sim x' \star y'$ et $\overline{x \star y} = \overline{x' \star y'}$. ∎

Exemple. La relation $\equiv_9$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$; on peut donc additionner et multiplier des classes. Par exemple, comme $\overline{4} = \overline{13}$ et $\overline{17} = \overline{-1}$,on peut indifféremment calculer $\overline{4}+\overline{17} = \overline{21}$ ou $\overline{13}+\overline{-1} = \overline{12}$ et obtenir le même résultat $\overline{21} = \overline{12}$.

Exercice 2.

Montrer que la relation $\equiv_{2\pi}$ est compatible avec l'addition dans $\mathbb{R}$. Donner un exemple d'addition de classes. Cette relation est-elle compatible avec la multiplication dans $\mathbb{R}$?

Solution. Soient x, x', y, y' des réels tels que $x' \equiv_{2\pi} x$ et $y' \equiv_{2\pi} y$. Il existe donc des entiers relatifs a, b tels que $x' - x = a \times 2\pi$ et $y' - y = b \times 2\pi$, d'où $(x' + y') - (x + y) = (a + b) \times 2\pi$, d'où $x' + y' \equiv_{2\pi} x + y$: la relation $\equiv_{2\pi}$ est bien compatible avec l'addition. On reconnaît dans $(\mathbb{R}/\equiv_{2\pi}, +)$ le groupe $\mathbb{R}/2\pi\mathbb{Z}$ rencontré dans l'étude des nombres complexes. Par exemple, comme $\overline{\pi} = \overline{-\pi}$ et $\overline{3\pi/2} = \overline{-\pi/2}$, on peut indifféremment calculer $\overline{\pi} + \overline{3\pi/2} = \overline{5\pi/2}$ ou $\overline{-\pi} + \overline{-\pi/2} = \overline{-3\pi/2}$ et obtenir le même résultat : $\overline{5\pi/2} = \overline{-3\pi/2}$.

Avec les notations ci-dessus, aucun calcul ne permet de conclure que $x'y' - xy$ est un multiple entier de 2π. De fait, si $x = y = 0$, $x' = a \times 2\pi$ et $y' = b \times 2\pi$, on a $x'y' - xy = (2\pi ab) \times 2\pi$ et $2\pi ab$ n'est en général pas un entier. La relation $\equiv_{2\pi}$ n'est donc pas compatible avec la multiplication. Ainsi, on ne saurait dire ce que vaut $\overline{\pi} \times \overline{3\pi/2}$ ou $\overline{-\pi} \times \overline{-\pi/2}$ car $\overline{3\pi^2/2}$ et $\overline{\pi^2/4}$ ne sont pas égaux.

PROPRIÉTÉS HÉRITÉES PAR LA LOI QUOTIENT. *Avec les mêmes notations, les propriétés qui suivent se déduisent de la surjectivité du morphisme $\pi : (E, \star) \to (\overline{E}, \diamond)$:*

1. *Si $\star$ est commutative (resp. associative), $\diamond$ est commutative (resp. associative).*
2. *Si e est un élément neutre (resp. neutre à gauche, resp. neutre à droite, resp. absorbant) pour $\star$, alors $\overline{e}$ est un élément neutre (resp. neutre à gauche, resp. neutre à droite, resp. absorbant) pour $\diamond$.*
3. *Si y est inverse de x (resp. inverse à droite, resp. inverse à gauche) pour $\star$, alors $\overline{y}$ est inverse de $\overline{x}$ (resp. inverse à droite, resp. inverse à gauche) pour $\diamond$.*
4. *En particulier, si $\star$ est une loi de groupe, la loi quotient $\diamond$ est une loi de groupe.*
5. *Dans le cas d'une relation d'équivalence compatible avec deux lois $\star$ et $\top$, telle que $\top$ est distributive (resp. à gauche, resp. à droite) par rapport à $\star$, la loi quotient $\overline{\top}$ est distributive (resp. à gauche, resp. à droite) par rapport à $\overline{\star}$.*
6. *La régularité ne s'hérite pas :* exercice I.1.3 de la page 50.

Théorème 6 (Théorème de factorisation pour les morphismes).
Soit $\sim$ une relation d'équivalence sur E compatible avec la loi $\star$. Notons $\overline{E}$ et $\overline{\star}$ le quotient et la loi quotient et $\pi : E \to \overline{E}$ la projection canonique.
Soit par ailleurs $f : (E, \star) \to (F, \diamond)$ un morphisme. Pour que f soit compatible avec $\sim$, il faut, et il suffit, qu'il existe un morphisme $\overline{f} : (\overline{E}, \overline{\star}) \to (F, \diamond)$ tel que $f = \overline{f} \circ \pi$.
Le morphisme $\overline{f}$ est alors unique.

Démonstration. On applique la proposition 3 de la page 5, ce qui fournit l'application $\overline{f}$ (qui est unique). Il reste à voir que f est un morphisme si, et seulement si, $\overline{f}$ l'est.
Dans le sens direct, c'est évident (composé de deux morphismes). Réciproquement, si f est un morphisme, on a, avec des notations évidentes :

$$\overline{f}(\overline{x}\ \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Comme π est surjective, $\overline{x}$ et $\overline{y}$ sont arbitraires dans $\overline{E}$ et $\overline{f}$ est un morphisme. ∎

Théorème 7 (Théorème d'isomorphisme). (i) Soit $f : (E, \star) \to (F, \diamond)$ un morphisme. La relation $\sim$ sur E définie par $x \sim y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence compatible avec la loi $\star$. On notera $\overline{E}$ l'ensemble quotient, $\overline{\star}$ la loi induite et $\overline{f} : \overline{E} \to F$ l'application obtenue par passage au quotient.
(ii) Le sous-ensemble $F' = \operatorname{Im} f$ de F est stable pour la loi $\diamond$.
(iii) L'application $\overline{f}$ induit un isomorphisme de $(\overline{E}, \overline{\star})$ sur $(F', \diamond)$.

Démonstration. (i) D'après l'exercice 1 de la page 6, $\sim$ est une relation d'équivalence.
Si $x \sim y$ et $x' \sim y'$, alors $f(x) = f(y)$ et $f(x') = f(y')$, donc

$$f(x \star x') = f(x) \diamond f(x') = f(y) \diamond f(y') = f(y \star y'),$$

d'où $x \star x' \sim y \star y'$: on a bien la compatibilité.

(ii) Deux éléments quelconques de F' sont de la forme $f(x), f(y)$ et leur composé est $f(x) \diamond f(y) = f(x \star y) \in F'$: cet ensemble est bien un sous-ensemble stable.

(iii) Le morphisme $\overline{f} : \overline{E} \to F$ induit par corestriction un morphisme $\overline{f} : \overline{E} \to F'$, qui est bijectif d'après l'exercice 1 de la page 6. ∎

Exemple. L'application $t \mapsto \mathrm{e}^{\mathrm{i}t}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$ et la relation $\sim$ associée est $\equiv_{2\pi}$. L'image est le cercle unité $\mathbb{U}$ et l'on obtient par passage au quotient un isomorphisme de $(\mathbb{R}/\equiv_{2\pi}, +) = \mathbb{R}/2\pi\mathbb{Z}$ sur $(\mathbb{U}, \times)$. D'après les propriétés d'héritage de la page précédente, il s'agit d'un isomorphisme de groupes.

1.2.1 Retour sur la construction de $\mathbb{Z}$

Soit M un ensemble non vide muni d'une loi de composition interne associative et commutative notée additivement, et disposant d'un élément neutre 0. On dit alors que $(M, +)$ est un *monoïde commutatif*. Notons additivement la loi produit sur $M \times M$: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$.

Ainsi $(M \times M, +)$ est un monoïde commutatif d'élément neutre $(0,0)$. Définissons sur $M \times M$ une relation $\sim$ par : $(a,b) \sim (a',b') \Leftrightarrow \exists c \in M \ : \ a + b' + c = a' + b + c$. Par exemple, $(a,a) \sim (0,0)$ pour tout a. On démontre alors que $\sim$ est une relation d'équivalence compatible avec l'addition de $M \times M$. Notons G l'ensemble quotient et $+$ la loi quotient ; alors $(G,+)$ est un groupe commutatif, dans lequel l'élément neutre est $\overline{(0,0)}$ et l'opposé de la classe $\overline{(a,b)}$ est $\overline{(b,a)}$. L'application $i : a \mapsto \overline{(a,0)}$ est un morphisme de $(M,+)$ dans $(G,+)$. Deux éléments $a, b \in M$ ont même image si, et seulement si, $\exists c \in M \ : \ a + c = b + c$. En particulier, si tous les éléments de M sont simplifiables, le morphisme i est injectif. Le groupe G est appelé *groupe des fractions du monoïde* M. Dans le cas du monoïde $(\mathbb{N},+)$, on obtient ainsi le groupe $G = \mathbb{Z}$ et le morphisme injectif $\mathbb{N} \to \mathbb{Z}$ ([L1], module « Arithmétique »).

1.2.2 Retour sur la construction du corps des fractions

Soient A un anneau commutatif et S une partie *multiplicative* de A, autrement dit : S est stable pour la multiplication et $1 \in S$; ainsi, $(S,\times)$ est (en un sens évident) un sous-monoïde du monoïde commutatif $(A,\times)$. On suppose de plus que $0 \notin S$ (il en résulte d'ailleurs que S ne contient aucun élément nilpotent). On définit sur $A \times S$ deux lois de composition interne, notées additivement et multiplicativement : $(a_1,s_1)+(a_2,s_2) = (a_1s_2+a_2s_1, s_1s_2)$ et $(a_1,s_1)\times(a_2,s_2) = (a_1a_2, s_1s_2)$. La deuxième loi est simplement la loi produit définie à partir des monoïdes commutatifs $(A,\times)$ et $(S,\times)$. La première loi, plus compliquée, est modelée sur le calcul des fractions. On définit également sur $A\times S$ une relation $\sim$ comme suit : $(a,s) \sim (a',s') \iff \exists t \in S \ : \ t(as'-a's) = 0$. On démontre alors que $\sim$ est une relation d'équivalence compatible avec les lois $+$ et $\times$ sur $A\times S$. Notons B l'ensemble quotient et $+$ et $\times$ les lois quotients. Alors $(B,+,\times)$ est un anneau commutatif dont les éléments neutres sont $\overline{(0,1)}$ (pour l'addition) et $\overline{(1,1)}$ (pour la multiplication). L'opposé de $\overline{(a,s)}$ est $\overline{(-a,s)}$. L'application $i : a \mapsto \overline{(a,1)}$ est un morphisme d'anneaux de A dans B, de noyau : $\operatorname{Ker} i = \{a \in A \mid \exists s \in S \ : \ sa = 0\}$. Si S ne contient aucun diviseur de zéro dans A, en particulier si A est intègre, le morphisme i est injectif. L'anneau B est noté $S^{-1}A$ et l'on dit que c'est un *anneau de fractions de* A. L'image de $(a,s) \in A \times S$ dans $S^{-1}A$ est notée $s^{-1}a$ ou $\dfrac{a}{s}$. Lorsque A est intègre, en prenant $S = A \setminus \{0\}$, on reconnaît dans $S^{-1}A$ le corps des fractions de A ([L1], module « Groupes, anneaux, corps »).

1.3 Groupes quotients

1.3.1 Relations compatibles et sous-groupes distingués

Lemme 8. (i) Soient G un groupe et H un sous-groupe de G. Alors la relation $\sim$ définie par $a \sim b \Leftrightarrow a^{-1}b \in H$ (resp. $ab^{-1} \in H$) est une relation d'équivalence sur G compatible à gauche (resp. à droite) avec la loi interne ; la classe d'équivalence de $a \in G$ est sa *classe à gauche* aH (resp. sa *classe à droite* Ha).
(ii) Réciproquement, toutes les relations d'équivalence sur G compatibles à gauche (resp. à droite) avec la loi interne sont obtenues de cette manière.

Démonstration. (i) Nous ne traiterons que le cas des classes à gauche, l'autre côté étant entièrement similaire. De l'équivalence logique $a^{-1}b \in H \Leftrightarrow aH = bH$ (dont la preuve facile est laissée au lecteur), on déduit que $\sim$ est une relation d'équivalence et que la classe d'équivalence de $a \in G$ est aH. De l'implication évidente $aH = bH \Rightarrow caH = cbH$, on

déduit que $\sim$ est compatible à gauche avec la loi interne.
(ii) Soit $\sim$ une relation d'équivalence sur G compatible à gauche avec la loi interne. Soit H la classe de l'élément neutre e. Le sous-ensemble H contient e et l'on a les implications :

$$(a, b \in H) \Longrightarrow (a \sim e \text{ et } b \sim e) \Longrightarrow (a^{-1}b \sim a^{-1}e \sim a^{-1}a = e) \Longrightarrow (a^{-1}b \in H),$$

ce qui entraîne que H est un sous-groupe de G. On a maintenant les équivalences logiques :

$$a \sim b \Longleftrightarrow a^{-1}a \sim a^{-1}b \Longleftrightarrow a^{-1}b \in H,$$

ce qui achève la démonstration. ∎

Théorème et définition 9. Les propriétés suivantes sont équivalentes :
(i) Les relations d'équivalence sur G respectivement définies par $a^{-1}b \in H$ et par $ab^{-1} \in H$ coïncident.
(ii) Pour tout $a \in G$, la classe à gauche et la classe à droite coïncident : $aH = Ha$.
(iii) Le sous-groupe H est invariant par les *automorphismes intérieurs* $x \mapsto axa^{-1}$ ($a \in G$) : quel que soit $a \in G$, on a $aHa^{-1} = H$.
Le sous-groupe H de G est alors dit *distingué* dans G. On parle également de sous-groupe *invariant* ou de sous-groupe *normal*. On note alors : $H \lhd G$.

Démonstration. C'est immédiat en vertu du lemme 8 de la page précédente. ∎

Précisons le sens de la troisième propriété. Pour tout $a \in G$ fixé, l'application $x \mapsto axa^{-1}$ est un automorphisme de G ([L1], module « Groupes, anneaux, corps »); c'est ce que l'on appelle un automorphisme intérieur. Pratiquement, il suffit de vérifier que, pour tout $a \in G$, on a l'inclusion $aHa^{-1} \subset H$. En effet, l'inclusion correspondante pour a^{-1} s'écrit $a^{-1}Ha \subset H$, qui entraîne $H \subset aHa^{-1}$ et l'on obtient finalement l'égalité.
Les sous-groupes G et $\{e\}$ de G sont évidemment distingués. Si G est commutatif, tout automorphisme intérieur est égal à l'identité et tout sous-groupe est distingué.

Exercice 3.
Montrer que le centre Z du groupe G en est un sous-groupe distingué.
Solution. Rappelons ([L1]) que $Z = \{a \in G \mid \forall b \in G\ ,\ ab = ba\}$. Tout élément de Z est fixé par tout automorphisme intérieur, *a fortiori*, le sous-groupe Z est globalement invariant par tout automorphisme intérieur.

Proposition 10. Le noyau $\operatorname{Ker} f$ d'un morphisme de groupes $f : G \to G'$ est distingué. La relation associée est définie par $a \sim b \Leftrightarrow f(a) = f(b)$.

Démonstration.
Si $x \in \operatorname{Ker} f$, alors $f(x) = e'$ (neutre de G'), donc $f(axa^{-1}) = f(a)e'f(a)^{-1} = e'$, donc $axa^{-1} \in \operatorname{Ker} f$: c'est bien un sous-groupe distingué. De plus, on a les équivalences :

$$a^{-1}b \in \operatorname{Ker} f \Longleftrightarrow f(a^{-1}b) = e' \Longleftrightarrow f(a) = f(b).$$

∎

Corollaire 11. Soit $n \in \mathbb{N}^*$. Le groupe alterné $\mathfrak{A}_n$ est distingué dans le groupe symétrique $\mathfrak{S}_n$. Soit E un ensemble fini non vide. Le groupe alterné $\mathfrak{A}(E)$ est distingué dans le groupe symétrique $\mathfrak{S}(E)$.

Démonstration. C'est le noyau du morphisme signature. ∎

Définition 2. Soit $n \in \mathbb{N}^*$. On appelle *groupe spécial linéaire d'ordre* n, et l'on note $SL_n(K)$ le sous-groupe du groupe linéaire $GL_n(K)$ formé des matrices de déterminant 1. De même, si E est un K-espace vectoriel de dimension finie, on appelle *groupe spécial linéaire de* E, et l'on note $\mathcal{SL}(E)$ le sous-groupe du groupe linéaire $\mathcal{GL}(E)$ formé des automorphismes de déterminant 1.

Corollaire 12. Le groupe spécial linéaire $SL_n(K)$ est un sous-groupe distingué du groupe linéaire $GL_n(K)$. Le groupe spécial linéaire $\mathcal{SL}(E)$ est un sous-groupe distingué du groupe linéaire $\mathcal{GL}(E)$.

Démonstration. C'est, dans chaque cas, le noyau du morphisme déterminant. ∎

1.3.2 Quotient par un sous-groupe distingué

Théorème 13. (i) Soit $H \lhd G$ un sous-groupe distingué. Les égalités $a^{-1}b \in H$ et $ab^{-1} \in H$ définissent une même relation, notée $a \equiv b \pmod{H}$, qui est une relation d'équivalence sur G compatible (à gauche et à droite) avec la loi interne ; la classe d'équivalence de $a \in G$ est $aH = Ha$. Réciproquement, toutes les relations d'équivalence sur G compatibles (à gauche et à droite) avec la loi interne sont obtenues de cette manière à partir d'un sous-groupe distingué H.
(ii) La loi quotient fait de l'ensemble quotient $\overline{G}$ un groupe.
La projection canonique $\pi : G \to \overline{G}$ est un morphisme surjectif de noyau H.

Démonstration.
(i) C'est immédiat à partir du lemme 8 de la page 9 et du théorème 9 de la page ci-contre.
(ii) On sait déjà que la projection canonique est un morphisme surjectif, et, d'après les propriétés d'héritage de la de la page 7, $\overline{G}$ est un groupe. Le noyau de π est la classe de l'élément neutre, c'est-à-dire H. ∎

Définition 3. La relation $a \equiv b \pmod{H}$ est appelée *congruence modulo* H.
Le groupe $\overline{G}$ est appelé *groupe quotient de* G *par* H et noté G/H, ou, parfois $\dfrac{G}{H}$.

Théorème 14 (Théorème de factorisation pour les groupes).
Soient $H \lhd G$ un sous-groupe distingué et $\pi : G \to G/H$ la projection canonique.
Soit $f : G \to G'$ un morphisme de groupes.
Alors, pour que H soit inclus dans $\operatorname{Ker} f$, il faut, et il suffit, qu'il existe un morphisme de groupes : $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$.

Démonstration.
L'inclusion $H \subset \operatorname{Ker} f$ équivaut à l'implication $a^{-1}b \in H \Rightarrow f(a) = f(b)$, c'est-à-dire à la compatibilité de la congruence modulo H avec f : on peut donc appliquer le théorème 6 de la page 8. ∎

Théorème 15 (Premier théorème d'isomorphisme pour les groupes). Soit $f : G \to G'$ un morphisme de groupes. Soit $\pi : G \to G/\operatorname{Ker} f$ la projection canonique. Il existe alors un unique morphisme de groupes $\overline{f} : G/\operatorname{Ker} f \to G'$ tel que $f = \overline{f} \circ \pi$. Ce morphisme est injectif et induit par corestriction un isomorphisme $\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$.

Démonstration. On peut, au choix, appliquer le théorème 7 de la page 8 au cas des groupes ou bien appliquer le théorème 14 de la page précédente au cas de $H = \operatorname{Ker} f$. ∎

Proposition 16. Soient $H \lhd G$ et $\pi : G \to G/H$ la projection canonique. On définit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H de la manière suivante : à tout sous-groupe G' de G contenant H, on associe son image $\pi(G') \subset G/H$; à tout sous-groupe K de G/H, on associe son image réciproque $G' = \pi^{-1}(K) \subset G$. Avec ces notations, on a alors : $\overline{G'} := \pi(G') = G'/H$.

Démonstration. L'inclusion $G' \subset \pi^{-1}\big(\pi(G')\big)$ est vraie pour toute partie G' de G. Pour un sous-groupe G' contenant H, on montre l'inclusion réciproque : si $x \in \pi^{-1}\big(\pi(G')\big)$, alors $\pi(x) \in \pi(G')$, donc $\pi(x) = \pi(g)$ avec $g \in G'$; alors $x^{-1}g \in \operatorname{Ker}\pi = H \subset G'$, d'où $x^{-1}g \in G'$, d'où $x \in G'$ (car $g \in G'$). On a donc $\pi^{-1}\big(\pi(G')\big) \subset G'$, d'où $G' = \pi^{-1}\big(\pi(G')\big)$. Puisque π est surjective, l'égalité $F = \pi\big(\pi^{-1}(F)\big)$ est vraie pour toute partie F de G/H. Pour tout sous-groupe G' de G contenant H, $F := \pi(G')$ est un sous-groupe de G/H. Pour tout sous-groupe F de G/H, $G' := \pi^{-1}(F)$ est un sous-groupe de G contenant $\pi^{-1}(e) = H$.
Ainsi, les applications $F \mapsto \pi^{-1}(F)$ et $G' \mapsto \pi(G')$ sont des bijections réciproques l'une de l'autre entre les sous-groupes de G/H et les sous-groupes de G contenant H. La restriction-corestriction de π à $G' \to \overline{G'}$ est surjective de noyau H, donc (théorème 15) induit un isomorphisme $G'/H \simeq \overline{G'}$ qui permet l'identification. ∎

Théorème 17 (Deuxième théorème d'isomorphisme pour les groupes). La correspondance de la proposition 16 induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.
Si $G' \lhd G$, G' contenant H, on a de plus un isomorphisme : $\dfrac{G/H}{G'/H} \simeq \dfrac{G}{G'}$.

Démonstration. Si G' est distingué, l'égalité $aG'a^{-1} = G'$ donne, par application du morphisme π, l'égalité $bFb^{-1} = F$, où $F := \pi(G')$ et où $b := \overline{a}$ est un élément quel-

conque de G/H (puisque π est surjective); F est donc distingué. Si $F = G'/H$ est distingué dans $\overline{G} = G/H$, le morphisme composé $G \to \overline{G} = G/H \to \overline{G}/F$ est surjectif de noyau G', qui est donc distingué; on applique alors le premier théorème d'isomorphisme. ∎

Exercice 4.
Quels sont les sous-groupes de $GL_n(K)$ (resp. de $\mathfrak{S}_n$) contenant $SL_n(K)$ (resp. $\mathfrak{A}_n$)?
Solution. Les premiers sont en bijection avec les sous-groupes de $GL_n(K)/SL_n(K)$. Or, $SL_n(K)$ est le noyau du morphisme surjectif $\det : GL_n(K) \to K^*$. Pour tout sous-groupe F de K^*, on définit donc un sous-groupe $G' := \det^{-1}(F)$, et tous les sous-groupes de $GL_n(K)$ contenant $SL_n(K)$ s'obtiennent de cette façon. Comme K^* est commutatif, ils sont distingués. Un argument analogue s'applique à la seconde question, avec la signature ε à la place du déterminant. Comme $\operatorname{Im}\varepsilon = \{+1, -1\}$ n'admet comme sous-groupes que $\{+1\}$ et lui-même, les seuls sous-groupes de $\mathfrak{S}_n$ contenant $\mathfrak{A}_n$ sont $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

1.3.3 Le cas d'un groupe commutatif

Dans le cas d'un groupe commutatif G, tout sous-groupe H est distingué et l'on peut former le quotient G/H, qui est commutatif d'après les propriétés d'héritage de la page 7. Pratiquement tous les quotients que nous rencontrerons cette année sont de ce type : cela concerne en particulier les anneaux et les espaces vectoriels (sections suivantes). Décrivons rapidement le mode d'emploi d'un tel quotient; on suppose que les groupes sont notés additivement. Lorsque l'on veut additionner deux éléments quelconques a et b de G/H, on en choisit des *représentants*, c'est à dire des éléments x et y dans G tels que $a = \overline{x}$ et $b = \overline{y}$. On a alors $a + b = \overline{x + y}$. Cette somme ne dépend pas du choix des représentants x, y. Nous avons déjà rencontré deux exemples de tels calculs : le calcul des congruences modulo n (il correspond au cas du sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$; le théorème 18 l'explicite); et le calcul des congruences modulo 2π, pour les arguments de nombres complexes (il correspond au cas du sous-groupe $2\pi\mathbb{Z}$ de $\mathbb{R}$, le groupe quotient étant $\mathbb{R}/2\pi\mathbb{Z}$).

Théorème 18. (i) Soit $n \in \mathbb{N}^*$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les groupes $d\mathbb{Z}/n\mathbb{Z}$, où $d \in \mathbb{N}^*$ est un diviseur de n. Le quotient de $\mathbb{Z}/n\mathbb{Z}$ par $d\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Le nombre de ces sous groupes est donc le nombre de diviseurs de n dans $\mathbb{N}^*$.
(ii) Soit G un groupe cyclique d'ordre n. Pour tout diviseur d de n, G admet un unique sous-groupe H d'ordre d, celui-ci est cyclique ainsi que le quotient G/H. Tous les sous-groupes de G s'obtiennent ainsi. Dans le cas où G est le groupe μ_n des racines $n^{\text{èmes}}$ de l'unité dans $\mathbb{C}$, le sous-groupe d'ordre d est μ_d.

Démonstration. (i) Puisque tous les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $m\mathbb{Z}/n\mathbb{Z}$, où m est un diviseur de n (proposition 16 de la page 12). Selon le théorème 17 de la page précédente, le quotient de $\mathbb{Z}/n\mathbb{Z}$ par $m\mathbb{Z}/n\mathbb{Z}$ s'identifie à $\mathbb{Z}/m\mathbb{Z}$. L'assertion (ii) est alors immédiate. ∎

1.4 Anneaux quotients

Nous ne considérerons que des anneaux commutatifs.

Théorème 19. (i) Soit I un idéal de l'anneau commutatif A. La congruence modulo le sous-groupe I est compatible avec la multiplication de A. Soit réciproquement $\sim$ une relation d'équivalence sur A compatible avec l'addition et la multiplication. Alors la classe de 0 est un idéal I et $\sim$ est la congruence modulo I.
(ii) La loi quotient de la multiplication de I fait alors du groupe quotient $(A/I, +)$ un anneau commutatif. La projection canonique $\pi : A \to A/I$ est un morphisme surjectif d'anneaux, de noyau I.

On dit que l'image $\overline{a} := \pi(a) \in A/I$ s'obtient par *réduction modulo* I de $a \in A$.
Démonstration. Presque tout cet énoncé fait partie du théorème 13 de la page 11.
(i) Notons $\sim$ la congruence modulo l'idéal I. Alors, si $a \sim b$ et si c est quelconque, $a-b \in I \Rightarrow c(a-b) \in I$ (car I est un idéal), donc $ca \sim cb$, ce qui suffit par commutativité. Si $\sim$ est une relation d'équivalence sur A compatible avec l'addition et la multiplication, on sait déjà que la classe I de 0 est un sous-groupe et que $\sim$ est la congruence modulo I. Reste à voir que c'est un idéal. Si $a \in I$ et $c \in A$, alors $a \sim 0 \Rightarrow ca \sim c0 \Rightarrow ca \in I$.
(ii) Les propriétés d'héritage de la de la page 7 entraînent que $(A/I, +, \times)$ est un anneau commutatif, et il est immédiat que π est un morphisme surjectif d'anneaux, de noyau I. ∎

Exemples. Si l'idéal est trivial : $I = 0$ (notation abusive abrégée pour $I := \{0\}$), alors $A/I = A$. Si $I = A$, le quotient est l'anneau trivial 0 (notation abusive abrégée pour $\{0\}$). Si $A = \mathbb{Z}$ et $I = n\mathbb{Z}$ ($n \in \mathbb{N}^*$), le quotient est l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exercice 5.
Décrire tous les anneaux quotients de l'anneau $\mathbb{Z}$ et ceux de l'anneau $K[X]$.
Solution. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$. Les anneaux quotients de $\mathbb{Z}$ sont donc les anneaux de classes de congruence $\mathbb{Z}/n\mathbb{Z}$ (donc $\mathbb{Z}$ si $n = 0$).
De même, les idéaux de $K[X]$ sont tous principaux et de la forme $<P>$, où P est soit 0 soit un polynôme unitaire. Si $P = 0$, l'idéal est nul et le quotient est $K[X]$. Si $P = 1$, l'idéal est $K[X]$ et le quotient est trivial. Supposons que P est de degré n. De la division euclidienne, on déduit que tout polynôme de $K[X]$ est congru modulo P à un unique polynôme de $K_{n-1}[X]$. Comme on le verra à la section 1.5, de la décomposition $K[X] = <P> \oplus K_{n-1}[X]$ ([L1], module sur les polynômes), on peut déduire l'isomorphisme des *espaces vectoriels*, donc des *groupes* $K[X]/<P>$ et $K_{n-1}[X]$ (proposition 28 de la page 17). Cependant, la multiplication dans $K_{n-1}[X]$ doit alors s'effectuer modulo P : pour multiplier A et B selon la loi quotient, on calcule AB puis on prend le reste $AB \mod P$. Ce type de calcul est illustré dans l'exercice 6 de la page suivante.

Théorème 20 (Théorème de factorisation pour les anneaux). Soient I un idéal de A et $\pi : A \to A/I$ la projection canonique. Soit $f : A \to A'$ un morphisme d'anneaux. Alors, pour que I soit inclus dans $\mathrm{Ker}\, f$, il faut, et il suffit, qu'il existe un morphisme d'anneaux : $\overline{f} : A/I \to A'$ tel que $f = \overline{f} \circ \pi$.

Démonstration. On invoque le théorème 14 de la page 11 ; il ne reste qu'à vérifier que $\overline{f}$ est bien un morphisme pour la multiplication, ce qui est facile.

Exemple. L'application $P \mapsto P(\mathrm{i})$ de $\mathbb{R}[X]$ dans $\mathbb{C}$ est un morphisme surjectif d'anneaux. Son noyau contient l'idéal $<X^2+1>$. D'après le théorème, on a donc par passage au quotient un morphisme surjectif d'anneaux $\mathbb{R}[X]/<X^2+1> \to \mathbb{C}$ (voir également l'exercice 6 ci-dessous).

Corollaire 21. Soit $f : A \to B$ un morphisme d'anneaux et soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A et l'on a un morphisme injectif : $A/f^{-1}(J) \to B/J$. En particulier, si $A \subset B$ est un sous-anneau et J un idéal de B, alors $A \cap J$ est un idéal de A et l'on a un morphisme injectif : $A/(A \cap J) \to B/J$.

Démonstration. Le noyau du morphisme composé $A \to B \to B/J$ est l'idéal $f^{-1}(J)$. Si $A \subset B$ et si f est l'inclusion de A dans B, $f^{-1}(J) = A \cap J$.

Théorème 22 (Premier théorème d'isomorphisme pour les anneaux). Soient $f : A \to A'$ un morphisme d'anneaux et $\pi : A \to A/\operatorname{Ker} f$ la projection canonique. Il existe alors un unique morphisme d'anneaux $\overline{f} : A/\operatorname{Ker} f \to A'$ tel que $f = \overline{f} \circ \pi$. Ce morphisme est injectif et induit un isomorphisme de $A/\operatorname{Ker} f$ sur $\operatorname{Im} f$.

Démonstration. On invoque le théorème 15 de la page 12 ; il ne reste qu'à vérifier que $\overline{f}$ est bien un morphisme pour la multiplication, ce qui est facile.

Exercice 6.

Appliquer ce qui précède au morphisme $P \mapsto P(\mathrm{i})$ de $\mathbb{R}[X]$ dans $\mathbb{C}$ et à l'image de $\mathbb{Q}[X]$.

Solution. De la division euclidienne $P = (X^2+1)Q + (a+bX)$, on déduit les équivalences $P(\mathrm{i}) = 0 \Leftrightarrow a + b\mathrm{i} = 0 \Leftrightarrow a = b = 0$. Le noyau est donc l'idéal $<X^2+1>$, d'où un isomorphisme $\mathbb{R}[X]/<X^2+1> \simeq \mathbb{C}$. On peut donc décrire $\mathbb{C}$ comme le groupe $\mathbb{R}_1[X] = \mathbb{R} + \mathbb{R}X$, muni de la multiplication pour laquelle le produit de $a+bX$ et de $c+dX$ est le reste de la division de $(a+bX)(c+dX)$ modulo X^2+1. On vérifie sans peine que ce reste vaut $(ac-bd)+(ad+bc)X$. C'est donc la classe de X modulo X^2+1 qui joue le rôle de i. L'image de $\mathbb{Q}[X]$ est évidemment $\mathbb{Q}[\mathrm{i}]$.

En prenant, dans le corollaire 21, $A := \mathbb{Q}[X]$, $B := \mathbb{R}[X]$ et $J := (X^2+1)\mathbb{R}[X]$, on trouve $A \cap J = (X^2+1)\mathbb{Q}[X]$ (pourquoi ?) et un morphisme injectif

$$\mathbb{Q}[X]/<X^2+1> \to \mathbb{R}[X]/<X^2+1>,$$

qui s'identifie à l'inclusion $\mathbb{Q}[\mathrm{i}] \subset \mathbb{C}$.

Théorème 23 (Deuxième théorème d'isomorphisme pour les anneaux). Soient A un anneau, I un idéal de A et $\pi : A \to A/I$ la projection canonique. La correspondance du théorème 17 de la page 12 établit une bijection entre les idéaux de A contenant I et les idéaux de A/I. Si $J \subset A$ est un idéal contenant I et si $\pi(J) = J/I$ est l'idéal de A/I qui lui correspond, on a un isomorphisme d'anneaux : $\dfrac{A/I}{J/I} \simeq \dfrac{A}{J}$.

Démonstration. Il suffit de vérifier que les constructions correspondantes pour les sous-groupes distingués sont bien compatibles avec la multiplication, ce qui est facile. ∎

Exercice 7.
Décrire les idéaux et les anneaux quotients de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (où $n \in \mathbb{N}$). On détaillera le cas particulier $n := 6$. Décrire de même les idéaux et les anneaux quotients de l'anneau $A := K[X]/<P>$ (où $P \in K[X]$ est un polynôme unitaire de degré $n \in \mathbb{N}^*$). On détaillera le cas $n := 2$ (en admettant que la caractéristique de K n'est pas 2).

Solution. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $m\mathbb{Z}/n\mathbb{Z}$, où m divise n, et les quotients correspondants sont les anneaux $\mathbb{Z}/m\mathbb{Z}$. Par exemple, les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont tous ses sous-groupes : $1\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, $3\mathbb{Z}/6\mathbb{Z}$ et $6\mathbb{Z}/6\mathbb{Z} = \{0\}$; et les anneaux quotients correspondants sont les anneaux $\mathbb{Z}/1\mathbb{Z} = \{0\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

Les idéaux de A sont les $<Q>/<P>$, où Q est un polynôme unitaire qui divise P, et les quotients correspondants sont les $K[X]/<Q>$. Si $P = X^2 + pX + q$, les diviseurs $Q = 1$ et $Q = P$ donnent respectivement les idéaux $K[X]/<P> = A$ et $<P>/<P> = 0$, et les quotients correspondants sont 0 et A. Pour d'éventuels autres idéaux et quotients, une discussion est nécessaire :

1. Si $\Delta := p^2 - 4q$ n'est pas un carré dans K, le polynôme P est irréductible et A n'admet pas d'autre idéal que 0 et lui-même. Nous verrons plus loin qu'en fait, A est un corps (exemple de la page 20).
2. Si $\Delta = 0$, P admet pour seul diviseur unitaire non trivial $X + p/2$, et A admet un seul idéal autre que 0 et lui-même.
3. Si Δ est un carré non nul, $P = (X - a)(X - b)$ avec $a \neq b$ et l'anneau A admet deux idéaux et deux quotients non triviaux. De plus, comme aucun des deux facteurs de P ne divise l'autre, ces deux idéaux ne sont pas contenus l'un dans l'autre. Nous verrons plus loin que A est le produit de deux corps (exercice I.1.25 de la page 53).

1.5 Espaces vectoriels quotients

Théorème et définition 24. Soit W un sous–espace vectoriel d'un K-espace vectoriel V. Le groupe V/W admet une unique structure d'espace vectoriel telle que l'application $\pi : V \to V/W$ soit linéaire. On définit ainsi *l'espace vectoriel quotient* V/W et la *projection canonique* π.

Démonstration. Puisque l'on veut avoir $\forall x \in V\ ,\ \pi(\lambda x) = \lambda\pi(x)$, on doit définir la loi externe sur V/W en posant $\lambda a := \overline{\lambda x}$, où $x \in V$ est un représentant de a. D'après les

implications : $x \sim x' \Rightarrow x - x' \in W \Rightarrow \lambda x - \lambda x' \in W \Rightarrow \lambda x \sim \lambda x'$, la relation $\sim$ sur V est *compatible avec la loi externe* et cette définition ne dépend pas du choix du représentant x de a. On vérifie sans peine que l'on obtient bien un espace vectoriel. Les règles de calcul y sont donc les suivantes : $\overline{x} + \overline{y} = \overline{x+y}$ et $\lambda\overline{x} = \overline{\lambda x}$. ∎

Comme dans le cas des anneaux, les principaux théorèmes concernant les quotients de groupes s'étendent facilement au cas des espaces vectoriels. Il s'agit simplement de vérifier chaque fois des compatibilités avec la loi externe, comme nous venons de le faire. Nous ne détaillerons donc pas la démonstration des théorèmes qui suivent, laissant ce soin au lecteur.

Théorème 25 (Théorème de factorisation pour les espaces vectoriels). Soient $W \subset V$ un sous–espace vectoriel et $\pi : V \to V/W$ la projection canonique. Soit $f : V \to V'$ une application linéaire. Alors, pour que W soit inclus dans $\operatorname{Ker} f$, il faut, et il suffit, qu'il existe une application linéaire : $\overline{f} : V/W \to V'$ telle que $f = \overline{f} \circ \pi$.

Ce théorème admet une utile généralisation que nous détaillerons (une fois n'est pas coutume). Soit $f : V \to V'$ une application linéaire et soient $W \subset V$ et $W' \subset V'$ des sous-espaces vectoriels tels que $f(W) \subset W'$. Si $x, x' \in V$ sont deux représentants de $a \in V/W$, on vérifie aisément que $f(x) - f(x') \in W'$. En posant $\overline{f}(\overline{x}) := \overline{f(x)}$, on définit donc sans ambiguïté une application linéaire $\overline{f} : V/W \to V'/W'$ (*application induite par passage au quotient*). En particulier, *si f est un endomorphisme de V et W un sous-espace stable par f, on obtient ainsi un endomorphisme $\overline{f}$ de V/W.*

Théorème 26 (Premier théorème d'isomorphisme pour les espaces vectoriels). Soit $f : V \to V'$ une application linéaire. Le morphisme de groupes $\overline{f} : V/\operatorname{Ker} f \to V'$ (théorème 15 de la page 12) est linéaire. En particulier, les espaces vectoriels $V/\operatorname{Ker} f$ et $\operatorname{Im} f$ sont isomorphes.

Théorème 27 (Deuxième théorème d'isomorphisme pour les espaces vectoriels). Soient $G \subset F \subset E$ des sous-espaces vectoriels. L'isomorphisme de groupes $\dfrac{E/G}{F/G} \simeq \dfrac{E}{F}$ (théorème 17 de la page 12) est linéaire, donc un isomorphisme d'espaces vectoriels.

Voir aussi le troisième théorème d'isomorphisme pour les espaces vectoriels à l'exercice I.1.18 de la page 52.

1.5.1 Quotients et supplémentaires

Proposition 28. Soit W' un supplémentaire de W dans V. Alors la restriction à W' de l'application $\pi : V \to V/W$ est un isomorphisme.

Démonstration. Le noyau de $\pi_{|W'}$ est $W' \cap \operatorname{Ker} \pi = W' \cap W = \{0\}$. Son image est le sous-espace $\operatorname{Im} \pi_{|W'} = \pi(W') = \pi(W) + \pi(W') = \pi(W + W') = \pi(V) = V/W$. ∎

On obtient ainsi une nouvelle preuve du fait que tous les supplémentaires de W sont isomorphes entre eux (*cf.* [L1]). On peut d'ailleurs vérifier que l'isomorphisme entre deux supplémentaires obtenu par l'une ou l'autre méthode est le même.

Définition 4. On appelle *codimension* du sous–espace vectoriel W de V, et l'on note $\operatorname{codim}_V W$ la dimension (si elle existe) du quotient V/W. On dit alors que W est *de codimension finie dans* V.

La codimension de W est relative à l'espace ambiant V, et il est absolument nécessaire d'indiquer celui-ci dans la notation. Bien sûr, la codimension dépend également du corps de base, mais la notation ci-dessus ne le mentionne pas : il faudra donc si nécessaire indiquer soigneusement le corps de référence pour éviter les ambiguïtés.

De nombreuses propriétés des sous-espaces vectoriels d'un espace vectoriel de dimension finie s'étendent à des sous-espaces vectoriels de codimension finie d'un espace vectoriel quelconque, et cela aura son utilité en analyse. En voici un échantillon. D'après ce qui précède, la codimension de W est égale à la dimension de l'un quelconque de ses supplémentaires ; par exemple, les sous-espaces vectoriels de codimension 1 sont les hyperplans. Soient W_1 et W_2 deux sous-espaces vectoriels de codimension finie de V. Alors $W_1 \cap W_2$ est de codimension finie et l'on a l'inégalité : $\operatorname{codim}_V(W_1 \cap W_2) \leqslant \operatorname{codim}_V W_1 + \operatorname{codim}_V W_2$ (notant π_1, π_2 les projections canoniques de V sur $V/W_1, V/W_2$, le noyau de l'application linéaire $(\pi_1, \pi_2) : V \to V/W_1 \times V/W_2$ est en effet $W_1 \cap W_2$). L'intersection de k hyperplans est donc un sous–espace vectoriel de codimension inférieure ou égale à k. Sa codimension est exactement k si, et seulement si, des formes linéaires définissant ces hyperplans sont linéairement indépendantes (exercice I.1.20 de la page 52).

Proposition 29. Soit $f : V \to V'$ une application linéaire.
(i) Le noyau $\operatorname{Ker} f$ est de codimension finie si, et seulement si, $\operatorname{Im} f$ est de dimension finie et, dans ce cas : $\operatorname{codim}_V(\operatorname{Ker} f) = \dim(\operatorname{Im} f)$.
(ii) Si V' est de dimension finie, $\operatorname{Ker} f$ est de codimension finie et $\operatorname{codim}_V(\operatorname{Ker} f) \leqslant \dim V'$, avec égalité si, et seulement si, f est surjective.

Démonstration. Cela découle du théorème 26 de la page précédente. ∎

2 Anneaux commutatifs

2.1 Idéaux

Nous rappelons ou introduisons ici quelques constructions utiles. Le lecteur pourra s'exercer à leur application à l'aide de l'exercice I.1.22 de la page 52. Rappelons que l'on note $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$ ($p \in \mathbb{N}$ premier). Soit A un anneau commutatif.

1. L'idéal engendré par une partie $X \subset A$ est, par définition, le plus petit idéal de A contenant X, c'est-à-dire l'intersection des idéaux de A contenant X. Il est égal à l'ensemble $\{\sum a_k x_k \mid \forall k\ ,\ a_k \in A, x_k \in X\}$ des combinaisons linéaires d'éléments de X à coefficients dans A. Par exemple, l'idéal engendré par $\bigcup I_k$ est $\sum I_k$.
2. Soient I et J deux idéaux de A. Alors $I \cap J$ est un idéal de A, ainsi que $I + J := \{i + j \mid i \in I, j \in J\}$. Plus généralement, si (I_k) est une famille d'idéaux,

l'intersection $\bigcap I_k$ et la somme $\sum I_k$ sont des idéaux ; cette dernière est l'ensemble des sommes $\sum i_k$ de familles (i_k) à support fini et telles que $\forall k\ ,\ i_k \in I_k$. On note IJ l'idéal engendré par $\{ij \mid i \in I, j \in J\}$ (*produit* des idéaux I et J). On a : $IJ = \{\sum i_k j_k \mid \forall k\ ,\ i_k \in I, j_k \in J\}$. On vérifie facilement que $IJ \subset I \cap J$. La multiplication des idéaux est commutative, associative et admet pour élément neutre A ; elle est distributive par rapport à l'addition. Les puissances d'un idéal forment une suite décroissante : $I^0 = A \supset I^1 = I \supset \cdots \supset I^n \supset \cdots$

3. Si A est un sous-anneau de B et I un idéal de A, l'idéal de B engendré par I est $IB = \{\sum i_k b_k \mid \forall k\ ,\ i_k \in I, b_k \in B\}$.
4. L'image $\overline{J}$ de l'idéal J dans l'anneau quotient $\overline{A} := A/I$ est un idéal de $\overline{A}$. Le morphisme composé $A \to \overline{A} \to \overline{A}/\overline{J}$ est surjectif, de noyau $I + J$, d'où un isomorphisme : $\overline{A}/\overline{J} \simeq A/(I + J)$. Retenons le principe : pour quotienter l'anneau A par $I + J$, on peut quotienter successivement par I puis par (l'image de) J.

Exercice 8.
Quels sont les idéaux d'un corps commutatif K ? Réciproque ?
Solution. Les seuls idéaux d'un corps K sont 0 et K. En effet, soit I un idéal non nul, et soit $x \in I \setminus \{0\}$. Alors $1 = x^{-1}x \in I$; or, le seul idéal d'un anneau qui contienne 1 est l'anneau tout entier. Supposons réciproquement que l'anneau K n'a pour idéaux que 0 et lui-même. Soit $x \in K \setminus \{0\}$. L'idéal principal Kx est non nul, donc égal à K, donc il contient 1, donc x est inversible : l'anneau K est un corps.

2.1.1 Idéaux maximaux et idéaux premiers

Rappelons qu'un anneau est dit *trivial* s'il ne contient qu'un élément, et que cela équivaut à $1 = 0$. Par convention, les anneaux intègres (et en particulier les corps) sont non triviaux. Il découlera donc des définitions ci-dessous que l'idéal A de l'anneau A n'est ni maximal ni premier.
Un idéal *propre* de l'anneau commutatif A est un idéal I de A distinct de A. Il revient au même de dire que I ne contient pas 1, ou qu'il ne contient aucun élément inversible. Les idéaux propres I sont ceux tels que l'anneau quotient A/I est non trivial.

Théorème et définition 30. On dit qu'un idéal I de A est *maximal* s'il possède les propriétés équivalentes suivantes :
(i) L'idéal I est maximal pour l'inclusion parmi les idéaux propres de A.
(ii) L'idéal I est propre et, pour tout $x \in A \setminus I$, l'idéal $I + Ax$ est égal à A.
(iii) L'anneau quotient A/I est un corps.

Démonstration. Si I est maximal et si $x \in A \setminus I$, l'idéal $I + Ax$ contient strictement I, donc il est égal à A (par maximalité). Supposons que, pour tout $x \in A \setminus I$, l'idéal $I + Ax$ est égal à A. Soit $\overline{x}$ un élément non nul de l'anneau quotient A/I. Alors $x \in A \setminus I$, et, par hypothèse, il existe $a \in A$ et $i \in I$ tels que $i + ax = 1$, ce qui entraîne que $\overline{ax} = 1$ dans A/I. Ainsi, tout élément non nul de A/I est inversible et cet anneau est un corps.

Supposons enfin que A/I soit un corps. Ses seuls idéaux sont donc 0 et lui-même. D'après le théorème 23 de la page 16, il y a une bijection entre les idéaux de A contenant I et les idéaux de A/I : le seul idéal propre de A contenant I est donc I lui-même. ∎

Corollaire 31. L'idéal 0 est maximal si, et seulement si, A est un corps. Les idéaux maximaux de A/I sont les $\mathfrak{M}/I$, où $\mathfrak{M}$ est un idéal maximal de A contenant I.

Exemples.

1. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ ($n \in \mathbb{N}$) et $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m|n$. Les idéaux maximaux de $\mathbb{Z}$ sont donc les $p\mathbb{Z}$, p premier. Les anneaux quotients correspondants sont les corps finis $\mathbb{F}_p$. Soit $m \in \mathbb{N} \setminus \{0,1\}$. Les idéaux maximaux de $\mathbb{Z}/m\mathbb{Z}$ sont les $p\mathbb{Z}/m\mathbb{Z}$, p premier divisant m. Les quotients correspondants sont les $\mathbb{F}_p$.
2. Les idéaux non nuls de $K[X]$ sont de la forme $<P>$ (P unitaire) et $<P> \subset <Q> \Leftrightarrow Q|P$. Les idéaux maximaux de $K[X]$ sont donc les $<P>$, P irréductible. L'anneau quotient $K[X]/<P>$ est alors une extension de K de degré $n := \deg P$, c'est-à-dire un corps L tel que $K \subset L$ et $\dim_K L = n$. Soit Q un polynôme unitaire. Les idéaux maximaux de $K[X]/<Q>$ sont les $<P>/<Q>$, P irréductible divisant Q. Les quotients correspondants sont les $K[X]/<P>$.
3. Soit $A = \mathcal{F}(E,K)$ l'anneau des applications d'un ensemble E non vide dans le corps K. Pour tout $x \in E$, l'application $f \mapsto f(x)$ est un morphisme surjectif d'anneaux de A sur K. Son noyau est l'idéal $\mathfrak{M}_x$ des applications nulles en x. D'après le premier théorème d'isomorphisme, on a : $A/\mathfrak{M}_x \simeq K$, et $\mathfrak{M}_x$ est maximal.

Théorème 32 (Théorème de Krull). Soit A un anneau et soit I un idéal propre de A. Alors I est contenu dans un idéal maximal.

Démonstration. Considérons l'ensemble E dont les éléments sont les idéaux propres de A, ordonné par inclusion. Cet ensemble est inductif ([L1], module « Fondements »). En effet, si (I_k) est une famille totalement ordonnée d'idéaux propres, il est clair que $\bigcup I_k$ est un idéal ; de plus, aucun des I_k ne contient 1, donc $\bigcup I_k$ non plus. D'après le lemme de Zorn (*cf.* [L1]), tout élément de E est donc majoré par un élément maximal. ∎

Théorème et définition 33. On appelle *idéal premier* de A un idéal propre I possédant les propriétés équivalentes suivantes :
(i) On a l'implication : $\forall x, y \in A\ ,\ xy \in I \Rightarrow x \in I \quad$ ou $\quad y \in I$.
(ii) L'anneau quotient A/I est intègre.

Démonstration. Notons $\overline{x}$ la classe de $x \in A$ dans $\overline{A} := A/I$, alors $\overline{x} = 0 \Leftrightarrow x \in I$; et tous les éléments de $\overline{A}$ sont de la forme $\overline{x}$, $x \in A$. L'implication de la définition se réécrit donc : $\forall \overline{x}, \overline{y} \in \overline{A}\ ,\ \overline{x}\,\overline{y} = 0 \Rightarrow \overline{x} = 0 \quad$ ou $\quad \overline{y} = 0$, ce qui caractérise l'intégrité de $\overline{A}$. ∎

Exemples. Les idéaux premiers de $\mathbb{Z}$ sont 0 et les $p\mathbb{Z}$, p premier.
Les idéaux premiers de $K[X]$ sont 0 et les $<P>$, P irréductible.

Corollaire 34. Tout idéal maximal est premier. Tout anneau non trivial admet donc des idéaux premiers. L'idéal 0 de A est premier si, et seulement si, A est intègre. Les idéaux premiers de A/I sont les idéaux $\mathcal{P}/I$, où $\mathcal{P}$ est un idéal premier de A.

Exercice 9.
Montrer que les éléments nilpotents de A forment un idéal et que celui-ci est contenu dans l'intersection des idéaux premiers de A.

Solution. Si x est nilpotent, il est évident que ax l'est quel que soit a (car, l'anneau étant commutatif, on a $(ax)^n = a^n x^n$). D'autre part, si $x^n = y^m = 0$, on déduit de la formule du binôme de Newton que $(x+y)^{m+n-1} = 0$ (dans chacun des termes $x^i y^j$ avec $i + j = m + n - 1$, on a $i \geqslant n$ ou $j \geqslant m$). On a donc bien un idéal (appelé *radical* ou *nilradical* de A). Si $x^m = 0$ et si $\mathcal{P}$ est un idéal premier, alors $\overline{x}$ est nilpotent dans l'anneau intègre $A/\mathcal{P}$, donc nul, et $x \in \mathcal{P}$ (voir également l'exercice I.1.31 de la page 53).

Proposition 35. Soient $f : A \to B$ un morphisme d'anneaux et $\mathcal{Q} \subset B$ un idéal premier. Alors $f^{-1}(\mathcal{Q})$ est un idéal premier de A. Si par exemple $A \subset B$, pour tout idéal premier $\mathcal{Q}$ de B, l'idéal $\mathcal{P} := \mathcal{Q} \cap A$ est premier.

Démonstration. L'idéal $\mathcal{P} := f^{-1}(\mathcal{Q})$ est le noyau du morphisme composé $A \to B \to B/\mathcal{Q}$, d'où une injection de $A/\mathcal{P}$ dans l'anneau intègre $B/\mathcal{Q}$ ∎

La proposition ne se transpose pas aux idéaux maximaux : 0 est un idéal maximal de $\mathbb{Q}$, mais son intersection avec $\mathbb{Z}$ n'est pas un idéal maximal de $\mathbb{Z}$.

2.1.2 Idéaux étrangers, théorème chinois

Définition 5. On dit que les idéaux I et J sont *étrangers* si $I + J = A$, autrement dit, s'il existe $i \in I$ et $j \in J$ tels que $i + j = 1$. On dit aussi que I *est étranger à* J.

Exemples.

1. Tout idéal est étranger à A. Le seul idéal étranger à lui-même est A. Un idéal maximal est étranger à tout idéal qu'il ne contient pas ; deux idéaux maximaux distincts sont étrangers.
2. Dans l'anneau $\mathbb{Z}$, les idéaux $m\mathbb{Z}$ et $n\mathbb{Z}$ sont étrangers si, et seulement si, m et n sont premiers entre eux (théorème de Bézout dans $\mathbb{Z}$).
3. Dans l'anneau $K[X]$, les idéaux $<P>$ et $<Q>$ sont étrangers si, et seulement si, P et Q sont premiers entre eux (théorème de Bézout dans $K[X]$).

Proposition 36. Si I est étranger à J et à K, alors I est étranger à JK. En particulier, si I et J sont étrangers, I^m et J^n sont étrangers pour $m, n \in \mathbb{N}$.

Démonstration. On a $i_1 + j = 1$ et $i_2 + k = 1$, avec $i_1, i_2 \in I$, $j \in J$ et $k \in K$.
Alors $i + jk = 1$, où $i := i_1 i_2 + i_1 k + i_2 j \in I$ et $jk \in JK$.
La deuxième assertion s'ensuit par récurrence sur m et n. ∎

Théorème 37 (Théorème chinois).
Soient I et J deux idéaux étrangers de l'anneau A.
Le morphisme d'anneaux $x \mapsto (x \mod I, x \mod J)$ de A dans $(A/I) \times (A/J)$ est surjectif de noyau $I \cap J$. On obtient par passage au quotient un isomorphisme : $A/(I \cap J) \to (A/I) \times (A/J)$. On a de plus l'égalité $I \cap J = IJ$.

Démonstration. Soient $i \in I$ et $j \in J$ tels que $i + j = 1$.
Tout élément de $(A/I) \times (A/J)$ est de la forme $(a \mod I, b \mod J)$, où $a, b \in A$. L'élément $x = aj + bi$ est tel que $x - a = (b - a)i \in I$ et $x - b = (a - b)j \in J$, d'où $(x \mod I, x \mod J) = (a \mod I, b \mod J)$, ce qui prouve la surjectivité. L'élément x est dans le noyau si, et seulement si, $(x \mod I, x \mod J) = (0, 0)$, c'est-à-dire si, et seulement si, $x \in I$ et $x \in J$. Le noyau est donc $I \cap J$. On applique alors le premier théorème d'isomorphisme. L'inclusion $IJ \subset I \cap J$ est vraie pour des idéaux quelconques. Soit $x \in I \cap J$; alors $xi \in IJ$ et $xj \in IJ$, d'où $x = xi + xj \in IJ$. ∎

Corollaire 38. Soient $I_1, \ldots, I_k$ des idéaux étrangers deux à deux.
On a alors un isomorphisme : $A/(I_1 \cap \cdots \cap I_k) \to A/I_1 \times \cdots \times A/I_k$ et une égalité : $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$.

Démonstration. Pour $k = 2$, c'est le théorème ; on passe de $k - 1$ à k en remarquant que I_k est étranger à $I_1 \cap \cdots \cap I_{k-1} = I_1 \cdots I_{k-1}$ (proposition 36 de la page précédente). ∎

Réciproquement, si le morphisme $A \to (A/I) \times (A/J)$ est surjectif, soit i un antécédent de $(0, 1)$: alors $i \in I$ et $i - 1 \in J$, d'où $1 \in I + J$, et I et J sont étrangers.

2.2 Polynômes sur un anneau commutatif

On fixe un anneau commutatif A. Soit B une *extension* de A, c'est-à-dire un anneau commutatif dont A est un sous-anneau. Pour tout élément x de B, le *sous-anneau de B engendré par A et x* (ou encore *engendré sur A par x*) est, par définition, le plus petit sous-anneau de B contenant A et x, ou encore l'intersection des sous-anneaux de B contenant A et x. On le note parfois $A[x]$, mais on prendra garde à l'ambiguïté de cette notation (qui sous-entend l'extension B). L'anneau $A[x]$ contient évidemment toutes les expressions de la forme $\sum_{i \geqslant 0} a_i x^i$, où la suite $(a_i)_{i \in \mathbb{N}}$ de $A^{\mathbb{N}}$ est à support fini (*expressions polynomiales en x à coefficients dans A*). Par ailleurs, l'ensemble de ces expressions forme clairement un sous-anneau de B contenant A et x, et l'on a donc : $A[x] = \left\{ \sum_{i \geqslant 0} a_i x^i \;\middle|\; (a_i)_{i \in \mathbb{N}} \in A^{(\mathbb{N})} \right\}$.

Exemple. Dans l'extension $\mathbb{C}$ de $\mathbb{Z}$, le sous-anneau engendré par $\mathbb{Z}$ et i est l'anneau $\mathbb{Z}[\mathrm{i}]$ des entiers de Gauß. Naturellement, un élément de $\mathbb{Z}[\mathrm{i}]$ admet de nombreuses écritures comme expression polynomiale en i à coefficients dans $\mathbb{Z}$: par exemple, $0 = 1 + \mathrm{i}^2 = 1 - \mathrm{i}^4 = \cdots$

Théorème et définition 39. Il existe une extension B de A et un élément X de B tels que tout élément b de B admet une écriture *unique* : $b = \sum_{i\geqslant 0} a_i X^i$, où la suite $(a_i)_{i\in\mathbb{N}}$ de $A^{\mathbb{N}}$ est à support fini. L'anneau B est appelé *anneau des polynômes à coefficients dans A en l'indéterminée X* et on le note $A[X]$. On dit que l'anneau $A[X]$ est *librement engendré sur A par X*.

Démonstration. Nous plagions la construction de l'anneau des polynômes sur un corps. On pose $B = A^{(\mathbb{N})}$, que l'on munit de la loi de groupe produit, qui est commutative, et de la multiplication : $(a_i)_{i\in\mathbb{N}}(b_i)_{i\in\mathbb{N}} = (c_i)_{i\in\mathbb{N}}$, où : $\forall n \in \mathbb{N}\ ,\ c_n := \sum_{i+j=n} a_i b_j$.
On a bien un anneau, l'élément neutre de la multiplication étant la suite $(1, 0, \ldots)$.
Si l'on pose $X := (0, 1, 0, \ldots)$, on vérifie que $(a_i)_{i\in\mathbb{N}} = \sum_{i\geqslant 0} a_i X^i$, et que c'est bien l'unique écriture de $(a_i)_{i\in\mathbb{N}}$ comme expression polynomiale en X à coefficients dans A. ∎

Lorsque A est un corps, on retrouve la définition de [L1]. On vérifie facilement les faits suivants : si A est un sous-anneau de B, $A[X]$ est un sous-anneau de $B[X]$; si $f : A \to B$ est un morphisme d'anneaux, l'application $\sum_{i\geqslant 0} a_i X^i \mapsto \sum_{i\geqslant 0} f(a_i) X^i$ est un morphisme d'anneaux de $A[X]$ dans $B[X]$.

2.2.1 Règles de calcul

Définition 6. Le *degré* d'un polynôme non nul $P := \sum_{i\geqslant 0} a_i X^i$ est l'entier

$$\deg P := \max\{i \in \mathbb{N} \mid a_i \neq 0\}.$$

Par convention, le degré du polynôme nul est $\deg 0 := -\infty$.
Le *coefficient dominant* et le *terme dominant* du polynôme $P := \sum_{i\geqslant 0} a_i X^i$ de degré $n \geqslant 0$ sont respectivement $\mathrm{cd}(P) := a_n$ et $\mathrm{td}(P) := a_n X^n$.

Pour tous $P, Q \in A[X]$, on a $\deg(P + Q) \leqslant \max(\deg P, \deg Q)$, avec égalité si, et seulement si, les termes dominants ne s'annulent pas, par exemple si $\deg P \neq \deg Q$.
En revanche, l'égalité $\deg PQ = \deg P + \deg Q$ ne va pas de soi si A n'est pas intègre, comme le montre l'exemple qui suit.

Exercice 10.
Étudier l'exemple des polynômes $P := \overline{2}X + \overline{1}$ et $Q := \overline{3}X + \overline{1}$ sur $\mathbb{Z}/6\mathbb{Z}$. Montrer que, dans l'anneau $\mathbb{Z}/4\mathbb{Z}[X]$, le polynôme non constant $\overline{1} + \overline{2}X$ est inversible.
Solution. On a $\overline{2} + \overline{3} = -\overline{1}$ et $\overline{2}.\overline{3} = \overline{0}$, d'où $PQ = -X + \overline{1}$, de degré $1 < 1 + 1$.
Dans $\mathbb{Z}/4\mathbb{Z}[X]$, le polynôme $\overline{1} + \overline{2}X$ est son propre inverse car :

$$(\overline{1} + \overline{2}X)^2 = \overline{1} + \overline{4}X + \overline{4}X^2 = \overline{1}.$$

Pour abréger les écritures, nous adopterons fréquemment la convention suivante : si P est un polynôme non nul, la notation $P = aX^m + \cdots$ signifie que $aX^m = \mathrm{td}(P)$; ainsi, $a \neq 0$ et les points $\cdots$ désignent « des termes de degré strictement inférieur ».

Lemme 40. Si $\mathrm{cd}(P)$ ou $\mathrm{cd}(Q)$ n'est pas diviseur de 0 dans A, alors on a les règles : $\deg(PQ) = \deg(P) + \deg(Q)$, $\mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q)$ et $\mathrm{td}(PQ) = \mathrm{td}(P)\,\mathrm{td}(Q)$.

Démonstration. Écrivons $P = aX^m + \cdots$ et $Q = bX^n + \cdots$ (donc $a, b \neq 0$).
Alors $ab \neq 0$ (hypothèse sur a et b) et $PQ = abX^{m+n} + \cdots$ ∎

Proposition 41.
Supposons l'anneau A intègre ; alors $A[X]$ l'est également. On a les règles :
$\deg(PQ) = \deg(P) + \deg(Q), \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q)$ et $\mathrm{td}(PQ) = \mathrm{td}(P)\,\mathrm{td}(Q)$.
En particulier, si un polynôme P divise un polynôme R tel que $\deg R < \deg P$, alors $R = 0$. Les éléments inversibles de $A[X]$ sont les polynômes constants $a \in A^*$ (*i.e.* les éléments inversibles de A).

Démonstration. On peut invoquer, au choix, le lemme ou bien le fait que $A[X]$ est un sous-anneau de $K[X]$, où K est le corps des fractions de A. ∎

Proposition 42. Si L est le corps des fractions de l'anneau commutatif intègre A, alors $L(X)$ est le corps des fractions de $A[X]$.

Démonstration. Puisque $A[X]$ est un sous-anneau du corps $L(X)$, il suffit de voir que tout élément de $L(X)$ est quotient de deux éléments de $A[X]$, ce qui est facile et laissé au lecteur. ∎

Proposition 43.
(i) Soit P un polynôme de terme dominant aX^n ($a \in A \setminus \{0\}$, $n \in \mathbb{N}$). Pour tout polynôme $F \in A[X]$, il existe alors un entier k et des polynômes Q et R tels que :

$$a^k F = PQ + R \quad \text{et} \quad \deg R < \deg P.$$

(ii) Si l'on suppose de plus $a = \mathrm{cd}(P)$ inversible, il existe des polynômes uniques Q et R tels que $F = PQ + R$ et $\deg R < \deg P$.

Démonstration.
(i) Si $\deg F < \deg P$, on peut prendre $k := 0$, $Q := 0$ et $R := F$. Si $\deg F \geqslant \deg P$, on écrit $\mathrm{td}\, F = bX^p$ et l'on introduit le polynôme $F_1 := aF - bX^{p-n}P$, qui est de degré strictement inférieur à p ; on peut alors itérer le procédé. On voit même que k peut être choisi égal à $\deg F - \deg P + 1$.
(ii) L'existence découle de (i) et d'une division par a^k. Supposons $PQ + R = PQ_1 + R_1$, avec $\deg R, \deg R_1 < \deg P$. Alors le lemme 40, appliqué à l'égalité $P(Q - Q_1) = R_1 - R$ entraîne (par contraposée) $Q - Q_1 = R_1 - R = 0$. ∎

Exemple. Prenons $A := \mathbb{Z}$, $P := 2X + 1$ et $F := X^3 + X^2 + X + 1$. Alors :
$F_1 := 2F - X^2P = X^2 + 2X + 2$, $F_2 := 2F_1 - XP = 3X + 4$ et $F_3 := 2F_2 - 3P = 5$.
Finalement :

$$\begin{aligned} 8F = 4X^2P + 4F_1 &= 4X^2P + 2XP + 2F_2 \\ &= 4X^2P + 2XP + 3P + F_3 = (4X^2 + 2X + 3)P + 5. \end{aligned}$$

2.2.2 Idéaux de $A[X]$

Commençons par une motivation pour l'étude des idéaux de $A[X]$.

Exemple. L'application $\sum_{n\geqslant 0} a_n X^n \mapsto \sum_{n\geqslant 0} a_n \mathrm{i}^n$ est un morphisme surjectif de l'anneau des polynômes $\mathbb{Z}[X]$ sur l'anneau des entiers de Gauß $\mathbb{Z}[\mathrm{i}]$. Déterminons son noyau. Pour tout polynôme $P \in \mathbb{Z}[X]$, on peut écrire $P = (X^2 + 1)Q + (aX + b)$ avec $Q \in \mathbb{Z}[X]$ et $a, b \in \mathbb{Z}$ (proposition 43 de la page précédente). Alors P est dans le noyau, *i.e.* $P(\mathrm{i}) = 0$, si, et seulement si, $a\mathrm{i}+b = 0$, c'est-à-dire $a = b = 0$. Le noyau est donc l'idéal $<X^2+1>$ de $\mathbb{Z}[X]$, et, d'après le premier théorème d'isomorphisme : $\mathbb{Z}[X]/<X^2 + 1> \simeq \mathbb{Z}[\mathrm{i}]$.

Exercice 11.

Décrire de manière analogue l'extension $\mathbb{Z}[j]$ de $\mathbb{Z}$ engendrée par $j := \dfrac{-1 + \mathrm{i}\sqrt{3}}{2}$.

Solution. L'application $\sum_{n\geqslant 0} a_n X^n \mapsto \sum_{n\geqslant 0} a_n j^n$ est un morphisme surjectif de l'anneau des polynômes $\mathbb{Z}[X]$ sur l'anneau $\mathbb{Z}[j]$. On sait que $j^2 + j + 1 = 0$. On écrit donc un élément quelconque de $\mathbb{Z}[X]$ sous la forme $P = (X^2 + X + 1)Q + (aX + b)$ avec $Q \in \mathbb{Z}[X]$ et $a, b \in \mathbb{Z}$ (proposition 43 de la page ci-contre), et l'on a $P(j) = 0$, si, et seulement si, $aj + b = 0$, c'est-à-dire $a = b = 0$. Le noyau est donc l'idéal $<X^2 + X + 1>$ de $\mathbb{Z}[X]$, et, d'après le premier théorème d'isomorphisme : $\mathbb{Z}[X]/<X^2 + X + 1> \simeq \mathbb{Z}[j]$.

Exercice 12.

Soit $d \in \mathbb{Z}$ un entier qui n'est pas un carré. Si $d < 0$, on note $\sqrt{d} := \mathrm{i}\sqrt{-d}$.
Décrire l'extension $\mathbb{Z}[\sqrt{d}]$ de $\mathbb{Z}$ comme un quotient de $\mathbb{Z}[X]$.

Solution.

Raisonnement analogue : tout polynôme de $\mathbb{Z}[X]$ s'écrit $P = (X^2 - d)Q + (aX + b)$ avec $Q \in \mathbb{Z}[X]$ et $a, b \in \mathbb{Z}$, et l'on a $P(\sqrt{d}) = 0$, si, et seulement si, $a\sqrt{d} + b = 0$, c'est-à-dire $a = b = 0$. Ce dernier point mérite d'être détaillé. Si $d < 0$, il est évident ; sinon, on observe que, si d était le carré d'un élément de $\mathbb{Q}$, il serait le carré d'un élément de $\mathbb{Z}$ (cela a été démontré dans le [L1], exercices sur les polynômes : « $\mathbb{Z}$ est intégralement clos »). En fin de compte : $\mathbb{Z}[X]/<X^2 - d> \simeq \mathbb{Z}[\sqrt{d}]$.

Proposition 44. (i) Pour tout idéal I de A, l'idéal $IA[X]$ de $A[X]$ engendré par I est $\{\sum i_k X^k \mid \forall k\ ,\ i_k \in I\}$. C'est le noyau du morphisme surjectif $A[X] \to A/I[X]$, d'où un isomorphisme : $A/I[X] \simeq A[X]/IA[X]$.
(ii) L'idéal $IA[X]$ est premier si, et seulement si, l'idéal I est premier.

Démonstration. (i) La preuve est mécanique et laissée à la patience du lecteur.
(ii) Si $A/I[X] \simeq A[X]/IA[X]$ est intègre, son sous-anneau A/I est évidemment intègre ; la réciproque est vraie en vertu de la proposition 41 de la page 24. ∎

Pratiquement, la *réduction modulo* $IA[X]$ *d'un polynôme* $P \in A[X]$ se calcule en réduisant modulo I les coefficients de P.

Exercice 13.
Décrire de deux manières le quotient $\mathbb{Z}[X]/<2, X^2+1>$. L'idéal $<2>$ de l'anneau $\mathbb{Z}$[i] est-il premier ?
Solution.
L'anneau $\mathbb{Z}[X]/<2, X^2+1>$ est isomorphe à $\mathbb{F}_2[X]/<X^2+1> = \mathbb{F}_2[X]/<(X+1)^2>$, et aussi à $\mathbb{Z}$[i]$/<2>$. Notons x la classe de X dans $\mathbb{F}_2[X]/<(X+1)^2>$. L'élément $x+1$ est nilpotent non nul, et cet anneau n'est donc pas intègre, donc $\mathbb{Z}$[i]$/<2>$ non plus. L'idéal $<2>$ de $\mathbb{Z}$[i] n'est donc pas premier.

---

3 Algèbres sur un corps commutatif

Définition 7. On suppose V muni des deux structures suivantes : d'une part, $(V, +, .)$ est un K-espace vectoriel ; d'autre part, $(V, +, \star)$ est un anneau (l'addition $+$ est la même dans les deux cas). On dit que l'on a ainsi muni V d'une structure d'*algèbre sur* K, ou encore de K*-algèbre*, si les deux lois de multiplication sont compatibles :

$$\forall \lambda \in K \ , \ \forall x, y \in V \ , \ \begin{cases} (\lambda.x) \star y = \lambda.(x \star y) \\ x \star (\lambda.y) = \lambda.(x \star y). \end{cases}$$

Une *sous-algèbre* de V est une partie W qui est à la fois un sous-espace vectoriel et un sous-anneau. Un *morphisme* de l'algèbre V dans l'algèbre V' est une application $f : V \to V'$ qui est à la fois une application linéaire et un morphisme d'anneaux.

On ne suppose pas l'anneau commutatif. Cependant, on le suppose unitaire, et sa multiplication interne est, bien sûr, associative. Comme de coutume, les symboles de multiplication (interne et externe) seront omis dans l'écriture courante. Pour démontrer que $W \subset V$ est une sous-algèbre, on doit vérifier qu'elle est stable par combinaisons linéaires de deux éléments, qu'elle est stable par multiplication et qu'elle contient l'élément neutre de la multiplication de l'anneau V. On a alors automatiquement une structure d'algèbre sur W.

Exemple.
Soient $\lambda, \mu \in K$ et $x, y \in V$. Calculons dans V le carré de $\lambda x + \mu y$. Le calcul dans l'anneau $(V, +, \star)$ donne d'abord : $(\lambda.x)^2 + (\mu.y)^2 + (\lambda.x) \star (\mu.y) + (\mu.y) \star (\lambda.x)$. Puis l'on applique les règles de compatibilité, et l'on trouve : $\lambda^2.x^2 + \mu^2.y^2 + \lambda\mu.(x \star y) + \mu\lambda.(y \star x)$. Noter dans cette dernière formule la présence de carrés et de produits dans K d'une part, dans V d'autre part. Finalement : $(\lambda.x + \mu.y)^2 = \lambda^2.x^2 + \mu^2.y^2 + \lambda\mu.(x \star y + y \star x)$.

Exercice 14.

Notons e l'unité de l'algèbre non triviale V (donc $e \neq 0$). Montrer que l'application $\lambda \mapsto \lambda.e$ est un morphisme injectif d'algèbres. Que peut-on dire de son image ?

Solution. On a déjà vu que c'est une application linéaire. L'image de l'unité 1 de K est $1.e = e$ (axiomes des espaces vectoriels), donc l'unité de V. La compatibilité des lois interne et externe entraîne : $(\lambda.e) \star (\mu.e) = (\lambda\mu).e$. On a donc un morphisme d'anneaux, donc d'algèbres. Comme tout morphisme d'anneaux dont la source est un corps, il est injectif. Enfin, son image est un sous-anneau de V, et aussi un sous-espace vectoriel (c'est le sous-espace vectoriel Ke), donc une sous-algèbre.

On s'autorisera parfois de ce résultat pour identifier K à la sous-algèbre Ke de V et le scalaire λ à l'élément λe de V. C'est par exemple ce qui se passe lorsque l'on identifie le nombre réel $C \in \mathbb{R}$ à la fonction constante C ou le scalaire $a \in K$ au polynôme constant a (voir les exemples ci-dessous).

Exemples.

1. Les endomorphismes du K-espace vectoriel E forment la K-algèbre $\mathcal{L}_K(E)$. L'image de K dans cette algèbre par l'application de l'exercice est la sous-algèbre des homothéties. De même, les matrices carrées de taille n sur le corps K forment la K-algèbre $M_n(K)$. L'image de K dans cette algèbre par l'application de l'exercice est la sous-algèbre des matrices scalaires.
2. Les polynômes sur le corps K forment la K-algèbre $K[X]$. L'image de K dans cette algèbre par l'application de l'exercice est la sous-algèbre des polynômes constants, que l'on identifiera à K.
3. En définissant le produit fg de deux fonctions, on fait du $\mathbb{R}$-espace vectoriel $\mathcal{F}(I, \mathbb{R})$ une $\mathbb{R}$-algèbre. L'image de $\mathbb{R}$ dans cette algèbre par l'application de l'exercice est la sous-algèbre des fonctions constantes, que l'on identifiera à $\mathbb{R}$. Les fonctions continues forment la sous-algèbre $\mathcal{C}(I, \mathbb{R})$; et l'on a de même la sous-algèbre des fonctions dérivables, des fonctions de classe $\mathcal{C}^k$, etc.
4. Soient I un ensemble d'indices et $(V_i)_{i\in I}$ une famille de K-algèbres indexée par I. On fait du produit $\prod_{i\in I} V_i$ un anneau en posant (avec les notations de la définition) :

$$\forall (x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} V_i \ , \ (x_i)_{i\in I} \star (y_i)_{i\in I} = (x_i \star y_i)_{i\in I}.$$

   La structure de K-espace vectoriel et la structure d'anneau de $\prod_{i\in I} V_i$ sont compatibles et en font une K-algèbre. Si, pour chaque indice i, W_i est une sous-algèbre de V_i, alors $\prod_{i\in I} W_i$ est une sous-algèbre de $\prod_{i\in I} V_i$. Par exemple, K^I est une K-algèbre. Le sous-espace $K^{(I)}$ des familles à support fini (voir le module II.3 de [L1]) est stable par multiplication mais ne contient l'unité que si I est fini : sinon, ce n'est donc pas une sous-algèbre.

Exercice 15.
Soit L un corps (que l'on ne suppose pas commutatif) dont K est un sous-corps (commutatif). On a fait de L un K-espace vectoriel. D'autre part, c'est évidemment un anneau. Est-ce une K-algèbre ? Que dire des cas de $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ (où $\mathbb{H}$ désigne le corps des quaternions) ?
Solution. Puisque la loi interne et la loi externe sont toutes deux la multiplication de L, il s'agit de vérifier l'égalité $\lambda xy = x\lambda y$ lorsque $\lambda \in K$ et $x, y \in L$. Cela revient à exiger que tout élément de K commute avec tout élément de L : on dit que K est *central* dans L. Les inclusions $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ fournissent autant d'exemples d'algèbres. Le corps $\mathbb{H}$ est une algèbre sur $\mathbb{Q}$ et sur $\mathbb{R}$, mais pas sur $\mathbb{C}$ (car $\mathbb{C}$ n'est pas central dans $\mathbb{H}$).

De l'égalité $(\lambda.e)\star x = \lambda.x$, on déduit que tout idéal I d'une K-algèbre commutative A en est également un sous–espace vectoriel, et l'on obtient donc naturellement une K-algèbre quotient A/I. Par exemple, si P est un polynôme, l'anneau $K[X]/<P>$ est une K-algèbre. Le théorème chinois se transpose tel quel au cas des algèbres : si I et J sont des idéaux étrangers de la K-algèbre A, le morphisme $x \mapsto (x \mod I, x \mod J)$ de A dans $(A/I) \times (A/J)$ est un isomorphisme de K-algèbres.

Proposition et définition 45. Soit x un élément de l'algèbre V. Le sous-espace vectoriel de V engendré par la famille $(x^n)_{n\in\mathbb{N}}$ est une sous-algèbre commutative de V. Cette sous-algèbre est appelée *sous-algèbre engendrée par* x et notée $K[x]$.

On prendra garde à ne pas confondre cette notation avec celle qui désigne l'algèbre $K[X]$ des polynômes. Pour rappeler que, dans cette dernière, la lettre X dénote une « indéterminée », nous essaierons d'utiliser systématiquement une lettre majuscule dans le cas des polynômes.

Démonstration. Par convention, x^0 est l'élément neutre de la multiplication. Il reste à vérifier que $K[x]$ est stable par multiplication. Les éléments de $K[x]$ sont les combinaisons linéaires des x^n, donc de la forme $\sum_{i\in I} a_i x^i$, où I est une partie finie de $\mathbb{N}$ et les $a_i \in K$. Tout élément de $K[x]$ peut donc se mettre sous la forme $a_0x^0 + \cdots + a_mx^m = \sum_{i=0}^{m} a_i x^i$, avec $m \in \mathbb{N}$ et $a_0, \ldots, a_m \in K$. Le calcul de $\left(\sum_{i=0}^{m} a_i x^i\right) \star \left(\sum_{j=0}^{n} b_j x^j\right)$ donne alors :

$$\sum_{i=0,j=0}^{i=m,j=n} (a_i x^i) \star (b_j x^j) = \sum_{i=0,j=0}^{i=m,j=n} (a_i b_j) x^i \star x^j = \sum_{i=0,j=0}^{i=m,j=n} (a_i b_j) x^{i+j} = \sum_{k=0}^{m+n} c_k x^k,$$

où $c_k := \sum_{\substack{i+j=k \\ 0\leqslant i\leqslant m \\ 0\leqslant j\leqslant n}} a_i b_j$. Cette formule entraîne la stabilité pour la multiplication. On en déduit également la commutativité, car, de l'égalité évidente $\sum a_i b_j = \sum b_j a_i$, découle la relation :

$$\left(\sum_{i=0}^{m} a_i x^i\right) \star \left(\sum_{j=0}^{n} b_j x^j\right) = \left(\sum_{j=0}^{n} b_j x^j\right) \star \left(\sum_{i=0}^{m} a_i x^i\right).$$

∎

Théorème 46 (Propriété universelle de l'algèbre des polynômes).
Soit A une K-algèbre. Alors, pour tout $x \in A$, il existe un unique morphisme de K-algèbres $K[X] \to A$ tel que $X \mapsto x$.
L'image de ce morphisme est la sous-algèbre $K[x]$ de A.

Démonstration. Soit φ un tel morphisme ; l'image du polynôme $\sum a_i X^i$ est :

$$\varphi\big(\sum a_i X^i\big) = \sum a_i \varphi(X^i) = \sum a_i \varphi(X)^i = \sum a_i x^i,$$

d'où l'unicité. Réciproquement, en posant $\varphi\big(\sum a_i X^i\big) := \sum a_i X^i$, on prouve facilement que l'on a un morphisme d'algèbres : on étend ainsi les calculs et la définition de « l'évaluation de P en x » ([L1], module II.6 sur les polynômes). ∎

Proposition et définition 47. Avec les notations ci-dessus, on a l'alternative :
(i) Soit le morphisme $P \mapsto P(x)$ est injectif et la K-algèbre $K[x]$ est de dimension infinie. Dans ce cas, on dit que x est *transcendant* sur K.
(ii) Soit la K-algèbre $K[x]$ est de dimension finie. Le noyau du morphisme $P \mapsto P(x)$ est un idéal principal non trivial dont les éléments sont appelés *polynômes annulateurs de* x et dont l'unique générateur unitaire est appelé *polynôme minimal de* x ; on le note μ_x. Dans ce cas, on dit que x est *algébrique* sur K. Le degré de μ_x, qui est la dimension de $K[x]$, est appelé *degré de* x (sur K). On a un isomorphisme : $K[x] \simeq \dfrac{K[X]}{<\mu_x>}$.

Démonstration. Si le morphisme est injectif, $K[x]$ est isomorphe à $K[X]$, qui est de dimension infinie. Sinon, son noyau est un idéal $<P>$, où P est unitaire et non constant (il faut en effet avoir $P(x) = 0$). C'est ce polynôme P qui est le polynôme (annulateur) minimal μ_x. Les polynômes annulateurs, *i.e.* les polynômes P tels que $P(x) = 0$, sont les éléments du noyau, donc les multiples de μ_x. D'après le premier théorème d'isomorphisme, on a un isomorphisme $K[x] \simeq \dfrac{K[X]}{<\mu_x>}$, et la dimension de $K[x]$ est donc $\deg \mu_x$. ∎

Corollaire 48. Si x est algébrique et si $\mu_x = P_1^{r_1} \cdots P_k^{r_k}$, (décomposition en facteurs irréductibles dans $K[X]$), on a un isomorphisme : $K[x] \simeq \dfrac{K[X]}{<P_1^{r_1}>} \times \cdots \times \dfrac{K[X]}{<P_k^{r_k}>}$.

Démonstration. Cela découle du théorème chinois. ∎

Exemples.

1. En prenant $K := \mathbb{Q}$ et $A := \mathbb{C}$, on retrouve la notion de nombres algébriques ou transcendants de [L1].
2. Dans une K-algèbre de dimension finie n, tout élément est algébrique et de degré inférieur ou égal à n. En particulier, dans les $\mathbb{R}$-algèbres $\mathbb{C}$ et $\mathbb{H}$, dans les K-algèbres $M_n(K)$, $\mathcal{L}_K(E)$, tout élément est algébrique.

4 Séries formelles

Les séries de fonctions de la forme $\sum_{n\geqslant 0} a_n z^n$ sont étudiées en analyse sous le nom de *séries entières* (modules II.2 et II.6). Les coefficients a_n sont alors, en général, des nombres réels ou complexes. Il y a cependant de bonnes raisons d'étudier de telles séries d'un point de vue purement algébrique (indépendamment des questions de convergence) et pour des coefficients arbitraires. On parle alors de *séries formelles*. Comme pour les polynômes, cette étude est possible sur un *anneau* de coefficients et avec *plusieurs* indéterminées, mais nous n'approfondirons que le cas d'un *corps* de coefficients et d'*une* indéterminée.
Notre but est de donner une signification et des règles de calcul pour des expressions de la forme $\sum_{n\geqslant 0} a_n X^n$, où, pour commencer, les coefficients a_n appartiennent à un anneau commutatif A (nécessairement unitaire par définition). De telles expressions s'apparentent à des « polynômes de degré infini » et c'est cette idée vague qui guide leur construction.

Construction des séries formelles sur un anneau A

Rappelons que l'on a construit $A[X]$ en dotant d'une structure d'anneau le groupe $A^{(\mathbb{N})}$ des suites d'éléments de A *à support fini*. Nous considérons donc ici le groupe $A^{\mathbb{N}}$ de *toutes* les suites $(a_n)_{n\in\mathbb{N}}$ d'éléments de A. Nous définissons un produit sur $A^{\mathbb{N}}$ par la formule (*produit de Cauchy*) :

$$(a_n)_{n\in\mathbb{N}}\,(b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}},\ \text{où, } \forall n\in\mathbb{N}\ ,\ c_n := \sum_{i+j=n} a_i b_j = \sum_{i=0}^{n} a_i b_{n-i}.$$

Bien que les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ ne soient pas supposées à support fini, la formule qui définit c_n ne fait intervenir qu'un nombre fini de termes. Comme pour les polynômes, on vérifie que l'on a fait de $A^{\mathbb{N}}$ un anneau commutatif unitaire dont l'élément neutre est la suite $(1,0,\ldots)$. Il est immédiat que $A^{(\mathbb{N})}$ en est un sous-anneau. On note encore X l'élément défini par la suite $(0,1,0,\ldots)$ et $A[[X]]$ l'anneau $A^{\mathbb{N}}$. Ses éléments sont appelés *séries formelles en X à coefficients dans A*. La suite $(a_n)_{n\in\mathbb{N}}$ est alors notée $\sum_{n\geqslant 0} a_n X^n$.
Cette notation ne doit pas être considérée comme une somme ou une combinaison linéaire infinie, ce qui n'aurait aucun sens. Sa signification sera éclaircie à la section 4.2. L'anneau $A[X]$ des polynômes en X à coefficients dans A est donc un sous-anneau de l'anneau $A[[X]]$ des séries formelles en X à coefficients dans A.

Ainsi, l'expression $f := \sum_{n\geqslant 0} X^n Y^n$ désigne évidemment un élément de $\mathbb{Z}[[X]][[Y]]$, et même de $\mathbb{Z}[X][[Y]]$, puisque l'on peut écrire $f = \sum_{n\geqslant 0} a_n Y^n$, où chaque $a_n := X^n$ est élément de $\mathbb{Z}[X]$. Mais elle ne désigne pas un élément de $\mathbb{Z}[[X]][Y]$, car on ne peut mettre f sous la forme d'une somme *finie* $\sum_{n=0}^{d} a_n Y^n$ où chaque a_n est élément de $\mathbb{Z}[[X]]$.

4.1 La K-algèbre des séries formelles

Dorénavant, la lettre K désigne un corps commutatif et $K[[X]] := \Big\{ \sum_{n\geqslant 0} a_n X^n \;\Big|\; (a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}} \Big\}$ l'anneau des séries formelles en X à coefficients dans K. C'est, de manière évidente, un K-espace vectoriel et même une K-algèbre. Les opérations y sont définies par les formules :

$$\lambda\Big(\sum_{n\geqslant 0} a_n X^n\Big) + \mu\Big(\sum_{n\geqslant 0} b_n X^n\Big) := \sum_{n\geqslant 0} c_n X^n \quad \text{où} \quad \forall n \in \mathbb{N}\,,\ c_n := \lambda a_n + \mu b_n,$$

$$\Big(\sum_{n\geqslant 0} a_n X^n\Big)\Big(\sum_{n\geqslant 0} b_n X^n\Big) := \sum_{n\geqslant 0} c_n X^n \quad \text{où} \quad \forall n \in \mathbb{N}\,,\ c_n := \sum_{i+j=n} a_i b_j = \sum_{i=0}^{n} a_i b_{n-i}.$$

La K-algèbre $K[X]$ des polynômes en X à coefficients dans K est donc une sous-algèbre de la K-algèbre $K[[X]]$ des séries formelles en X à coefficients dans K. Nous ferons appel à la commode notation suivante : si $n \in \mathbb{N}$ et si $f := \sum_{n\geqslant 0} a_n X^n$, alors $[X^n]f$ désigne le coefficient a_n (coefficient de X^n dans f).
Ainsi, $[X^n](\lambda f + \mu g) = \lambda [X^n]f + \mu [X^n]g$, etc.

Exercice 16.
La famille des X^n est-elle une base de $K[[X]]$?
Solution. Non : c'est une famille libre, mais le sous–espace vectoriel qu'elle engendre est $K[X]$. On ne connaît aucune base de $K[[X]]$. On peut démontrer que toute base du K-espace vectoriel $K[X]$ est dénombrable ; mais, par exemple, que toute base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[[X]]$ a la puissance du continu (pour la signification de ces termes, voir la section sur les cardinaux du module « Fondements » de [L1]).

On appelle *terme constant* de la série formelle $f := \sum_{n\geqslant 0} a_n X^n$ le scalaire $\mathrm{tc}(f) := a_0 = [X^0]f$. On le note également $f(0)$. *Cette notation ne doit pas être considérée comme une évaluation de f en $X := 0$, ce qui n'aurait aucun sens*. Sa signification sera éclaircie à la section 4.2.3. Les règles de calcul (combinaisons linéaires, produits) peuvent se résumer ainsi : $f \mapsto \mathrm{tc}(f)$ est un morphisme de K-algèbres de $K[[X]]$ sur K. Ce morphisme s'identifie d'ailleurs au passage au quotient $K[[X]] \to K[[X]]/{<X>} \simeq K$ par l'idéal principal $<X>$.

Proposition et définition 49.
(i) Soit $f := \sum_{n\geqslant 0} a_n X^n \in K[[X]]$ non nulle. Le plus grand entier i tel que X^i divise f est également le plus petit entier n tel que $a_n \neq 0$. On le note $\omega(f)$ et on l'appelle *ordre* ou *valuation* de f. Par convention, l'ordre de 0 est $+\infty$.
(ii) On a, pour $\lambda \in K^*$ et $f, g \in K[[X]]$, les formules :

$$\omega(\lambda f) = \omega(f),\ \omega(f+g) \geqslant \min\big(\omega(f), \omega(g)\big) \quad \text{et} \quad \omega(fg) = \omega(f) + \omega(g).$$

De plus, si $\omega(f) \neq \omega(g)$, alors $\omega(f+g) = \min\big(\omega(f), \omega(g)\big)$. Les règles de calcul concernant $+\infty$ sont indiquées dans le module sur les polynômes de [L1].

La démonstration est identique à celle donnée pour les polynômes. En utilisant l'ordre au lieu du degré (qui n'est pas défini ici), on en déduit de même :

Corollaire 50. L'anneau $K[[X]]$ est intègre.

Proposition 51.
Pour que $f \in K[[X]]$ soit inversible, il faut, et il suffit, que $\omega(f) = 0$.

Démonstration. Puisque $fg = 1 \Rightarrow \omega(f) + \omega(g) = 0$, la condition est évidemment nécessaire. On peut aussi bien invoquer l'égalité $\mathrm{tc}(f)\,\mathrm{tc}(g) = 1$.
Supposons réciproquement que $\omega(f) = 0$ et écrivons $f := \sum_{n\geqslant 0} a_n X^n$, avec $a_0 \neq 0$. La série formelle $g := \sum_{n\geqslant 0} b_n X^n$ est inverse de f si, et seulement si, $a_0 b_0 = 1$ et, pour tout $n \geqslant 1$, $\sum_{i+j=n} a_i b_j = 0$. On pose donc $b_0 := a_0^{-1}$ et, pour tout $n \geqslant 1$, la relation de récurrence : $b_n := -a_0^{-1} \sum_{i=0}^{n-1} a_{n-i} b_i$. ∎

Exemple. La série $1 + X + X^2 \in \mathbb{C}[[X]]$ est inversible. Son inverse est $\sum_{n\geqslant 0} b_n X^n$, où $b_0 := 1$, $b_0 + b_1 = 0$, d'où $b_1 := -1$; puis, pour $n \geqslant 2$, la relation de récurrence linéaire à deux pas : $b_n + b_{n-1} + b_{n-2} = 0$. On trouve que la suite des b_n est périodique : $b_{3p} = 1$, $b_{3p+1} = -1$, $b_{3p+2} = 0$.

Exercice 17.
Calculer l'inverse de $1 - X^a$ ($a \in \mathbb{N}^*$).
En déduire un nouveau calcul de l'inverse de $1 + X + X^2 \in \mathbb{C}[[X]]$.
Solution. On trouve que $(1 - X^a)^{-1} = \sum_{n\geqslant 0} b_n X^n$, où $b_n = 1$ si n est multiple de a, et 0 sinon ; autrement dit, $(1 - X^a)^{-1} = \sum_{p\geqslant 0} X^{ap}$. Comme $(1 - X)(1 + X + X^2) = 1 - X^3$, on en déduit que l'inverse de $1 + X + X^2$ est $(1 - X) \sum_{p\geqslant 0} X^{3p} = \sum_{p\geqslant 0} X^{3p} - \sum_{p\geqslant 0} X^{3p+1}$, comme précédemment (voir également l'exercice I.1.48 de la page 55).

Théorème 52. (i) Tout élément non nul de $K[[X]]$ admet une unique écriture uX^k, où u est inversible. L'élément f divise l'élément g si, et seulement si, $\omega(f) \leqslant \omega(g)$.
(ii) L'anneau $K[[X]]$ est principal. Tous ses idéaux non nuls sont de la forme $<X^k>$.

Pour la notion d'anneau principal, voir le module d'arithmétique de [L1].

Démonstration. (i) Pour la première assertion, il suffit de prendre $k := \omega(f)$. La deuxième assertion en découle.
(ii) Si I est un idéal non nul, soit $f \in I$ d'ordre minimum.
Alors, d'après (i), $I = <f> = <X^k>$, avec $k := \omega(f)$. ∎

Ainsi, étant donnés f et g dans $K[[X]]$, l'un divise l'autre : on dit que $K[[X]]$ est un *anneau de valuation*. L'assertion (ii) se résume en disant que $K[[X]]$ est un *anneau de valuation discrète* (c'est une propriété plus forte). On en déduit qu'il admet un seul idéal maximal, l'idéal $<X>$: on dit que $K[[X]]$ est un *anneau local*. Enfin, ses seuls idéaux premiers sont $\{0\}$ et $<X>$.

4.1.1 Développements d'une fraction rationnelle en série de Laurent

L'anneau $K[[X]]$ étant intègre, on peut construire son corps des fractions, que l'on notera $K((X))$: c'est le corps des *séries de Laurent formelles en X à coefficients dans K*. Une série de Laurent formelle est dite *entière* si elle est élément de $K[[X]]$. De l'assertion (i) du théorème 52 de la page précédente, on déduit que toute série de Laurent g qui n'est pas entière est de la forme $\dfrac{1}{f} = \dfrac{1}{uX^k} = \dfrac{v}{X^k}$, où $v \in K[[X]]$ est inversible. On peut donc écrire :

$$g = \sum_{n \geqslant -k} b_n X^n = b_{-k}X^{-k} + \cdots + b_0 + \cdots ,$$

avec $b_{-k} \neq 0$. L'entier $-k$ est *l'ordre $\omega(g)$ de la série de Laurent g*. L'extension de ω à $K((X))$ vérifie les mêmes propriétés qu'à la proposition 49 de la page 31. On a donc les égalités :

$$K((X)) = K[[X]][X^{-1}] = \Big\{ \sum_{n \geqslant n_0} a_n X^n \mid n_0 \in \mathbb{Z} \quad \text{et} \quad \forall n \geqslant n_0 \ , \ a_n \in K \Big\}.$$

Chaque série de Laurent $f := \sum\limits_{n \geqslant n_0} a_n X^n$ admet une unique décomposition en une *partie entière* $\lfloor f \rfloor := \sum\limits_{n \geqslant 0} a_n X^n \in K[[X]]$ et une *partie polaire* :

$$f - \lfloor f \rfloor := \sum_{n_0 \leqslant n < 0} a_n X^n \in X^{-1}K[X^{-1}].$$

Il y correspond une décomposition en somme directe :

$$K((X)) = K[[X]] \oplus X^{-1}K[X^{-1}].$$

Le morphisme d'anneaux intègres : $K[X] \to K[[X]]$ s'étend en un morphisme entre leurs corps de fractions : $K(X) \to K((X))$. On dit que l'on a associé à chaque fraction rationnelle son *développement en série de Laurent*. Par exemple, la fraction rationnelle $\dfrac{X+1}{X^2 - X}$ admet pour développement en série de Laurent le produit de $(X+1)$ par la série de Laurent inverse de la série formelle $X^2 - X$:

$$\frac{X+1}{X^2-X} = -\frac{1}{X}\frac{1+X}{1-X} = -\frac{1}{X}(1+X)(1+X+X^2+\cdots) = -X^{-1}-2-2X-2X^2-\cdots$$

Il y a un rapport entre le développement en série de Laurent et les développements limités du module sur les polynômes de [L1]. Soit $R \in K(X)_0$, autrement dit, R est définie en 0. Son dénominateur est donc inversible dans $K[[X]]$, et son développement en série de Laurent est une série formelle $\sum\limits_{n \geqslant 0} a_n X^n$ (on parle plutôt dans ce cas de *développement en série*

formelle). Alors chaque $DL_m(R)$ (développement limité à l'ordre m) est la troncature à l'ordre m de cette série formelle, c'est-à-dire le polynôme $S := \sum_{n=0}^{m} a_n X^n$. Rappelons que, si $R = \dfrac{P}{Q}$, S s'obtient par *division selon les puissances croissantes de P par Q* : c'est l'unique polynôme de $K_m[X]$ tel que $\omega(P - SQ) \geqslant m+1$.

Exercice 18.

Quel est le développement en série formelle de $\dfrac{1}{(1-X^{a_1})\cdots(1-X^{a_k})}$, où les $a_i \in \mathbb{N}^*$ sont distincts ?

Solution. C'est $\sum_{n\geqslant 0} b_n X^n$, où b_n est le nombre de solutions en entiers naturels de l'équation $a_1x_1 + \cdots + a_kx_k = n$. Le raisonnement est le même que dans le cas de $\dfrac{1}{(1-X^2)(1-X^3)}$ (exercice II.6.29 de [L1]).

Proposition 53. Pour que la série formelle $f := \sum_{n\geqslant 0} a_n X^n$ soit le développement en série formelle d'une fraction rationnelle, il faut, et il suffit, qu'il existe $d \in \mathbb{N}$ et $\lambda_0, \ldots, \lambda_q \in K$ non tous nuls tels que :

$$\forall n \geqslant d\ ,\ a_n\lambda_0 + \cdots + a_{n+q}\lambda_q = 0.$$

Démonstration. Notons $P := \lambda_0 X^q + \cdots + \lambda_q$. Alors $a_n\lambda_0 + \cdots + a_{n+q}\lambda_q$ est le coefficient $[X^{n+q}](Pf)$ de X^{n+q} dans la série formelle Pf. La condition de l'énoncé équivaut donc à dire que Pf est un polynôme de degré strictement inférieur à $d+q$, c'est-à-dire que f est le développement en série formelle d'une fraction rationnelle (de dénominateur P). ∎

Comme le montre l'exercice suivant, d'autres critères de rationalité sont basés sur les *déterminants de Hankel* :

$$H_n^{(k)} := \det A_n^{(k)},\ \text{où}\ A_n^{(k)} := \begin{pmatrix} a_n & a_{n+1} & \cdots & a_{n+k-1} \\ a_{n+1} & a_{n+2} & \cdots & a_{n+k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n+k-1} & a_{n+k} & \cdots & a_{n+2k-2} \end{pmatrix}.$$

Exercice 19.

Soit $f := \sum_{n\geqslant 0} a_n X^n \in K[[X]]$. Montrer que si $H_{d+j}^{(q+1)} = 0$ et $H_{d+j}^{(q)} \neq 0$ pour tout entier naturel j, alors f est rationnelle.

Solution. Puisque $H_d^{(q)} \neq 0$, le système $A_d^{(q)} \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_{q-1} \end{pmatrix} = -\begin{pmatrix} a_{d+q} \\ \vdots \\ a_{d+2q-1} \end{pmatrix}$ admet une unique solution. Puisque $H_d^{(q+1)} = 0$, la dernière ligne de $A_d^{(q)}$ est combinaison linéaire

des précédentes (qui ne sont pas liées parce que $H_d^{(q)} \neq 0$) et l'on tire de ce système l'égalité $a_{d+q}\lambda_0 + \cdots + a_{d+2q-1}\lambda_{q-1} = -a_{d+2q}$, d'où $A_{d+1}^{(q)} \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_{q-1} \end{pmatrix} = - \begin{pmatrix} a_{d+1+q} \\ \vdots \\ a_{d+2q} \end{pmatrix}$. En itérant, on trouve une relation analogue pour tout $n \geqslant d$, et l'on peut appliquer la proposition (ce critère est complété dans l'exercice I.1.51 de la page 55).

Le développement en série de Laurent décrit ci-dessus s'apparente aux développements limités *à l'origine* d'une fonction numérique. L'analogue des développements limités *en d'autres points* s'obtient comme suit. Soit $a \in K$ et soit $R \in K(X)$. En posant $X = a+Y$ et $R(X) = R(a+Y) = S(Y)$, on définit une fraction rationnelle $S \in K(Y)$. Celle-ci admet un développement en série de Laurent $S = \sum_{n \geqslant n_0} a_n Y^n \in K[[Y]]$. On remplace alors Y par $X - a$, et l'on écrit :

$$R(X) = \sum_{n \geqslant n_0} a_n (X-a)^n.$$

Ainsi, le développement en série de Laurent de $\dfrac{1}{X}$ au voisinage de 1 s'écrit-il :

$$\frac{1}{X} = \frac{1}{1+(X-1)} = \sum_{n \geqslant 0} (-1)^n (X-1)^n.$$

Il ne faut toutefois pas attacher un sens littéral à ces écritures. En particulier, $X - a$ doit être traité comme une indéterminée et $(X-a)^n$ ne doit pas être développé.

Il y a enfin un analogue pour les développements limités à l'infini, le *développement en série de Laurent à l'infini* d'une fraction rationnelle $R \in K(X)$. De tels développements apparaîtront lors de l'étude des fractions continues dans les modules « Compléments d'arithmétique » et « Polynômes orthogonaux » de [L3]. On applique à R l'isomorphisme de $K(X)$ sur $K(\xi)$ défini par $X \mapsto \dfrac{1}{\xi}$, que l'on compose avec le plongement de $K(\xi)$ dans $K((\xi))$ (c'est-à-dire le morphisme de corps qui a été défini au début de 4.1.1, page 33). Autrement dit, on pose $S(\xi) := R(1/\xi)$ et l'on développe S en série de Laurent.

Exercice 20.
Développer en série de Laurent à l'infini la fraction rationnelle $R := \dfrac{X^3}{X^2+1}$.

Solution. On note $\xi := \dfrac{1}{X}$.

$$R = \frac{\xi^{-3}}{\xi^{-2}+1} = \frac{1}{\xi+\xi^3} = \frac{1}{\xi}\frac{1}{1+\xi^2} = \frac{1}{\xi}(1-\xi^2+\xi^4-\cdots) = \xi^{-1} - \xi + \xi^3 - \cdots$$

Proposition 54. Notons $\varphi : K(X) \to K((\xi))$ le morphisme qui associe à R son développement en série de Laurent à l'infini. On a alors :

$$\omega\big(\varphi(R)\big) = -\deg R.$$

De plus, la partie polaire de $\varphi(R)$ est $\varphi(P) - \mathrm{tc}(P)$, où P est la partie entière de R.

Démonstration. Si $R = a_0 + \cdots + a_n X^n$ est un polynôme de degré n, alors $P = R$, $\mathrm{tc}(P) = a_0$ et $\varphi(R) = a_n\xi^{-n} + \cdots + a_1\xi^{-1} + a_0$ a pour ordre $-n = -\deg P$ et pour partie polaire $a_n\xi^{-n} + \cdots + a_1\xi^{-1} = \varphi(P) - \mathrm{tc}(P)$.
Dans le cas général, écrivons $R = P + \dfrac{b_0 + \cdots + b_p X^p}{c_0 + \cdots + c_q X^q}$, où $P \in K[X]$, $b_p c_q \neq 0$ et $p < q$ et conservons les mêmes notations pour P. Alors :

$$\varphi(R - P) = \xi^{q-p}\frac{b_0\xi^p + \cdots + b_p}{c_0\xi^q + \cdots + c_q}$$

est entière et d'ordre $q - p > 0$ puisque $b_p c_q \neq 0$. La conclusion découle de même. ∎

4.1.2 Dérivation dans l'anneau $K[[X]]$

Appelons *dérivation* de la K-algèbre A un endomorphisme D du K-espace vectoriel A qui vérifie la *règle de Leibniz* : $\forall f, g \in A\ ,\ D(fg) = fD(g) + gD(f)$. La démonstration de la proposition suivante est similaire à celle donnée pour les polynômes et les fractions rationnelles (module sur les polynômes de [L1]). Cette définition étend d'ailleurs celle donnée pour $K(X)$.

Proposition et définition 55.
Pour toute série de Laurent $f := \sum_{n \geqslant n_0} a_n X^n \in K((X))$, on appelle *dérivée de* f la série de Laurent : $f' := \sum_{n \geqslant n_0} n a_n X^{n-1}$. L'application $f \mapsto f'$ est une dérivation de la K-algèbre $K((X))$. La dérivée d'une série formelle est une série formelle.

On en déduit les règles usuelles de calcul. Par exemple, introduisant la *dérivée logarithmique* $\dfrac{f'}{f}$, on constate que la dérivée logarithmique de fg (resp. de f/g) est égale à la somme (resp. à la différence) des dérivées logarithmiques de f et de g, etc.

La preuve de la proposition suivante est facile et laissée au lecteur.

Proposition 56. On suppose le corps K de caractéristique nulle. Alors, si $\omega(f) \neq 0$, on a : $\omega(f') = \omega(f) - 1$. De plus, $f' = 0$ si, et seulement si, f est constante (*i.e.* $f \in K$). Les séries de Laurent admettant une primitive (*i.e.* une série dont elles sont la dérivée) sont celles dont le coefficient de X^{-1} est nul. Les primitives d'une série donnée diffèrent entre elles d'une constante.