UNIVERSITÉ DE LIMOGES

École doctorale Science et Ingénierie pour l'Information (ED 521)

Faculté des Sciences et Techniques
Département de Mathématiques et Informatique
Laboratoire XLIM

Année : 2013 Thèse N° X

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques et Applications

présentée et soutenue publiquement par

Amal GHEFFAR

le 12 décembre 2013 à 10h

Analyse polyadique ; équations linéaires aux différences

dirigée par Alain SALINIER et codirigée par Abdelkader NECER

devant le jury composé de

Rapporteurs :	**Mark van HOEIJ**	Professeur, Université d'Etat de Floride
	Nicolas MAÏNETTI	Professeur, Université d'Auvergne Clermont 1
Examinateurs :	**Sergei ABRAMOV**	Professeur, Université de Moscou
	Lionel DUCOS	Maître de Conférences HDR, Université de Poitiers
	Alain ESCASSUT	Professeur émérite, Université de Clermont-Ferrand
	Abbas MOVAHHEDI	Professeur, Université de Limoges
	Abdelkader NECER	Maître de Conférences, Université de Limoges
	Alain SALINIER	Professeur, Université de Limoges
Invité :	**Bertin DIARRA**	Chargé de Recherches, CNRS, Université de Clermont-Ferrand

« La logique est l'hygiène des mathématiques »

André WEIL

À mes parents,
mes frères et soeurs,
mes nièces et neveux.

Remerciements

Ce travail a été effectué à la faculté des Sciences de l'Université de Limoges, au sein du laboratoire XLIM, au Département Mathématiques Informatique dirigé par le Professeur Moulay BARKATOU, à qui, j'exprime toute ma gratitude pour l'accueil chaleureux qui m'a été réservé dans ce laboratoire et surtout pour sa disponibilité sans limites.

Je profite de ces quelques lignes pour remercier toutes les personnes qui ont contribué à la réussite de ce travail, et qui grâce à eux, a pu voir le jour.

Je remercie particulièrement Monsieur Alain SALINIER, Professeur à l'Université de Limoges pour m'avoir accueillie dans son équipe de recherche et pour l'encadrement de mes travaux durant mes années de thèse. Je le remercie particulièrement pour sa disponibilité, sa confiance, sa patience qu'il m'a constamment accordée surtout dans des moments difficiles, ce qui m a aidé à rebondir. Sa rigueur scientifique et son exigence ont sans aucun doute contribué au bon déroulement de cette thèse. J'associe à ces remerciements Monsieur Abdelkader NECER, Maître de conférences à l'Université de Limoges, qui a également encadré mes travaux pendant ces années de thèse. Il a su me donner de précieux conseils tout en me laissant une grande autonomie.

Je suis très sensible à l'honneur que m'ont fait Monsieur Mark van HOEIJ, Professeur à l'Université de l'état de Floride et Monsieur Nicolas MAINETTI, Professeur à l'IUT d'Aurillac, en acceptant de rapporter sur ma thèse. Je les remercie pour le temps qu'ils ont consacré pour lire ce manuscrit, pour leurs remarques constructives et pour leurs jugements pertinents.

J'exprime toute ma reconnaissance à Monsieur Alain ESCASSUT, Professeur à l'Université de Blaise Pascal, qui m'a fait un grand honneur de présider le jury de cette thèse.

Je remercie chaleureusement Monsieur Sergei ABRAMOV, Professeur à l'académie des sciences en Russie, pour sa grande confiance en moi, son aide, sa gentillesse, son encadrement qui m'a permis d'enrichir mes connaissances dans la partie Calcul formel.

J'exprime ma gratitude à Monsieur Lionel DUCOS, Maître de conférences-HDR à l'Université de Poitiers, pour son bon accueil lors de ma visite à Poitiers, ainsi que toute son équipe, pour ses remarques constructives et sa contribution.

J'exprime ma gratitude à Monsieur Abbas MOVAHHEDI, Professeur à l'Université de Limoges, d'avoir accepter d'examiner cette thèse et pour tous les échanges durant les années que j'ai passé à Limoges.

J'exprime ma gratitude à Monsieur Bertin DIARRA, Chargé de Recherches honoraire, CNRS à l'Université Blaise Pascal, d'avoir accepter d'examiner cette thèse, pour

les moments fructueux qu'on a passé lors des rencontres du BIDDIUM. Un merci à sa femme pour sa gentillesse.

Mes très vifs remerciements vont à Monsieur Denis E. KHMELNOV pour les échanges malgré la distance et le travail en commun via email (malgré qu'on ne s'est jamais vu), je remercie encore Sergei de nous avoir mis en contact.

Je remercie tout particulièrement Monsieur le Professeur François LAUBIE.

Je remercie le Professeur Hendrik W. LENSTRA qui m'a mis en contact avec Monsieur Bart ZEVENHEK et pour les emails que nous avons échangé. Je tiens à remercier l'affdu de m'avoir attribuer une aide pour financer ma thèse.

J'exprime ma gratitude aux personnels (membres permanents, secrétaires, techniciens, étudiants, stagiaires et ater) du DMI de l'Université de Limoges de m'avoir accueillie chaleureusement parmi eux. Merci à Samir ADLY, François ARNAULT, Anne BELLIDO, Thierry BERGER, Driss BOULARAS, Thomas CLUZEAU, Pierre DUSART, Jean GUILLERME, Noureddine IGBDA, olivier PROT, Marc RYBOWICZ, Olivier RUATTA, Pascale SENECHAUD, Hakim SMATI, Michel THERA, Stéphane VINATIER et à Jacques-Arthur WEIL pour ses encouragements et ses conseils concernant ma présentation (bouteille d'eau). Merci à tous ceux que j'ai eu des échanges fructueux.

Je remercie également Odile DUVAL, Henri MASSIAS, Annie NICOLAS, Patricia VAREILLE, Yolande VICELLI et Sandrine pour leurs disponibilités à répondre à nos questionnements toujours avec le sourire. Sans oublié le personnel de l'IREM.

Je remercie ma chère amie Meriem HERAOUA qui a été comme une soeur pour moi ici à Limoges, j'en profite pour remercier son mari Karim.

Une pensée à tous ceux que j'ai partagé mon bureau au bâtiment de Mathématiques et à Xlim. Aux docteurs Ainhoa APARICIO-MONFORTE, Ahmed AIT MOKHTAR, Julien ANGELI, Aurore BERNARD, Boualem BENSEBAA, Elsa BOUSQUET, Daouda DIATTA, Carole El BACHA, Ismail KHAY, Ba KHIET LE, Sandrine JEAN, ...

Une pensée aux doctorants Jacob DIA, Jean-Christophe DENEUVILLE, Nora EL AMRANI, Nga Ta NGUYET, Riadh OMHENI, Gaël THOMAS, Young AHN, Sadok CHAKROUN, Delphine POINGT, zhenzhong SONG, ...

Une pensée à tous mes professeurs, enseignants ainsi que mes collègues de l'USTHB Université d'Alger.

Je me permets de réserver quelques lignes pour remercier mon père, ma mère et mes proches que malgré la distance étaient là pour m'encourager et m'aider à me battre et à rebondir dans les moments les plus difficiles.

Table des matières

Introduction **7**

I Mise au point sur la limite projective **13**
I.1 Introduction . . . 13
I.2 Catégories et ensembles préordonnés . . . 14
I.3 Système projectif . . . 15
I.4 Cônes . . . 16
I.5 Limites projectives . . . 17
I.6 Limite projective d'espaces topologiques . . . 29
I.7 Limite projective de groupes et d'anneaux . . . 32
I.8 Limite projective de groupes topologiques et d'anneaux topologiques . . . 34
I.9 Espaces topologiques profinis . . . 37
I.10 Groupes et anneaux profinis . . . 42

II Filtration factorielle **47**
II.1 Introduction . . . 47
II.2 Filtration factorielle d'un groupe abélien . . . 48
II.2.1 Définition et propriétés . . . 48
II.2.2 La topologie factorielle . . . 49
II.3 Le complété factoriel . . . 52
II.3.1 Définition et premières propriétés . . . 52
II.3.2 Le morphisme canonique κ_A et sa propriété universelle . . . 54
II.3.3 Le foncteur de complétion . . . 56
II.4 Limites projectives de groupes abéliens séparés et complets . . . 57
II.5 Filtration factorielle sur un anneau . . . 61

II.6 L'anneau des entiers polyadiques 63
II.6.1 L'anneau $\widehat{\mathbb{Z}}$ et sa filtration factorielle 63
II.6.2 Le groupe additif des entiers polyadiques 64
II.6.3 Propriétés des idéaux de $\widehat{\mathbb{Z}}$ 67
II.6.4 Arithmétique factorielle dans $\mathbb{N}$ 68

III Interpolation polyadique de suites récurrentes linéaires **71**
III.1 Introduction 71
III.2 Suites récurrentes linéaires 72
III.2.1 Interprétation Matricielle 72
III.2.2 La périodicité des suites récurrentes linéaires 73
III.2.3 Cas de la suite de Fibonacci 77
III.3 Prolongement polyadique d'une suite récurrente linéaire 81

IV Base de van der Put **85**
IV.1 Introduction 85
IV.2 Les coefficients de van der Put d'une fonction 86
IV.3 Parties initiales d'un entier polyadique 87
IV.4 La formule d'interpolation de van der Put 89
IV.5 Le théorème de van der Put 90

V La fonction logarithme **93**
V.1 Introduction 93
V.2 Définition du logarithme 94
V.2.1 Propriétés de la fonction de Carmichael 94
V.2.2 Définition de la suite A_n 95
V.2.3 Convergence de la suite A_n 96
V.2.4 Le logarithme 98
V.2.5 Non dérivabilité de la fonction exponentielle de base a 98
V.3 Dérivabilité du logarithme 99
V.3.1 Une propriété arithmétique 100
V.3.2 Divisibilité de A_n par $a-1$ dans l'anneau des fonctions continues sur $\widehat{\mathbb{Z}}^*$ 101
V.3.3 Convergence de la suite B_n 103
V.4 Exponentielle 104

V.4.1 Quelques lemmes . . . 104
V.4.2 Le radical de Jacobson de l'anneau des entiers polyadiques . . . 106
V.4.3 Puissances divisées sur le radical de Jacobson . . . 109
V.4.4 La série exponentielle . . . 111
V.4.5 La fonction exponentielle . . . 113

VI Solutions rationnelles d'équations linéaires aux différences 117
VI.1 Introduction . . . 117
VI.2 Préliminaires . . . 119
VI.3 Les ensembles $\mathcal{M}$, $\mathcal{S}$, $\mathcal{S}_{k[x]}$ et $\mathcal{D}$ . . . 121
VI.3.1 L'ensemble $\mathcal{M}$ . . . 121
VI.3.2 Les ensembles $\mathcal{S}$ et $\mathcal{S}_{k[x]}$ . . . 123
VI.3.3 L'ensemble de dispersion $\mathcal{D}$ . . . 125
VI.4 Algorithmes de construction du dénominateur universel et des bornes à dénominateur . . . 125
VI.4.1 L'algorithme de Abramov . . . 126
VI.4.2 L'algorithme de Barkatou . . . 126
VI.4.3 L'algorithme de van Hoeij . . . 127
VI.5 Versions modifiées de l'algorithme de construction des bornes à dénominateur (algorithm $\mathbf{A}_B$) . . . 128
VI.6 Nouveaux algorithmes de construction de dénominateur universel . . . 131
VI.6.1 L'algorithme $\mathbf{A}_U$ . . . 131
VI.6.2 Une version améliorée de l'algorithme $\mathbf{A}_U$ (l'algorithme $\mathbf{A}'_U$) . . . 134
VI.7 Analyse des algorithmes $\mathbf{A}_D$, $\mathbf{A}_G$, $\mathbf{A}_U$ and $\mathbf{A}'_U$ . . . 134
VI.7.1 Equivalence des résultats . . . 134
VI.7.2 Comparaison de complexité de $\mathbf{A}_D$ et $\mathbf{A}'_U$ . . . 135
VI.8 Complexité de $\langle \mathbf{A}_B \rangle$ et $\langle \mathbf{A}'_U \rangle$ . . . 137
VI.8.1 Le schéma RS . . . 137
VI.8.2 Équation indicielle à l'infini . . . 138
VI.8.3 Certaines propriétés de l'équation indicielle à l'infini . . . 139
VI.8.4 Comparaison de complexité . . . 141
VI.9 Expérimentations . . . 145
VI.9.1 Comparaison de $\mathbf{A}'_U$ avec $\mathbf{A}_D$ . . . 146
VI.9.2 Comparaison de $\langle \mathbf{A}'_U \rangle$ avec $\langle \mathbf{A}_B \rangle$ (cas scalaire) . . . 147
VI.9.3 Comparaison de $\langle \mathbf{A}'_U \rangle$ avec $\langle \mathbf{A}_B \rangle$ (cas d'un système) . . . 148

VI.10 Équations scalaires homogènes 148
VI.10.1 Un nouveau Schéma 149
VI.10.2 Critère d'arrêt supplémentaire 150

Bibliographie **153**

Résumé

Cette thèse comprend deux parties indépendantes. La première partie regroupe des contributions à l'analyse polyadique. On récapitule les propriétés de l'anneau (non intègre) des entiers polyadiques vu de façon globale comme limite projective des quotients finis de l'anneau des entiers rationnels, plutôt que comme produit d'anneaux p-adiques. On étudie les suites récurrentes linéaires, en donnant un critère simple pour qu'elles soient prolongeables en une fonction continue définie sur l'anneau des entiers polyadiques. On donne une base de « van der Put » des fonctions continues sur l'anneau des entiers polyadiques, et on termine par l'étude de la théorie du logarithme en analyse polyadique.

La seconde partie présente de nouveaux algorithmes qui recherchent des solutions rationnelles des systèmes linéaires aux différences à coefficients polynomiaux (ou bien d'équations linéaires scalaires aux différences) dans un corps de caractéristique nulle. Nous examinons les algorithmes usuels de calcul formel et nous proposons quelques nouveaux algorithmes pour résoudre ce problème. La complexité et une comparaison en temps des implémentations des algorithmes sous Maple sont présentées.

Abstract

This thesis consists in two independent parts. The first one gathers some contribution to polyadic analysis. We summarize properties of the (not entire) ring of the polyadic integers, seen in a global way as the projective limit of the finite quotients of the ring of rational integers, rather than as a product of p-adic rings. We study linear recurrence sequences, giving a natural criterium for the interpolation of linear recurrence sequences to continuous functions over the ring of polyadic integers. We give a « van der Put » basis for continuous functions on the ring of polyadic integers, and we end by investigation of the theory of logarithm in polyadic analysis.

In the second part, we consider the problem of computing rational solutions of linear difference systems (or scalar equations) with polynomial coefficients over a field of zero characteristic. We discuss algorithms that are currently used and propose some new algorithms for solving this problem. A complexity analysis and a time comparison of the algorithms implemented in Maple are presented.

Introduction

Dans cette thèse, il y a deux parties indépendantes, correspondant à deux objectifs distincts.

Le premier est de contribuer au développement de l'analyse polyadique (chapitres I à V), car ce sujet, bien qu'il soit d'un abord simple et d'un intérêt certain, est assez peu développé jusqu'à présent ; Lenstra [37] par exemple écrit : « *Profinite integers do not enjoy widespread popularity among mathematicians* », tout en soulignant que le sujet est « *eenvoudig en aanstekelijk* » (simple et accrocheur).

Le second (chapitre VI) est de donner certains algorithmes de calcul formel qui construisent des solutions rationnelles d'équations aux différences linéaires à coefficients polynomiaux sur un corps de caractéristique nulle.

Commençons par le premier objectif : l'objet fondamental de l'analyse polyadique (que Lenstra appelle pour sa part « *profinite analysis* ») est l'anneau $\widehat{\mathbb{Z}}$ défini comme limite projective des quotients finis de $\mathbb{Z}$. Prüfer [46], von Neumann [54] et van Dantzig [51] sont parmi les premiers qui ont étudié cet anneau et certaines de ses propriétés. C'est pourquoi cet anneau $\widehat{\mathbb{Z}}$ est parfois appelé l'*anneau de Prüfer*. Ses éléments ont reçu des noms divers : Prüfer les a appelés nombres idéaux, von Dantzig a proposé le vocable de nombres universels ; quant à Lenstra, il parle d'entier profini. C'est, semble-t-il, Novoselov [43] qui les a baptisés nombres polyadiques, terminologie que nous reprenons, car elle montre bien le parallèle avec les nombres p-adiques. Novoselov est celui qui en a fait les études les plus poussées, publiant en particulier une monographie que nous n'avons pu malheureusement lire car elle est en russe. Il a en particulier étudié les développements en séries entières des fonctions usuelles par analogie à l'analyse complexe ou p-adique. Lenstra [37] a utilisé cette théorie, pour en particulier déterminer les points fixes de la fonction polyadique qui interpole les nombres de Fibonacci.

La raison essentielle pour laquelle l'analyse polyadique est si peu utilisée réside sans

doute dans l'idée qu'elle devrait se ramener à l'analyse p-adique. On sait en effet que l'anneau $\widehat{\mathbb{Z}}$ des entiers polyadiques est le produit direct de tous les anneaux p-adiques $\mathbb{Z}_p$ (en termes plus savants, un entier polyadique est la partie finie d'un adèle entier de $\mathbb{Q}$) ; ainsi, pour qu'une suite d'éléments de $\widehat{\mathbb{Z}}$ soit convergente, il faut et il suffit que ses composantes p-adiques convergent p-adiquement pour tous les nombres premiers p. Or, un grand nombre de travaux ont développé l'analyse p-adique, qui est par exemple bien synthétisée par Alain Robert [49], Yvette Amice [14], etc. C'est pourquoi on pourrait penser que l'analyse polyadique n'est qu'une manière détournée d'énoncer des propriétés qui relèvent en fait de l'analyse p-adique, ou non archimédienne. Nous verrons cependant qu'il est possible d'utiliser des méthodes globales permettant dans certains cas une étude plus directe de propriétés analytiques. Plus spécifiquement, notre contribution à l'analyse polyadique regroupe trois études : a) un critère général d'interpolation polyadique des suites récurrentes linéaires (chapitre III) ; b) la construction de « bases de van der Put » pour les fonctions continues (chapitre IV) ; c) la théorie du logarithme sur $\widehat{\mathbb{Z}}$ (chapitre V).

Ces ébauches de théories sont intéressantes car elles permettent de voir jusqu'où peuvent mener les méthodes globales que nous développons. Nous verrons que le caractère non intègre de l'anneau $\widehat{\mathbb{Z}}$ n'est en aucun cas un obstacle dirimant pour ces études. Nous les proposons comme une approche possible, laissant à des travaux ultérieurs la possibilité de développer des théories analogues sur des objets plus généraux : on pense par exemple à la théorie du logarithme sur des extensions finies de $\widehat{\mathbb{Z}}$.

En ce qui concerne le second objectif : les solutions rationnelles d'une équation linéaire aux différences sont très importantes, car elles sont en principe calculables et peuvent parfois servir à construire d'autres types solutions. Nous nous intéressons au problème du calcul de ces solutions rationnelles d'équations linéaires. De façon équivalente, on considère le cas d'un système linéaire aux différences de la forme $Y(x+1) = A(x)Y(x)$, où $A(x)$ est une matrice carrée inversible à coefficients dans le corps $k(x)$, où k est un corps de caractéristique nulle ; une solution rationnelle est alors un vecteur rationnel. Van Hoeij [52] a montré que toute équation non-homogène se ramène à une équation homogène, par conséquent nous nous restreignons aux équations homogènes. Nous discutons des algorithmes de calcul formel actuellement utilisés (voir [45; 11; 12; 53], etc.) et proposons de nouveaux algorithmes pour résoudre ce problème. Une analyse de complexité et une comparaison de la rapidité d'exécution des algorithmes implémentés dans Maple sont présentées.

Passons à la description sommaire du contenu des différents chapitres.

Dans le chapitre premier, nous faisons une mise au point sur la notion de limite projective. En effet, cette notion est souvent présentée sous une forme restrictive, en n'utilisant que des systèmes projectifs indexés par des ensembles partiellement ordonnés filtrants. Dans le but d'avoir une théorie plus souple, certains auteurs comme Mac Lane [39] ont étendu ce cadre à des systèmes indexés par des catégories, et nous reprenons ce point de vue qui permet de voir qu'un produit n'est qu'un cas particulier de limite projective. Nous retrouvons des résultats bien connus caractérisant les espaces topologiques profinis, les groupes topologiques profinis et les anneaux topologiques profinis. Les propositions I.5.3 et I.5.4 fournissent un critère d'invariance de la limite projective qui semble nouveau, plus simple mais plus faible que la cofinalité développée par Grothendieck et Verdier [16] mais qui est largement suffisant pour pouvoir montrer que $\widehat{\mathbb{Z}}$ est limite projective des anneaux $\mathbb{Z}/n!\mathbb{Z}$.

Le chapitre II étudie de façon générale la notion de filtration factorielle d'un groupe abélien quelconque : c'est une façon très simple de topologiser un groupe abélien, que nous n'avons pas retrouvée dans la littérature sur les groupes topologiques. Le théorème II.1.10 montre une raison possible de cette lacune : c'est que la topologie d'un groupe topologique profini de type fini est toujours sa topologie factorielle, ce qui pourrait expliquer pourquoi les auteurs ont choisi une autre voie d'approche de ces topologies. Cette filtration factorielle permet de définir pour tout groupe abélien A un groupe abélien $\hat{A}$ jouant à l'égard de A le rôle d'un complété pour la topologie factorielle, dans la même position que $\widehat{\mathbb{Z}}$ à l'égard de $\mathbb{Z}$. Le lemme II.2.3 permet de relier les filtrations factorielles de A et de $\hat{A}$; cette relation est un outil indispensable pour la suite. La proposition II.2.10 explicite une propriété universelle de $\hat{A}$. Le résultat le plus fort que nous obtenons dans l'étude de la filtration factorielle est notre proposition II.3.2 : tout sous-groupe fermé d'un groupe séparé complet est lui-même séparé complet ; malgré son aspect tautologique, cet énoncé est hautement non trivial, car la topologie induite sur le sous-groupe par la topologie factorielle du sur-groupe n'est pas en général la topologie factorielle du sous-groupe. Il en résulte en particulier que $\hat{A}$ est toujours séparé et complet pour la topologie factorielle (corollaire II.3.5). Dans un dernier paragraphe, nous étudions plus spécialement les propriétés de $\widehat{\mathbb{Z}}$.

Le chapitre III résume les propriétés des suites récurrentes linéaires et spécialement de la suite de Fibonacci. Un critère d'uniforme continuité pour les suites d'éléments d'un groupe abélien (proposition III.2.1) fournit directement, par un théorème de pro-

longement très connu en topologie générale, notre critère d'interpolation pour les suites récurrentes linéaires (théorème III.2.2).

Le chapitre IV fournit une introduction à une théorie possible des modules topologiques de fonctions, encore qu'on n'y étudie que l'unique exemple du module des fonctions continues de $\widehat{\mathbb{Z}}$ dans un anneau filtré séparé R : en effet nous définissons une notion de base orthonormale, et nous montrons l'existence d'une telle base, directement analogue à la base de van der Put bien connue en analyse p-adique.

Dans le chapitre V, nous étudions comment définir une « fonction logarithme », c'est-à-dire un homomorphisme continu du groupe multiplicatif $\widehat{\mathbb{Z}}^*$ des éléments inversibles de $\widehat{\mathbb{Z}}$ dans le groupe additif $\widehat{\mathbb{Z}}$. L'idée de base est fournie par la remarque suivante : si $a \in \mathbb{R}_+^*$, alors

$$\lim_{x\to 0} \frac{a^x - 1}{x} = \ln(a) \ .$$

Par analogie, nous essayons de définir le logarithme de $a \in \widehat{\mathbb{Z}}^*$ comme limite (au sens de la topologie factorielle de $\widehat{\mathbb{Z}}$) du « rapport » de $a^{n!} - 1$ à $n!$ quand n tend vers l'infini. Mais ici, l'existence même de ce rapport dans $\widehat{\mathbb{Z}}$ n'est pas évidente, puisque $n!$ n'est pas inversible dans $\widehat{\mathbb{Z}}$ (sauf si $n = 1$). Nous commençons donc par montrer l'existence d'un nombre polyadique $A_n(a)$ tel que

$$a^{n!} - 1 = n! A_n(a)$$

et montrons que la suite de fonctions $(A_n)_{n\geqslant 1}$ converge uniformément sur $\widehat{\mathbb{Z}}^*$. La limite fournit donc le logarithme voulu. Nous étudions aussi la dérivabilité (au sens de Novoselov) de ce logarithme. Cette étude est complétée par celle de l'exponentielle.

Dans le chapitre VI, on se donne une équation linéaire aux différences, cas scalaire (VI.2) ou sous forme d'un système (VI.1). Comme notre algorithme est basé sur la construction de l'ensemble $\mathcal{M}$ que nous définissons ainsi que l'ensemble analogue à l'ensemble $\mathcal{S}$ de [52] dans la section VI.3. Nous décrivons dans les sections VI.4.1, VI.4.2 l'algorithme (connu) qui construit le dénominateur universel et les bornes à dénominateurs (*denominator bounds*).

Notre algorithme est proposé dans la section VI.6.1. Il est basé sur la construction de l'ensemble des polynômes irréductibles qui divisent les dénominateurs des solutions rationnelles, et sur la recherche d'une borne des puissances (exposants) de ces polynômes, de plus, cet algorithme $\mathbf{A}_U$ les trouve d'une manière tout à fait simple. Une version de cet algorithme qui calcule rapidement l'ensemble de telles puissances est

proposée dans la section VI.6.2, il s'agit de l'algorithme $\mathbf{A}'_U$.

Dès qu'on construit le dénominateur universel, on peut réduire, par la substitution (VI.5) (respectivement. (VI.6)), le problème de trouver des solutions rationnelles des équations (VI.2) et (VI.3) (respectivement. du système VI.1) au problème de trouver des solutions polynomiales. Donc, on peut utiliser les deux algorithmes suivants, à savoir l'algorithme [2; 7] dans le cas des équations scalaires, et celui qui lui correspond [6; 18; 35] dans le cas d'un système.

Dans la section VI.4.3, nous décrivons l'algorithme van Hoeij [52], appliqué sur le corps des nombres complexes ($k = \mathbb{C}$) pour résoudre le système (VI.1). Il trouve des solutions rationnelles appelées « bornes à dénominateur » (*denominator bounds*). La substitution convenable est utilisée. Dans la section VI.5, nous proposons une version appropriée de cet algorithme (algorithme $\mathbf{A}_B$) appliquée dans un corps de caractéristique nulle, et sur des équations scalaires de la forme (VI.2) et (VI.3).

Dans la section VI.7, on montre que l'algorithme $\mathbf{A}'_U$ construit le même dénominateur universel et a un coût plus faible (faible complexité) que les algorithmes décrits dans les sections VI.4.1, VI.4.2.

L'approche liée à l'algorithme de van Hoeij [52], peut donner une substitution plus productive. Mais ce n'est pas si simple, dans le cas général. En combinant l'un des deux algorithmes $\mathbf{A}'_U, \mathbf{A}_B$ avec un algorithme (c'est la même chose dans les deux cas) qui trouve toutes les solutions polynomiales, on obtient les algorithmes $\langle \mathbf{A}'_U \rangle$, $\langle \mathbf{A}_B \rangle$ qui construisent toutes les solutions rationnelles.

Dans la Section VI.8, on montre que, pour trouver les solutions polynomiales d'une équation, la complexité de $\langle \mathbf{A}'_U \rangle$ est plus faible que celle de $\langle \mathbf{A}_B \rangle$. Dans la Section VI.9, nous rapportons quelques expérimentations qui confirment l'avantage de notre approche qui permet de trouver les solutions rationnelles (pour ces expérimentations, D.Khmelnov a implémenté ces algorithmes).

Dans la Section VI.10, nous proposons quelques changements du schéma traditionnel pour trouver les solutions rationnelles des équations homogènes scalaires à coefficients polynomiaux. Dans de nombreux cas, ces changements permettront de prédire (à un stade précoce) l'absence de solutions rationnelles.

Le contenu de ce chapitre est publié dans [31; 8; 30; 10; 9].

Mise au point sur la limite projective

I.1 Introduction

La notion de limite projective fournit le cadre de construction des entiers polyadiques, objet de base de notre étude. C'est une notion très générale et très bien connue, que nous allons néanmoins revisiter car son traitement diffère selon les sources.

En effet, la notion de limite projective est définie d'au moins deux façons différentes selon les auteurs. Alors que certains [48; 32] la réservent aux limites de diagrammes indexés par un ensemble partiellement ordonné filtrant, d'autres comme [39] admettent des cas plus généraux, en permettant de l'appliquer à des diagrammes indexés par des catégories. Dans ce travail, nous reprenons la deuxième définition car elle est plus flexible et en particulier nous permettra de considérer directement les produits comme un cas particulier de limite projective.

I.2 Catégories et ensembles préordonnés

La notion de catégorie est fondamentale en mathématiques. Pour une catégorie $\mathcal{C}$ notons $ob(\mathcal{C})$ la classe dont les éléments sont les objets de $\mathcal{C}$ et $Fl(\mathcal{C})$ la classe dont les éléments sont les flèches de $\mathcal{C}$. Si f est une flèche de la catégorie $\mathcal{C}$, notons par $\mathrm{dom}_{\mathcal{C}}(f)$ le domaine de f dans la catégorie $\mathcal{C}$ et par $\mathrm{cod}_{\mathcal{C}}(f)$ le codomaine de la flèche f dans $\mathcal{C}$. Ces derniers doivent par définition satisfaire certaines propriétés voir [32]. Dans la suite on note par $\mathrm{Id}_E \in Fl(\mathcal{C})$ l'identité de l'objet $E \in ob(\mathcal{C})$, et par $\mathrm{Hom}_{\mathcal{C}}(E,F)$ l'ensemble des $\mathcal{C}$-flèches de domaine E et de codomaine F.

Nous allons expliquer le lien entre catégories et ensembles préordonnés.

Définition I.2.1. *On appelle ensemble préordonné la donnée $(I,\mathcal{R})$ d'un ensemble I et d'une relation binaire $\mathcal{R}$ sur I telle que :*

$\mathcal{R}$ est réflexive, c'est à dire pour tout i dans I , $i\mathcal{R}i$;

$\mathcal{R}$ est transitive, c'est à dire pour tout $(i,j,k) \in I^3$, si $i\mathcal{R}j$ et $j\mathcal{R}k$ alors $i\mathcal{R}k$.

Soit $(I,\mathcal{R})$ un ensemble préordonné. On note par $\mathbb{I}$ la catégorie telle que $ob(\mathbb{I}) = I$ et

$$Fl(\mathbb{I}) = \{(i,j) \in I^2;\ \ i\mathcal{R}j\};$$

avec la loi de composition partielle $\circ$ telle que

$$\forall (i,j),\ (j,k) \in Fl(\mathbb{I}),\ \ (j,k)\circ(i,j) = (i,k).$$

On considère $\mathrm{dom}_{\mathbb{I}}$ et $\mathrm{cod}_{\mathbb{I}}$: $Fl(\mathbb{I}) \to ob(\mathbb{I})$ sont de sorte que

$$\forall (i,j) \in Fl(\mathbb{I}),\quad \mathrm{cod}_{\mathbb{I}}(i,j) = j \ \text{ et } \ \mathrm{dom}_{\mathbb{I}}(i,j) = i.$$

Le fait que $\mathbb{I}$ vérifie les conditions de définition d'une catégorie découle directement de la réflexivité et de la transitivité de $\mathcal{R}$. On remarque que pour tout couple (i,j) d'objets de $\mathbb{I}$, la classe $\mathrm{Hom}_{\mathbb{I}}(i,j)$ a au plus un élément.

La construction de la catégorie $\mathbb{I}$ est fonctorielle. En effet les flèches dans la catégorie des ensembles préordonnés sont les applications $f : I \to I'$ isotones au sens que

$$\forall (i,j) \in I^2,\quad i\mathcal{R}j \ \text{ implique } \ f(i)\mathcal{R}'f(j),$$

en notant $\mathcal{R}$ la relation de préordre sur I et $\mathcal{R}'$ celle sur I'. À une telle application isotone

$f : I \to I'$ on peut associer une fonction F de $Fl(\mathbb{I})$ dans $Fl(\mathbb{I}')$ par

$$\forall (i,j) \in Fl(\mathbb{I}), \quad F(i,j) = (f(i), f(j)) \in Fl(\mathbb{I}').$$

Alors la donnée de $f : ob(\mathbb{I}) \to ob(\mathbb{I}')$ et de $F : Fl(\mathbb{I}) \to Fl(\mathbb{I}')$ constitue un foncteur $\tilde{f}$ de $\mathbb{I}$ dans $\mathbb{I}'$. Ici $f \to \tilde{f}$ est un foncteur de la catégorie des ensembles préordonnés vers la catégorie des catégories, dont les flèches sont les foncteurs.

Dans la suite nous identifierons toujours un ensemble préordonné I avec une catégorie : c'est pourquoi nous utiliserons la même notation I pour un ensemble préordonné quelconque et la catégorie qui lui est associée.

I.3 Système projectif

Définition I.3.1. *Soit $\mathcal{C}$ une catégorie. Un système projectif (ou système inverse) dans $\mathcal{C}$ est la donnée d'une catégorie I et d'un foncteur contravariant F de I dans $\mathcal{C}$.*

On appelle I la catégorie des indices du système projectif (I, F). On dit aussi que le système projectif F est indexé par la catégorie I. Par abus de notation, on se contente souvent d'utiliser la notation F pour désigner le système projectif (I, F).

Exemple I.3.2. *Si on prend, $\mathcal{C}$ la catégorie des anneaux et $I = (\mathbb{N}, \leqslant)$ la catégorie de l'ensemble des entiers naturels avec la relation d'ordre usuelle. Le foncteur F de I dans $\mathcal{C}$ qui associe à tout objet i de $\mathbb{N}$ l'anneau $F(i) = \mathbb{Z}/p^i\mathbb{Z}$ et à toute flèche $ij = j \to i$ avec $j \leqslant i$ le morphisme naturel $F(ij)$ de $F(i)$ dans $F(j)$ (qui associe à $a + p^i\mathbb{Z}$ l'élément $a + p^j\mathbb{Z}$). On obtient le système*

$$\cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^0\mathbb{Z} = \{0\}$$

Soit I une catégorie fixée, les systèmes projectifs de la catégorie $\mathcal{C}$ indexés par I forment une catégorie $\mathcal{C}^I$, dont les morphismes sont les transformations naturelles. On rappelle la définition des transformations naturelles

Définition I.3.3. *Soient $\mathcal{C}$, I deux catégories et F, G deux foncteurs contravariants de la catégorie I vers $\mathcal{C}$. Une transformation naturelle η de F dans G consiste en la donnée pour tout objet A de $ob(I)$ d'une flèche $\eta(A) = \eta_A : F(A) \to G(A)$ de la catégorie $\mathcal{C}$, vérifiant la condition*

que si $f : A \to B$ est une flèche quelconque de I, le diagramme

$$\begin{array}{ccc} F(B) & \xrightarrow{\eta_B} & G(B) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(A) & \xrightarrow[\eta_A]{} & G(A) \end{array}$$

commute. La flèche $\eta(A) = \eta_A$ est appelée composante en A de la transformation naturelle η.

I.4 Cônes

Dans ce paragraphe, on reprend les mêmes notations que [39], les objets d'une catégorie quelconque sont notés par $ob()$ et les flèches par $Fl()$. Soient I et $\mathcal{C}$ deux catégories, A un objet de $\mathcal{C}$, on associe à ces données un objet $\Delta(A)$ de $\mathcal{C}^I$ par

$$\begin{aligned} &\forall j \in ob(I), \qquad \Delta(A)(j) = A, \\ &\forall f \in Fl(I), \qquad \Delta(A)(f) = \mathrm{Id}_A. \end{aligned}$$

Cet objet $\Delta(A)$ de $\mathcal{C}^I$ prend le nom de système projectif constant associé à l'objet A de $ob(\mathcal{C})$. De plus, si $m : A \to B$ est une flèche de la catégorie $\mathcal{C}$, on lui associe $\Delta(m)$ la transformation naturelle de $\Delta(A)$ dans $\Delta(B)$ telle que la composante en un objet j de I de la transformation $\Delta(m)$ est

$$\Delta(m)_j = m \in \mathrm{Hom}_{\mathcal{C}}(\Delta(A)(j), \Delta(B)(j)).$$

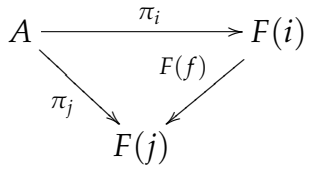
En effet le diagramme

$$\begin{array}{ccc} \Delta(A)(i) & \xrightarrow{\Delta(m)_i} & \Delta(B)(i) \\ {\scriptstyle \Delta(A)(f)}\downarrow & & \downarrow{\scriptstyle \Delta(B)(f)} \\ \Delta(A)(j) & \xrightarrow[\Delta(m)_j]{} & \Delta(B)(j) \end{array}$$

commute pour toute flèche $f : j \to i$. Ainsi Δ est un foncteur covariant de $\mathcal{C}$ dans $\mathcal{C}^I$ appelé *foncteur diagonal*. Dans la suite on a besoin de la définition suivante (cf. [39])

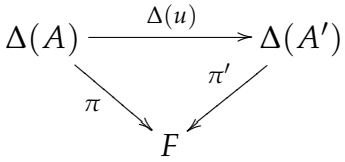
Définition I.4.1. *Soit (I, F) un système projectif de la catégorie $\mathcal{C}$ indexée par la catégorie I. Un cône au-dessus de F est la donnée (A, π) d'un objet A de $\mathcal{C}$ et d'une transformation naturelle $\pi : \Delta(A) \to F$. Ceci signifie que pour tout objet i de I on se donne une composante*

$\pi_i : A = \Delta(A)(i) \to F(i)$ *de sorte que le triangle*



commute pour toute flèche $f : j \to i$ *dans la catégorie des indices.*

Les cônes au-dessus d'un foncteur contravariant F d'une catégorie I dans $\mathcal{C}$ sont les objets d'une catégorie **Cone**(F). Les flèches de la catégorie **Cone**(F) de domaine (A, π) et de codomaine (A', π') sont les $\mathcal{C}$-flèches $u : A \to A'$ telles que $\pi' \circ \Delta(u) = \pi$, ce qui revient à dire que le diagramme (dans la catégorie $\mathcal{C}^I$)



est commutatif.

I.5 Limites projectives

Définition et unicité des limites projectives

Définition I.5.1. *Soit* (I, F) *un système projectif d'une catégorie* $\mathcal{C}$ *indexée par la catégorie* I*. On appelle limite projective de* (I, F) *ou tout simplement limite projective de* F*, tout objet terminal de la catégorie* **Cone***(*F*).*

Cette définition signifie qu'un cône (L, π) est limite projective de F si seulement si, pour tout cône (A, p) au-dessus de F, il existe une unique flèche de (A, p) dans (L, π) de la catégorie **Cone**(F). Autrement dit, le cône (L, π) est limite projective de F si et seulement si il satisfait la propriété universelle : pour tout cône (A, p) au-dessus de F, il existe une unique flèche $m : A \to L$ de la catégorie $\mathcal{C}$ telle que $\pi \circ \Delta(m) = p$.

Proposition I.5.2 (Propriété d'unicité)**.** *Soit* (I, F) *un système projectif d'une catégorie* $\mathcal{C}$ *indexé par une catégorie* I*. Si* (L, π) *et* (L', π') *sont deux limites projectives de* F *alors il existe un unique isomorphisme* $u : L \to L'$ *de la catégorie* $\mathcal{C}$ *tel que* $\pi' \circ \Delta(u) = \pi$*.*

Démonstration. En effet, il y a unicité d'un objet terminal à isomorphisme près dans n'importe quelle catégorie (cf. [32] page 47). Il suffit d'appliquer ce résultat à la catégorie **Cone**(F). □

Notation Soit (I, F) un système projectif d'une catégorie $\mathcal{C}$ indexé par une catégorie I. On convient de noter $\varprojlim_I F$ tout objet L de la catégorie $\mathcal{C}$ tel qu'il existe une transformation naturelle $\pi : \Delta(L) \to F$ de sorte que (L, π) soit une limite projective de F. D'après la propriété d'unicité, un tel objet, s'il existe, est unique à isomorphisme près.

Changement de variable dans les limites projectives

Une propriété importante des limites projectives est leur invariance (à isomorphisme près) par rapport à certains "changements de variable". Cette propriété est souvent exprimée, dans le contexte plus restreint des limites projectives de systèmes indexés par un ensemble préordonné filtrant, par une condition dite de cofinalité [23; 48]. Une étude très poussée des généralisations de la cofinalité figure dans l'article [16]. Nous nous contenterons ici d'une version plus faible et plus simple, mais qui reste bien adaptée à l'étude des limites projectives de systèmes indexés par une catégorie.

Proposition I.5.3. *Soit (I, F) un système projectif dans une catégorie $\mathcal{C}$ (au sens de notre définition I.3.1). On se donne une catégorie I', munie de deux foncteurs covariants $G : I' \to I$ et $H : I \to I'$. On suppose qu'il existe une transformation naturelle φ du foncteur identité Id_I de la catégorie I dans le foncteur $G \circ H$, et une transformation naturelle ψ du foncteur identité $Id_{I'}$ de la catégorie I' dans le foncteur $H \circ G$ telles que*

$$\forall i' \in ob(I'), \qquad G(\psi_{i'}) = \varphi_{G(i')} \, .$$

Notons (L, π) l'éventuelle limite projective du système projectif (I, F), et (L', ρ) l'éventuelle limite projective du système projectif $(I', F \circ G)$. Alors (L, π) existe si et seulement si (L', ρ) existe ; en outre, quand elles existent, L et L' sont isomorphes dans la catégorie $\mathcal{C}$.

Démonstration. Supposons d'abord que (L, π) existe. On pose alors $L' = L$ et, pour tout objet i' de la catégorie I', posons

$$\rho_{i'} = \pi_{G(i')} : L \to F(G(i')) = (F \circ G)(i') \, .$$

Pour toute flèche $f' : i' \to j'$ de la catégorie I', on a, puisque (L, π) est un cône au-dessus de F :

$$(F \circ G)(f') \circ \rho_{j'} = F(G(f')) \circ \pi_{G(j')} = \pi_{G(i')} = \rho_{i'} \ ,$$

ce qui montre que (L, ρ) est un cône au-dessus de $F \circ G$.

Il nous reste à vérifier que ce cône (L, ρ) au-dessus de $F \circ G$ satisfait la propriété universelle des limites projectives. Soit (A, q) un cône au-dessus de $F \circ G$. Posons, pour tout objet i de la catégorie I,

$$p_i = F(\varphi_i) \circ q_{H(i)} : A \to F(i).$$

Alors, pour toute flèche $f : i \to j$ dans la catégorie I, nous avons, en exploitant la fonctorialité de F et la naturalité de φ :

$$F(f) \circ p_j = F(f) \circ (F(\varphi_j) \circ q_{H(j)}) = F(\varphi_j \circ f) \circ q_{H(j)} = F((G \circ H)(f) \circ \varphi_i) \circ q_{H(j)}.$$

En utilisant une nouvelle fois la fonctorialité de F, on en tire

$$F(f) \circ p_j = F(\varphi_i) \circ ((F \circ G)(H(f)) \circ q_{H(j)}) \ .$$

Or, puisque $H(f) : H(i) \to H(j)$ et (A, q) est un cône au-dessus de $F \circ G$, on a

$$(F \circ G)(H(f)) \circ q_{H(j)} = q_{H(i)},$$

ce qui permet de conclure à l'égalité

$$F(f) \circ p_j = F(\varphi_i) \circ q_{H(i)} = p_i,$$

ce qui achève de montrer que (A, p) est un cône au-dessus de F. Comme (L, π) est limite projective de F, on en déduit qu'il existe une unique flèche $u : A \to L$ de la catégorie $\mathcal{C}$ telle que

$$\forall i \in ob(I), \qquad p_i = \pi_i \circ u \ .$$

Soit maintenant i' un objet quelconque de la catégorie I'. On a

$$\rho_{i'} \circ u = \pi_{G(i')} \circ u = p_{G(i')} = F(\varphi_{G(i')}) \circ q_{(H \circ G)(i')} = (F \circ G)(\psi_{i'}) \circ q_{(H \circ G)(i')}.$$

En outre, puisque $\psi_{i'}$ est une flèche de la catégorie I' dont le domaine est i' et le codo-

maine est $(H \circ G)(i')$, le fait que (A, q) est un cône au-dessus de $F \circ G$ entraîne l'égalité

$$(F \circ G)(\psi_{i'}) \circ q_{(H \circ G)(i')} = q_{i'}.$$

On en déduit que $\rho_{i'} \circ u = q_{i'}$ pour tout objet i' de la catégorie I'. D'autre part, s'il existe une autre flèche $v : A \to L$ de la catégorie $\mathcal{C}$ telle que $\rho_{i'} \circ v = q_{i'}$ pour tout objet i' de la catégorie I', on a, pour tout objet i de la catégorie I :

$$p_i = F(\varphi_i) \circ q_{H(i)} = F(\varphi_i) \circ \rho_{H(i)} \circ v = F(\varphi_i) \circ \pi_{G(H(i))} \circ v.$$

Or, puisque (L, π) est un cône au-dessus de F, on sait que

$$F(\varphi_i) \circ \pi_{G(H(i))} = \pi_i \ .$$

On voit donc que $p_i = \pi_i \circ v$ pour tout objet i de la catégorie I, donc $v = u$ par unicité de u. Ceci achève de montrer que (L, ρ) est limite projective de $F \circ G$.

Réciproquement, supposons l'existence de la limite projective (L', ρ) du foncteur contravariant $F \circ G : I' \to \mathcal{C}$. On pose alors $L = L'$ et, pour tout objet i de la catégorie I

$$\pi_i = F(\varphi_i) \circ \rho_{H(i)} : L \to F(i) \ .$$

Pour toute flèche $f : i \to j$ dans la catégorie I, on a

$$F(f) \circ \pi_j = F(f) \circ F(\varphi_j) \circ \rho_{H(j)} = F(\varphi_j \circ f) \circ \rho_{H(j)}.$$

Par naturalité de φ, on sait que $\varphi_j \circ f = G(H(f)) \circ \varphi_i$, par conséquent

$$F(f) \circ \pi_j = F(\varphi_i) \circ (F \circ G)(H(f)) \circ \rho_{H(j)} \ .$$

Or, puisque ρ est transformation naturelle de $\Delta(L')$ vers $F \circ G$, on a $(F \circ G)(H(f)) \circ \rho_{H(j)} = \rho_{H(i)}$. En définitive, on trouve l'égalité

$$F(f) \circ \pi_j = F(\varphi_i) \circ \rho_{H(i)} = \pi_i$$

qui exprime la naturalité de $\pi : \Delta(L) \to F$. Cela veut dire que (L, π) est un cône au-dessus de F.

Vérifions ensuite que ce cône (L, π) satisfait la propriété universelle des limites pro-

jectives. Soit (A, p) un cône au-dessus de F. Posons alors, pour tout objet i' de la catégorie I'

$$q_{i'} = p_{G(i')} : L \to (F \circ G)(i') \ .$$

Alors, pour toute flèche $f' : i' \to j'$ dans la catégorie I', nous avons

$$(F \circ G)(f') \circ q_{j'} = F(G(f')) \circ p_{G(j')} = p_{G(i')} = q_{i'}$$

ce qui fait voir que (A, q) est un cône au-dessus de $F \circ G$. Comme (L', ρ) est limite projective du foncteur $F \circ G$, on en déduit qu'il existe une unique flèche $u : A \to L$ tel que

$$\forall i' \in ob(I'), \qquad q_{i'} = \rho_{i'} \circ u \ .$$

Pour un objet i de la catégorie I, on a alors

$$\pi_i \circ u = F(\varphi_i) \circ \rho_{H(i)} \circ u = F(\varphi_i) \circ q_{H(i)} = F(\varphi_i) \circ p_{(G \circ H)(i)}.$$

Comme $p : \Delta(A) \to F$ est naturelle, on a $F(\varphi_i) \circ p_{(G \circ H)(i)} = p_i$. On en tire

$$\forall i \in ob(I), \qquad \pi_i \circ u = p_i.$$

Il reste seulement à montrer l'unicité de la flèche $u : A \to L$ satisfaisant cette dernière égalité. Supposons donc donnée une flèche $v : A \to L$ telle que

$$\forall i \in ob(I), \qquad \pi_i \circ v = p_i.$$

Alors, pour tout objet i' de la catégorie I', on a

$$\begin{aligned}
q_{i'} &= p_{G(i')} && \text{(définition de } q\text{)} \\
&= \pi_{G(i')} \circ v && \text{(hypothèse sur } v\text{)} \\
&= F(\varphi_{G(i')}) \circ \rho_{H(G(i'))} \circ v && \text{(définition de } \pi\text{)} \\
&= (F \circ G)(\psi_{i'}) \circ \rho_{(H \circ G)(i')} \circ v && \text{(relation entre } \varphi \text{ et } \pi\text{)} \\
&= \rho_{i'} \circ v && \text{(naturalité de } \rho : \Delta(L) \to F \circ G\text{).}
\end{aligned}$$

Par définition de u, on en conclut $v = u$, achevant de montrer que (L, π) est limite projective de F.

En outre, si (L, π) et (L', ρ) existent en tant que limites projectives respectivement

du système projectif (I, F) et du système projectif $(I', F \circ G)$, alors d'après ce qui précède, on peut choisir ρ' pour que (L, ρ') soit aussi limite projective de $(I', F \circ G)$, d'où l'isomorphisme $L \simeq L'$ dans la catégorie $\mathcal{C}$ par la proposition I.5.2. □

Dans le cas particulier où I et I' sont des ensembles préordonnés, la propriété d'invariance prend la forme qui suit.

Proposition I.5.4. *Soit (I, F) un système projectif dans une catégorie $\mathcal{C}$ indexé par l'ensemble préordonné I. Soit I' un ensemble préordonné, muni de deux applications isotones $G : I' \to I$ et $H : I \to I'$. On suppose que ces deux applications vérifient les propriétés :*

$$\forall i \in ob(I), \quad i \leqslant G(H(i)) \qquad et \quad \forall i' \in ob(I'), \quad i' \leqslant H(G(i')).$$

Notons (L, π) l'éventuelle limite projective du système projectif (I, F), et (L', ρ) l'éventuelle limite projective du système projectif $(I', F \circ G)$. Alors (L, π) existe si et seulement si (L', ρ) existe ; en outre, quand elles existent, L et L' sont isomorphes dans la catégorie $\mathcal{C}$.

Rapports entre les notions de produit et de limite projective

Définition I.5.5. *Une catégorie I est dite discrète si toutes ses flèches sont des identités, c'est à dire lorsqu'on a*

$$Fl(I) = \{Id_A \ , \ A \in ob(I)\}.$$

Quand la catégorie d'indices I du système projectif (I, F) est discrète, une éventuelle limite projective de F prend le nom de produit, et est noté $\prod_{i \in ob(I)} F(i)$. Nous allons voir que ce cas particulier de limite projective peut être utilisé pour décrire des limites projectives quelconques.

Définition I.5.6. *Soit I une catégorie quelconque. La discrétisée de I est la catégorie I_0 telle que*

$$ob(I_0) = ob(I), \quad Fl(I_0) = \{Id_A \ , \ A \in ob(I)\}.$$

Pour toute catégorie I, soit I_0 sa discrétisée (qui est une sous catégorie de I). On a évidemment un foncteur d'oubli $O : I_0 \to I$, notons par Δ_0 le foncteur diagonal de $\mathcal{C}$ dans $\mathcal{C}^{I_0}$. Si (I, F) est un système projectif d'une catégorie $\mathcal{C}$ indexée par la catégorie I, on peut lui associer le système projectif $(I_0, F \circ O)$, en effet $F \circ O$ est un foncteur contravariant de I_0 dans $\mathcal{C}$.

On fait maintenant l'hypothèse que ces deux systèmes projectifs $(I,\ F)$ et $(I_0,\ F\circ O)$ ont chacun une limite projective dans $\mathcal{C}$. On va noter (L,π) une limite projective de F et $(P=\prod_{i\in ob(I)}F(i),p)$ une limite projective de $F\circ O$.

Dans cette situation, nous identifierons toute transformation naturelle de $\Delta(L)$ dans F à une transformation naturelle de $\Delta_0(L)$ dans $F\circ O$; en effet, ces deux types de transformations naturelles sont (l'une et l'autre) constituées par la donnée, pour tout objet i de $ob(I)$, d'une $\mathcal{C}$-flèche $\pi_i : L\to F(i)$, le tout assujetti à certaines conditions de commutations, et il est facile de voir, puisque I_0 est une sous catégorie de I, que les conditions pour être transformation naturelle de $\Delta(L)$ dans F sont plus restrictives que celles qui permettent d'être transformation naturelle de $\Delta_0(L)$ dans $F\circ O$.

Puisque (L,π) est limite projective de F, on sait que π est une transformation naturelle de $\Delta(L)$ dans F. On peut aussi la voir comme transformation naturelle de $\Delta_0(L)$ dans $F\circ O$, c'est à dire que (L,π) peut être considéré comme un cône au-dessus de $F\circ O$. Par définition de (P,p) comme limite projective du système projectif $(I_0,F\circ O)$, on en déduit l'existence d'une unique $\mathcal{C}$-flèche $m : L\to P$ telle que

$$\pi = p\circ\Delta_0(m) \tag{I.1}$$

Rappelons que le membre de gauche π de (I.1), qui était a priori une transformation naturelle de $\Delta(L)$ dans F, doit être interprété comme une transformation naturelle de $\Delta_0(L)$ dans $F\circ O$. Remarquons, en outre que la relation (I.1) entre transformations naturelles équivaut à la condition

$$\forall\, i\in ob(I),\quad \pi_i = p_i\circ m. \tag{I.2}$$

La propriété suivante de cette flèche m nous montre qu'une limite projective quelconque peut toujours être vue comme un sous-objet d'un produit, à la seule condition que ce produit existe.

Proposition I.5.7. *Soit $(\varprojlim F,\pi)$ une limite projective de F et $(P=\prod_{i\in ob(I)}F(i),p)$ une limite projective de $F\circ O$. La flèche m de L dans P est un monomorphisme.*

Démonstration. Soit un objet A de $\mathcal{C}$ et deux flèches parallèles $u,v : A\rightrightarrows L$ telles que $m\circ u = m\circ v$. D'après l'unicité de (I.1) la transformation naturelle $\pi\circ\Delta(u)$ de $\Delta(A)$ dans F a mêmes composantes que la transformation naturelle $p\circ\Delta_0(m)\circ\Delta_0(u)$ de $\Delta_0(A)$ dans $F\circ O$.

Or on a

$$p \circ \Delta_0(m) \circ \Delta_0(u) = p \circ \Delta_0(m \circ u) = p \circ \Delta_0(m \circ v) = p \circ \Delta_0(m) \circ \Delta_0(v).$$

Toujours d'après l'égalité (I.1), la transformation naturelle $p \circ \Delta_0(f) \circ \Delta_0(v)$ à mêmes composantes que la transformation naturelle $p \circ \Delta(v)$ on en déduit que

$$p \circ \Delta(u) = \pi \circ \Delta(v)$$

ce qui par définition de la limite projective (L, π) entraîne que $u = v$. □

Dans les bons cas, on peut aller plus loin et montrer que la flèche m est un égaliseur (pour rappeler la définition de l'égaliseur cf. [32] §16). Soit (I, F) un système projectif de la catégorie $\mathcal{C}$ indexée par une catégorie I. Soit D la catégorie discrète dont les objets sont les I-flèches. On définit un unique foncteur S (contravariant aussi bien que covariant) de D dans $\mathcal{C}$ en spécifiant l'objet de $\mathcal{C}$ associé à un objet de D par

$$S(f) = F(dom_I(f)).$$

On suppose maintenant que les produits

$$Q = \prod_{f \in Fl(I)} F((dom_I(f)) = \prod_{f \in ob(D)} S(f)$$

et

$$P = \prod_{i \in ob(I)} F(i)$$

existent dans la catégorie $\mathcal{C}$. Par conséquent, on dispose de deux transformations naturelles

$$\begin{aligned} & q \ : \Delta(Q) \to S, \\ \text{et} \quad & p \ : \Delta(P) \to F \circ O. \end{aligned} \tag{I.3}$$

On définit deux $\mathcal{C}$-flèches parallèles α, β de P dans Q, en exploitant le fait que Q est le

produit des $S(f)$, en posant

$$\forall f \in ob(D) = Fl(I), \quad q_f \circ \alpha = p_{dom_I(f)} \tag{I.4}$$

$$\text{et} \quad q_f \circ \beta = F(f) \circ p_{cod_I(f)}. \tag{I.5}$$

Proposition I.5.8. *Si (L, π) est une limite projective de F dans la catégorie $\mathcal{C}$, alors l'unique flèche $m : L \to P$ telle que*

$$\forall i \in ob(I), \quad p_i \circ m = \pi_i$$

est un égaliseur de α et β.

Démonstration. La première étape est de montrer que $\alpha \circ m = \beta \circ m$. Les $\mathcal{C}$-flèches $\alpha \circ m$ et $\beta \circ m$ sont de même domaine L et codomaine Q. D'après la propriété universelle du produit Q, l'égalité $\alpha \circ m = \beta \circ m$ équivaut à l'égalité

$$\forall f \in ob(D), \quad q_f \circ \alpha \circ m = q_f \circ \beta \circ m.$$

Or, d'après (I.4)

$$q_f \circ \alpha \circ m = p_{dom_I(f)} \circ m = \pi_{dom_I(f)}$$

et d'après (I.5)

$$\begin{aligned} q_f \circ \beta \circ m &= F(f) \circ p_{cod_I(f)} \circ m \\ &= F(f) \circ \pi_{cod_I(f)} \\ &= \pi_{dom_I(f)}. \end{aligned}$$

La deuxième étape consiste à montrer que toute $\mathcal{C}$-flèche qui égalise α et β se factorise de manière unique à travers la flèche m. Soit donc $e : E \to P$ une $\mathcal{C}$-flèche telle que

$$\alpha \circ e = \beta \circ e.$$

Il faut montrer l'unicité et l'existence de la $\mathcal{C}$-flèche

$$u : E \to L$$

telle que $m \circ u = e$.

Pour montrer l'unicité, on suppose que $m \circ u = e = m \circ u'$. Alors $u = u'$ car m est un

monomorphisme (voir. Proposition I.5.7).

Pour montrer l'existence, on prend i un objet de I, alors $p_i \circ e$ est une $\mathcal{C}$-flèche de domaine E et de codomaine $F(i)$. La collection de ces flèches lorsque i parcourt la classe des objets de I, est un cône au-dessus de F ; en effet, nous avons pour toute flèche $f : i \to j$ de la catégorie I (d'après les formules (I.4) et (VI.30) qui caractérisent les flèches α et β)

$$F(f) \circ p_j \circ e = q_f \circ \beta \circ e = q_f \circ \alpha \circ e = p_i \circ e.$$

Par conséquent, par la propriété universelle de la limite projective (L, π) du foncteur F ; il existe une unique $\mathcal{C}$-flèche $u : E \to L$ telle que

$$\forall i \in ob(I), \quad \pi_i \circ u = p_i \circ e.$$

D'après la propriété universelle du produit P, l'égalité $m \circ u = e$ entre $\mathcal{C}$-flèches de E dans P équivaut à

$$\forall i \in ob(I), \quad p_i \circ m \circ u = p_i \circ e.$$

Or

$$\forall i \in ob(I), \quad p_i \circ e = \pi_i \circ u = p_i \circ m \circ u$$

d'où $e = m \circ u$. □

Nous montrons dans ce qui suit la réciproque.

Proposition I.5.9. *Avec les notations précédentes, si les flèches α et β de P dans Q admettent dans la catégorie $\mathcal{C}$ un égaliseur $e : E \to P$, alors*

(i) La famille $\pi = (\pi_i)_{i \in ob(I)}$ définie par

$$\forall i \in ob(I), \quad \pi_i = p_i \circ e$$

est un cône au-dessus de F.

(ii) Le cône (E, π) est limite projective de F.

Démonstration. (i) Si $f \in Fl(I)$ telle que $f : i \to j$, alors l'égalité

$$F(f) \circ p_j \circ e = p_i \circ e$$

se déduit de

$$F(f) \circ p_j \circ e = q_f \circ \beta \circ e = q_f \circ \alpha \circ e = p_i \circ e.$$

(ii) Si (A, ρ) est un cône au-dessus de F, nous allons montrer qu'il existe une unique $\mathcal{C}$-flèche $u : A \to E$ telle que

$$\forall i \in ob(I), \quad \rho_i = \pi_i \circ u.$$

En effet, montrons d'abord l'unicité de u, on suppose qu'il existe deux flèches u et u' telles que

$$\forall i \in ob(I), \quad \rho_i = \pi_i \circ u = \pi_i \circ u'.$$

Alors

$$\forall i \in ob(I), \quad p_i \circ (e \circ u) = p_i \circ (e \circ u').$$

La propriété universelle du produit P donne l'égalité $e \circ u = e \circ u'$. Comme e de E dans P est un égaliseur de α et β on a

$$\alpha \circ e \circ u = \beta \circ e \circ u = \alpha \circ e \circ u' = \beta \circ e \circ u'.$$

Par définition de l'égaliseur, comme $e \circ u = e \circ u'$ égalise α et β, alors il existe une unique flèche v de A dans E telle que

$$e \circ u = e \circ v = e \circ u'$$

d'où $u = v = u'$.

Reste à montrer l'existence de la flèche u ; d'après la propriété du produit P, il existe une unique flèche $\lambda : A \to P$ telle que

$$\forall i \in ob(I), \quad p_i \circ \lambda = \rho_i.$$

Alors, soit $f : i \to j$ une flèche quelconque de I. On a d'abord d'après la relation(I.4)

$$q_f \circ \alpha \circ \lambda = p_i \circ \lambda = \rho_i$$

et ensuite, d'après la relation (VI.30)

$$q_f \circ \beta \circ \lambda = F(f) \circ p_j \circ \lambda = F(f) \circ \rho_j.$$

Puisque ρ est une transformation naturelle, on en déduit l'égalité

$$\forall f \in Fl(I), \quad q_f \circ \alpha \circ \lambda = q_f \circ \beta \circ \lambda.$$

Par la propriété universelle du produit Q en tire

$$\alpha \circ \lambda = \beta \circ \lambda.$$

Puisque e est un égaliseur de α et β on en déduit l'existence et l'unicité de la flèche u de domaine A et codomaine E telle que

$$\lambda = e \circ u.$$

On a alors

$$\rho_i = p_i \circ \lambda = p_i \circ e \circ u = \pi_i \circ u.$$

□

Une conséquence sur la condition de l'existence de la limite projective d'un foncteur F est donnée par le corollaire suivant

Corollaire I.5.10. *Pour que toutes les limites projectives existent dans une catégorie, il faut et il suffit que, dans cette catégorie, existent tous les produits et tous les égaliseurs.*

Exemple I.5.11. *Considérons la catégorie des ensembles, notée* $\mathbb{E}ns$ *: ses objets sont les ensembles, et ses flèches sont les applications. Toute famille d'ensembles (c'est-à-dire tout foncteur d'une catégorie discrète dans la catégorie* $\mathbb{E}ns$*) a un produit dans la catégorie* $\mathbb{E}ns$ *: il s'agit du produit cartésien muni des projections naturelles. Soit d'autre part* A, B *deux ensembles, et* f, g *deux applications de* A *dans* B*. On pose*

$$E = \{x \in A, \quad f(x) = g(x)\} \tag{I.6}$$

qui est un sous-ensemble de A*. Alors l'injection canonique de* E *dans* A *est un égaliseur des flèches* f *et* g*. On conclut d'après le Corollaire I.5.10 que dans la catégorie des ensembles* $\mathbb{E}ns$*, toutes les limites projectives existent.*

Dans ce qui suit, on montre que la limite projective existe quand la catégorie $\mathcal{C}$, a priori quelconque, est la catégorie des espaces topologiques, ou des groupes, ou des anneaux unifères, ou des groupes topologiques, ou des anneaux topologiques.

I.6 Limite projective d'espaces topologiques

Dans ce paragraphe, on applique ce qui précède dans le cas particulier où la catégorie $\mathcal{C}$ est la catégorie des espaces topologiques, notée $\mathbb{T}op$: c'est la catégorie dont les objets sont les espaces topologiques, et les flèches sont les applications continues.

D'après Bourbaki [23], nous reprenons la définition de la topologie initiale. On se donne I un ensemble d'indices, E un ensemble quelconque, et une famille $(Y_i)_{i\in I}$ d'espaces topologiques. Pour tout i dans I, on se donne également une application f_i de E dans Y_i. Soit alors $\mathfrak{G}$ l'ensemble des parties de E de la forme $f_i^{-1}(U_i)$, avec i dans I, U_i ouvert de Y_i. On note $\mathfrak{B}$ l'ensemble des intersections finies d'éléments de $\mathfrak{G}$. Alors la topologie initiale pour les applications f_i est par définition la topologie sur E de base $\mathfrak{B}$. On caractérise la topologie initiale pour les applications f_i comme la topologie la moins fine rendant continues toutes les applications f_i.

Propriété I.6.1. *Soit I un ensemble d'indices, la famille $(Y_i)_{i\in I}$ d'espaces topologiques. Soit E muni de la topologie initiale pour les applications $f_i : E \to Y_i$. Si on se donne X un espace topologique et g une application de X dans E. Alors g est continue si et seulement si pour tout $i \in I$, les applications $f_i \circ g$ sont continues.*

Démonstration. Voir Bourbaki [23]. □

Exemples I.6.2. *1) Par définition, la topologie produit sur l'espace produit $P = \prod_{i\in I} E_i$ d'espaces topologiques $(E_i, i \in I)$ est la topologie initiale pour les projections $pr_i (i \in I)$ définies par $pr_i((x_j)_{j\in I}) = x_i$.*
2) Par définition, la topologie induite sur une partie F d'un espace topologique E, est la topologie initiale pour l'injection canonique $F \hookrightarrow E$.

Lemme I.6.3. *Soit F un foncteur d'une catégorie discrète I dans la catégorie des espaces topologiques $\mathbb{T}op$, et $P = \prod_{i\in ob(I)} F(i)$ le produit muni de la topologie produit.*

Si (S, γ) est un cône au-dessus de F, alors il existe une unique application continue f de S dans P telle que

$$\forall i \in ob(I), \quad pr_i \circ f = \gamma_i. \tag{I.7}$$

Démonstration. L'ensemble P étant le produit des $F(i)$ dans la catégorie des ensembles $\mathbb{E}ns$, l'existence et l'unicité d'une application $f : S \to P$ satisfaisant l'équation (I.7) sont claires. On déduit de la Proposition I.6.1 que l'application f ainsi définie est continue. □

Corollaire I.6.4. *L'espace topologique, constitué par le produit ensembliste P muni de la topologie produit, est un produit dans la catégorie $\mathbb{T}op$.*

Soient A, B deux objets de la catégorie $\mathbb{T}op$, c'est-à-dire deux espaces topologiques, et soient $f, g : A \to B$ deux applications continues. On note

$$E = \{x \in A, \quad f(x) = g(x)\} \tag{I.8}$$

l'égaliseur de f et g dans la catégorie des ensembles, et $i : E \hookrightarrow A$ l'injection canonique.

Lemme I.6.5. *On munit E de la topologie induite par celle de A. Pour tout espace topologique X, et pour toute application continue $\varphi : X \to A$ satisfaisant $f \circ \varphi = g \circ \varphi$, il existe une unique application continue $\psi : X \to E$ telle que $\varphi = i \circ \psi$.*

Démonstration. Puisque $f \circ \varphi = g \circ \varphi$, l'application φ prend ses valeurs dans E, d'où l'existence et l'unicité de l'application $\psi : X \to E$ telle que $\varphi = i \circ \psi$. L'application ψ est de plus continue en vertu de la Proposition I.6.1. □

Corollaire I.6.6. *L'espace topologique, constitué par l'égaliseur ensembliste E muni de la topologie induite sur E par la topologie de A, est un égaliseur de f et de g dans la catégorie $\mathbb{T}op$.*

Corollaire I.6.7. *Toutes les limites projectives existent dans la catégorie $\mathbb{T}op$ des espaces topologiques. Plus précisément, soit (I, F) un système projectif dans la catégorie $\mathbb{T}op$. Alors, si*

$$P = \prod_{i \in ob(I)} F(i)$$

la limite projective $\varprojlim_I F$ s'identifie au sous-espace de P formé par les $x = (x_i)_{i \in ob(I)}$ vérifiant

$$\forall (f : i \to j) \in Fl(I), \quad x_i = F(f)(x_j).$$

Plus particulièrement, si I est un ensemble muni d'une relation de préordre notée $\leqslant$, ceci devient

$$\forall (i, j) \in I^2, \quad \text{si } \ i \leqslant j, \ \text{ alors } \ x_i = f_{ij}(x_j).$$

où f_{ij} est l'image par le système projectif de la flèche $(i, j) \in Fl(I)$.

La remarque suivante est une propriété particulière des limites projectives d'espaces topologiques séparés (au sens de Hausdorff).

Remarque I.6.8. *On suppose que, pour tout objet i de I, l'espace topologique $F(i)$ est séparé. Alors le sous-espace L de $P = \prod_{i\in ob(I)} F(i)$ formé par les $x = (x_i)_{i\in ob(I)}$ vérifiant*

$$\forall (f : i \to j) \in Fl(I), \quad x_i = F(f)(x_j),$$

qui, comme on vient de le voir, s'identifie à la limite projective de F, est un fermé de P.

Démonstration. Soit $a \in P \setminus L$, montrons l'existence d'un voisinage de a qui ne rencontre pas L.

En effet, puisque par hypothèse $a \notin L$, il existe dans la catégorie I une flèche $f : i \to j$ telle que

$$pr_i(a) \neq F(f)(pr_j(a)) \ .$$

Les éléments $pr_i(a)$ et $F(f)(pr_j(a))$ de l'espace $F(i)$ étant ainsi distincts, il résulte de notre hypothèse qu'il existe deux ouverts U_i et V_i de l'espace topologique $F(i)$ tels que

$$pr_i(a) \in U_i, \quad F(f)(pr_j(a)) \in V_i, \quad \text{et } U_i \cap V_i = \varnothing \ .$$

Puisque les applications $pr_i : P \to F(i)$, $pr_j : P \to F(j)$ et $F(f) : F(j) \to F(i)$ sont continues, les ensembles $pr_i^{-1}(U_i)$ et $pr_j^{-1}(F(f)^{-1}(V_i))$ sont des ouverts de P. Par conséquent, l'ensemble

$$\Omega = pr_i^{-1}(U_i) \cap pr_j^{-1}(F(f)^{-1}(V_i))$$

est un ouvert de P qui contient évidemment a. S'il existait un élément $x = (x_i)_{i\in ob(I)}$ dans $\Omega \cap L$, alors on aurait

$$x_i = pr_i(x) \in U_i \qquad \text{et} \qquad x_i = F(f)(x_j) = (F(f) \circ pr_j)(x) \in V_i,$$

ce qui contredit le fait que les ouverts U_i et V_i sont disjoints. Par conséquent, on a bien $\Omega \cap L = \varnothing$. □

Remarque I.6.9. *Si $(L = \varprojlim_I F, \pi)$ est une limite projective d'espaces topologiques, la topologie sur L est la topologie initiale pour les projections $\pi_i : L \to F(i)$*

Démonstration. D'après notre corollaire I.6.7, on peut identifier L à un sous-espace du produit $P = \prod_{i\in ob(I)} F(i)$; dans cette identification, il est essentiel d'observer que, pour tout objet i de I, la projection π_i correspond à la restriction à L de la projection $pr_i : P \to F(i)$. Il est alors immédiat de vérifier que la topologie induite sur L par la topologie produit sur P, est exactement la topologie initiale pour les restrictions des pr_i à L. □

I.7 Limite projective de groupes et d'anneaux

Dans ce paragraphe, on note par $\mathbb{G}rp$ la catégorie des groupes. Les objets de la catégorie $\mathbb{G}rp$ sont les groupes et ses flèches sont les homomorphismes de groupes. On note en outre $\mathbb{A}nn$ la catégorie des anneaux : les objets de la catégorie $\mathbb{A}nn$ sont les anneaux associatifs unifères, (pour abréger, ces objets seront désignés dans la suite par le seul vocable d'anneau), et les flèches sont les homomorphismes d'anneaux (par définition, on exige qu'un homomorphisme d'anneaux envoie l'élément unité de la source sur l'élément unité de la cible).

On rappelle la définition du groupe produit d'une famille $(G_i)_{i\in I}$ de groupes : il s'agit du produit ensembliste $\prod_{i\in I} G_i$ des ensembles sous-jacents, muni de l'opération produit définie par

$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I} \, .$$

Il est facile de vérifier que cette opération satisfait les axiomes des groupes.

De même, l'anneau produit d'une famille $(R_i)_{i\in I}$ d'anneaux est le produit ensembliste de leurs ensembles muni des deux opérations produits fabriquées à l'aide des additions et des multiplications des facteurs R_i : il est immédiat de vérifier que les axiomes des anneaux sont satisfaits par ces opérations.

Lemme I.7.1. *Soit F un foncteur d'une catégorie discrète I dans la catégorie des groupes $\mathbb{G}rp$ (resp. dans la catégorie des anneaux $\mathbb{A}nn$), et $P = \prod_{i\in ob(I)} F(i)$ le groupe produit (resp. l'anneau produit). On note $pr_i : P \to F(i)$ la projection sur le facteur $F(i)$. Alors pr_i est un homomorphisme de groupes (resp. d'anneaux).*

Si (S, γ) est un cône au-dessus de F dans la catégorie $\mathbb{G}rp$ (resp. $\mathbb{A}nn$), alors il existe une unique flèche f de la catégorie $\mathbb{G}rp$ (resp. $\mathbb{A}nn$) de domaine S et de codomaine P telle que

$$\forall i \in ob(I), \quad pr_i \circ f = \gamma_i. \tag{I.9}$$

Démonstration. Comme l'ensemble sous-jacent à P est le produit ensembliste des $F(i)$, il existe une unique application $f : S \to P$ satisfaisant les relations voulues ; il suffit de vérifier que cette application

$$f : s \mapsto (\gamma_i(s))_{i\in I}$$

est un homomorphisme de groupes (resp. d'anneaux), ce qui est immédiat. □

Corollaire I.7.2. *Le groupe produit (resp. anneau produit) des $F(i)$ est un produit dans la*

catégorie des groupes (resp. des anneaux).

Soient maintenant A et B deux groupes (resp. deux anneaux), et f et g deux homomorphismes de groupes (resp. d'anneaux) de A vers B. On note

$$E = \{x \in A, \quad f(x) = g(x)\}$$

l'égaliseur ensembliste de f et g. Il est immédiat de vérifier que E est un sous-groupe (resp. un sous-anneau) de A. On le munit de la structure de groupe (resp. d'anneau) induite par celle de A. Soit alors $i : E \hookrightarrow A$ l'injection canonique : c'est donc un homomorphisme de groupes (resp. d'anneaux).

Lemme I.7.3. *Pour tout groupe (resp. anneau) X et pour tout homomorphisme de groupes (resp. d'anneaux) $\varphi : X \to A$ tel que $f \circ \varphi = g \circ \varphi$, il existe un unique homomorphisme de groupes (resp. d'anneaux) $\psi : X \to E$ tel que $\varphi = i \circ \psi$.*

Démonstration. En effet, la condition $f \circ \varphi = g \circ \varphi$ signifie que, pour tout élément x de X, l'élément $\varphi(x)$ de A appartient à E, ce qui permet de définir une unique application $\psi : X \to E$ telle que $\varphi = i \circ \psi$. Il est alors facile de vérifier que cette application ψ est un homomorphisme de groupes (resp. d'anneaux). □

Corollaire I.7.4. *L'égaliseur ensembliste E, muni de la structure induite par celle de A est un égaliseur de f et de g dans la catégorie des groupes (resp. des anneaux).*

Corollaire I.7.5. *Toutes les limites projectives existent dans la catégorie des groupes (resp. des anneaux).*

Plus précisément, étant donné (I, F) un système projectif dans la catégorie des groupes (resp. des anneaux), la limite projective de ce système s'identifie au sous-groupe (resp. sous-anneau) du groupe produit (resp. de l'anneau produit)

$$P = \prod_{i \in ob(I)} F(i)$$

constitué par les familles $(x_i)_{i \in I}$ telles que

$$\forall (f : i \to j) \in Fl(I), \qquad x_i = F(f)(x_j) \ .$$

Démonstration. Utiliser le Corollaire I.5.10. La version plus précise se déduit de notre proposition I.5.9. □

Puisque le produit d'une famille de groupes abéliens est un groupe abélien, et qu'un sous-groupe d'un groupe abélien est un groupe abélien, la description des limites projectives de groupes donnée par le corollaire I.7.5 donne immédiatement le résultat suivant.

Remarque I.7.6. *Une limite projective de groupes abéliens est un groupe abélien.*

I.8 Limite projective de groupes topologiques et d'anneaux topologiques

Comme dans les sections précédentes, nous montrons maintenant l'existence des limites projectives dans certaines catégories. Nous nous intéressons à une sous catégorie de la catégorie des groupes $\mathbb{G}rp$ (resp. une sous catégorie de la catégorie des anneaux $\mathbb{A}nn$). En effet, il s'agit de $\mathbb{T}op\mathbb{G}rp$ la catégorie des groupes topologiques, dont les objets sont des groupes topologiques et les flèches sont les homomorphismes continus. Rappelons qu'un groupe topologique est un groupe G muni d'une topologie telle que l'opération du groupe est une application continue de $G \times G$ (muni de la topologie produit des topologies des deux facteurs G)dans G, et telle que de plus l'application inverse $x \mapsto x^{-1}$ est une application continue de G dans G. Nous traiterons également le cas de la catégorie $\mathbb{T}op\mathbb{A}nn$ des anneaux topologiques, dont les objets sont les anneaux unifères muni d'une topologie compatible avec la structure d'anneau et les les flèches sont les homomorphismes continus d'anneaux. Une topologie sur un anneau R est dite compatible avec la structure d'anneau lorsqu'elle fait du groupe additif de l'anneau un groupe topologique au sens précédent, si de plus la multiplication de l'anneau définit une application continue de $R \times R$ dans R.

Soit $(G_i)_{i\in I}$ une famille de groupes topologiques, d'après la section I.7 le groupe produit $G = \prod_{i\in I} G_i$ existe ; de plus, on vérifie aisément que, muni de la topologie produit, c'est un groupe topologique. De même, R l'anneau produit d'une famille $(R_i)_{i\in I}$ d'anneaux topologiques est un anneau topologique lorsqu'on le munit de la topologie produit.

Lemme I.8.1. *Soit F un foncteur d'une catégorie discrète I dans la catégorie des groupes topologiques $\mathbb{T}op\mathbb{G}rp$ (resp. dans la catégorie des anneaux topologiques $\mathbb{T}op\mathbb{A}nn$), et $P = \prod_{i\in ob(I)} F(i)$ le groupe produit (resp. l'anneau produit) muni de la topologie produit. On note*

$pr_i : P \to F(i)$ la projection sur le facteur $F(i)$. Alors pr_i est un homomorphisme continu de groupes (resp. d'anneaux).

Si (S, γ) est un cône au-dessus de F dans la catégorie $\mathbb{T}op\mathbb{G}rp$ (resp. $\mathbb{T}op\mathbb{A}nn$), alors il existe une unique flèche f de la catégorie $\mathbb{T}op\mathbb{G}rp$ (resp. $\mathbb{T}op\mathbb{A}nn$) de domaine S et de codomaine P telle que

$$\forall i \in ob(I), \quad pr_i \circ f = \gamma_i. \tag{I.10}$$

Démonstration. Comme le groupe topologique (resp. anneau topologique) sous-jacent à P est le produit des $F(i)$, d'après le lemme I.7.1 il existe un unique morphisme de groupes (resp. d'anneaux) $f : S \to P$ satisfaisant les relations voulues, de sorte que

$$f : s \mapsto (\gamma_i(s))_{i \in I}\,.$$

De la propriété I.6.1, comme pr_i (le produit est muni de la topologie initiale pour les pr_i) sont continues alors le morphisme f est une application continue, et d'après le lemme I.6.3 cette application est unique. □

Corollaire I.8.2. *Le groupe topologique produit (resp. l'anneau topologique produit) des $F(i)$ est un produit dans la catégorie des groupes topologiques (resp. anneaux topologiques).*

On se donne maintenant A et B deux groupes topologiques (resp. deux anneaux topologiques), et f et g deux homomorphismes continus de groupes (resp. d'anneaux) de A vers B. On note

$$E = \{x \in A, \quad f(x) = g(x)\}$$

le groupe (resp. anneau) égaliseur de f et g. Il est immédiat de vérifier que E est un sous-groupe (resp. un sous-anneau) de A. On le munit de la structure de groupe (resp. d'anneau) induite par celle de A. Soit alors $i : E \hookrightarrow A$ l'injection canonique : c'est donc un homomorphisme de groupes (resp. d'anneaux). On munit E de la topologie induite par celle de A : autrement dit, la topologie initiale pour l'application i, de sorte que l'injection i est continue, et donc est une flèche de la catégorie $\mathbb{T}op\mathbb{G}rp$ (resp. $\mathbb{T}op\mathbb{A}nn$).

Lemme I.8.3. *Le groupe (resp. anneau) topologique, constitué par l'égaliseur E muni de la topologie induite par celle de la topologie de A, est un égaliseur de f et g dans la catégorie des groupes topologiques (resp. anneaux topologiques).*

Démonstration. Ceci découle immédiatement des corollaires I.6.6 et I.7.5. □

Corollaire I.8.4. *Toutes les limites projectives existent dans la catégorie des groupes (resp. des anneaux) topologiques.*

Plus précisément, étant donné (I, F) un système projectif dans la catégorie des groupes (resp. des anneaux) topologiques, la limite projective de ce système s'identifie au sous-groupe (resp. sous-anneau) topologique du groupe produit (resp. de l'anneau produit)

$$P = \prod_{i \in ob(I)} F(i)$$

constitué par les familles $(x_i)_{i \in I}$ telles que

$$\forall (f : i \to j) \in Fl(I), \qquad x_i = F(f)(x_j) \ .$$

Démonstration. La preuve se déduit de notre proposition I.5.9. □

D'après la remarque I.6.8, on peut d'ailleurs ajouter que le sous-groupe (resp. sous-anneau) topologique du groupe produit (resp. de l'anneau produit)

$$P = \prod_{i \in ob(I)} F(i)$$

constitué par les familles $(x_i)_{i \in I}$ telles que

$$\forall (f : i \to j) \in Fl(I), \qquad x_i = F(f)(x_j)$$

est fermé dans P, si les groupes (resp. anneaux) topologiques $F(i)$ sont des espaces topologiques séparés.

Exemple I.8.5. *L'anneau des entiers p-adiques*

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

On définit une famille d'homomorphismes surjectifs

$$\forall n, m \in \mathbb{N}, \textit{tels que } m \leqslant n \quad \varphi_{nm} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$$

$$\mathbb{Z}_p = \{(x_n + p^n\mathbb{Z}) / \ x_n \in \mathbb{Z}; \quad x_n \equiv x_m \bmod p^m, \quad m \leqslant n\}$$

I.9 Espaces topologiques profinis

Définition I.9.1. *Un espace topologique est dit profini s'il est limite projective d'espaces finis discrets.*

Proposition I.9.2. *Un espace profini est compact.*

Démonstration. D'après notre remarque I.6.8, un espace profini s'identifie à un fermé d'un produit d'espaces finis discrets. Or un tel produit est un espace compact d'après le théorème de Tychonoff [34, Chap. 5]. □

Rappelons qu'un espace topologique X est dit *totalement discontinu* lorsque ses seules parties connexes non vides sont les singletons $\{x\}$, avec $x \in X$.

Lemme I.9.3. *Dans un espace topologique compact X, étant donné un point $a \in X$, l'intersection D de toutes les parties G de X à la fois ouvertes et fermées telles que $a \in G$ est connexe pour la topologie induite.*

Démonstration. Notons $\mathcal{F}$ l'ensemble de toutes les parties G de X à la fois ouvertes et fermées telles que $a \in G$. On a toujours $X \in \mathcal{F}$, et donc $\mathcal{F} \neq \varnothing$. On a $D = \cap_{G\in\mathcal{F}} G$. Il est clair que $a \in D$, et que D est un fermé de X comme intersection de fermés de X.

Supposons que D n'est pas connexe. Alors il existe deux fermés K et L de X tels que $D = K \cup L$, $K \cap L = \varnothing$, $K \neq \varnothing \neq L$, $a \in K$. On utilise ensuite le fait que l'espace topologique X est normal, puisque compact [34, Theorem 9, page 141]. Donc il existe deux ouverts U et V de X tels que $K \subseteq U$, $L \subseteq V$ et $U \cap V = \varnothing$. Alors le fermé $F = X \setminus (U \cup V)$ ne rencontre pas $D = \cap_{G\in\mathcal{F}} G$. Or, l'ensemble F étant compact pour la topologie induite, on en déduit qu'il existe des éléments $G_1, \ldots, G_r$ de $\mathcal{F}$ en nombre fini tels que $F \cap (G_1 \cap \ldots \cap G_r) = \varnothing$. On peut prendre $r = 1$ puisque $G_1 \cap \ldots G_r$ est un élément de $\mathcal{F}$. On trouve ainsi un élément G_1 de $\mathcal{F}$ qui est contenu dans $U \cup V$. On considère l'intersection $G_1 \cap U$ qui est un ouvert de X comme intersection de deux ouverts de X, montrons que c'est aussi un fermé de X. Soit x un point adhérent à $G_1 \cap U$; puisque G_1 est fermé, on a $x \in G_1$, donc $x \in U \cup V$. D'autre part, le point x est adhérent à U. Il ne peut donc appartenir à l'ouvert V qui est disjoint de U. Donc $x \in U$. Finalement, tout point adhérent à $G_1 \cap U$ est élément de $G_1 \cap U$, ce qui montre que $G_1 \cap U \in \mathcal{F}$ et donc que $D \subseteq G_1 \cap U$, d'où $L \subseteq D \cap V \subseteq G_1 \cap U \cap V = \varnothing$, ce qui contredit l'assertion $L \neq \varnothing$. □

Lemme I.9.4. *Dans un espace topologique compact et totalement discontinu, tout point admet un système fondamental de voisinages dont les éléments sont des ouverts fermés.*

Démonstration. Soit X un espace topologique compact et totalement discontinu, et $a \in X$, et N un voisinage ouvert de a. On considère l'intersection D de toutes les parties ouvertes fermées G de l'espace X telles que $a \in G$. D'après le lemme I.9.3, on sait que D est connexe. Comme on a évidemment $a \in D$, il résulte de l'hypothèse de totale disconnexité de X que $D = \{a\}$. On a par conséquent

$$(X \setminus N) \cap \cap_{G \in \mathcal{F}} G = \varnothing \ ,$$

où $\mathcal{F}$ désigne, comme précédemment, l'ensemble des parties ouvertes fermées G de l'espace X telles que $a \in G$. Par hypothèse de compacité de X, on en déduit qu'il existe des éléments $G_1, \ldots, G_r$ de $\mathcal{F}$ en nombre fini tels que

$$(X \setminus N) \cap G_1 \cap \ldots \cap G_r = \varnothing,$$

ce qui équivaut à dire que $G_1 \cap \ldots \cap G_r \subseteq N$. Or, la partie $G_1 \cap \ldots \cap G_r$ est un ouvert fermé dont a est élément. □

Proposition I.9.5. *Toute limite projective d'espaces topologiques totalement discontinus est un espace topologique totalement discontinu.*

Démonstration. On suppose que (L, π) est limite projective dans la catégorie $\mathbb{T}op$ d'un système projectif (I, F), où I est une catégorie d'indices et $F : I \to \mathcal{C}$ est un foncteur contravariant tel que, pour tout objet i de la catégorie I, l'espace topologique $F(i)$ est totalement discontinu.

Soit C une partie connexe non vide de L, et i un objet quelconque de la catégorie I. Puisque $\pi_i : L \to F(i)$ est une application continue, l'ensemble $\pi_i(C)$ est une partie connexe non vide de $F(i)$. Comme l'espace topologique $F(i)$ est totalement discontinu, il existe un unique élément $\xi_i \in F(i)$ tel que :

$$\pi_i(C) = \{\xi_i\}.$$

Considérons deux éléments a et b de la partie C et montrons que $a = b$, ce qui prouvera que C est un singleton et donc que L est totalement discontinu. On introduit l'espace topologique $S = \{0\}$ (nécessairement muni de la topologie discrète) et les deux

applications $u : S \to L$ et $v : S \to L$ telles que $u(0) = a$ et $v(0) = b$. Les applications u et v sont continues, et d'après ce qui vient d'être montré, on a :

$$\forall i \in ob(I), \qquad \pi_i \circ u(0) = \xi_i = \pi_i \circ v(0) \ .$$

On a donc $\pi_i \circ u = \pi_i \circ v$ pour tout objet i de la catégorie I. Comme (L, π) est limite projective de (I, F), la propriété universelle de la limite projective entraîne que $u = v$, et donc que $a = u(0) = v(0) = b$. □

Corollaire I.9.6. *Si A est un espace topologique profini, alors il est totalement discontinu.*

Théorème I.9.7. *Un espace topologique est profini si et seulement si il est à la fois compact et totalement discontinu.*

Démonstration. Si l'espace topologique X est profini, alors il est compact (proposition I.9.2) et totalement discontinu (proposition I.9.5). Il reste à montrer la réciproque.

Soit donc X un espace topologique compact et totalement discontinu. On se limite au cas où X est non vide, car l'espace vide est limite projective du système projectif (I, F) donné par :
- la catégorie I à deux objets

$$1 \underset{g}{\overset{f}{\rightrightarrows}} 2$$

ayant, en dehors des identités, deux flèches parallèles f et g ;
- le foncteur F tel que $F(1) = \{0, 1\}$, $F(2) = \{0\}$ (ces deux espaces étant munis de la topologie discrète), $F(f) : \{0\} \to \{0, 1\}$ tel que $F(f)(0) = 0$ et $F(g)\{0\} \to \{0, 1\}$ tel que $F(g)(0) = 1$. Par conséquent, l'espace vide est bien profini.

Notons $\mathcal{O}$ l'ensemble des ouverts de X. Considérons alors l'ensemble I dont les éléments sont les parties finies $P \subseteq \mathcal{O}$ telles que :

i) $\forall \omega \in P, \quad \omega \neq \varnothing$;

ii) $\forall \omega \in P, \forall \omega' \in P, \quad \omega \neq \omega' \Rightarrow \omega \cap \omega' = \varnothing$;

iii) $\forall x \in X, \exists \omega \in P, \quad x \in \omega$.

On peut remarquer que I est non vide, car $\{X\} \in I$.

On met sur I une relation $\leqslant$ en convenant que $P_1 \leqslant P_2$ équivaut à

$$\forall \omega_2 \in P_2, \exists \omega_1 \in P_1, \quad \omega_2 \subseteq \omega_1 \ .$$

On remarque d'ailleurs que, si $P_1 \leqslant P_2$, étant donné $\omega_2 \in P_2$, l'élément ω_1 de P_1 tel que $\omega_2 \subseteq \omega_1$ est unique d'après la condition ii). On convient de le noter $f_{P_1,P_2}(\omega_2)$. On

vérifie aisément que cette relation $\leqslant$ est une relation d'ordre partiel sur l'ensemble I : en particulier, I est un ensemble préordonné et donc aussi une catégorie.

Soit alors $F : I \to \mathbb{T}op$ le foncteur contravariant tel que

$$\forall P \in I, \quad F(P) = P \text{ avec sa topologie discrète}$$

$$\forall (P, Q) \in I^2, \text{ avec } P \leqslant Q, F((P, Q)) = f_{P,Q}.$$

Le fait que F soit un foncteur contravariant se déduit de l'observation suivante : si on a trois éléments P, Q, R de I tels que $P \leqslant Q \leqslant R$, alors $f_{P,R} = f_{P,Q} \circ f_{Q,R}$.

Pour $P \in I$, on définit aussi une application $\pi_P : X \to P$ en convenant que

$$\forall x \in X, \forall \omega \in P, \qquad \pi_P(x) = \omega \Leftrightarrow x \in \omega \ .$$

En effet, si on se donne l'élément x de X, la relation $x \in \omega$ est satisfaite par un élément ω de P en vertu de la condition iii) ci-dessus ; de plus, cet ω est unique d'après la condition ii). De plus cette application π_P est localement constante (car tous les éléments de P sont des ouverts), et donc continue.

On vérifie alors que (X, π) est un cône au-dessus de F : cela revient à dire que, si on se donne deux éléments P et Q de I tels que $P \leqslant Q$, alors $\pi_P = f_{P,Q} \circ \pi_Q$, ce qui est clair.

Il reste à vérifier que, sous l'hypothèse que X est compact et totalement discontinu, ce cône (X, π) satisfait la propriété universelle qui caractérise la limite projective. Soit donc (Y, ρ) un cône au-dessus de F, donné par un espace topologique Y et par une famille $(\rho_P)_{P \in I}$ d'applications continues $\rho_P : Y \to P$ telle que

$$\forall (P, Q) \in I^2, \quad P \leqslant Q \Rightarrow \rho_P = f_{P,Q} \circ \rho_Q \ .$$

Soit maintenant un point y de Y. Montrons que l'intersection des parties $\rho_P(y)$ de l'espace X, quand P décrit l'ensemble I, est exactement un singleton de X. On procède en deux temps, en montrant d'abord que cette intersection est non vide, puis en montrant qu'elle ne peut jamais contenir deux points distincts.

Tout d'abord, on remarque que, si $P \in I$, tout élément ω de P est complémentaire de la réunion des ouverts $\omega' \in P \setminus \{\omega\}$, donc est aussi un fermé de X. Par compacité de X, l'intersection des fermés $\rho_P(y)$, pour P décrivant I, est non vide si et seulement si toute intersection finie extraite est non vide. Il s'agit donc de vérifier que, si l'on se donne un

nombre fini $P_1, P_2, \ldots, P_r$ d'éléments de I, alors l'intersection

$$\rho_{P_1}(y) \cap \cdots \cap \rho_{P_r}(y) \tag{I.11}$$

n'est jamais vide. Pour cela, on utilisera le fait que l'ensemble ordonné I est filtrant, ce qui signifie qu'il existe toujours un $Q \in I$ tel qu'on a simultanément $P_1 \leqslant Q, \ldots, P_r \leqslant Q$.

Pour vérifier cette propriété, il suffit évidemment de traiter le cas où $r = 2$. Soit donc P_1 et P_2 deux éléments de I. On définit Q comme l'ensemble des intersections non vides de la forme $\omega_1 \cap \omega_2$, où $\omega_1 \in P_1$ et $\omega_2 \in P_2$. On vérifie alors facilement que $Q \in I$, que $P_1 \leqslant Q$ et que $P_2 \leqslant Q$.

Soit donc à montrer que l'intersection (I.11) est non vide. On sait qu'il existe $Q \in I$ tel que $P_j \leqslant Q$ pour tout indice $j \in \{1, \ldots, r\}$. Alors on sait que $\rho_{P_j}(y) = f_{P_j,Q}(\rho_Q(y))$ pour tout indice $j \in \{1, \ldots, r\}$. Par définition des applications $f_{P_j,Q}$, ceci entraîne que $\rho_Q(y) \subseteq \rho_{P_j}(y)$. Par conséquent l'intersection (I.11) contient l'ouvert non vide $\rho_Q(y)$, et donc est elle-même non vide. L'argument de compacité de l'espace topologique X achève de montrer que l'intersection $\cap_{P \in I} \rho_P(y)$ est non vide.

Supposons maintenant que cette intersection contient deux points distincts $a \neq b$ de X. L'espace X étant compact est séparé, donc il existe un ouvert N de X tel que $a \in N$ et $b \notin N$. D'après le lemme I.9.4, il existe une partie $U \subseteq X$ à la fois ouverte et fermée telle que $a \in U \subseteq N$, et donc $b \notin U$. Soit $P_U = \{U, X \setminus U\}$. Puisque la partie U est à la fois ouverte et fermée, non vide, et non égale à X, on voit que $P_U \in I$. Donc a et b sont tous deux éléments de $\rho_{P_U}(y)$ qui est soit U, soit $X \setminus U$, ce qui contredit le fait que $a \in U$ et $b \notin U$. Ceci montre que l'intersection de tous les $\rho_P(y)$, quand P décrit I, est réduite à un point.

Ceci étant établi, on définit une application u de Y dans X en associant à $y \in Y$ l'unique élément $u(y) \in X$ de l'intersection de tous les $\rho_P(y)$. On a donc l'équivalence

$$\forall (x, y) \in X \times Y, \qquad u(y) = x \Leftrightarrow (\forall P \in I, x \in \rho_P(y)) \, .$$

Soit $v : Y \to X$ une application continue telle que $\pi_P \circ v = \rho_P$ pour tout $P \in I$. L'application π_P ayant été définie comme l'application de X vers P qui à tout élément $x \in X$ associe l'unique élément ω de P tel que $x \in \omega$, la définition entraîne que $v(y) \in \rho_P(y)$ pour tout $P \in I$. Donc $v = u$, ce qui prouve l'unicité de v. Pour vérifier ensuite son existence, il suffit de montrer que u est continue en tout point $y_0 \in Y$. Soit donc N un voisinage ouvert de $u(y_0)$; par le lemme I.9.4, on sait qu'il existe une partie $U \subseteq X$,

à la fois ouverte et fermée, telle que $u(y_0) \in U \subseteq N$. Reprenant la notation P_U pour l'élément $\{U, X \setminus U\}$ de I, on voit que $\rho_{P_U}(y_0) = U$. Comme l'application $\rho_{P_U} : Y \to P_U$ est continue, il existe un voisinage ouvert W de y_0 dans N tel que $\rho_{P_U}(y) = U$ pour tout $y \in W$. Alors $u(y) \in U \subseteq N$ pour tout $y \in W$. Par conséquent, l'image réciproque de N par u est un voisinage de y_0, ce qui montre la continuité de u.

Finalement, on voit que l'application v existe et est unique : ceci veut dire que (X, π) est limite projective dans $\mathbb{T}op$ du système projectif (I, F). Ainsi tout espace topologique compact et totalement discontinu est limite projective d'espaces topologiques finis discrets. □

I.10 Groupes et anneaux profinis

Définition I.10.1. *Un groupe (resp. anneau) topologique est dit profini s'il est limite projective de groupes (resp. anneaux) finis discrets.*

En particulier, un groupe (resp. anneau) profini s'identifie à une partie bien déterminée du produit cartésien des $F(i)$, et est donc limite projective dans la catégorie $\mathbb{T}op$ d'espaces finis discrets : c'est donc un espace topologique profini. On en déduit :

Proposition I.10.2. *Tout groupe (resp. anneau) profini est compact et totalement discontinu.*

Démonstration. C'est une propriété des espaces profinis, comme on l'a démontré précédemment. [23, Chap. I]. □

Lemme I.10.3. *Dans un groupe topologique compact totalement discontinu, tout voisinage de l'élément neutre contient un sous-groupe distingué ouvert.*

Démonstration. Soit N un voisinage de l'élément neutre 1 du groupe topologique G compact et totalement discontinu, noté multiplicativement. On veut montrer que N contient un sous-groupe distingué ouvert. En vertu du lemme I.9.4, on peut supposer que N est à la fois ouvert et fermé. Soit F l'ensemble des éléments de G de la forme xy ($x \in N, y \in N$) qui n'appartiennent pas à N. L'ensemble F est fermé dans le compact G, donc est un compact. Soit $x \in N$. Comme $x \notin F$, par continuité de la multiplication de G, il existe des voisinages ouverts V_x de x et W_x de 1 tels que

$$(a \in V_x, b \in W_x) \Rightarrow ab \notin F\ .$$

Les ouverts V_x, pour x décrivant N, forment un recouvrement ouvert du compact N, donc on peut en extraire un sous-recouvrement fini, de sorte qu'il existe des éléments $x_1, \ldots, x_r$ de N en nombre fini tels que

$$N \subseteq V_{x_1} \cup \cdots \cup V_{x_r} .$$

On pose alors $W' = W_{x_1} \cap \cdots \cap W_{x_r} \cap N$: c'est un voisinage ouvert de 1. On en déduit un voisinage ouvert symétrique $W = W' \cap W'^{-1}$. Le produit d'un élément de N et d'un élément de W n'appartient jamais à F ; puisque $W \subseteq N$, c'est donc un élément de N. Comme W est en outre symétrique, on en déduit que le sous-groupe H engendré par W est contenu dans N. Le sous-groupe H contenant W, c'est en outre un voisinage de 1, donc il est ouvert. L'intersection H_0 des conjugués de H est donc un sous-groupe fermé de G qui contient 1. D'autre part, c'est le noyau de l'homomorphisme de G dans le groupe symétrique de l'ensemble G/H des classes à gauche modulo H défini par l'action naturelle de G sur G/H. Comme G/H est fini, le groupe symétrique en question l'est également, de sorte que H_0 est d'indice fini, donc est un sous-groupe ouvert de G contenu dans N, ce qui achève la démonstration. □

Lemme I.10.4. *Dans un anneau topologique compact et totalement discontinu, tout voisinage de l'élément neutre du groupe additif contient un idéal bilatère ouvert.*

Démonstration. Soit N un voisinage ouvert de l'élément neutre 0 du groupe additif de l'anneau topologique R compact. On veut montrer que N contient un idéal bilatère ouvert. D'après le lemme I.10.3, on peut supposer que N est un sous-groupe ouvert du groupe additif de l'anneau R.

Soit $(a, b) \in R^2$. L'application de R^3 dans R qui envoie (x, t, y) sur le produit xty étant continue en $(a, 0, b)$, il existe un voisinage ouvert $U_{a,b}$ de a, un voisinage ouvert $V_{a,b}$ de 0 et un voisinage $W_{a,b}$ de b tels que

$$(x \in U_{a,b}, t \in V_{a,b}, y \in W_{a,b}) \Rightarrow xty \in N .$$

Le carré cartésien R^2 étant compact, il existe des couples $(a_1, b_1), \ldots, (a_r, b_r)$ de R^2 en nombre fini tels que

$$R^2 = \cup_{i=1}^{r} U_{a_i,b_i} \times W_{a_i,b_i} .$$

Posons alors $V = \cap_{i=1}^{r} V_{a_i,b_i} \cap N$. En tant qu'intersection finie de voisinages ouverts de 0, c'est un voisinage ouvert de 0. Soit I l'idéal bilatère de R engendré par V. Puisqu'il

contient V, c'est un voisinage de 0. Puisque ce voisinage de 0 est aussi un sous-groupe du groupe additif de R, c'est aussi un ouvert de R. D'autre part, tout élément de I est de la forme

$$\sum_{j=1}^{h} x_j t_j y_j \qquad (h \in \mathbb{N}^*, x_j \in R, t_j \in V, y_j \in R)\ .$$

Or, si $x \in R, t \in V, y \in R$, il existe un indice $i \in \{1, \ldots, r\}$ tel que $(x, y) \in U_{a_i,b_i} \times W_{a_i,b_i}$. Comme $t \in V \subseteq V_{a_i,b_i}$, on a toujours $xty \in N$. Comme N est un sous-groupe du groupe additif, on en déduit que I est contenu dans N. Finalement, on a bien trouvé un idéal bilatère ouvert contenu dans N. □

La réciproque de la proposition I.10.2 est vraie.

Théorème I.10.5. *Un groupe (resp. anneau) topologique est profini si et seulement si il est à la fois compact et totalement discontinu.*

Démonstration. Soit G (resp. R) un groupe noté multiplicativement (resp. un anneau) topologique compact et totalement discontinu.

Considérons alors l'ensemble I des sous-groupes distingués ouverts (resp. idéaux bilatères ouverts) de G (resp. de R) d'indice fini dans G (resp. R).

On peut remarquer que I est non vide, car $G \in I$ (resp. $R \in I$).

On met sur I la relation $\leqslant$ réciproque de l'inclusion, c'est-à-dire qu'étant donnés deux éléments A et B de I, on écrit $A \leqslant B$ pour $A \supseteq B$. Ainsi I est un ensemble préordonné, et donc une catégorie. Lorsque les deux éléments A et B de I sont tels que $A \leqslant B$, on définit l'homomorphisme de groupes (resp. d'anneaux) $f_{A,B} : G/B \to G/A$ (resp. $f_{A,B} : R/B \to R/A$ par $f_{A,B}(xB) = xA$ (resp. $f_{A,B}(x + B) = x + A$). On peut aussi observer que $f_{A,B}([x]) \supseteq [x]$ pour tout élément $[x]$ de G/B (resp. R/B).

Soit alors $F : I \to \mathbb{T}op\mathbb{G}rp$ (resp. $F : I \to \mathbb{T}op\mathbb{A}nn$) le foncteur contravariant tel que

$$\forall A \in I, \quad F(P) = G/A (\text{resp. } R/A) \text{ avec sa topologie discrète}$$

$$\forall (A, B) \in I^2, \text{ avec } A \leqslant B, F((A, B)) = f_{A,B}.$$

Le fait que F soit un foncteur contravariant se déduit de l'observation suivante : si on a trois éléments A, B, C de I tels que $A \leqslant B \leqslant C$, alors $f_{A,C} = f_{A,B} \circ f_{B,C}$.

Pour $A \in I$, on note $\pi_A : G \to G/A$ (resp. $\pi_A : R \to R/A$) la surjection canonique, qui est un homomorphisme continu du moment que le sous-groupe (resp. idéal) A est ouvert.

On vérifie alors que (G, π) (resp. (R, π)) est un cône au-dessus de F : cela revient à dire que, si on se donne deux éléments A et B de I tels que $A \leqslant B$, alors $\pi_A = f_{A,B} \circ \pi_B$, ce qui est clair.

Il reste à montrer que, sous que l'hypothèse que G (resp. R) est compact et totalement discontinu, ce cône (G, π) (resp. (R, π)) satisfait la propriété universelle qui caractérise la limite projective. Soit donc (Y, ρ) un cône au-dessus de F, donné par un groupe (resp. anneau) topologique Y et par une famille $(\rho_A)_{A \in I}$ d'homomorphismes continus $\rho_A : Y \to G/A$ (resp. $\rho_A : Y \to R/A$) telle que

$$\forall (A, B) \in I^2, \quad A \leqslant B \Rightarrow \rho_A = f_{A,B} \circ \rho_B \, .$$

Soit maintenant un point y de Y. Montrons que l'intersection des classes $\rho_A(y)$du groupe G (resp. de l'anneau R), quand A décrit l'ensemble I, est exactement un singleton de G (resp. R). On procède en deux temps, en montrant d'abord que cette intersection est non vide, puis en montrant elle ne peut jamais contenir deux points distincts.

Tout d'abord, on remarque que, si $A \in I$, alors il est fermé dans G (resp. R). Par compacité de G (resp ; R), l'intersection des fermés $\rho_A(y)$, pour A décrivant I, est non vide si et seulement si toute intersection finie extraite est non vide. Il s'agit donc de vérifier que, si l'on se donne un nombre fini $A_1, A_2, \ldots, A_r$ d'éléments de I, alors l'intersection

$$\rho_{A_1}(y) \cap \cdots \cap \rho_{A_r}(y) \tag{I.12}$$

n'est jamais vide. Pour cela, on utilisera le fait que l'ensemble ordonné I est filtrant, ce qui signifie qu'il existe toujours un $B \in I$ tel qu'on a simultanément $A_1 \leqslant B, \ldots, A_r \leqslant B$.

Pour vérifier cette propriété, il suffit évidemment de traiter le cas où $r = 2$. Soit donc A_1 et A_2 deux éléments de I. On définit B comme l'intersection $A_1 \cap A_2$. On vérifie que $B \in I$, car il existe un homomorphisme injectif $G/B \to G/A_1 \times G/A_2$ (resp. $R/B \to R/A_1 \times R/A_2$), et il est évident que $A_1 \leqslant B$ et que $A_2 \leqslant B$.

Soit donc à montrer que l'intersection (I.12) est non vide. On sait qu'il existe $B \in I$ tel que $A_j \leqslant B$ pour tout indice $j \in \{1, \ldots, r\}$.Alors l'intersection (I.12) contient l'ensemble non vide $\rho_B(y)$, et donc est elle-même non vide. L'argument de compacité de l'espace topologique X achève de montrer que l'intersection $\cap_{P \in I} \rho_P(y)$ est non vide.

Supposons maintenant que cette intersection contient deux points distincts $a \neq b$ de X. L'espace X étant compact est séparé, donc il existe un ouvert N de X tel que $a \in N$ et $b \notin N$. D'après le lemme I.10.3 (resp. lemme I.10.4), il existe un sous-groupe ouvert

(resp. idéal bilatère ouvert) A de G (resp. R) tel que $a + A \subseteq N$, et donc $b - a \notin A$. Mais a et b sont tous deux éléments de $\rho_A(y)$ qui est une classe modulo A, d'où contradiction. Ceci montre que l'intersection de tous les $\rho_A(y)$, quand A décrit I, est réduite à un point.

Ceci étant établi, on définit une application u de Y dans G (resp. R) en associant à $y \in Y$ l'unique élément $u(y)$ de l'intersection de tous les $\rho_A(y)$. On a donc l'équivalence

$$\forall (x,y) \in G \times Y (\text{resp. } R \times Y), \qquad u(y) = x \Leftrightarrow (\forall A \in I, x \in \rho_A(y)) \ .$$

Soit $v : Y \to G$ (resp. $v : Y \to R$) un homomorphisme continu tel que $\pi_A \circ v = \rho_A$ pour tout $A \in I$. La définition de l'application π_A entraîne que $v(y) \in \rho_A(y)$ pour tout $A \in I$. Donc $v = u$, ce qui prouve l'unicité de v. Pour vérifier ensuite son existence, il suffit de montrer que u est un homomorphisme continu. Pour vérifier est un homomorphisme, il suffit d'observer que les ρ_A sont des homomorphismes, donc $u(yy')$ (resp. $u(y+y'), u(yy')$) est bien $u(y)u(y')$ (resp. $u(y) + u(y'), u(y)u(y')$). Compte tenu de cette première propriété, pour montrer que u est continu, il suffit de montrer qu'il est continu en 1 (resp. 0). Soit donc un voisinage ouvert N de 1 dans G (resp. de 0 dans R) ; par le lemme I.10.3 (resp. lemme I.10.4), on sait qu'il contient un sous-groupe ouvert (resp. idéal bilatère ouvert) A. Puisque ρ_A est un homomorphisme, on a $\rho_A(1) = A$ (resp. $\rho_A(0) = A$). Comme ρ_A est continu, il existe un voisinage ouvert W de 1 (resp. de 0) dans Y tel que $\rho_A(y) = A$ pour tout $y \in W$. Par conséquent, $u(y)$ appartient à A, et donc à N, dès que $y \in W$. Ce qui montre la continuité de u.

Finalement, on voit que l'homomorphisme continu v existe et est unique : ceci veut dire que (X, π) est limite projective dans $\mathbb{T}op\mathbb{G}rp$ (resp. $\mathbb{T}op\mathbb{A}nn$) du système projectif (I, F). Ainsi tout groupe (resp. anneau) topologique compact et totalement discontinu est limite projective de groupes (resp. anneaux) topologiques finis discrets. □

II

Filtration factorielle

II.1 Introduction

Dans ce chapitre, nous munissons tout groupe abélien d'une filtration très simple, que nous appelons la *filtration factorielle*. Bien que cette filtration ait été déjà utilisée dans un grand nombre de cas particuliers, elle n'a, à notre connaissance, jamais été étudiée dans cette généralité. En particulier, nous construisons le complété factoriel d'un groupe abélien.

Dans ce chapitre, on suppose sauf mention du contraire que tous les groupes sont abéliens.

II.2 Filtration factorielle d'un groupe abélien

II.2.1 Définition et propriétés

La filtration factorielle

Soit A un groupe. Puisque pour $d \geqslant 0$ entier naturel, la suite des sous-groupes $(d+1)!A$ est décroissante, elle constitue une filtration (décroissante) au sens de [22]. Ces filtrations peuvent aussi être caractérisées par l'application appelée « fonction d'ordre » dans la terminologie de [22]. Cependant à la suite de [21] nous emploierons le nom de filtration pour cette fonction d'ordre.

Définition II.2.1. *La filtration factorielle sur le groupe abélien A est l'application φ_A de A vers $\mathbb{N} \cup \{\infty\}$ telle que*

$$\forall a \in A, \qquad \varphi_A(a) = \sup\{d \in \mathbb{N} \; ; \; a \in (d+1)!A\}.$$

La filtration factorielle sur le groupe abélien A jouit évidemment des propriétés suivantes.

Proposition II.2.2 (Propriétés de la filtration factorielle)**.** *Soient $a, b \in A$. On a :*

$$\varphi_A(a-b) \geqslant \min(\varphi_A(a), \varphi_A(b));$$

$$\varphi_A(-a) = \varphi_A(a);$$

$$\varphi_A(a) = +\infty \iff a \in \cap_{n \geqslant 1} n!A \; .$$

Proposition II.2.3. *Soit A un groupe abélien sans torsion. Pour tout a de A, et pour tout entier naturel $m \geqslant 1$, on a*

$$\varphi_A(ma) \leqslant \varphi_A(a) + m.$$

Démonstration. Si d est un entier tel que $d > m$ et $ma \in (d+1)!A$, alors, comme on sait que $(d+1)!$ est un multiple de $m(d-m+1)!$, on en déduit que ma est élément de $m(d-m+1)!A$. Puisque A est supposé sans torsion, il en résulte que a appartient à $(d-m+1)!A$, c'est-à-dire que $\varphi_A(a) \geqslant d-m$. D'où le résultat. □

II.2.2 La topologie factorielle

Sur tout groupe abélien A, la filtration factorielle φ_A nous permet de définir une topologie en spécifiant une notion de boule ouverte de la façon suivante : une boule ouverte de centre $a \in A$ est une partie de A de la forme $\{x \in A; \varphi_A(x-a) > k\}$ pour un certain entier $k \in \mathbb{N}$, c'est la classe $a + (k+2)!A$. Il est immédiat par la proposition II.2.2 que la structure du groupe A est compatible avec la topologie ainsi définie, que nous appellerons la *topologie factorielle* de A. Par conséquent, cette topologie confère à A une structure de groupe topologique. De plus, la topologie factorielle de A est toujours pseudo-métrisable [34, page 119], puisqu'elle est engendrée par l'écart

$$(a,b) \mapsto d(a,b) = \begin{cases} 2^{-\varphi_A(a-b)} & \text{si } \varphi_A(a-b) \neq +\infty \\ 0 & \text{sinon} \end{cases} . \tag{II.1}$$

Proposition II.2.4. *Un groupe abélien A est discret pour sa topologie factorielle si et seulement si il est d'exposant fini.*

Démonstration. Si A est supposé discret pour sa topologie factorielle, alors $\{0\}$ est un ouvert, donc il existe un entier naturel k tel que la boule $\{x \in A; \varphi_A(x) > k\}$ est réduite à $\{0\}$, ce qui montre que $(k+2)!A = 0$, et par conséquent A est d'exposant fini divisant $(k+2)!$.

Réciproquement, si A a un exposant fini $e \in \mathbb{N}^*$, alors $e!A = 0$, et donc, pour tout a dans A, le singleton $\{a\}$ est la boule ouverte $\{x \in A; \varphi_A(x-a) > \max(e-2, 0)\}$. □

Proposition II.2.5. *La topologie factorielle du groupe abélien A est la topologie grossière de A si et seulement si le groupe A est divisible.*

Démonstration. En effet, si la topologie factorielle de A est grossière, comme $n!A$ est pour tout entier $n \geqslant 1$ un ouvert de la topologie grossière, évidemment non vide, on a $n!A = A$ pour tout entier $n \geqslant 1$.

Réciproquement, si A est divisible, on a $n!A = A$ pour tout entier $n \geqslant 1$, ce qui montre que A est la seule boule ouverte de la topologie factorielle de A, et donc le seul ouvert non vide dans cette topologie. □

Proposition II.2.6. *Pour tout homomorphisme de groupes abéliens $f : A \to B$, on a :*

$$\forall x \in A, \qquad \varphi_B(f(x)) \geqslant \varphi_A(x) ,$$

de sorte que l'application f est toujours continue pour les topologies factorielles.

Démonstration. En effet $f(d!A) = d!f(A) \subseteq d!B$ pour tout entier naturel $d \geqslant 1$, ce qui donne bien l'inégalité $\varphi_B(f(x)) \geqslant \varphi_A(x)$. Cette inégalité montre immédiatement que f est continue en 0. Puisque f est un homomorphisme de groupes abéliens, il en résulte que f est continue en tout point. □

D'après la proposition II.2.4, la topologie factorielle du groupe quotient A/mA est la topologie discrète. Il résulte de la proposition précédente

Corollaire II.2.7. *Soit A un groupe muni de la topologie factorielle. Pour tout entier naturel $m \geqslant 1$, on munit le groupe quotient A/mA de la topologie discrète. Alors la projection naturelle de A sur A/mA est une application continue.*

On voit en outre que

Proposition II.2.8. *Pour tout entier naturel $m \geqslant 1$ et pour tout $a \in A$, la classe de congruence $a + mA$ est un ouvert fermé de A (pour sa topologie factorielle).*

Démonstration. La classe de congruence $a + mA$ est la réunion des classes $b + m!A$ pour $b \equiv a \bmod mA$. Or une classe $b + m!A$ est l'ensemble des éléments $z \in A$ tels que $\varphi(z - b) > \max(m - 2, 0)$, c'est-à-dire une boule ouverte, et donc un ouvert. Comme toute réunion d'ouverts est un ouvert, toute classe $a + mA$ est donc ouverte, et donc toute réunion de telles classes est un ouvert. En particulier le complémentaire de $a + mA$ étant la réunion des classes $b + mA$ pour $b \not\equiv a \bmod mA$, on en déduit que la classe $a + mA$ est également fermée. □

Proposition II.2.9. *Soit A un groupe, $m \geqslant 1$ un entier naturel. La topologie initiale sur A pour les projections naturelles $p_{m,A} : A \to A/m!A$ (où $A/m!A$ est muni de la topologie discrète) coïncide avec la topologie factorielle de A.*

Démonstration. Il s'agit de comparer les deux topologies définies sur le groupe A. Par définition [23] la topologie initiale est la topologie la moins fine qui rende continues toutes les applications $p_{m,A}$, avec $m \geqslant 1$, de A dans $A/m!A$. La topologie factorielle rendant continues toutes ces applications, par le corollaire II.2.7, il en résulte qu'elle est moins fine que la topologie factorielle de A. Réciproquement, toute boule ouverte pour l'écart (II.1) est une classe $a + d!A, d \geqslant 1$; or cette classe est image réciproque de l'ouvert $\{p_{d,A}(a)\}$ par l'application continue $p_{d,A}$ de A, muni de la topologie initiale, dans $A/d!A$, muni de la topologie discrète ; ainsi tout ouvert pour la topologie factorielle est un ouvert pour la topologie initiale. □

Le théorème suivant montre que la topologie d'un groupe profini « pas trop gros » est certainement sa topologie factorielle.

Théorème II.2.10. *Si A est un groupe profini (compact totalement discontinu) de type fini (c'est-à-dire admettant pour ensemble de générateurs topologiques une partie finie), alors sa topologie est nécessairement sa topologie factorielle.*

Démonstration. Soit $X = \{x_1, \ldots, x_d\}$ $(d \in \mathbb{N})$, une partie finie du groupe abélien A qui l'engendre topologiquement. Fixons un entier naturel $n \geqslant 1$ et montrons que $A/n!A$ est un groupe fini. Pour cela, soit $F_n \subseteq A$ l'ensemble des combinaisons $r_1x_1 + \cdots + r_dx_d$, où $r_j \in \mathbb{N} \cap [0, n![$ pour tout indice $j \in \{1, \ldots, d\}$. La partie F_n est finie, donc c'est une partie fermée de l'espace topologique séparé A. Étant donné un quelconque élément a de A, il suffit de montrer qu'il existe $f \in F_n$ tel que $a \equiv f \bmod n!$. Puisque le groupe engendré par X est dense dans A, pour tout voisinage V de a dans A, il existe un élément $(m_1(V), \cdots, m_d(V))$ de $\mathbb{Z}^d$ tel que l'élément $a(V) = m_1(V)x_1 + \cdots + m_d(V)x_d \in V$. Par division euclidienne, il existe, pour tout voisinage V de a dans A et pour tout indice $j \in \{1, \ldots, d\}$, des entiers $q_j(V) \in \mathbb{Z}$ et $r_j(V) \in \mathbb{N} \cap [0, n![$ tels que $m_j(V) = n!q_j(V) + r_j(V)$. Posons alors $b(V) = q_1(V)x_1 + \cdots + q_d(V)x_d$ et $f(V) = r_1(V)x_1 + \cdots + r_d(V)x_d$. De la suite généralisée $(b(V))_{V \in \mathcal{N}}$ indexée par l'ensemble filtrant $\mathcal{N}$ des voisinages de a dans l'espace compact A, on peut extraire une sous-suite généralisée $(b(V_t))_{t \in T}$ convergente vers $b \in A$. Alors la suite $f(V_t) = a(V_t) - n!b(V_t)$ est une suite de points de F_n qui converge vers $a - n!b$. Comme F_n est fermé, sa limite $f = a - n!b \in F_n$, et on a bien la congruence $a \equiv f \bmod n!$.

Comme $n!A$ est fermé dans A, puisque c'est l'image du compact A par l'application continue $x \mapsto n!x$, on voit maintenant que c'est un sous-groupe fermé de A d'indice fini, donc un sous-groupe ouvert de A. Ceci prouve que la topologie factorielle du groupe A est moins fine que la topologie de A. En particulier, l'identité Id_A de A est continue quand on munit son espace de départ de la topologie donnée de A et son espace d'arrivée de la topologie factorielle.

D'autre part, soit $D = \cap_{n \geqslant 1} n!A$. La partie D est l'intersection de sous-groupes fermés de A, donc c'est un sous-groupe fermé de A, donc elle est compacte. Vérifions que le groupe D est divisible. En effet, soit $d \in D$. Pour tout $n \geqslant 1$, il existe un élément α_n de A tel que $d = n!\alpha_n$. Pour un entier $m \in \mathbb{N}$, on pose alors $z_m = m!\binom{n+m}{n}\alpha_{n+m}$. De la suite $(z_m)_{m \in \mathbb{N}}$ de points de l'espace compact A, on peut extraire une suite $(z_{m_k})_{k \in \mathbb{N}}$ convergeant vers $z_\infty \in A$. On peut supposer que $m_k \geqslant k$ pour tout $k \in \mathbb{N}$, de sorte que $z_{m_k} \in m!A$ pour tout entier $k \geqslant m$. Comme $m!A$ est fermé dans A, on en déduit

que z_∞ est élément de $m!A$ pour tout $m \in \mathbb{N}$, ce qui prouve que z_∞ est élément de D. D'autre part, on a $n!z_\infty = \lim_{k\to\infty} n!z_{m_k} = \lim_{k\to\infty}(n+m_k)!\alpha_{n+m_k} = d$. Ainsi tout élément de D appartient à $n!D$ pour tout entier $n \geqslant 1$, c'est-à-dire que le groupe abélien D est divisible.

Comme tout groupe divisible compact est connexe [33, page 385], mais que A est supposé totalement discontinu, on voit que $D = \{0\}$. Par conséquent la topologie factorielle de A est séparée. L'image d'un fermé de A par l'application continue Id_A est donc un compact de la topologie factorielle de A. Ainsi tout fermé de A est un fermé de la topologie factorielle de A, et on en conclut que la topologie factorielle de A est plus fine que la topologie de A. □

II.3 Le complété factoriel

II.3.1 Définition et premières propriétés

L'ensemble $\mathbb{N}^*$ des entiers naturels non nuls est un ensemble ordonné pour la relation de divisibilité. Nous pouvons donc le voir comme une catégorie. Étant donné un groupe abélien A, nous définissons le *système projectif naturel* de A en associant à tout objet n de $\mathbb{N}^*$ le quotient A/nA et associant à toute flèche $m \to n$ de $\mathbb{N}^*$ (c'est-à-dire que l'entier naturel non nul m est un diviseur de l'entier naturel non nul n) l'homomorphisme naturel $f_{m,n,A} : A/nA \to A/mA$ tel que

$$\forall a \in A, \qquad f_{m,n,A}(a+nA) = a+mA\ .$$

Définition II.3.1. *Étant donné un groupe abélien A, son complété factoriel $\hat{A}$ est la limite projective du système projectif naturel des groupes abéliens A/nA, où $n \in \mathbb{N}^*$.*

D'après la remarque I.7.6, on voit que le complété factoriel $\hat{A}$ du groupe abélien A est aussi un groupe abélien.

Pour travailler dans $\hat{A}$, on a souvent intérêt à utiliser le théorème d'invariance des limites projectives en remplaçant le système projectif naturel de A par le *système projectif factoriel* de A : il s'agit du système projectif indexé par les entiers naturels non nuls, mais cette fois-ci muni de l'ordre usuel, où l'on associe à tout objet n de $\mathbb{N}^*$ le groupe $A/n!A$, et à toute flèche $m \leqslant n$ de $\mathbb{N}^*$ l'homomorphisme $f_{m!,n!,A}$. Comme les applications

$$G : \mathbb{N}^* \to \mathbb{N}^*, \forall n \in \mathbb{N}^*, G(n) = n! \quad \text{et} \quad H : \mathbb{N}^* \to \mathbb{N}^*, \forall n \in \mathbb{N}^*, H(n) = n$$

sont isotones pour les relations de préordre que nous avons considérées (l'isotonie de G signifie que, lorsque $m \leqslant n$, alors $m!$ est un diviseur de $n!$; l'isotonie de H que, lorsque m est un diviseur de n, alors $m \leqslant n$), et que de plus n divise $G(H(n))$ et que $n \leqslant H(G(n))$ pour tout entier naturel n, la proposition I.5.4 montre que $\hat{A}$ est aussi la limite projective du système projectif factoriel de A.

Pour manipuler les éléments de cette limite projective, on peut utiliser la description de la limite projective (proposition I.5.9) : ses éléments s'identifient à des suites éléments de $\prod_{n\in\mathbb{N}^*}\left(\frac{A}{n!A}\right)$ satisfaisant certaines conditions.

Ainsi, en notant, pour tout entier $n \geqslant 1$, par $p_{n,A}$ la projection naturelle du groupe A sur $A/n!A$, nous pouvons considérer son complété factoriel $\hat{A}$ comme l'ensemble des suites $(p_{n,A}(a_n))_{n\geqslant 1}$ de classes résiduelles modulo $n!A$ d'éléments $a_n \in A$ telles que

$$\forall m \geqslant n \geqslant 1, \qquad a_m - a_n \in n!A. \tag{II.2}$$

Notre premier résultat consiste à caractériser les éléments de $\widehat{A}$ comme des combinaisons A-linéaires de factorielles. Ce point de vue est souvent utile pour travailler dans $\widehat{A}$.

Lemme II.3.2. *Soit $\hat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$ un élément du groupe produit $\prod_{n\geqslant 1} A/n!A$. La suite $\hat{a}$ est élément de $\widehat{A}$ si et seulement s'il existe une suite $(c_n)_{n\in\mathbb{N}}$ d'éléments de A telle qu'on ait*

$$a_n = \sum_{j=0}^{n-1} j!c_j$$

pour tout entier naturel $n \geqslant 1$.

Démonstration. La condition (II.2) qui caractérise les suites $(p_{n,A}(a_n))_{n\geqslant 1}$ éléments de $\widehat{A}$ entraîne en effet l'existence, pour tout entier naturel n, d'un élément c_n de A tel que $a_1 = c_0$ pour $n = 0$ et $a_{n+1} - a_n = n!c_n$ pour tout entier naturel $n \geqslant 1$. La relation $a_n = \sum_{j=0}^{n-1} j!c_j$ s'en déduit par récurrence sur l'entier naturel $n \geqslant 1$.

Réciproquement, l'écriture $a_n = \sum_{j=0}^{n-1} j!c_j$ entraîne que, si on a deux entiers naturels m et n vérifiant $m \geqslant n \geqslant 1$, on a $a_m - a_n = \sum_{j=n}^{m-1} j!c_j$. Comme $j!$ est divisible par $n!$ pour tout entier naturel $j \geqslant n$, on obtient bien la condition (II.2). □

Lemme II.3.3. *Soit A un groupe abélien. On se donne $\hat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$ un élément de $\widehat{A}$, un entier naturel $d \geqslant 1$, et un entier naturel m divisant $d!$. Les deux propriétés suivantes sont équivalentes.*

(i) a_d est élément de mA ;
(ii) $\hat{a}$ est élément de $m\hat{A}$.

Démonstration. Supposons d'abord que $\hat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$ est élément de $m\widehat{A}$. Il existe dans $\widehat{A}$ un $\hat{b} = (p_{n,A}(b_n))_{n\geqslant 1}$ tel que $\hat{a} = m\hat{b}$, d'où $\hat{a} = (p_{n,A}(mb_n))_{n\geqslant 1}$, donc $a_d \equiv mb_d \bmod d!A$. Puisque $d! \in m\mathbb{Z}$ par hypothèse, on voit que a_d est bien élément de mA.

On suppose réciproquement que a_d est élément de mA, c'est-à-dire qu'il existe un élément b_0 de A tel que $a_d = mb_0$. Puisque m est supposé diviseur de $d!$, il existe m' entier naturel tel que $d! = mm'$. On utilise le lemme II.3.2 qui nous assure de l'existence d'une suite $(c_n)_{n\in\mathbb{N}}$ d'éléments de A telle qu'on ait l'égalité $a_n = \sum_{j=0}^{n-1} j!c_j$ pour tout entier naturel $n \geqslant 1$. On pose alors, pour tout entier naturel $n \geqslant 1$, $b_n = b_0 + \sum_{j=0}^{n-1} m'j!\binom{j+d}{d}c_{j+d}$. Par récurrence, on vérifie immédiatement que $mb_n = a_{n+d}$ pour tout entier naturel n. D'autre part, la suite $(b_n)_{n\geqslant 1}$ vérifie évidemment la propriété (II.2), de sorte que $\hat{b} = (p_{n,A}(b_n))_{n\geqslant 1}$ est élément de $\widehat{A}$. On a alors $m\hat{b} = (p_{n,A}(mb_n))_{n\geqslant 1} = (p_{n,A}(a_{n+d}))_{n\geqslant 1}$. Or, d'après la condition (II.2), on a $p_{n,A}(a_{n+d}) = p_{n,A}(a_n)$. Finalement, on obtient que $\hat{a} = m\hat{b}$ est bien un élément de $m\widehat{A}$. □

Proposition II.3.4. *Si le groupe abélien A est sans torsion, alors son complété factoriel $\widehat{A}$ est sans torsion.*

Démonstration. Soit $\widehat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$ un élément de torsion de $\widehat{A}$; il existe un entier $q \geqslant 1$ tel que $q\widehat{a} = 0$. Soit $n \geqslant 1$ un entier quelconque. Puisque $q\widehat{a}$ appartient à $qn!\widehat{A}$, et que $qn!$ est un diviseur de $(q+n)!$, le lemme II.3.3 montre que qa_{n+q} appartient à $qn!A$. Puisque A est supposé sans torsion, on en déduit que a_{n+q} appartient à $n!A$. Utilisant la condition (II.2), on conclut que $n!$ divise a_n. Ceci étant vrai quel que soit l'entier naturel $n \geqslant 1$, on obtient $\widehat{a} = 0$. □

II.3.2 Le morphisme canonique κ_A et sa propriété universelle

Il est intéressant d'étudier le morphisme κ_A de A dans $\widehat{A}$ tel que $\kappa_A(a) = (p_{n,A}(a))_{n\geqslant 1}$ pour tout élément a de A. On remarque que, comme tout morphisme, κ_A est continu quand on munit son domaine A et son codomaine $\widehat{A}$ des topologies factorielles (proposition II.2.6). Il est clair que le noyau du morphisme κ_A est égal à l'intersection $\cap_{n\geqslant 1} n!A$.

Lemme II.3.5. *Pour tout groupe abélien A, et pour tout élément a de A, on a l'égalité*

$$\varphi_A(a) = \varphi_{\widehat{A}}(\kappa_A(a)) \,.$$

Démonstration. Conséquence directe du lemme II.3.3. □

Proposition II.3.6. *L'image de κ_A est dense dans $\widehat{A}$.*

Démonstration. Soit une boule ouverte $B_k(\hat{a}) = \{\hat{x} \in \widehat{A}; \varphi_{\widehat{A}}(\hat{x} - \hat{a}) > k\}$ de $\widehat{A}$, où $\hat{a} \in \widehat{A}$ et $k \in \mathbb{N}$. Alors le centre $\hat{a}$ de cette boule s'écrit $\hat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$. Par le lemme II.3.3, puisque $a_{k+2} - a_{k+2} = 0$ est élément de $(k+2)!A$, la différence $\kappa_A(a_{k+2}) - \hat{a}$ est élément de $(k+2)!\widehat{A}$. Mais, par définition de la filtration factorielle $\varphi_{\widehat{A}}$, ceci signifie que $\kappa_A(a_{k+2})$ appartient à la boule $B_k(\hat{a})$. □

Proposition II.3.7. *Si A est séparé et complet pour sa topologie factorielle, alors l'application κ_A est un isomorphisme de A sur $\widehat{A}$.*

Démonstration. La topologie factorielle étant engendrée par l'écart d, elle est séparée si et seulement si d est une distance, c'est-à-dire si et seulement si κ_A est injective. D'autre part, en vertu du lemme II.3.5, une suite $(\kappa_A(a_h))_{h\in\mathbb{N}}$ est de Cauchy dans $\kappa_A(A)$ si et seulement si la suite $(a_h)_{h\in\mathbb{N}}$ est de Cauchy dans A. Donc $\kappa_A(A)$ est complet, et par conséquent fermé dans $\widehat{A}$. La proposition II.3.6 montre alors que κ_A est surjective. □

Proposition II.3.8. *Pour tout groupe abélien A, et pour tout entier naturel $n \geqslant 1$, l'homomorphisme κ_A induit un isomorphisme entre $A/n!A$ et $\widehat{A}/n!\widehat{A}$.*

Démonstration. Composant κ_A avec la surjection canonique de $\widehat{A}$ sur $\widehat{A}/n!\widehat{A}$, on obtient un homomorphisme de groupes abéliens, surjectif d'après la proposition II.3.6, et de noyau $n!A$ par le lemme II.3.3. □

Corollaire II.3.9. *Soit A un groupe, $m \geqslant 1$ un entier naturel. La topologie initiale sur $\widehat{A}$ pour les projections naturelles $\widehat{A} \to A/m!A$ (où $A/m!A$ est muni de la topologie discrète) coïncide avec la topologie factorielle de $\widehat{A}$.*

Démonstration. Par la proposition II.2.9, nous savons que la topologie factorielle de $\widehat{A}$ coïncide avec la topologie initiale pour les surjections canoniques $\widehat{A} \to \widehat{A}/n!\widehat{A}$. Mais nous venons de voir que

$$a + n!A \mapsto \kappa_A(a) + n!\widehat{A} \qquad (a \in A)$$

est une bijection de $A/n!A$ sur $\widehat{A}/n!\widehat{A}$. □

Le morphisme $\kappa_A : A \to \widehat{A}$ jouit d'une propriété universelle, qu'on peut énoncer comme suit.

Proposition II.3.10. *Soit A un groupe abélien et B un groupe abélien qui est complet et séparé pour sa topologie factorielle. Étant donné un homomorphisme $f : A \to B$ de groupes abéliens, il existe un unique homomorphisme g de $\widehat{A}$ dans B tel que $f = g \circ \kappa_A$.*

Démonstration. Puisque, d'après la proposition II.2.6) tout homomorphisme de groupes est continu pour les topologies factorielles, l'unicité de l'homomorphisme g de $\widehat{A}$ dans B tel que $f = g \circ \kappa_A$ résulte directement de la proposition II.3.6.

Pour montrer l'existence de l'homomorphisme g, on se donne $\widehat{a} = (p_{n,A}(a_n))_{n\geqslant 1}$ un quelconque élément de $\widehat{A}$. Alors, par la condition II.2, on a $a_m - a_n \in n!A$ pour tous les entiers m et n tels que $m \geqslant n \geqslant 1$. Il en résulte que $f(a_m) - f(a_n) \in n!B$ dès que $m \geqslant n \geqslant 1$. Par conséquent, la suite $(f(a_n))_{n\geqslant 1}$ est de Cauchy dans l'espace séparé complet B. Elle admet donc une unique limite. Si d'autre part, on représente le même élément $\widehat{a}$ sous la forme $\widehat{a} = (p_{n,A}(a'_n))_{n\geqslant 1}$ pour d'autres éléments a'_n de A, on a $a_n - a'_n \in n!A$, et donc $f(a_n) - f(a'_n) \in n!B$ pour tout entier $n \geqslant 1$. Par conséquent, la suite $(f(a_n) - f(a'_n))_{n\geqslant 1}$ converge vers 0 dans l'espace séparé B. On en déduit que la limite de la suite $(f(a_n))_{n\geqslant 1}$ ne dépend que de l'élément $\widehat{a}$ de $\widehat{A}$. On peut donc définir une application $g : \widehat{A} \to B$ par

$$\forall\, \widehat{a} = (p_{n,A}(a_n))_{n\geqslant 1} \in \widehat{A}, \qquad g(\widehat{a}) = \lim f(a_n)\ .$$

En particulier, puisque $\kappa_A(a) = (p_{n,A}(a))_{n\geqslant 1}$ pour tout a de A, on voit que $g(\kappa_A(a)) = f(a)$, et on a bien $g \circ \kappa_A = f$. Il reste seulement à vérifier que g est un homomorphisme de groupes, ce qui résulte immédiatement de sa définition et du fait que f est un homomorphisme. □

II.3.3 Le foncteur de complétion

Soit $f : A \to B$ un homomorphisme de groupes abéliens. Alors $\kappa_B \circ f$ est un homomorphisme du groupe abélien dans le groupe abélien $\widehat{B}$ qui est complet et séparé pour sa topologie factorielle (corollaire II.4.5). Par la proposition II.3.10, il existe donc un unique homomorphisme $\widehat{f}$ de $\widehat{A}$ dans $\widehat{B}$ tel que $\kappa_B \circ f = \widehat{f} \circ \kappa_A$. Le diagramme suivant est commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \kappa_A}\downarrow & & \downarrow{\scriptstyle \kappa_B} \\ \widehat{A} & \xrightarrow[\widehat{f}]{} & \widehat{B} \end{array}$$

Il est clair que la donnée pour tout groupe abélien A de son complété factoriel $\widehat{A}$, conjointement à la donnée pour tout homomorphisme de groupes abéliens $f : A \to B$ de l'homomorphisme $\widehat{f} : \widehat{A} \to \widehat{B}$ constitue un foncteur de la catégorie $\mathbb{AB}$ des groupes abéliens dans la sous-catégorie pleine $\mathbb{ABCF}$ des groupes abéliens qui sont complets et séparés pour leur topologie factorielle. Les morphismes κ_A forment une transformation naturelle du foncteur identité de la catégorie $\mathbb{AB}$ vers le composé du foncteur de complétion de la catégorie $\mathbb{AB}$ dans la catégorie $\mathbb{ABCF}$ avec le foncteur d'oubli $\mathbb{ABCF} \to \mathbb{AB}$.

II.4 Limites projectives de groupes abéliens séparés et complets

Proposition II.4.1. *Si $(A_i)_{i\in I}$ est une famille de groupes abéliens qui sont séparés et complets pour la topologie factorielle, alors leur produit $A = \prod_{i\in I} A_i$ est aussi séparé et complet pour la topologie factorielle.*

Démonstration. La démonstration repose sur l'observation que, pour tout entier naturel $n \geqslant 1$, un élément $a = (a_i)_{i\in I}$ du produit $A = \prod_{i\in I} A_i$ est un élément de $n!A$ si et seulement si $a_i \in n!A_i$ pour tout indice i de I.

Montrons d'abord que A est séparé, c'est-à-dire que l'intersection des sous-groupes $n!A$ est réduite à zéro. Si $a = (a_i)_{i\in I}$ est dans cette intersection, alors d'après notre observation préalable, $a_i \in n!A_i$ pour tout indice $i \in I$ et pour tout entier naturel $n \geqslant 1$. Puisque les groupes A_i sont supposés être séparés pour leur topologie factorielle, on en déduit que $a_i = 0$ pour tout $i \in I$. Ainsi a est nécessairement nul, ce qui montre que A est séparé.

Pour vérifier que le groupe A est complet, et puisqu'on sait que sa topologie est pseudo-métrisable, il suffit [34, théorème 24, page 193], de vérifier que toute suite de Cauchy $(a_h)_{h\in\mathbb{N}}$ d'éléments de A est convergente dans A. Écrivons, pour tout entier $h \in \mathbb{N}$, l'élément a_h de A sous la forme $a_h = (a_h(i))_{i\in I}$ pour des éléments $a_h(i)$ de A_i.

Puisque la suite $(a_h)_{h\in\mathbb{N}}$ est de Cauchy, on sait que, pour tout entier naturel $n \geqslant 1$, il existe un entier $h_0(n) \in \mathbb{N}$ tel que, pour tout couple d'entiers (r,s) satisfaisant les inégalités $r \geqslant h_0(n)$ et $s \geqslant h_0(n)$, on ait la congruence $a_r \equiv a_s \bmod n!A$. En traduisant cette dernière congruence grâce à notre observation préalable, on voit que

$$\forall n \geqslant 1, \exists h_0(n) \in \mathbb{N}, \forall (r,s) \in \mathbb{N}^2, \forall i \in I, \min(r,s) \geqslant h_0(n) \Rightarrow a_r(i) \equiv a_s(i) \bmod n!A_i\ . \tag{II.3}$$

Cette relation (II.3) entraîne que, pour tout indice i de I, la suite $(a_h(i))_{h\in\mathbb{N}}$ est de Cauchy dans le groupe A_i. Puisque le groupe A_i est supposé complet, nous en déduisons que cette suite converge dans A_i. Soit $\ell_i \in A_i$ sa limite.

Puisque $n!A_i$ est fermé dans A_i (proposition II.2.8), il résulte de (II.3) que

$$\forall n \geqslant 1, \exists h_0(n) \in \mathbb{N}, \forall s \in \mathbb{N}, \forall i \in I, \quad s \geqslant h_0(n) \Rightarrow \ell_i \equiv a_s(i) \bmod n!A_i. \tag{II.4}$$

Définissons l'élément ℓ de A en posant $\ell = (\ell_i)_{i\in I}$. Alors de (II.4) et de notre observation préalable, on tire

$$\forall n \geqslant 1, \exists h_0(n) \in \mathbb{N}, \forall s \in \mathbb{N}, \quad s \geqslant h_0(n) \Rightarrow \ell \equiv a_s \bmod n!A. \tag{II.5}$$

Par conséquent, la suite $(a_h)_{h\in\mathbb{N}}$ converge dans A vers ℓ. □

Proposition II.4.2. *Si A est un groupe abélien qui est séparé et complet pour sa topologie factorielle, et si B est un sous-groupe de A qui est fermé au sens de la topologie factorielle de A, alors B est séparé et complet pour sa propre topologie factorielle.*

Démonstration. Comme A est séparé, l'intersection des sous-groupes $n!A$ de A est réduite à $\{0\}$. A fortiori, l'intersection des sous-groupes $n!B$ de B est réduite à $\{0\}$, c'est-à-dire que B est séparé.

Pour vérifier que le groupe B est complet, et puisqu'on sait que sa topologie factorielle est pseudo-métrisable, il suffit [34, théorème 24, page 193], de vérifier que toute suite $(b_h)_{h\in\mathbb{N}}$ d'éléments de B qui est de Cauchy au sens de la topologie factorielle de B converge nécessairement dans B pour cette topologie. On remarque que, puisque $n!B \subseteq n!A$ pour tout entier naturel $n \geqslant 1$, la suite $(b_h)_{h\in\mathbb{N}}$ est aussi de Cauchy au sens de la topologie factorielle de A. Puisque A est complet, la suite $(b_h)_{h\in\mathbb{N}}$ converge au sens de la topologie factorielle de A vers une limite $\ell \in A$. Puisque par hypothèse, B est un fermé de la topologie factorielle de A, la limite ℓ est élément de B. Posons alors $b'_h = b_h - \ell$. La suite $(b'_h)_{h\in\mathbb{N}}$ est une suite d'éléments de B qui est

de Cauchy au sens de la topologie factorielle de B et qui converge vers 0 au sens de la topologie factorielle de A. On a donc, en posant, pour tout entier naturel h, $q(h) = \min\big(\{\varphi_A(b'_h)\} \cup \{\varphi_B(b'_{h+k} - b'_h), k \in \mathbb{N}\}\big)$:

$$\lim_{h\to\infty} q(h) = +\infty\ .$$

En particulier, si n est un entier naturel quelconque, il existe un entier naturel $h(n)$ tel qu'on ait l'implication

$$h \geqslant h(n) \Rightarrow q(h) \geqslant n-1\ .$$

On pose alors $H(n) = \max\{h(j) : 0 \leqslant j \leqslant n\} + n$. La suite $(H(n))_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers naturels, de sorte que la suite $(b'_{H(n)})_{n\in\mathbb{N}}$ est une suite extraite de la suite $(b'_h)_{h\in\mathbb{N}}$. De plus on a $H(n) \geqslant h(n)$ et donc $q(H(n)) \geqslant n-1$. Par conséquent $\varphi_A(b'_{H(n)}) \geqslant n-1$ et de même $\varphi_B(b'_{H(n+1)} - b'_{H(n)}) \geqslant n-1$.

Il suffit maintenant de montrer que cette suite extraite $(b'_{H(n)})_{n\in\mathbb{N}}$ converge vers 0 au sens de la topologie factorielle de B. Il est en effet bien connu qu'une suite de Cauchy dont on peut extraire une suite convergente est elle-même convergente. Posons $b''_n = b'_{H(n)}$. On a simultanément $\varphi_A(b''_n) \geqslant n-1$ et $\varphi_B(b''_{n+1} - b''_n) \geqslant n-1$. Donc, pour tout entier natuel n, il existe un élément α_n de A et un élément β_n de B tels que $b''_n = n!\alpha_n$ et $b''_{n+1} - b''_n = n!\beta_n$. On considère alors la suite $(\gamma_n)_{n\in\mathbb{N}}$ d'éléments de A définie par

$$\forall n \in \mathbb{N}, \qquad \gamma_n = (n+1)\alpha_{n+1} - \alpha_n - \beta_n\ .$$

On constate que

$$n!\gamma_n = (n+1)!\alpha_{n+1} - n!\alpha_n - n!\beta_n = b''_{n+1} - b''_n - (b''_{n+1} - b''_n) = 0\ ,$$

ce qui signifie que γ_n est élément du sous-groupe $A[n!]$ défini comme le noyau de l'endomorphisme $x \mapsto n!x$ de A. Comme cet endomorphisme est continu pour la topologie factorielle de A (proposition II.2.6), et que A est séparé par hypothèse pour cette topologie, ce sous-groupe $A[n!]$ est fermé au sens de la topologie factorielle de A.

Pour un entier n donné, on considère les deux suites $(S_q(n))_{q\geqslant n}$ et $(T_q(n))_{q\geqslant n}$ d'éléments de A définies par :

$$S_q(n) = -\sum_{j=n}^{q-1}(j-n)!\binom{j}{n}\beta_j \quad \text{et} \quad T_q(n) = -\sum_{j=n}^{q-1}(j-n)!\binom{j}{n}\gamma_j \quad .$$

Ces deux suites sont évidemment de Cauchy pour la topologie factorielle de A, donc elles convergent dans A vers des limites que nous notons $S_\infty(n)$ et $T_\infty(n)$. D'autre part, pour tout entier $q \geqslant n$, la somme $S_q(n)$ appartient au sous-groupe B et la somme $T_q(n)$ appartient au sous-groupe $A[n!]$. Comme ces deux sous-groupes sont fermés dans A, on voit que $S_\infty(n) \in B$ et que $T_\infty(n) \in A[n!]$. Or

$$S_q(n) + T_q(n) = \sum_{j=n}^{q-1} (j-n)! \binom{j}{n} (-\beta_j - \gamma_j) = \sum_{j=n}^{q-1} (j-n)! \binom{j}{n} (\alpha_j - (j+1)\alpha_{j+1}) \, .$$

Comme $(j+1)\binom{j}{n} = (j+1-n)\binom{j+1}{n}$, on en tire :

$$S_q(n) + T_q(n) = \sum_{j=n}^{q-1} (j-n)! \binom{j}{n} \alpha_j - \sum_{j=n}^{q-1} (j+1-n)! \binom{j+1}{n} \alpha_{j+1} = \alpha_n - (q-n)! \binom{q}{n} \alpha_q \, .$$

En passant à la limite au sens de la topologie factorielle de A pour q tendant vers l'infini, on obtient

$$S_\infty(n) + T_\infty(n) = \alpha_n \, ,$$

d'où, puisque $T_\infty(n)$ est élément de $A[n!]$, l'égalité $n! S_\infty(n) = n! \alpha_n = b''_n$. Comme $S_\infty(n) \in B$, on a montré que b''_n est élément de $n!B$. Ainsi la suite $(b''_n)_{n \in \mathbb{N}}$ converge vers 0 au sens de la topologie factorielle de B, ce qui achève la démonstration. □

Remarque II.4.3. *Cette dernière proposition n'était nullement évidente, car la topologie factorielle de B n'est pas en général la topologie induite sur B par la topologie factorielle de A.*

Par exemple, si on prend $A = \prod_{m \geqslant 2} \mathbb{Z}/m!\mathbb{Z}$, qui est bien un groupe complet et séparé d'après la proposition II.4.1, et si on considère le sous-groupe $B = A[2]$ des éléments $x \in A$ tels que $2x = 0$, on obtient un sous-groupe fermé, dont la topologie factorielle est la topologie discrète. Pourtant, il existe dans B une suite convergente pour la topologie factorielle de A et qui n'est pas stationnaire. En effet, il suffit de considérer la suite $(a_n)_{n \in \mathbb{N}}$ telle que $a_n = (p_{m,\mathbb{Z}}(a(n,m)))_{m \geqslant 2}$ où on a posé

$$a(n,m) = \begin{cases} 0 & \text{si } m \leqslant n \\ \frac{m!}{2} & \text{si } m > n \end{cases} \, .$$

On vérifie facilement que $a_n \in (n-1)!A$. Ainsi la suite $(a_n)_{n \in \mathbb{N}}$ est une suite de points de $A[2]$ qui converge vers 0 au sens de la topologie factorielle de A, mais qui n'est pas

stationnaire.

Corollaire II.4.4. *Toute limite projective de groupes séparés et complets pour leurs topologies factorielles est un groupe séparé et complet pour sa topologie factorielle.*

Démonstration. En effet, soit I une catégorie, et $F : I \to \mathbb{ABCF}$ un foncteur contravariant, de sorte que (I, F) est un système projectif de groupes abéliens séparés et complets pour leurs topologies factorielles. La limite projective $\varprojlim_I F$ se réalise comme le sous-groupe L du produit $A = \prod_{i \in ob(I)} A_i$ déterminé par la condition

$$a = (a_i)_{i \in I} \in L \iff \left(\forall f : i \to j \in Fl(I), F(f)(a_i) = a_j\right).$$

D'après la proposition II.4.1, on sait que A est un groupe séparé et complet. Comme les projections $\mathrm{pr}_i : A \to A_i$ sont des homomorphismes de groupes, elle sont continues pour les topologies factorielles (proposition II.2.6), donc L est, en tant qu'intersection des images réciproques des diagonales $\{(a_j, a_j); a_j \in A_j\}$ par les applications continues $(f_{i,j} \circ \mathrm{pr}_i, \mathrm{pr}_j)$, pour $j \leqslant i$, un sous-groupe de A fermé pour la topologie factorielle de A. Par la proposition II.4.2, on en conclut que la limite projective L est un groupe complet et séparé pour sa propre topologie factorielle. □

Corollaire II.4.5. *Pour tout groupe abélien A, le groupe $\widehat{A}$ est séparé et complet pour la topologie factorielle.*

Démonstration. C'est un cas particulier du corollaire II.4.4, où l'on considère le système projectif des groupes quotients $A/n!A$, avec les morphismes naturels de $A/m!A$ dans $A/n!A$ pour $m \geqslant n$. En effet, la topologie factorielle d'un groupe $A/n!A$ est la topologie discrète, donc ce groupe est bien séparé et complet pour sa topologie factorielle. □

II.5 Filtration factorielle sur un anneau

Soit R un anneau unifère (non nécessairement commutatif). Le groupe additif de R est un groupe abélien, donc on peut définir sa filtration factorielle. Mais cette filtration ne donne pas à R la structure d'anneau filtré au sens défini par exemple dans Bourbaki [22]. En effet, le produit d'un élément de $m!R$ par un élément de $n!R$ n'appartient pas en général à $(m+n)!R$.

Cependant, les sous-groupes $n!R$ qui définissent la filtration factorielle de R sont aussi des idéaux bilatères. Ceci indique une certaine compatibilité entre la structure d'anneau et la filtration factorielle. Les propriétés suivantes précisent ce lien.

On note R^* le groupe multiplicatif de R, dont les éléments sont les inversibles de R.

Proposition II.5.1. *(Propriétés multiplicatives de la multiplication factorielle). Soit φ_R la filtration factorielle sur le groupe additif de l'anneau R, au sens de la définition II.2.1. Outre les propriétés de la proposition II.2.2, cette application φ_R vérifie les propriétés :*

$$\forall a, b \in R, \qquad \varphi_R(ab) \geqslant \max(\varphi_R(a), \varphi_R(b)) \tag{II.6}$$

$$\forall a \in R, \forall n \in \mathbb{N}, \qquad \varphi_R(a^{n+1}) \geqslant \varphi_R(a^n) \tag{II.7}$$

$$\varphi_R(1) = \sup\{k \in \mathbb{N}; \forall j \in [1, k+1], j \cdot 1 \in R^*\}. \tag{II.8}$$

Démonstration. Pour justifier l'équation (II.6), il suffit de remarquer que si l'un des facteurs a ou b est élément de $n!R$, alors il en est de même de leur produit ab.

L'équation (II.7) se déduit de (II.6). On a en effet $a^{n+1} = a^n a$, donc $\varphi_R(a^{n+1}) \geqslant \varphi_R(a^n)$.

Enfin, l'équation (II.8) s'obtient en remarquant que $1 \in n!R$ équivaut à dire que l'élément $d \cdot 1$ est inversible pour tout entier $d \in \mathbb{N} \cap [1, n]$.

□

Lorsqu'on munit R de la topologie factorielle et R^2 de la topologie produit, l'équation (II.6) montre que l'application multiplication $(a, b) \mapsto ab$ est continue en $(0, 0)$. Comme cette application est bi-additive, on en déduit facilement qu'elle est continue en tout point. Ceci montre le résultat suivant.

Remarque II.5.2. *La topologie factorielle d'un anneau est compatible avec sa multiplication, et confère donc à cet anneau la structure d'un anneau topologique.*

En outre, puisque $n!R$ est toujours un idéal bilatère de R, nous pouvons munir le quotient $R/n!R$ d'une structure d'anneau, et donc aussi le produit $P = \prod_{n\geqslant 1} (\frac{R}{n!R})$. Alors le complété factoriel $\hat{R}$ s'identifie à la partie L de P constituée par les éléments $(p_{n,R}(a_n))_{n\geqslant 1}$ satisfaisant la condition (II.2). Il est clair que cette partie L est en fait un sous-anneau de P, et que c'est d'ailleurs une limite projective des anneaux $R/n!R$. Par conséquent le complété factoriel $\hat{R}$ peut aussi être considéré comme la limite projective du système projectif factoriel de R dans la catégorie $\mathbb{A}nn$ des anneaux. En particulier, il

est naturellement muni d'une structure d'anneau, et le morphisme canonique $\kappa_R : R \to \hat{R}$ est un morphisme d'anneaux. On vérifie d'ailleurs facilement l'énoncé suivant, qui est l'analogue de notre proposition II.3.10.

Proposition II.5.3. *Soit R un anneau et S un anneau qui est complet et séparé pour sa topologie factorielle. Étant donné un homomorphisme $f : R \to S$ d'anneaux, il existe un unique homomorphisme d'anneaux g de $\hat{R}$ dans S tel que $f = g \circ \kappa_R$.*

On peut ainsi définir un foncteur de complétion d'anneaux, de manière analogue à ce qui a été fait dans les groupes abéliens, de sorte que les κ_R forment une transformation naturelle du foncteur identité de la catégorie $\mathbb{A}nn$ dans le foncteur de complétion.

II.6 L'anneau des entiers polyadiques

II.6.1 L'anneau $\widehat{\mathbb{Z}}$ et sa filtration factorielle

Dans le cas particulier de l'anneau $\mathbb{Z}$, tout ce qui précède s'applique. Pour simplifier, on note dans cette section p_n, pour un entier naturel $n \geqslant 1$, la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n!\mathbb{Z}$. À la suite de Novoselov [43], nous appelons *entier polyadique* (ou *entier profini* [37], ou *nombre idéal au sens de Prüfer* [46], ou encore *nombre universel* [51]) une suite $(p_n(x_n))_{n\geqslant 1}$ de classes résiduelles modulo $n!$ d'entiers relatifs x_n assujettie à la condition :

$$\forall n \geqslant 1, \qquad x_{n+1} - x_n \in n!\mathbb{Z}\ , \tag{II.9}$$

ou, ce qui est équivalent, à la condition

$$\forall m \geqslant n \geqslant 1, \qquad x_m - x_n \in n!\mathbb{Z}\ . \tag{II.10}$$

Autrement dit, l'anneau $\widehat{\mathbb{Z}}$ des nombres polyadiques est la limite projective des anneaux $\mathbb{Z}/n!\mathbb{Z}$ pour les projections naturelles. Nous considérerons le morphisme canonique $\kappa_{\mathbb{Z}} : \mathbb{Z} \to \widehat{\mathbb{Z}}$ comme une inclusion, en identifiant un entier $x \in \mathbb{Z}$ à la suite $(p_n(x))_{n\geqslant 1}$.

Muni de sa topologie factorielle, $\widehat{\mathbb{Z}}$ est un anneau topologique. On sait (proposition II.3.9) que cette topologie factorielle coïncide avec la topologie initiale pour les applications naturelles de $\widehat{\mathbb{Z}}$ dans $\mathbb{Z}/n!\mathbb{Z}$. Mais cette topologie initiale peut aussi s'interpréter comme la topologie de la limite projective du système projectif factoriel de $\mathbb{Z}$, vu comme

système projectif d'anneaux topologiques discrets. Ainsi l'anneau topologique $\widehat{\mathbb{Z}}$ est un anneau topologique profini, donc compact et totalement discontinu.

Proposition II.6.1. *Soit un élément $x = (p_n(x_n))_{n\geqslant 1}$ de $\widehat{\mathbb{Z}}$. Alors la suite $(x_m)_{m\geqslant 1}$ converge vers x dans $\widehat{\mathbb{Z}}$.*

Démonstration. Identifiant la topologie de $\widehat{\mathbb{Z}}$ avec la topologie initiale pour les applications naturelles $\widehat{\mathbb{Z}} \to \mathbb{Z}/n!\mathbb{Z}$, ceci revient à montrer que, pour tout $n \geqslant 1$ fixé, la suite $(p_n(x_m))_{m\geqslant 1}$ stationne en $p_n(x)$ pour m assez grand : en fait $m \geqslant n$ suffit. □

En particulier, on retrouve ainsi le fait que $\mathbb{Z}$ est une partie dense de $\widehat{\mathbb{Z}}$ (proposition II.3.6). D'après le lemme II.3.2, tout élément x de l'anneau des entiers polyadiques $\widehat{\mathbb{Z}}$, s'écrit sous la forme d'une série convergente

$$x = \sum_{k\geqslant 1} a_k \cdot k! \ (a_k \in \mathbb{Z}).$$

L'anneau topologique $\widehat{\mathbb{Z}}$ est aussi complet d'après notre corollaire II.4.5. La topologie de $\widehat{\mathbb{Z}}$ étant sa topologie factorielle, on peut la caractériser par la fonction « filtration factorielle », c'est-à-dire l'application $\varphi : \widehat{\mathbb{Z}} \to \mathbb{N} \cup \{+\infty\}$ telle que :

$$\forall x = (p_n(x_n))_{n\geqslant 1} \in \widehat{\mathbb{Z}}, \qquad \varphi(x) = \sup\{d \in \mathbb{N} \ ; \ x \in (d+1)!\widehat{\mathbb{Z}}\} \ .$$

D'après le lemme II.3.3, ceci équivaut à

$$\forall x = (p_n(x_n))_{n\geqslant 1} \in \widehat{\mathbb{Z}}, \qquad \varphi(x) = \sup\{d \in \mathbb{N} \ ; \ x_{d+1} \equiv 0 \bmod (d+1)!\} \ . \tag{II.11}$$

L'existence de cette filtration φ et de la distance qui s'en déduit comme ci-dessus (formule (II.1)) montre en particulier que la topologie de $\widehat{\mathbb{Z}}$ est métrisable.

II.6.2 Le groupe additif des entiers polyadiques

Nous allons citer quelques propriétés utiles du groupe topologique additif sous-jacent à $\widehat{\mathbb{Z}}$, que nous utiliserons dans la suite.

Proposition II.6.2. *Le groupe additif de $\widehat{\mathbb{Z}}$ est sans torsion.*

Démonstration. Cas particulier de la proposition II.3.4. □

Corollaire II.6.3. *Pour tout x de $\widehat{\mathbb{Z}}$, et pour tout entier naturel $m \geqslant 1$, on a*

$$\varphi(mx) \leqslant \varphi(x) + m\ .$$

Démonstration. Posons $d = \varphi(mx)$. Si $d \leqslant m$, il n'y a rien à montrer ; supposons donc $d > m$. Par définition de φ, il suffit de montrer que $x \in (d-m+1)!\widehat{\mathbb{Z}}$. Or, du fait que $mx \in (d+1)!\widehat{\mathbb{Z}}$, et que $(d+1)! = \binom{d+1}{m} m!(d-m+1)!$, on voit que $mx \in m(d-m+1)!\widehat{\mathbb{Z}}$. Par la proposition II.3.4 précédente, on conclut en effet que $x \in (d-m+1)!\widehat{\mathbb{Z}}$. □

Pour tout entier rationnel $a \neq 0$, on a une espèce de « division euclidienne par a » dans $\widehat{\mathbb{Z}}$, comme l'exprime l'énoncé suivant.

Proposition II.6.4. *Soit $x \in \widehat{\mathbb{Z}}$ et $a \in \mathbb{Z} \setminus \{0\}$. Il existe un unique entier rationnel r tel qu'on ait simultanément $0 \leqslant r < |a|$ et $x \equiv r \bmod a\widehat{\mathbb{Z}}$.*

Démonstration. On écrit $x = (p_n(x_n))_{n\geqslant 1}$, où les entiers rationnels x_n satisfont la condition (II.9). Par division euclidienne dans $\mathbb{Z}$, on sait qu'il existe un unique entier rationnel r tel que $0 \leqslant r < |a|$ et $x_a \equiv r \bmod a\mathbb{Z}$. Comme $x_a - r \in a\mathbb{Z}$, le lemme II.3.3 montre que $x - r \in a\widehat{\mathbb{Z}}$, ce qui prouve l'existence de r.

Si r' est un autre entier rationnel tel que $0 \leqslant r' < |a|$ et $x \equiv r' \bmod a\widehat{\mathbb{Z}}$, alors $r - r'$ est un entier de valeur absolue strictement moindre que celle de a et qui appartient à $a\widehat{\mathbb{Z}}$. Donc il existe $y = (p_n(y_n))_{n\geqslant 1} \in \widehat{\mathbb{Z}}$ tel que $r - r' = ay$, en particulier $r - r' \equiv ay_a \bmod a!\mathbb{Z}$, ce qui entraîne que $r - r' \in a\mathbb{Z}$. Comme $|r - r'| < |a|$, on en déduit $r = r'$. □

Proposition II.6.5. *Soit G un groupe profini et a un élément de G. Il existe un unique homomorphisme continu f de $\widehat{\mathbb{Z}}$ dans G tel que $f(1) = a$.*

Démonstration. Soit (I, F) le système projectif de groupes finis dont G est limite, de sorte que I est une catégorie d'indices et F est un foncteur contravariant de I dans la catégorie des groupes topologiques tel que, pour tout objet i de I, le groupe $F(i)$ est fini discret. Pour chaque objet i de la catégorie I, le groupe G se trouve muni d'un homomorphisme continu de groupes topologiques $\delta_i : G \to F(i)$; on demande de plus que, pour toute flèche $f : i \to j$ dans la catégorie I, on ait $F(f) \circ \delta_j = \delta_i$. On rappelle que la topologie de G est la topologie initiale pour les applications $\delta_i,\ i \in ob(I)$. Nous convenons de noter multiplicativement les groupes G et $F(i),\ i \in ob(I)$.

Justifions d'abord l'unicité de l'homomorphisme continu f de $\widehat{\mathbb{Z}}$ dans G tel que $f(1) = a$. Si f et g sont deux tels homomorphismes, on a forcément $f(x) = a^x = g(x)$

pour tout entier $x \in \mathbb{Z}$. Comme on l'a observé ci-dessus, $\mathbb{Z}$ est dense dans $\widehat{\mathbb{Z}}$; puisque f et g sont continues, on a donc $f = g$.

Pour montrer l'existence de l'homomorphisme continu f, on observe que si $x = (p_n(x_n))_{n\geqslant 1}$ alors, pour tout objet i de la catégorie I, comme le groupe $F(i)$ est par hypothèse fini, l'ordre de $\delta_i(a)$ dans $F(i)$ est un entier $d_i \geqslant 1$, de sorte qu'on a $\delta_i(a)^{d_i} = 1$. Par conséquent, d'après la condition (II.9), la suite $(\delta_i(a)^{x_n})_{n\geqslant 1}$ est stationnaire à partir de $n = d_i$, donc est convergente dans le groupe discret $F(i)$. La topologie de G étant la topologie initiale pour les applications $\delta_i (i \in ob(I))$, on en déduit que la suite $(a^{x_n})_{n\geqslant 1}$ converge dans le groupe profini G. De plus, si x est représenté sous une autre forme $(p_n(x'_n))_{n\geqslant 1}$, on a alors $x_n \equiv x'_n \bmod n!\mathbb{Z}$ pour tout entier naturel $n \geqslant 1$, donc pour tout $i \in I$, on a $\delta_i(a)^{x_n} = \delta_i(a)^{x'_n}$ pour $n \geqslant d_i$, donc la limite dans $F(i)$ de la suite $(\delta_i(a^{x_n}))_{n\geqslant 1}$ est égale à la limite de la suite $(\delta_i(a^{x'_n}))_{n\geqslant 1}$, ce qui prouve que la limite dans G de la suite $(a^{x_n})_{n\geqslant 1}$ est indépendante de la représentation choisie pour $x \in \widehat{\mathbb{Z}}$. On a ainsi établi que la formule $f(x) = \lim_{n\to+\infty} a^{x_n}$ définit sans ambiguïté une application f de $\widehat{\mathbb{Z}}$ dans G. C'est un homomorphisme : en effet si $x = (p_n(x_n))_{n\geqslant 1}$ et $y = (p_n(y_n))_{n\geqslant 1}$ sont deux éléments de $\widehat{\mathbb{Z}}$, on a $x + y = (p_n(x_n + y_n))_{n\geqslant 1}$ et $a^{x_n+y_n} = a^{x_n}a^{y_n}$ pour tout entier naturel $n \geqslant 1$, d'où la relation $f(x + y) = f(x)f(y)$. Reste à justifier la continuité de f. Par une propriété connue de la topologie initiale, la continuité de f équivaut à la continuité de toutes les applications $\delta_i \circ f, \quad i \in ob(I)$ de $\widehat{\mathbb{Z}}$ dans $F(i)$. Or la topologie de $\widehat{\mathbb{Z}}$ est sa topologie factorielle, et la topologie de $F(i)$ est sa topologie discrète, qui coïncide avec sa topologie factorielle dans le cas d'un groupe fini, car tout groupe fini est d'exposant fini. Donc l'homomorphisme de groupes $\delta_i \circ f : \widehat{\mathbb{Z}} \to F(i)$ est continu. Ceci achève de montrer que f est continue. □

L'image $f(x)$ d'un entier polyadique x par l'homomorphisme continu f tel que $f(1) = a$, dont l'existence et l'unicité sont assurées par la proposition II.3.10, est habituellement notée a^x.

Corollaire II.6.6. *Soit G un groupe profini abélien. La loi externe $(x, a) \mapsto a^x$ de $\widehat{\mathbb{Z}} \times G$ dans G définit sur le groupe abélien G une structure de $\widehat{\mathbb{Z}}$-module.*

Démonstration. La définition de a^x permet de vérifier facilement les identités $a^{x+y} = a^x a^y$, $a^0 = 1$, $(ab)^x = a^x b^x$ et $a^{xy} = (a^x)^y$ pour tous a, b dans G et pour tous x, y dans $\widehat{\mathbb{Z}}$. □

II.6.3 Propriétés des idéaux de $\widehat{\mathbb{Z}}$

Nous donnons ensuite des propriétés utiles des idéaux de l'anneau $\widehat{\mathbb{Z}}$.

Proposition II.6.7. *L'anneau $\widehat{\mathbb{Z}}$ est de Bézout au sens que tout idéal de type fini de $\widehat{\mathbb{Z}}$ est principal.*

Démonstration. Il suffit évidemment de montrer que l'idéal engendré par deux éléments $x = (p_n(x_n))_{n\geqslant 1}$ et $y = (p_n(y_n))_{n\geqslant 1}$ de $\widehat{\mathbb{Z}}$ est un idéal principal. Soit, pour tout entier naturel $n \geqslant 1$, d_n le plus grand commun diviseur des entiers rationnels x_n et y_n. Comme $\widehat{\mathbb{Z}}$ est compact, on peut extraire de la suite $(d_n)_{n\geqslant 1}$ une suite $(d_{n_k})_{k\in\mathbb{N}}$ qui converge dans $\widehat{\mathbb{Z}}$ vers un entier polyadique d. Pour tout entier naturel k, il existe des entiers rationnels u_k et v_k tels que $x_{n_k} = u_k d_{n_k}$ et de même $y_{n_k} = v_k d_{n_k}$. On peut extraire des suites $(u_k)_{k\in N}$ et $(v_k)_{k\in\mathbb{N}}$ des suites convergentes dans $\widehat{\mathbb{Z}}$, ce qui permet de montrer en passant à la limite que $x \in d\widehat{\mathbb{Z}}$ et $y \in d\widehat{\mathbb{Z}}$, de sorte que l'idéal de $\widehat{\mathbb{Z}}$ engendré par x et y est contenu dans $d\widehat{\mathbb{Z}}$. Réciproquement, on sait que pour tout entier naturel k, il existe des entiers rationnels a_k et b_k tels que $d_{n_k} = a_k x_{n_k} + b_k y_{n_k}$; on peut également extraire des suites $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ des suites qui convergent dans $\widehat{\mathbb{Z}}$ vers des limites respectives a et b, de sorte que par passage à la limite on obtient la relation $d = ax + by$ qui montre que $d\widehat{\mathbb{Z}}$ est contenu dans l'idéal engendré par x et y. On conclut donc que ce dernier idéal est l'idéal principal $d\widehat{\mathbb{Z}}$. □

Lemme II.6.8. *Tout idéal fermé de $\widehat{\mathbb{Z}}$ est topologiquement engendré par une partie dénombrable.*

Démonstration. Comme $\widehat{\mathbb{Z}}$ est métrisable et compact, toute partie fermée peut être réalisée comme adhérence d'une partie dénombrable [50]. Soit donc I un idéal fermé de $\widehat{\mathbb{Z}}$ et D une partie dense de I qui est dénombrable. Alors I est l'adhérence de l'idéal engendré par D. □

Le résultat suivant est dû à van Dantzig [51].

Proposition II.6.9. *Tout idéal fermé de $\widehat{\mathbb{Z}}$ est principal.*

Démonstration. D'après le lemme II.6.8, l'idéal fermé I est topologiquement engendré par une partie dénombrable D. Comme D est dénombrable, on sait qu'il existe une suite $(x_k)_{k\in\mathbb{N}}$ d'éléments de I telle que l'ensemble des valeurs prises par cette suite est exactement l'ensemble D. D'après la proposition II.6.7, il existe une suite $(y_k)_{k\in\mathbb{N}}$ à valeurs dans $\widehat{\mathbb{Z}}$ telle que, pour tout entier naturel k, l'idéal de $\widehat{\mathbb{Z}}$ engendré par les

éléments $x_0, x_1, \ldots, x_k$ est l'idéal $y_k\widehat{\mathbb{Z}}$. La partie $D' = \{y_k, k \in \mathbb{N}\}$ engendre alors le même idéal I. De la suite $(y_k)_{k\in\mathbb{N}}$, on peut extraire une suite $\left(y_{k_\ell}\right)_{\ell\in\mathbb{N}}$ qui converge dans $\widehat{\mathbb{Z}}$ vers une limite z. Comme I est fermé, on sait que z est élément de I. D'autre part, fixons un entier naturel k, il existe un entier naturel m tel que $k_m \geqslant k$; on sait que, puisque la suite d'idéaux $\left(y_k\widehat{\mathbb{Z}}\right)_{k\in\mathbb{N}}$ est croissante, l'élément y_k est, pour tout entier naturel r, un multiple de $y_{k_{m+r}}$, de sorte qu'il existe un élément $a_r \in \widehat{\mathbb{Z}}$ tel que $y_k = a_r y_{k_{m+r}}$. De la suite $(a_r)_{r\in\mathbb{N}}$, on peut alors extraire une suite $(a_{r_s})_{s\in\mathbb{N}}$ qui converge dans $\widehat{\mathbb{Z}}$ vers une limite a, ce qui par passage à la limite pour s tendant vers l'infini, fait voir que $y_k \in z\widehat{\mathbb{Z}}$. Comme I est topologiquement engendré par l'ensemble D', on en déduit que $I = z\widehat{\mathbb{Z}}$. □

II.6.4 Arithmétique factorielle dans $\mathbb{N}$

Représentation factorielle

Comme tout élément $x = (p_n(x_n))_{n\geqslant 1}$ de $\widehat{\mathbb{Z}}$ est la limite de la suite (x_n), et comme on peut évidemment imposer aux entiers $x_n \in \mathbb{Z}$ d'être positifs (sinon ajouter un multiple convenable de $n!$), il s'ensuit que l'ensemble des entiers naturels est dense dans $\widehat{\mathbb{Z}}$. Donc on peut considérer $\widehat{\mathbb{Z}}$ comme le complété de $\mathbb{N}$ pour la restriction de la distance factorielle. La représentation des éléments de $\mathbb{N}$ comme somme finie de factorielles donnée par le lemme suivant apparait donc comme la raison profonde du développement des éléments de $\widehat{\mathbb{Z}}$ en série de factorielles qui est un cas particulier du lemme II.3.2.

Lemme II.6.10. *Tout entier naturel non nul n peut s'écrire d'une manière unique sous la forme $n = \sum_{i=1}^{k} n_i \cdot i!$, pour des entiers naturels n_i vérifiant $0 \leqslant n_i \leqslant i$ et $n_k \neq 0$.*

Démonstration. Commençons d'abord par montrer l'existence d'une telle écriture. On l'établit par récurrence sur $n \in \mathbb{N}^*$.

Pour $n = 1$, on prend $k = 1$ et $n_1 = 1$.

Soit un entier fixé $n > 1$. On suppose que l'écriture considérée est vraie pour tout entier plus petit que n. Soit k le plus petit entier naturel tel que $(k+1)! > n$. On a bien sûr $k \geqslant 1$. Posons n_k le quotient dans la division euclidienne de n par $k!$. Comme $n \geqslant k!$ par définition de k, on a certainement $n_k \neq 0$. D'autre part, puisque $n < (k+1)!$, on a $n_k \leqslant k$. Le reste r dans la division euclidienne de n par $k!$ est un entier vérifiant $r < k! \leqslant n$. Deux cas sont possibles.

Si $r = 0$, alors $n = n_k k!$ est l'écriture cherchée.

Si $r > 0$, alors on lui applique l'hypothèse de récurrence et on écrit $r = \sum_{i=1}^{k'} n_i \cdot i!$. On a alors

$$r \geqslant \sum_{i=1}^{k'-1} 0 \cdot i! + n_{k'} k'! \geqslant k'! \,.$$

On en déduit l'encadrement $k'! \leqslant r < k!$. La suite des factorielles $(i!)_{i \geqslant 1}$ étant strictement croissante, alors , on a $k' < k$. Quitte à poser $n_i = 0$ pour $k' < i < k$, on peut donc écrire

$$n = n_k k! + r = \sum_{i=1}^{k} n_i i!$$

ce qui achève la démonstration de l'existence de la décomposition cherchée.

Pour montrer l'unicité, il suffit de remarquer que l'entier k étant fixé, le nombre de décompositions $\sum_{i=1}^{k} n_i i!$, compte tenu des conditions $0 \leqslant n_i \leqslant i$ et $n_k \neq 0$ est exactement $kk(k-1)\cdots 2 = (k+1)! - k!$ qui est le nombre d'entiers n tels que $k! \leqslant n < (k+1)!$. □

On écrit aussi

$$n = (n_k, \ldots, n_1)_!$$

les n_i sont appelés « Chiffres Factoriels », l'écriture de n en fonction des chiffres factoriels est appelée « Représentation Factorielle » ou encore un « Développement factoriel ».

On prolonge le lemme précédent sur l'anneau des entiers polyadiques

Lemme II.6.11. *Pour tout entier polyadique $x \in \widehat{\mathbb{Z}}$, il existe une unique suite $(n_i)_i$ tel que $x = \sum_{i \geqslant 1} n_i i!$ avec $0 \leqslant n_i \leqslant i$.*

Remarque II.6.12. *Pour tout entier $n \in \mathbb{N}$, Nous notons par $t(n)$ l'unique entier k de sorte que $k! \leqslant n < (k+1)!$.*

Nous donnons deux procédures, que nous avons testé sur Maple 13.
La première, détermine la valeur $k = t(n)$.

detk := **proc**(n) ;
local $k := 1$;
while $k * (k-1)! \leqslant n$ **do** $k := k+1$ **od** ;
return $k-1$;
end ;

Et la seconde, nous donne les « chiffres factoriels » (digits) n_i de l'entier n.

lesni := **proc**(n) ;

global tab ;
local k, r, i, $temp$, $n1$, S; $S := 0$;
$k := detk(n)$;
$tab := array(1..1, 1..k)$;
$n1 := n$;
for i **from** k **by** -1 **to** 1 **do** ;
$r := irem(n1, i!)$;
$tab[1, k-i+1] := \frac{(n1-r)}{i!}$;
$n1 := r$; **od** ;
$print(eval(tab))$;
end ;

III

Interpolation polyadique de suites récurrentes linéaires

III.1 Introduction

Dans ce chapitre nous étudions les propriétés des suites récurrentes linéaires et en particulier de la suite de Fibonacci. Nous nous intéressons au calcul de la période modulo un entier naturel m de cette dernière suite. En effet l'existence pour tout m d'une période modulo m est directement liée à la possibilité de prolonger cette suite en une fonction continue sur $\widehat{\mathbb{Z}}$. C'est ce que montre notre critère d'interpolation polyadique pour les suites récurrentes linéaires (théorème III.3.2).

Nous nous référons à la thèse de Necer [41] pour les définitions et les propriétés des suites récurrentes linéaires sur un anneau à valeurs dans un module. A ce jour, il y a des algorithmes qui recherche la période de la suite de Fibonacci, nous nous référons à Wall [55] pour les propriétés de périodicité de la suite de Fibonacci, et à [47] pour rappeler certaines de ses identités.

III.2 Suites récurrentes linéaires

Soit R un anneau unifère (non nécessairement commutatif), M un R-module à gauche et $u : \mathbb{N} \to M$ une suite d'éléments de M.

Définition III.2.1. *Soit $h \in \mathbb{N}^*$. On dit que u est une suite récurrente linéaire de longueur h sur R, s'il existe $a_1, \ldots, a_h$ des éléments de R tels que*

$$\forall n \in \mathbb{N}, \quad u(n+h) = a_1 u(n+h-1) + \cdots + a_h u(n) \tag{III.1}$$

Notons par $Srl_R(M)$ l'ensemble des suites récurrentes linéaires sur R à valeurs dans le R-module M. Et par $Srl(R) = Srl_R(R)$ l'ensemble des suites récurrentes linéaires sur R à valeurs dans R.

Définition III.2.2. *Le polynôme caractéristique de la relation de récurrence (III.1) de longueur $h \in \mathbb{N}^*$ est le polynôme de degré h*

$$P(x) = x^h - a_1 x^{h-1} - \cdots - a_h \quad \in R[x]. \tag{III.2}$$

Exemple III.2.3. *Soit $a \in R$, $m_0 \in M$, la suite « géométrique » $u(n) = a^n m_0$ est suite récurrente linéaire de longueur* 1.

Proposition III.2.4. *Soit M_1, M_2 deux R-modules à gauche, $u \in Srl_R(M_1)$, f une application R-linéaire à gauche de M_1 dans M_2. Alors $f \circ u \in Srl_R(M_2)$.*

III.2.1 Interprétation Matricielle

Afin de simplifier les calculs, dans ce paragraphe, on montre que toute suite récurrente linéaire de longueur $h \geqslant 1$, peut se ramener à une suite récurrente linéaire de longueur 1, c'est-à-dire une suite géométrique, quitte à modifier l'anneau de base.

Soit h un entier strictement positif. On note par $\mathrm{Mat}_h(R)$ l'anneau des matrices carrées d'ordre h à coefficients dans l'anneau R. On convient de noter les éléments du R-module à gauche M^h par des vecteurs colonnes, ce qui permet de voir M^h comme un $M_h(R)$-module à gauche. Soit $u \in Srl_R(M)$ une suite récurrente linéaire de longueur h

vérifiant la relation (III.1). Soit v la suite des vecteurs colonnes dans M^h

$$\forall n \in \mathbb{N}, \qquad v(n) = \begin{pmatrix} u(n) \\ \vdots \\ u(n+h-1) \end{pmatrix}$$

Soit la matrice carrée d'ordre h, à coefficients dans R

$$A = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ a_h & a_{h-1} & \dots & a_1 \end{pmatrix}. \tag{III.3}$$

La matrice A est appelée « la matrice compagnon » du polynôme caractéristique donné dans la définition III.2.2 . On a alors

$$\begin{aligned} \forall n \geqslant 0, \qquad v(n+1) &= Av(n) \\ &= A^{n+1}v(0) \end{aligned} \tag{III.4}$$

de sorte que la suite $v : \mathbb{N} \to M^h$ est une suite géométrique sur l'anneau $\mathrm{Mat}_h(R)$, à valeurs dans le $\mathrm{Mat}_h(R)$-module à gauche M^h. Cette écriture est aussi appelée une représentation matricielle de la suite u. En effet, on peut écrire la suite u en fonction de sa matrice compagnon, il suffit d'introduire un vecteur ligne $w = (1, 0, \dots, 0) \in \mathrm{Mat}_{1,h}(R)$ (avec $\mathrm{Mat}_{1,h}(R)$ l'ensemble des matrices à une ligne et h colonnes). On a

$$\begin{aligned} \forall n \geqslant 0, \qquad u(n) &= wv(n) \\ &= wA^n v(0) \end{aligned} \tag{III.5}$$

III.2.2 La périodicité des suites récurrentes linéaires

Dans ce paragraphe nous donnons les propriétés liées à la période des suites récurrentes linéaires définies sur un anneau unitaire commutatif fini. On essaye de généraliser la périodicité sur des R-modules (finis) ou de type fini.

Définition III.2.5. *Soit M un R-module, soit $u : \mathbb{N} \to M$ une suite d'éléments de M. On dit*

qu'elle est ultimement périodique si

$$\exists n_0 \in \mathbb{N}, \qquad \exists t \in \mathbb{N}^*, \quad \forall n \geqslant n_0, \quad u(n+t) = u(n)$$

L'entier $t > 0$ est appelé « période » de u. Plus précisément, on dira que t est une période de u à partir du rang n_0. Si $n_0 = 0$, alors cette suite est dite purement périodique.
Quand la suite est ultimement périodique, on dit aussi qu'elle est périodique.

Remarque III.2.6. *Toute suite périodique est récurrente linéaire. Si t est une période à partir du rang $n_0 \in \mathbb{N}$, la suite est récurrente linéaire de longueur $n_0 + t$.*

Lemme III.2.7. *Soit h un entier non nul, et u une suite récurrente linéaire de longueur h sur le R-module M. Les deux assertions suivantes sont équivalentes*

i) L'image $u(\mathbb{N})$ est une partie finie de M.

ii) La suite u est périodique.

Démonstration. L'implication (ii)⇒ (i) est évidente. Reste à montrer (i)⇒ (ii).

La partie $u(\mathbb{N})$ est fini se traduit par, la suite récurrente $u \in Srl_R(M)$ de longueur $h \geqslant 1$ prend un nombre fini de valeurs, disons s où $s \in \mathbb{N}^*$.
Posons pour tout entier naturel n, le vecteur colonne

$$v(n) = \begin{pmatrix} u(n) \\ u(n+1) \\ \vdots \\ u(n+h-1) \end{pmatrix}.$$

Le terme général de la suite géométrique v (cf. (III.4)) prend au plus s^h valeurs. Alors il existe au moins deux termes de la suite qui sont égaux

$$\exists n_0 \in \mathbb{N}, \ \exists t \leqslant s^h - 1, \qquad v(n_0) = v(t + n_0)$$

En vertu de la formule (III.4), on en déduit

$$\exists n_0 \in \mathbb{N}, \ \exists t \leqslant s^h - 1, \forall n \geqslant n_0, \quad v(n) = v(t+n)\ .$$

Et d'après la section III.2.1, ou plus précisément la relation (III.5) on a

$$\forall n \geqslant n_0, \quad u(n) = u(n+t)$$

□

Le cas particulier et intéréssant où l'anneau R est fini (par exemple $R = \mathbb{Z}/m\mathbb{Z}$, avec $m \in \mathbb{N}^*$) est donné par le résultat suivant.

Proposition III.2.8. *Soit R un anneau fini, et M un R-module. Alors toute suite u de $Srl_R(M)$ est périodique.*

Démonstration. Soit $u \in Srl_R(M)$ une suite récurrente linéaire de longueur $h \in \mathbb{N}^*$. Le sous-module M' de M engendré par les valeurs $u(0), u(1), \ldots, u(h-1)$ est de type fini sur l'anneau fini R, donc n'a qu'un nombre fini d'éléments. D'après la relation de récurrence (III.1), on a $u(n) \in M'$ pour tout $n \in \mathbb{N}$. Donc l'ensemble $u(\mathbb{N}) \subseteq M'$ est fini. Et d'après le lemme III.2.7, la suite u est périodique. □

Proposition III.2.9. *Soit u une suite récurrente linéaire vérifiant (III.1), de longueur h sur un anneau fini R. Si $a_h \in R^*$ alors la suite u est purement périodique.*

Démonstration. L'anneau R est fini, donc le groupe $GL(h, R)$ des matrices carrées inversibles d'ordre h est fini. Or l'hypothèse $a_h \in R^*$ revient à dire que la matrice compagnon A du polynôme caractéristique de la récurrence satisfaite par u est élément de $GL(h, R)$. En effet, un calcul facile montre que

$$\det(A) = \pm a_h \, .$$

L'ordre multiplicatif t de A dans ce groupe est un entier naturel non nul, divisant l'ordre du groupe $GL(h, R)$. Par conséquent, la suite géométrique v associée à u dans la section III.2.1, est purement périodique de période t. Il en est donc de même de u. □

Fixons u une suite périodique à valeurs dans un R-module M. Sa plus petite période > 0 est notée $T(u)$.

Remarque III.2.10. *Tout multiple d'une période de u est une période de u.*

Proposition III.2.11. *Soit R un anneau unifère, M un R-module, et $u : \mathbb{N} \to M$ une suite périodique. Sa plus petite période > 0, $T(u)$ divise toute autre période.*

Démonstration. Soit k une période de la suite u. Comme $T(u)$ est la plus petite période, on a $T(u) \leqslant k$. Effectuons la division euclidienne de k par $T(u)$

$$k = qT(u) + r, \quad \text{avec } 0 \leqslant r < T(u).$$

On suppose que $r \neq 0$, comme k est une période

$$\forall n \geqslant 0, \qquad u_{n+k} = u_{n+qT(u)+r} = u_n.$$

D'autre part $T(u)$ est une période

$$\forall n \geqslant 0, \qquad u_{qT(u)+n+r} = u_{n+r}.$$

Ceci implique que r est une période plus petite que $T(u)$. Contradiction, donc $r = 0$. □

Corollaire III.2.12. *Soit m un entier strictement positif. Soit A un groupe abélien d'exposant m, et (u_n) une suite récurrente linéaire de longueur h sur l'anneau $\mathbb{Z}/m\mathbb{Z}$, à valeurs $u_n \in A$. On suppose que la récurrence (III.1) satisfaite par cette suite est de la forme :*

$$\forall n \in \mathbb{N}, \quad u(n+h) = a_1 u(n+h-1) + \cdots \pm u(n). \tag{III.6}$$

Alors, la suite (u_n) est purement périodique.

Démonstration. Cas particulier de la proposition III.2.9. □

Le théorème suivant est une conséquence de ce qui précède.

Théorème III.2.13. *Soit $m \geqslant 1$ un entier naturel non nul. Toute suite récurrente linéaire sur $\mathbb{Z}/m\mathbb{Z}$ est périodique.*

Démonstration. En effet $\mathbb{Z}/m\mathbb{Z}$ est un anneau fini. Il suffit donc d'utiliser la proposition III.2.8. □

On rappelle (chapitre II) que, pour tout entier naturel $m \geqslant 1$ et pour tout groupe abélien A, la notation $p_{m,A}$ désigne la surjection canonique de A sur A/mA.

On peut aussi appliquer les résultats de périodicité précédents à une suite récurrente linéaire à valeurs dans un groupe abélien quelconque, si la relation de récurrence (III.1) qu'elle satisfait est à coefficients dans un anneau R sur lequel A est un module à gauche, à condition que, pour tout entier naturel $m \geqslant 1$, l'anneau quotient R/mR soit fini. Ceci s'appliquera en particulier si R est l'anneau des entiers d'un corps de nombres. Soit M un module à gauche sur un tel anneau R, $m \geqslant 1$ un entier naturel, et $u \in Srl_R(M)$. Alors $p_{m,M} \circ u$ est un élément de $Srl_{R/mR}(M/mM)$ qui satisfait la relation de récurrence

$$\forall n \in \mathbb{N}, \qquad x(n+h) = p_{m,R}(a_1)x(n+h-1) + \cdots + p_{m,R}(a_h)x(n).$$

D'après la proposition III.2.8, cette suite $p_{m,M} \circ u$ est périodique, on notera sa période $T(m,u)$ ou plus simplement $T(m)$ si le contexte permet de bien identifier u. De plus, si le coefficient a_h est inversible dans R, cette suite $p_{m,M} \circ u$ est purement périodique d'après la proposition III.2.9.

III.2.3 Cas de la suite de Fibonacci

La célèbre suite de Fibonacci est l'une des plus anciennes suites récurrentes linéaires. Elle est de longueur 2, définie sur $\mathbb{N}$ par la donnée de ses premiers termes $F_0 = 0, F_1 = 1$ et la relation de récurrence

$$\forall n \geqslant 0, \quad F_{n+2} = F_{n+1} + F_n \,. \tag{III.7}$$

On l'étend à l'ensemble $\mathbb{Z}$ des entiers rationnels par la formule

$$\forall n \geqslant 0, \quad F_{-n} = F_{-n+2} - F_{-n+1} = (-1)^{n-1} F_n \,.$$

Son polynôme caractéristique (voir définition III.2.2) est le polynôme

$$P(X) = X^2 - X - 1$$

Il admet deux racines réelles,

$$\alpha = \frac{1+\sqrt{5}}{2} \text{ (le nombre d'or) et } \beta = 1 - \alpha$$

vérifiant

$$\forall n \in \mathbb{Z}, \quad \alpha^n = \alpha F_n + F_{n-1}. \tag{III.8}$$

Et on a la formule

$$\forall n \in \mathbb{Z}, \quad F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{III.9}$$

En plus des propriétés de périodicité des suites récurrentes linéaires sur certains modules, vues ci-dessus (section III.2.2), on détaillera dans ce paragraphe certaines identités concernant la suite de Fibonacci.

Propriété III.2.14. *Soit $m \in \mathbb{N}^*$. Comme le terme constant du polynôme caractéristique de la suite de Fibonacci (F_n) est égal à -1, la suite de Fibonacci est purement périodique modulo m,*

on a donc

$$\forall n \geqslant 0, \quad F_{n+T(m)} \equiv F_n \bmod m \tag{III.10}$$

avec $T(m)$ la période de la suite.

Représentation matricielle de la suite de Fibonacci

On représente la suite de Fibonacci (III.7) sous une forme matricielle. Posons pour tout entier $n \in \mathbb{N}$ vecteur colonne

$$\forall n \geqslant 0, \qquad v_n = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}.$$

La suite géométrique v de terme général le vecteur v_n

$$\forall n \geqslant 0, \quad v_{n+1} = Av_n = A^n v_0$$

avec la matrice compagnon

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{III.11}$$

On vérifie facilement que la puissance de la matrice compagnon de la suite de Fibonacci est donnée par

$$\forall n \geqslant 0, \quad A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

Identités de la suite de Fibonacci

Proposition III.2.15. *Pour tout entier rationnel la suite de Fibonacci vérifie l'identité*

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n \tag{III.12}$$

Démonstration. On a pour tout n dans $\mathbb{Z}$, $det(A^n) = (det(A))^n$. □

Proposition III.2.16. *Pour tout entier rationnel, deux termes consécutifs de la suite de Fibonacci sont premiers entre eux.*

Démonstration. C'est une conséquence directe de l'identité (III.12) qui est l'identité analogue à celle de Bézout. □

Proposition III.2.17. *Pour tout couple $(n,m) \in \mathbb{Z}^2$, la suite de Fibonacci vérifie l'identité*

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}\,.$$

Démonstration. On obtient le résultat, par identification des deux matrices

$$\forall\ (n,m) \in \mathbb{Z}^2, \quad A^{n+m} = A^nA^m\,.$$

□

Proposition III.2.18. *Soit n un entier naturel non nul, pour tout $k \geqslant 2$. Alors F_n divise F_{nk}.*

Démonstration. On l'établit par récurrence sur k. Pour k=2

$$F_{2n} = F_{n+n} = F_{n-1}F_n + F_nF_{n+1} = F_n(F_{n-1} + F_{n+1})$$

On suppose que la proposition est vraie jusqu'à l'ordre $s = k-1$, c'est à dire

$$F_n \mid F_{ns}$$

Posons le vecteur

$$v_{nk} = \begin{pmatrix} F_{nk} \\ F_{nk+1} \end{pmatrix}$$

On a d'après sa représentation matricielle

$$\begin{aligned} v_{nk} &= A^{nk}v_0 \\ &= A^{ns}v_{n(k-s)}\,. \end{aligned}$$

Par identification vectorielle, en remplaçant s par $k-1$, on obtient la relation

$$F_{nk} = F_{n(k-1)-1}F_n + F_{n(k-1)}F_{n+1} \tag{III.13}$$

D'après la relation (III.13) et l'hypothèse de récurrence on a le résultat. □

Remarque III.2.19. *On peut montrer directement les égalités dans $\mathbb{Z}$*

$$F_{nk} = \frac{\alpha^{kn} - \beta^{kn}}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\alpha - \beta}\rho$$

avec ρ un entier qui vaut, $\rho = (\alpha^{m(k-1)} + \cdots + \beta^{m(k-1)})$.

Lemme III.2.20. *Pour tout entier n naturel non nul, on a l'identité*

$$F_n = \frac{1}{2^{n-1}} \left(\binom{n}{1} + \binom{n}{3} 5 + \binom{n}{5} 5^2 + \cdots + \binom{n}{n + \frac{(-1)^{n-1}-1}{2}} 5^{\frac{2n-3+(-1)^{n-1}}{4}} \right).$$

Démonstration. Voir la thèse de M. Renault ([47], page 15). □

Remarque III.2.21. *Posons, pour $n \geqslant 1$,*

$$u(n) = \begin{cases} n & si\ n\ est\ impair \\ n-1 & si\ n\ est\ pair \end{cases}$$

on a alors,

$$u(n+1) = (n+1) + \frac{(-1)^n - 1}{2}$$

Calcul de la période de F_n modulo m

Dans ce paragraphe, nous donnons les propriétés de la période $T(m)$de la suite de Fibonacci modulo m selon l'entier $m \geqslant 1$.

Soit $m = \prod_{i=1}^{r} p_i^{e_i}$ sa décomposition en facteurs premiers. D'après le théorème chinois des restes, on a immédiatement l'identité

$$T(m) = ppcm(T(p_i^{e_i})).$$

Soit p un nombre premier, et $e \in \mathbb{N}^*$. Nous étudions la periodicité de la suite de Fibonacci modulo p^e. Soit $G = GL(2, \mathbb{Z}/p^e\mathbb{Z})$ le groupe des matrices carrées d'ordre 2 inversibles à coefficients dans l'anneau fini $\mathbb{Z}/p^e\mathbb{Z}$. Rappelons que l'ordre k du groupe G est donné par

$$k = p^e(p^e - 1)^2(p^e + 1).$$

Ce nombre k, comme nous le montrons ci-dessous, est une majoration grossière de la période de (F_n) modulo p^e.

Propriété III.2.22. *Soit $e \in \mathbb{N}^*$. Soit p un nombre premier. Alors*

1. *$T(p^e)$ est pair, sauf $T(2)$;*

2. $T(p^e) \mid p^e(p^e-1)^2(p^e+1)$.

Démonstration.
1. Comme $1 \equiv -1 \mod 2$, un calcul direct donne $T(2) = 3$.
Maintenant vérifions la parité de la période $T(p^e)$. Soit A la matrice compagnon de la suite de Fibonacci $(F_n)_n$. On a

$$A^{T(p^e)} = \begin{pmatrix} F_{T(p^e)-1} & F_{T(p^e)} \\ F_{T(p^e)} & F_{T(p^e)+1} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^e ,$$

donc $det(A^{T(p^e)}) = (-1)^{T(p^e)} = +1$. Et par suite $T(p^e)$ est pair.
2. La matrice compagnon A est un élément d'un groupe fini. L'ordre de A est la période $T(p^e)$ modulo p^2 divise l'ordre du groupe. □

Le résultat suivant permet de calculer, pour e entier naturel, la période de la suite (F_n) modulo p^e quand on connaît la période modulo p. On trouvera une démonstration de cette proposition dans [47].

Proposition III.2.23. *Soit, pour $e \geqslant 1$, $T(p^e)$ la période de la suite (F_n) modulo p^e. Si t est le plus grand entier tel que $T(p^t) = T(p)$, alors*

$$\forall e \geqslant t, \quad T(p^e) = p^{e-t}T(p).$$

Une conjecture stipulant que $t = 1$ et datant de 1960 (voir [55]) résiste toujours. À notre connaissance, il n y a ni preuve ni contre exemple. Dans sa thèse, Renault [47] a vérifié que la conjecture $T(p^2) \neq T(p)$ est vraie pour tous les premiers p tels que : $p < 10000$.
Dans la suite, nous aurons besoin de la proposition suivante qui donne la période de la suite de Fibonacci modulo une puissance de 5.

III.3 Prolongement polyadique d'une suite récurrente linéaire

Le but dans ce paragraphe, est de vérifier dans quels cas une suite récurrente linéaire est prolongeable par continuité sur l'anneau des entiers polyadiques $\hat{\mathbb{Z}}$. D'après un théorème classique de prolongement (cf. Schwartz [50]), une fonction uniformément continue d'une partie dense d'un espace métrique dans un espace métrique complet est prolongeable en une unique fonction uniformément continue sur l'espace de départ. On

applique ce résultat à l'espace métrique $\widehat{\mathbb{Z}}$ avec sa partie dense $\mathbb{N}$. La question est donc de savoir quand est-ce qu'une suite récurrente linéaire $u : \mathbb{N} \to A$, où A est un groupe abélien quelconque, est uniformément continue.

Comme au chapitre I, pour $n \geqslant 1$ un entier naturel, et pour A un groupe abélien, on note $p_{n,A} : A \to A/nA$ la surjection canonique.

Proposition III.3.1. *Soit $u : \mathbb{N} \to A$ une suite d'éléments d'un groupe abélien A. Les deux assertions suivantes sont équivalentes.*

(1) L'application u est uniformément continue pour les distances factorielles.

(2) Pour tout entier naturel $d \geqslant 1$, la suite $(p_{d,A}(u_n))_{n\in\mathbb{N}}$ des valeurs de u modulo d est purement périodique.

Démonstration. Soit φ la filtration factorielle de $\widehat{\mathbb{Z}} \supset \mathbb{N}$, et φ_A celle du groupe abélien A. Par définition de l'uniforme continuité d'une application entre espaces métriques, l'assertion (1) équivaut à

$$\forall d \in \mathbb{N}, \exists k \in \mathbb{N}, \forall (m,n) \in \mathbb{N}^2, \varphi(m-n) \geqslant k \Rightarrow \varphi_A(u(m)-u(n)) \geqslant d\ .$$

Par définition de φ, ceci équivaut à

$$\forall d \in \mathbb{N}, \exists k \in \mathbb{N}, \forall (m,n) \in \mathbb{N}^2, m \equiv n \bmod (k+1)! \Rightarrow u(m) \equiv u(n) \bmod (d+1)!A\ . \tag{III.14}$$

Si ces implications sont vérifiées, alors on voit que pour $d \in \mathbb{N}$, les valeurs de u modulo $(d+1)!A$ admettent la période $(k+1)!$. Comme d est un diviseur de $(d+1)!$, on en déduit que la suite des valeurs de u modulo d est purement périodique.

Réciproquement, si (2) est vérifiée, alors fixons $d \in \mathbb{N}$. La suite des valeurs de u modulo $(d+1)!A$ est purement périodique par hypothèse, soit $t > 0$ l'une de ses périodes. Alors (III.14) est vérifiée avec $k = t$. □

Théorème III.3.2. *Soit R un anneau unifère tel que, pour tout entier naturel $d \geqslant 1$, l'anneau quotient R/dR est fini, et M un R-module à gauche. On note $\hat{R}$ (resp. $\hat{M}$) le complété factoriel de R (resp. de M). Soit $u : \mathbb{N} \to M$ une suite récurrente linéaire satisfaisant la relation de récurrence (III.1). La suite u est prolongeable en une unique fonction continue $f : \widehat{\mathbb{Z}} \to \hat{M}$ si le coefficient a_h est inversible dans $\hat{R}$.*

Démonstration. Soit $d \geqslant 1$ un entier naturel. Comme on sait que $R/dR \sim \hat{R}/d\hat{R}$, on voit que $p_{d,R}(a_h)$ appartient au groupe des éléments inversibles de l'anneau R/dR. Donc

la proposition III.2.9 montre que, pour tout entier naturel $d \geqslant 1$, la suite $(p_{d,M} \circ u$ est purement périodique. L'application $u : \mathbb{N} \to M$ est donc uniformément continue pour les distances factorielles d'après la proposition III.3.1 précédente, ce qui permet d'appliquer le résultat de prolongement donné par [50]. □

Exemple de la suite de Fibonacci

Le polynôme caractéristique $X^2 - X - 1$ de la suite de Fibonacci ayant un coefficient constant inversible dans $\mathbb{Z} \subset \widehat{\mathbb{Z}}$, le théorème III.3.2 assure l'existence et l'unicité d'une fonction continue $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ telle qu'on ait

$$\forall n \in \mathbb{N}, \qquad f(n) = F_n \, .$$

Cette fonction a été étudiée par Lenstra [37] qui a pu en particulier en déterminer les points fixes.

IV

Base de van der Put

IV.1 Introduction

L'objet de cette étude est l'anneau $\mathscr{C}$ des fonctions continues de $\widehat{\mathbb{Z}}$ dans $\widehat{\mathbb{Z}}$. L'instrument fondamental dans cette analyse est la *filtration factorielle* du groupe (ou de l'anneau) $\widehat{\mathbb{Z}}$ de la définition II.2.1 : c'est l'application $\varphi = \varphi_{\widehat{\mathbb{Z}}}$ de $\widehat{\mathbb{Z}}$ dans $\mathbb{N} \cup \{+\infty\}$ définie par

$$\forall x \in \widehat{\mathbb{Z}}, \qquad \varphi(x) = \max\left\{d \in \mathbb{N}; x \in (d+1)!\widehat{\mathbb{Z}}\right\} \text{ si } x \neq 0 \qquad \text{et} \quad \varphi(0) = +\infty.$$

L'anneau $\widehat{\mathbb{Z}}$, muni de la distance $d : \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}} \to [0,1]$ définie par

$$d(x,y) = 2^{-\varphi(x-y)} \text{ si } x \neq y \qquad \text{et} \quad d(x,y) = 0 \text{ si } x = y, \tag{IV.1}$$

est un espace métrique compact. Mais nous n'utiliserons jamais cette distance, dont la définition recèle une part d'arbitraire, et nous aurons recours systématiquement à la filtration φ. De façon analogue, la topologie de la convergence uniforme sur la $\widehat{\mathbb{Z}}$-algèbre

$\mathscr{C}$ sera manipulée à travers la filtration $\Phi : \mathscr{C} \to \mathbb{N} \cup \{+\infty\}$ telle que

$$\forall f \in \mathscr{C}, \qquad \Phi(f) = \min\left\{\varphi(f(x)); x \in \widehat{\mathbb{Z}}\right\}.$$

En effet, nous observons que la distance uniforme de deux éléments $f \neq g$ de $\mathscr{C}$ n'est autre que $2^{-\Phi(f-g)}$. L'espace topologique $\mathscr{C}$ est donc complet pour cette filtration. On remarque qu'on a

$$\Phi(af) \geqslant \max(\varphi(a), \Phi(f))$$

pour tout $a \in \widehat{\mathbb{Z}}$ et tout $f \in \mathscr{C}$.

Soit un ensemble I et un anneau filtré R (i,e. c'est un anneau muni d'une filtration φ_R). Notre objectif est de comparer le R-module topologique $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ au R-module topologique $c_0(I, R)$ constitué des suites $(a_i)_{i\in I}$ d'éléments de R indexées par I qui tendent vers 0 selon le filtre des complémentaires de parties finies de I. Pour cela, nous montrons que les développements de van der Put des fonctions continues sur $\mathbb{Z}_p$, présentés par Diarra [27], ont des analogues pour des fonctions continues sur $\widehat{\mathbb{Z}}$.

Si

$$\varphi_R : R \to \mathbb{N} \cup \{+\infty\}$$

est la filtration de R, nous définissons la topologie du R-module $c_0(I, R)$ par la filtration $\Phi_{I,R} : c_0(I, R) \to \mathbb{R} \cup \{+\infty\}$ telle que

$$\forall a = (a_i)_{i\in I} \in c_0(I, R), \qquad \Phi_{I,R}(a) = \inf\{\varphi_R(a_i); i \in I\}.$$

Soit R un anneau filtré séparé et complet. Par définition, une *base orthonormale* de $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ est une partie $\{e_i; i \in I\}$ de $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ telle que l'application de $c_0(I, R)$ dans $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ qui envoie $(a_i)_{i\in I}$ sur $\sum_{i\in I} a_i e_i$ est une bijection isométrique. On remarque que, lorsque l'anneau R est supposé complet, la famille des $(a_i e_i)_{i\in I}$ est sommable dès que la famille $(a_i)_{i\in I}$ est élément de $c_0(I, \widehat{\mathbb{Z}})$.

IV.2 Les coefficients de van der Put d'une fonction

À tout entier $n \geqslant 1$ nous associons l'entier $t(n) \geqslant 1$ défini comme le plus grand entier tel que $t(n)! \leqslant n$. Cet entier a déjà été présenté dans la chapitre II voir remarque II.6.12, où nous avons donné un algorithme de calcul de cet entier. On a donc $t(1) = 1, t(2) = t(3) = t(4) = t(5) = 2, t(6) = t(7) = \cdots = t(23) = 3, t(34) = 4, t(999) = 6, \ldots$. Nous

convenons en outre de poser $t(0) = 0$. Pour un entier $n \geqslant 1$, la notation n^- désigne le reste dans la division euclidienne de n par $t(n)!$.

Pour toute fonction f définie sur un ensemble $E \supseteq \mathbb{N}$ et à valeurs dans un groupe abélien A, nous définissons la suite des *coefficients de van der Put* de f comme la suite $(a_n(f))_{n\in\mathbb{N}}$ d'éléments de A donnée par les formules :

$$a_0(f) = f(0) \qquad \text{et} \qquad \forall n \geqslant 1,\ a_n(f) = f(n) - f(n^-).$$

Proposition IV.2.1. *Si A est un groupe topologique séparé abélien, et si f est une application continue de $\widehat{\mathbb{Z}}$ dans A, alors la suite des coefficients de van der Put de f tend vers 0 dans A.*

Démonstration. Puisque $\widehat{\mathbb{Z}}$ est un espace métrique compact, l'application f est uniformément continue sur $\widehat{\mathbb{Z}}$. Cela signifie qu'étant donné un quelconque voisinage U de 0 dans A, il existe un entier $N_U \in \mathbb{N}$ tel que

$$\forall (x,y) \in \widehat{\mathbb{Z}}\times\widehat{\mathbb{Z}}, \quad \varphi(x-y) \geqslant N_U \Rightarrow f(x) - f(y) \in U\ .$$

On remarque par ailleurs que, pour tout $n \geqslant 1$, on a $n \equiv n^- \pmod{t(n)!}$, c'est-à-dire $\varphi(n - n^-) \geqslant t(n) - 1$. Par conséquent, pour tout $n \geqslant (1 + N_U)!$, comme on a alors $t(n) - 1 \geqslant N_U$, on voit que $\varphi(n - n^-) \geqslant N_U$, de sorte qu'on a $f(n) - f(n^-) = a_n(f) \in U$, c'est-à-dire que la suite $(a_n(f))_{n\in\mathbb{N}}$ tend vers 0 dans A, comme on voulait l'établir. □

IV.3 Parties initiales d'un entier polyadique

Étant donné un entier $n \geqslant 0$, et un élément x de $\widehat{\mathbb{Z}}$, nous dirons que *n est une partie initiale de x* lorsqu'on a la congruence

$$x \equiv n \pmod{(t(n)+1)!}\ ,$$

ce qui équivaut aussi à l'inégalité $\varphi(x - n) \geqslant t(n)$.

Lemme IV.3.1. *La relation binaire $a \triangleleft b$ définie sur $\mathbb{N} \subseteq \widehat{\mathbb{Z}}$ par*

$$\forall (a,b) \in \mathbb{N}^2, \qquad a \triangleleft b \Leftrightarrow \textit{a est une partie initiale de b}$$

est une relation d'ordre partiel, pour laquelle 0 est élément minimal de $\mathbb{N}$. *De plus on a l'implication* $a \triangleleft b \Rightarrow a \leqslant b$.

Démonstration. Si $a > b$, alors $0 < a - b < a$, de sorte que $0 < t(a-b) \leqslant t(a) < t(a)+1$, donc $(t(a)+1)! > a - b \geqslant 1$, d'où résulte que $(t(a)+1)!$ ne peut être diviseur de $a-b$, et donc que $\varphi(b-a) = \varphi(a-b) < t(a)$, c'est-à-dire que a ne peut être partie initiale de b.

Ceci prouve en particulier que la relation $\triangleleft$ est antisymétrique. Elle est d'autre part réflexive, car, pour tout $a \in \mathbb{N}$, on a $\varphi(a-a) = +\infty \geqslant t(a)$. Reste à justifier qu'elle est transitive.

Donnons-nous trois entiers naturels a, b, c tels que $\varphi(b-a) \geqslant t(a)$ et $\varphi(c-b) \geqslant t(b)$. On a montré qu'on a forcément alors $a \leqslant b$, donc $t(a) \leqslant t(b)$. Par l'inégalité ultramétrique, on en déduit que $\varphi(c-a) \geqslant \min(\varphi(c-b), \varphi(b-a)) \geqslant t(a)$, c'est-à-dire que a est partie initiale de c.

Enfin, le fait que 0 est élément minimal de $\mathbb{N}$ pour la relation $\triangleleft$ est immédiat. □

Lemme IV.3.2. *Soit* x *un entier naturel, et* $E(x)$ *l'ensemble des entiers naturels qui sont parties initiales de* x. *Alors l'ensemble* $E(x)$ *est fini. De plus, l'application* $n \mapsto n^-$ *détermine une bijection de l'ensemble* $E(x) \setminus \{0\}$ *sur l'ensemble* $E(x) \setminus \{x\}$.

Démonstration. D'après le lemme IV.3.1, l'ensemble $E(x)$ est contenu dans l'ensemble fini $\mathbb{N} \cap [0, x]$, donc il est lui-même fini.

Si $n \in E(x) \setminus \{0\}$, alors on a $\varphi(x-n) \geqslant t(n)$ et $n = jt(n)! + n^-$, où $n^- \in \mathbb{N} \cap [0, t(n)! - 1]$; on a nécessairement $j > 0$, sinon $n = n^-$ serait moindre que $(t(n))!$, ce qui contredit la définition de $t(n)$; de même, on a $j \leqslant t(n)$ sinon au aurait $n \geqslant (t(n)+1)!$, ce qui contredirait aussi la définition de $t(n)$. Donc $\varphi(n - n^-) = \varphi(j(t(n))!) = t(n) - 1$. Par conséquent, le caractère ultramétrique de φ montre que $\varphi(x - n^-) = t(n) - 1$. Or l'inégalité $n^- < t(n)!$ montre que $t(n^-) \leqslant t(n) - 1$. Ainsi on a montré que $\varphi(x - n^-) \geqslant t(n^-)$, c'est-à- dire que $n^- \triangleleft x$. D'autre part $n^- < n \leqslant x$, donc n^- est différent de x. Nous avons ainsi montré que $n \mapsto n^-$ détermine une application de l'ensemble $E(x) \setminus \{0\}$ dans l'ensemble $E(x) \setminus \{x\}$. Reste à montrer qu'elle est bijective.

Pour cela, on peut observer que $0 \in E(x)$ et $x \in E(x)$, donc les deux ensembles finis $E(x) \setminus \{0\}$ et $E(x) \setminus \{x\}$ ont le même nombre d'éléments, de sorte qu'il suffit en fait de montrer la surjectivité de notre application pour établir que c'est une bijection. Soit donc m une partie initiale de x, et supposons que $m \neq x$. Alors $d = \varphi(x-m)$ est un entier naturel, et on sait que $d \geqslant t(m)$, donc $(d+1)! > m$. On a donc $x \equiv m \pmod{(d+1)!}$,

et il existe donc un entier y tel que $x = m + (d+1)!y$. On a $y > 0$ du fait que $x > m$ d'après le lemme IV.3.1. Mais de plus, comme on a exactement $d = \varphi(x-m)$, on est certain que $(d+2)!$ ne divise pas $x - m = (d+1)!y$, c'est-à-dire que $d+2$ ne divise pas y. On peut donc écrire par division euclidienne $y = (d+2)z + r$, où z est entier naturel et $r \in \mathbb{N} \cap [1, d+1]$. Alors posons $n = m + r(d+1)!$; nous avons $\varphi(x-n) = \varphi(z(d+2)!) \geqslant d+1$ et $(d+1)! \leqslant (d+1)!r \leqslant n < (d+1)! + (d+1)(d+1)! = (d+2)!$, d'où l'on tire $t(n) = d+1 \leqslant \varphi(x-n)$, de sorte que n est une partie initiale de x. On a forcément $n > 0$ et $n^- = m$ résulte alors de $n = m + r(d+1)!$, avec $t(n) = d+1$, $m < (d+1)!$ et $r > 0$. □

IV.4 La formule d'interpolation de van der Put

Soit A un groupe abélien. La n-ième *fonction de van der Put* e_n est l'application de $\widehat{\mathbb{Z}}$ dans $\mathbb{Z}$ telle que $e_n(x) = 1$ si n est une partie initiale de x, et $e_n(x) = 0$ sinon. Par conséquent, e_0 est la fonction constante égale à l'unité, e_1 est la fonction indicatrice des entiers polyadiques impairs, e_2 la fonction indicatrice des entiers polyadiques congrus à 2 modulo 6, etc.

Proposition IV.4.1. *Soit $f : \mathbb{N} \to A$ une suite d'éléments du groupe abélien A. Pour tout entier naturel x, l'ensemble des entiers n tels que $e_n(x) \neq 0$ est fini, et on a*

$$f(x) = \sum_{n=0}^{\infty} a_n(f) e_n(x) \ ,$$

où cette dernière série converge dans le groupe discret A.

Démonstration. L'ensemble des entiers n tels que $e_n(x) \neq 0$ est l'ensemble $E(x)$ des parties initiales de x, donc est fini par le lemme IV.3.2.

On en déduit que la série $\sum_{n=0}^{\infty} a_n(f) e_n(x)$ converge dans le groupe discret A, et que, puisque $0 \in E(x)$, sa somme est :

$$\sum_{n=0}^{\infty} a_n(f) e_n(x) = \sum_{n \in E(x)} a_n(f) = a_0(f) + \sum_{n \in E(x) \setminus \{0\}} a_n(f) = f(0) + \sum_{n \in E(x) \setminus \{0\}} f(n) - f(n^-) \ ,$$

d'où, par le lemme IV.3.2 :

$$\sum_{n=0}^{\infty} a_n(f)e_n(x) = \sum_{n\in E(x)} f(n) - \sum_{n\in E(x)\setminus\{x\}} f(n) = f(x)\ .$$

□

IV.5 Le théorème de van der Put

Soit R un anneau. On modifie la définition précédente des fonctions de van der Put e_n en considérant dorénavant que e_n est à valeurs dans R, et non plus dans $\mathbb{Z}$. Cela revient à remplacer $e_n : \widehat{\mathbb{Z}} \to \mathbb{Z}$ par sa composée avec le morphisme canonique $\mathbb{Z} \to R$.

Théorème IV.5.1. *Soit R un anneau filtré séparé et complet. L'ensemble $\{e_n; n \in \mathbb{N}\}$ est une base orthonormale du R-module topologique $\mathscr{C}(\widehat{\mathbb{Z}}, R)$.*

Démonstration. Nous allons montrer que l'application $f \mapsto (a_n(f))_{n\in\mathbb{N}}$ définie par les formules

$$a_0(f) = f(0) \qquad \text{et} \qquad \forall n \geqslant 1,\ a_n(f) = f(n) - f(n^-)$$

est une isométrie de $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ sur $c_0(\mathbb{N}, R)$.

Soit $f \in \mathscr{C}(\widehat{\mathbb{Z}}, R)$, et posons $a = (a_n(f))_{n\in\mathbb{N}} \in R^{\mathbb{N}}$ pour désigner la suite de ses coefficients de van der Put.

L'anneau R est muni d'une filtration φ_R qui est une application de R dans $\mathbb{N} \cup \{+\infty\}$ telle que

$$\forall (a,b) \in R^2, \qquad \varphi_R(a+b) \geqslant \min(\varphi_R(a), \varphi_R(b))$$

$$\forall a \in R \setminus \{0\}, \qquad \varphi_R(a) \neq +\infty$$

$$\varphi_R(0) = +\infty\ .$$

On munit $\mathscr{C}(\widehat{\mathbb{Z}}, R)$ de la filtration Φ telle que

$$\forall f \in \mathscr{C}(\widehat{\mathbb{Z}}, R), \qquad \Phi(f) = \min\left\{\varphi_R(f(x)); x \in \widehat{\mathbb{Z}}\right\}.$$

Quant à $c_0(\mathbb{N}, R)$, on le munit de la filtration

$$\forall b = (b_n)_{n\in\mathbb{N}}, \qquad \Phi_{\mathbb{N},R}(b) = \min\{\varphi_R(b_n); n \in \mathbb{N}\}.$$

On désire montrer l'égalité $\Phi(f) = \Phi_{\mathbb{N},R}(a)$. Or, si $x \in \mathbb{N}$, par la proposition IV.4.1, on a

$$f(x) = \sum_{n \in E(x)} a_n(f)$$

d'où

$$\varphi_R(f(x)) \geqslant \min\{\varphi_R(a_n(f)); n \in E(x)\} \geqslant \min\{\varphi_R(a_n(f)); n \in \mathbb{N}\} = \Phi_{\mathbb{N},R}(a) \ .$$

Maintenant, si x est élément de $\widehat{\mathbb{Z}}$, il est limite d'une suite d'entiers naturels $(x_k)_{k\in\mathbb{N}}$. On a alors $f(x) = \lim f(x_k)$ par continuité de $f \in \mathscr{C}(\widehat{\mathbb{Z}}, R)$, et donc $\varphi_R(f(x)) = \lim \varphi_R(f(x_k)) \geqslant \Phi_{\mathbb{N},R}(a)$. Cette inégalité étant vérifiée pour tout $x \in \widehat{\mathbb{Z}}$, on en déduit que

$$\Phi(f) \geqslant \Phi_{\mathbb{N},R}(a) \ .$$

Pour établir l'inégalité en sens contraire, considérons le plus petit entier $n_0 \in \mathbb{N}$ tel que $\Phi_{\mathbb{N},R}(a) = \varphi_R(a_{n_0}(f))$. Alors, d'après la proposition IV.4.1, on a

$$f(n_0) = \sum_{n \in E(n_0)} a_n(f) \ .$$

Mais, par définition de n_0, on sait que $\varphi_R(a_n(f)) > \varphi_R(a_{n_0}(f))$ pour tout entier naturel $n < n_0$. Il résulte de la propriété ultramétrique de φ_R qu'on a donc

$$\varphi_R(f(n_0)) = \varphi_R(a_{n_0}(f)) = \Phi_{\mathbb{N},R}(a) \ .$$

D'où $\Phi(f) \leqslant \varphi_R(f(n_0)) = \Phi_{\mathbb{N},R}(a)$. Ceci achève démontrer que la transformation de van der Put qui à $f \in \mathscr{C}(\widehat{\mathbb{Z}}, R)$ associe la suite de ses coefficients de van der Put est bien une isométrie. On va maintenant montrer que cette transformation est bijective. L'injectivité est évidente, puisque c'est une isométrie et que les filtrations Φ et $\Phi_{\mathbb{N},R}$ sont séparées. Soit $(b_n)_{n\in\mathbb{N}}$ un élément de $c_0(\mathbb{N}, R)$. Alors la série de fonctions de terme général $b_n e_n : \widehat{\mathbb{Z}} \to R$ est uniformément convergente sur $\widehat{\mathbb{Z}}$, de sorte que sa somme est une fonction continue de $\widehat{\mathbb{Z}}$ dans R, dont les coefficients de van der Put sont les b_n. On a ainsi montré que la transformation de van der Put est bijective, et que sa réciproque est l'application qui à la suite $(b_n)_{n\in\mathbb{N}} \in c_0(\mathbb{N}, R)$ associe la somme $\sum_{n\in\mathbb{N}} b_n e_n$, ce qui achève la démonstration. □

V

La fonction logarithme

V.1 Introduction

Pour illustrer l'intérêt de l'analyse sur les nombres polyadiques, ce chapitre va se concentrer sur la construction et l'étude des propriétés d'une fonction logarithme polyadique, définie sur le groupe des éléments inversibles de l'anneau $\widehat{\mathbb{Z}}$ des nombres polyadiques. Le logarithme doit être évidemment un homomorphisme continu du groupe multiplicatif $\widehat{\mathbb{Z}}^*$ dans le groupe additif $\widehat{\mathbb{Z}}$. Nous obtenons un tel homomorphisme comme limite uniforme d'une suite de fonctions $(A_n)_{n\in\mathbb{N}}$ à valeurs dans $\widehat{\mathbb{Z}}$ définie par l'identité

$$\forall n \in \mathbb{N}, \forall a \in \widehat{\mathbb{Z}}^*, \qquad a^{n!} = 1 + n! A_n(a) \ .$$

La possibilité de définir une telle fonction A_n est liée à son tour à des propriétés intéressantes de la fonction arithmétique de Carmichael, qui s'expriment à l'aide des factorielles.

Nous montrons également que cette définition du logarithme ne peut être comprise dans la notion de dérivée au sens de Novoselov de la fonction exponentielle. Par contre nous sommes en mesure de montrer que cette fonction logarithme est dérivable au sens

de Novoselov, avec bien sûr pour dérivée la fonction inverse.

Nous étudions ensuite le radical de Jacobson J de l'anneau $\widehat{\mathbb{Z}}$ et nous le munissons d'une structure d'idéal à puissances divisées, ce qui permet de construire une fonction exponentielle de $2J$ dans $1+2J \subset \widehat{\mathbb{Z}}^*$ qui est une section de la fonction logarithme. Pour établir cette dernière propriété, nous utilisons une espèce de lemme de Hensel pour les séries de Hurwitz. Ce lemme de Hensel, comme il se doit, est démontré par la méthode itérative de Newton.

V.2 Définition du logarithme

V.2.1 Propriétés de la fonction de Carmichael

Rappelons que la *fonction de Carmichael*, que nous noterons λ, est la fonction de $\mathbb{N}^*$ dans $\mathbb{N}^*$ telle que, pour tout entier naturel $n \geqslant 1$, le nombre $\lambda(n)$ est défini comme étant l'exposant du groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire le plus petit entier $m > 0$ tel que, pour tout entier naturel a premier à n, on a $a^m \equiv 1 \bmod n$. La propriété suivante est fondamentale pour notre construction.

Proposition V.2.1. *Pour tout nombre premier p et pour tout entier naturel $n \geqslant p-1$, le nombre $\lambda(n!p)$ est un diviseur de $n!$.*

Démonstration. L'ensemble des entiers $m \in \mathbb{Z}$ tels que $a^m \equiv 1 \bmod n!p$ pour tout entier naturel a premier à $n!$ étant un sous-groupe de $\mathbb{Z}$, doit nécessairement être l'ensemble des multiples de $\lambda(n!p)$. De ce fait, il suffit d'établir que, si $a \in \mathbb{N}$ est premier à $n!p$, alors $a^{n!} \equiv 1 \bmod n!p$. Soit $P(n)$ l'ensemble des nombres premiers non supérieurs à n et, pour tout $q \in P(n) \cup \{p\}$, soit $k(q,n) \geqslant 1$ la valuation q-adique de $n!p$. D'après le théorème chinois, il suffit de montrer que $a^{n!} \equiv 1 \bmod q^{k(q,n)}$ pour tout premier $q \in P(n) \cup \{p\}$. Or un théorème d'Euler assure que, puisque $k(q,n) \geqslant 1$ pour tout $q \in P(n) \cup \{p\}$, on a $a^{q^{k(q,n)-1}(q-1)} \equiv 1 \bmod q^{k(q,n)}$ dès que a est premier à q, en particulier pour a premier à $n!p$. Or, lorsque $q \in P(n) \cup \{p\}$, on a $q \leqslant n+1$, donc $q-1$ est un diviseur de $n!$; d'autre part, pour $q \in P(n) \setminus \{p\}$, puisque $q^{k(q,n)-1}$ est évidemment un diviseur de $q^{k(q,n)}$ qui divise $n!$, on voit que $q^{k(q,n)-1}$ est un diviseur de $n!$, alors que, pour $q = p$, le fait que $p^{k(p,n)}$ divise $n!p$ suffit à montrer que $p^{k(p,n)-1}$ est un diviseur de $n!$. Puisque, pour tout nombre premier $q \in P(n) \cup \{p\}$, les nombres $q-1$ et $q^{k(q,n)-1}$ sont premiers entre eux, on voit que leur produit $q^{k(q,n)-1}(q-1)$ est un diviseur de $n!$, et donc on a bien la congruence $a^{n!} \equiv 1 \bmod q^{k(q,n)}$ pour tout $q \in P(n) \cup \{p\}$. □

Corollaire V.2.2. *Pour tout entier naturel $n \geqslant 1$, le nombre $\lambda(n!)$ est un diviseur de $n!$.*

Démonstration. Il suffit de remarquer que $\lambda(n!)$ est un diviseur de $\lambda(2 \cdot n!)$. □

Dans le cas $n = p - 1$, on a un résultat qu'il est utile d'énoncer à part.

Corollaire V.2.3. *Pour tout entier naturel premier $p \geqslant 2$, le nombre $\lambda(p!)$ est un diviseur de $(p-1)!$.*

V.2.2 Définition de la suite A_n

Proposition V.2.4. *Si a est un élément inversible de l'anneau $\widehat{\mathbb{Z}}$, et si $n \geqslant 1$ est un entier naturel, alors $a^{n!} - 1$ est élément de $n!\widehat{\mathbb{Z}}$.*

Démonstration. Puisque $a \in \widehat{\mathbb{Z}}$, il existe une suite $(a_n)_{n\geqslant 1}$ d'entiers relatifs satisfaisant la condition (II.9) telle que $a = (p_n(a_n))_{n\geqslant 1}$. Puisque de plus, a est supposé inversible, on sait que $p_n(a_n)$ est inversible dans l'anneau $\mathbb{Z}/n!\mathbb{Z}$, c'est-à-dire que l'entier a_n est premier à $n!$. Par le corollaire V.2.2, on voit que $a_n^{n!} \equiv 1 \bmod n!$, c'est-à-dire que $a_n^{n!} - 1$ est élément de $n!\mathbb{Z}$, ce qui équivaut au résultat cherché d'après le lemme II.3.3. □

Cette proposition montre l'existence, pour tout élément inversible a de l'anneau $\widehat{\mathbb{Z}}$ et pour tout entier naturel $n \geqslant 1$, d'un entier polyadique $A_n(a)$ tel que

$$a^{n!} - 1 = n! A_n(a)\ . \tag{V.1}$$

De plus, la proposition II.3.4 prouve qu'un tel entier polyadique $A_n(a)$ est unique.

Notons $\widehat{\mathbb{Z}}^*$ le groupe des éléments inversibles de $\widehat{\mathbb{Z}}$. On a ainsi construit une suite $(A_n)_{n\geqslant 1}$ de fonctions de $\widehat{\mathbb{Z}}^*$ dans $\widehat{\mathbb{Z}}$. Nous allons dans la suite étudier la limite de cette suite. Pour étudier la continuité de la limite, il sera intéressant d'avoir montré la continuité de la fonction A_n pour tout entier $n \geqslant 1$. Ceci résulte en effet de la proposition suivante.

Proposition V.2.5. *Soit X un espace topologique, f une fonction de X dans $\widehat{\mathbb{Z}}$ et α un élément de $\widehat{\mathbb{Z}}$ qui n'est pas diviseur de zéro. Alors l'application f est continue si et seulement si l'application g de X dans $\widehat{\mathbb{Z}}$ définie par $g(x) = \alpha f(x)$ pour tout x de X est continue.*

Démonstration. En effet, l'application continue $y \mapsto n!y$ de $\widehat{\mathbb{Z}}$ dans $\alpha\widehat{\mathbb{Z}}$ est bijective. Par conséquent, puisque $\widehat{\mathbb{Z}}$ est compact, elle est fermée et donc bicontinue. □

D'après cette proposition, et puisque $n!$ n'est pas diviseur de zéro d'après la proposition II.3.4, la continuité de la fonction A_n sur $\widehat{\mathbb{Z}}^*$ équivaut à celle de la fonction $a \mapsto a^{n!} - 1$; or il s'agit là d'une fonction polynomiale, donc continue.

Nous aurons besoin de la remarque suivante. De la même manière que pour la proposition V.2.4 précédente que nous avons déduite du corollaire V.2.2, on peut à partir du corollaire V.2.3 montrer que, si a est un élément inversible de $\widehat{\mathbb{Z}}$ et si $p \geqslant 2$ est un nombre premier, alors $a^{(p-1)!} - 1$ est élément de $p!\widehat{\mathbb{Z}}$. Comme $a^{(p-1)!} - 1 = (p-1)!A_{p-1}(a)$ et que $\widehat{\mathbb{Z}}$ est sans torsion (proposition II.3.4), nous avons le résultat suivant.

Lemme V.2.6. *Pour tout $a \in \widehat{\mathbb{Z}}^*$, et pour tout nombre premier $p \geqslant 2$, l'entier polyadique $A_{p-1}(a)$ est élément de $p\widehat{\mathbb{Z}}$.*

Comme $\lambda(4!) = 2$ est aussi un diviseur de $3! = 6$, le même raisonnement montre aussi le fait suivant.

Lemme V.2.7. *Pour tout $a \in \widehat{\mathbb{Z}}^*$, l'entier polyadique $A_3(a)$ est élément de $4\widehat{\mathbb{Z}}$.*

V.2.3 Convergence de la suite A_n

Lemme V.2.8. *Soient deux entiers naturels n et k tels que $2 \leqslant k \leqslant n$. Alors l'entier naturel $\binom{n+1}{k} n!^k$ est divisible par $(n+1)!(n-2)!$.*

Démonstration. On part de la relation entre coefficients binomiaux

$$(n+1-k)\binom{n+1}{k} = (n+1)\binom{n}{k}.$$

Multipliant les deux membres de cette relation par l'entier $n!^k$, on trouve

$$(n+1-k)\binom{n+1}{k} n!^k = (n+1)!\ (n-2)!\ n(n-1)n!^{k-2}\binom{n}{k}.$$

Comme $n+1-k$ divise $n-1$ si $k=2$ et $n!^{k-2}$ si $k>2$, on obtient le résultat voulu. □

Lemme V.2.9. *Soit $n \geqslant 2$ un entier naturel et $a \in \widehat{\mathbb{Z}}^*$. Alors la somme $\sum_{k=2}^{n+1} \binom{n+1}{k} n!^k A_n(a)^k$ est élément de $(n+1)!(n-2)!\widehat{\mathbb{Z}}$.*

Démonstration. Tous les termes de la somme autres que le dernier sont dans $(n+1)!(n-2)!\widehat{\mathbb{Z}}$ d'après le lemme V.2.8. Il n'y a donc plus qu'à montrer que le dernier terme

$n!^{n+1}A_n(a)^{n+1}$ est lui aussi élément de $(n+1)!(n-2)!\widehat{\mathbb{Z}}$. Pour cela, nous examinons successivement trois cas.

Tout d'abord, si $n = 3$, le lemme V.2.7 assure que $A_3(a)$ est élément de $4\widehat{\mathbb{Z}}$, donc $3!A_3(a)$ est élément de $4!\widehat{\mathbb{Z}}$, et donc à plus forte raison, il en est de même de $3!^4A_3(a)^4$.

Dans le cas où $n+1$ est un nombre premier $\geqslant 3$, le lemme V.2.6 assure de même que $A_n(a) \in (n+1)\widehat{\mathbb{Z}}$, donc $n!A_n(a)$ est élément de $(n+1)!\widehat{\mathbb{Z}}$. Comme d'autre part $n!^n$ est divisible par $(n-2)!$, la conclusion s'ensuit.

Reste à examiner le cas où $n+1$ est un nombre composé différent de 4. Si $n+1$ admet une factorisation en deux nombres distincts, ces deux entiers sont $\leqslant n$, donc $n+1$ est un diviseur de $n!$. Si ce n'est pas le cas, c'est que $n+1$ est le carré d'un nombre premier $q \geqslant 3$, auquel cas q et $2q$ sont deux entiers distincts $< n$, donc leur produit est là aussi diviseur de $n!$, et donc pareillement $n+1$ est diviseur de $n!$. Alors $n!^{n+1}$ est un multiple de $(n+1)n!^n$ qui, puisque $n \geqslant 2$, est lui-même multiple de $(n+1)n!(n-2)! = (n+1)!(n-2)!$. □

Proposition V.2.10. *La suite de fonctions $(A_n)_{n\in\mathbb{N}}$ est de Cauchy uniformément sur $\widehat{\mathbb{Z}}^*$.*

Démonstration. On a $(n+1)!A_{n+1}(a) = a^{(n+1)!} - 1 = (a^{n!})^{n+1} - 1 = (1+n!A_n(a))^{n+1} - 1$, d'où par la formule du binôme

$$(n+1)!A_{n+1}(a) = \sum_{k=1}^{n+1} \binom{n+1}{k} n!^k A_n(a)^k = (n+1)!A_n(a) + \sum_{k=2}^{n+1} \binom{n+1}{k} n!^k A_n(a)^k \,.$$

D'après le lemme V.2.9, on sait que, si $n \geqslant 2$, il existe un entier polyadique $C(n,a)$ tel que $\sum_{k=2}^{n+1} \binom{n+1}{k} n!^k A_n(a)^k = (n+1)!(n-2)!C(n,a)$, on obtient donc :

$$(n+1)!A_{n+1}(a) = (n+1)!A_n(a) + (n+1)!(n-2)!C(n,a)\,,$$

d'où par la proposition II.3.4 :

$$A_{n+1}(a) - A_n(a) = (n-2)!C(n,a),$$

et donc d'après le lemme II.3.3

$$\forall a \in \widehat{\mathbb{Z}}^*, \qquad \varphi(A_{n+1}(a) - A_n(a)) \geqslant n-3\,.$$

Donc la suite de fonctions $(A_{n+1} - A_n)_{n\geqslant 1}$ converge vers 0 uniformément sur $\widehat{\mathbb{Z}}^*$, c'est-à-dire que la suite $(A_n)_{n\geqslant 1}$ est de Cauchy uniformément sur $\widehat{\mathbb{Z}}^*$. □

V.2.4 Le logarithme

Puisque $\widehat{\mathbb{Z}}$ est complet, la proposition V.2.10 implique que la suite $(A_n)_{n\geqslant 1}$ converge uniformément sur $\widehat{\mathbb{Z}}^*$.

Définition V.2.11. *Pour tout élément inversible a de $\widehat{\mathbb{Z}}$, la limite de la suite $(A_n(a))_{n\geqslant 1}$ est appelée logarithme de a. Elle est notée* $\log a$.

Proposition V.2.12. *La fonction* log *de $\widehat{\mathbb{Z}}^*$ dans $\widehat{\mathbb{Z}}$ est continue.*

Démonstration. La fonction log est la limite uniforme de la suite de fonctions $(A_n)_{n\geqslant 1}$. Comme on a remarqué comme conséquence de la proposition V.2.5 que chaque fonction A_n est continue sur $\widehat{\mathbb{Z}}^*$, le résultat s'en déduit. □

Proposition V.2.13. *La fonction* log *est une forme linéaire sur le $\widehat{\mathbb{Z}}$-module $\widehat{\mathbb{Z}}^*$.*

Démonstration. Remarquons que le groupe $\widehat{\mathbb{Z}}^*$ est la limite projective de la suite des groupes $(\mathbb{Z}/n!\mathbb{Z})^*)$ des éléments inversibles des anneaux finis $\mathbb{Z}/n!\mathbb{Z}$, et est donc un groupe profini, et par conséquent, d'après le corollaire II.6.6, un $\widehat{\mathbb{Z}}$-module. Il s'agit simplement de vérifier les deux identités

$$\log(ab) = \log a + \log b \qquad \text{et} \qquad \log(a^x) = x \log a$$

pour tous les éléments a, b de $\widehat{\mathbb{Z}}^*$ et x de $\widehat{\mathbb{Z}}$. La première identité s'obtient en passant à la limite dans la relation $A_n(ab) = A_n(a) + A_n(b) + n!A_n(a)A_n(b)$. Puisque $\mathbb{Z}$ est dense dans $\widehat{\mathbb{Z}}$, la deuxième se justifie en remarquant que ses deux membres sont des fonctions continues de $x \in \widehat{\mathbb{Z}}$ qui ont les mêmes valeurs en tout $x \in \mathbb{Z}$. □

V.2.5 Non dérivabilité de la fonction exponentielle de base a

Nous avons obtenu le logarithme d'un élément a inversible dans $\widehat{\mathbb{Z}}$ comme limite de $A_n(a)$ qui est en quelque sorte un taux d'accroissement de la fonction $x \mapsto a^x$ exponentielle de base a. On peut se demander si cette dernière fonction ne serait pas dérivable en 0, ce qui permettrait de définir aussi le logarithme de a comme le nombre dérivé en 0 de cette fonction exponentielle de base a. Pour interpréter cette question, nous pouvons avoir recours à la définition des fonctions dérivables proposée par Novoselov [43] : une fonction $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ est dite dérivable en 0 avec le nombre dérivé $A \in \widehat{\mathbb{Z}}$ s'il existe un voisinage $V(0)$ de 0 et une fonction $g : V(0) \to \widehat{\mathbb{Z}}$ tels que $f(x) - f(0) = xg(x)$ pour

tout $x \in V(0)$ et $\lim_{x\to 0} g(x) = A$. Évidemment, si $a = -1$, cette définition est satisfaite en prenant $V(0) = 2\widehat{\mathbb{Z}}$ et $g(x) = 0$. Nous allons voir qu'il n'en est pas de même en général, c'est-à-dire qu'il existe au moins un élément a inversible dans $\widehat{\mathbb{Z}}$ tel que la fonction exponentielle de base a n'est pas dérivable en 0 au sens de Novoselov.

Étant donné un nombre premier q, on sait qu'il existe une racine primitive g_q modulo q, c'est-à-dire tel que $g_q^d \equiv 1 \bmod q$ si et seulement si l'entier d est un multiple de $q-1$. Construisons par récurrence une suite $(a_n)_{n\geqslant 1}$ d'entiers naturels en posant $a_1 = 1$ et en définissant a_{n+1} comme égal à a_n si $n+1$ n'est pas premier et en choisissant, lorsque $n+1$ est premier, un entier naturel a_{n+1} tel que $a_{n+1} \equiv a_n \bmod n!$ et $a_{n+1} \equiv g_{n+1} \bmod n+1$, ce qui est possible en vertu du théorème chinois puisque $n+1$ est alors premier à $n!$. Comme la condition (II.9) est alors vraie pour tout entier naturel $n \geqslant 1$, on voit que $a = (p_n(a_n))_{n\geqslant 1}$ est un élément de $\widehat{\mathbb{Z}}$. Puisqu'il est immédiat de vérifier par récurrence que a_n est toujours premier à $n!$, c'est aussi un élément de $\widehat{\mathbb{Z}}^*$. Supposons maintenant que la fonction exponentielle de base a soit dérivable au sens de Novoselov. Alors il existe un entier $d \geqslant 1$ et une fonction $g : d!\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ telle que $a^x - 1 = xg(x)$ pour tout $x \in d!\widehat{\mathbb{Z}}$. Choisissons un nombre premier $r > d$; d'après le théorème de la progression arithmétique de Dirichlet, il existe un entier naturel ℓ tel que le nombre $q = \ell r + 1$ soit également premier. En vertu du théorème chinois des restes, il existe un entier $x \in \mathbb{Z}$ tel que x soit divisible par $d!q$ et $x \equiv 1 \bmod r$. Puisque x est divisible par $d!$, on peut écrire $a^x - 1 = xg(x)$. Ceci implique en particulier que $a_q^x - 1 \equiv xc_q \bmod q!$ pour un certain entier $c_q \in \mathbb{Z}$, donc $a_q^x - 1$ doit être divisible par q. Mais comme, par définition, nous avons $a_q \equiv g_q \bmod q$ et donc $g_q^x \equiv 1 \bmod q$; puisque g_q est supposé être une racine primitive modulo q, ceci entraîne que x est un multiple de $q-1 = \ell r$, et donc aussi du nombre r, ce qui n'est pas le cas par construction de x. Cette contradiction achève de montrer que la fonction exponentielle de base a n'est pas dérivable.

V.3 Dérivabilité du logarithme

Nous allons étudier la dérivabilité du logarithme sur $\widehat{\mathbb{Z}}^*$ en étendant la définition de Novoselov de la manière suivante.

Définition V.3.1. *Étant donnés une fonction $f : \widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$ et un point $a_0 \in \widehat{\mathbb{Z}}^*$, on dit que f est dérivable (au sens de Novoselov) en a_0 de nombre dérivé $f'(a_0)$ s'il existe un voisinage $V(a_0)$ de a_0 dans $\widehat{\mathbb{Z}}^*$ et une fonction $g : V(a_0) \to \widehat{\mathbb{Z}}$ telle que $f(a) - f(a_0) = (a - a_0)g(a)$ pour tout élément $a \in V(a_0)$, avec $\lim_{a\to a_0} g(a) = f'(a_0)$.*

Nous montrerons dans la proposition V.4.8 que le nombre dérivé $f'(a_0)$, s'il existe, est unique. Dans cette section, nous établissons que, au sens de Novoselov, la fonction inverse $a \mapsto a^{-1}$ est la dérivée sur $\widehat{\mathbb{Z}}^*$ de la fonction log.

V.3.1 Une propriété arithmétique

Introduisons, pour tout entier naturel $n \geqslant 1$ et tout entier $x \in \mathbb{Z}$, la somme $S_n(x) = \sum_{k=0}^{n-1} x^j$ des n premiers termes de la série géométrique de raison x.

Lemme V.3.2. *Soient $m \geqslant 1$ et $n \geqslant 1$ deux entiers naturels. Alors on a, pour tout entier $x \in \mathbb{Z}$:*

$$S_{mn}(x) = S_m(x)S_n(x^m) = S_m(x^n)S_n(x) \ .$$

Démonstration. On peut considérer les expressions S_m, S_n, S_{mn} comme des éléments de l'anneau intègre $\mathbb{Z}[x]$ et utiliser la formule $x^m - 1 = (x-1)S_m(x)$ et ses analogues, d'où $(x-1)S_{mn}(x) = x^{mn} - 1 = (x^m - 1)S_n(x^m) = (x-1)S_m(x)S_n(x^m) = (x^n - 1)S_m(x^n) = (x-1)S_m(x^n)S_n(x)$. □

L'énoncé qui suit caractérise le cas où $S_n(x)$ est divisible par n.

Proposition V.3.3. *Soient un entier naturel $n \geqslant 1$ et un entier $x \in \mathbb{Z}$. Alors n divise $S_n(x)$ si et seulement si $x^n \equiv 1 \bmod n$.*

Démonstration. D'un côté, l'identité $x^n - 1 = (x-1)S_n(x)$ montre que si $S_n(x)$ est divisible par n, alors $x^n - 1$ l'est aussi.

Réciproquement, soit E l'ensemble des nombres entiers naturels $n \geqslant 1$ tels que, pour tout $x \in \mathbb{Z}$ tel que $x^n \equiv 1 \bmod n$, on ait $S_n(x) \equiv 0 \bmod n$. Montrons par récurrence sur l'entier ν que, pour tout nombre premier q, l'entier $q^\nu \in E$. On remarque que $1 = q^0 \in E$; d'autre part, si $x^q \equiv 1 \bmod q$, le petit théorème de Fermat montre que $x \equiv 1 \bmod q$ et alors $S_q(x) \equiv \sum_{k=0}^{q-1} 1 = q \bmod q$, donc $q \in E$. Si donc on suppose que $\nu \geqslant 2$ est un entier naturel tel que $q^{\nu-1} \in E$, alors soit $x \in \mathbb{Z}$ tel que $x^{q^\nu} \equiv 1 \bmod q^\nu$; alors x est premier à q^ν et le théorème d'Euler montre que $x^{q^\nu - q^{\nu-1}} \equiv 1 \bmod q^\nu$, donc on a $x^{q^{\nu-1}} \equiv 1 \bmod q^\nu$, à plus forte raison $x^{q^{\nu-1}} \equiv 1 \bmod q^{\nu-1}$, de sorte que l'hypothèse de récurrence montre que $S_{q^{\nu-1}}(x)$ est divisible par $q^{\nu-1}$. D'autre part, comme $(x^{q^{\nu-1}})^q \equiv 1 \bmod q$ par hypothèse, le fait déjà observé que q est élément de E montre que $S_q(x^{q^{\nu-1}})$ est divisible par q. Or, par le lemme V.3.2, on a $S_{q^\nu}(x) = S_{q^{\nu-1}}(x)S_q(x^{q^{\nu-1}})$, de sorte que $S_{q^\nu}(x)$ est bien divisible par q^ν.

Montrons ensuite que, si m et n sont deux éléments de E premiers entre eux, alors leur produit mn est aussi élément de E ; en effet, soit $x \in \mathbb{Z}$ tel que $x^{mn} \equiv 1 \bmod mn$. Alors $(x^m)^n \equiv 1 \bmod n$, donc l'hypothèse que $n \in E$ entraîne que $S_n(x^m)$ est divisible par n ; or, le lemme V.3.2 montre que $S_n(x^m)$ est un diviseur de $S_{mn}(x)$; par conséquent, nous avons montré que n est un diviseur de $S_{mn}(x)$. Mais l'hypothèse que $m \in E$ entraîne de même que m est un diviseur de $S_{mn}(x)$. Les entiers m et n étant premiers entre eux, on a bien que mn divise $S_{mn}(x)$, ce qui montre que mn est élément de E, comme on voulait le montrer.

Finalement, si $n \geqslant 1$ est un entier naturel, le théorème fondamental de l'arithmétique assure que n est un produit de puissances de nombres premiers, donc un produit d'éléments de E qui sont deux à deux premiers entre eux ; il résulte de ce qui précède que n est élément de E, ce qui achève la démonstration. □

V.3.2 Divisibilité de A_n par $a-1$ dans l'anneau des fonctions continues sur $\widehat{\mathbb{Z}}^*$

Proposition V.3.4. *Soit $n \geqslant 1$ un entier naturel. Il existe une fonction continue $B_n : \widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$ telle que $A_n(a) = (a-1)B_n(a)$ pour tout élément a de $\widehat{\mathbb{Z}}^*$. On peut choisir B_n de sorte qu'elle satisfasse l'identité $n!B_n(a) = \sum_{k=0}^{n!-1} a^k$ pour tout $a \in \widehat{\mathbb{Z}}^*$.*

Démonstration. Soit $a = (p_n(a_n))_{n\geqslant 1}$ un élément inversible de $\widehat{\mathbb{Z}}^*$. Pour tout entier naturel $n \geqslant 1$, l'élément $p_n(a_n)$ est inversible dans l'anneau $\mathbb{Z}/n!\mathbb{Z}$, c'est-à-dire que a_n est premier à $n!$, et le corollaire V.2.2 montre que $a_n^{n!} \equiv 1 \bmod n!$, ce qui d'après la proposition V.3.3 équivaut à dire que $n!$ divise $S_{n!}(a_n)$, ce qui signifie par le lemme II.3.3 que $\sum_{k=0}^{n!-1} a^k$ est élément de $n!\widehat{\mathbb{Z}}$. Il existe donc un entier polyadique $B_n(a)$, unique par la proposition II.3.4, tel que $\sum_{k=0}^{n!-1} a^k = n!B_n(a)$. Multipliant les deux membres de cette égalité par $a-1$, on trouve $a^{n!} - 1 = n!(a-1)B_n(a)$. Comme on a $a^{n!} - 1 = n!A_n(a)$, on déduit par la proposition II.3.4 que $A_n(a) = (a-1)B_n(a)$. La fonction B_n est continue sur $\widehat{\mathbb{Z}}^*$ par application de la proposition V.2.5. □

Nous allons maintenant donner des formules de récurrence qui expriment $B_{n+1}(a)$ en fonction de $A_n(a)$ et $B_n(a)$.

Proposition V.3.5. *Si $n+1$ est un nombre composé différent de 4, il existe un entier naturel*

d_n tel que $n! = d_n(n+1)$, et on a alors

$$B_{n+1}(a) = B_n(a) + \binom{n}{2}(n-2)!nB_n(a)A_n(a) + d_nB_n(a)\sum_{k=2}^{n}\binom{n+1}{k+1}n!^{k-1}A_n(a)^k\ .$$

Démonstration. On a vu que $n+1$ divise $n!$ dans la démonstration du lemme V.2.9. On a par définition de B_n

$$(n+1)!B_{n+1}(a) = \sum_{k=0}^{(n+1)!-1} a^k = \left(\sum_{k=0}^{n!-1} a^k\right)\left(\sum_{j=0}^{n} a^{n!j}\right) = n!B_n(a)\left(\sum_{j=0}^{n} a^{n!j}\right)\ .$$

Soit $S_{n+1}(x)$ le polynôme $S_{n+1}(x) = \sum_{j=0}^{n} x^j$ de degré n. On écrit la formule de Taylor

$$S_{n+1}(x) = \sum_{k=0}^{n}(x-1)^k S_{n+1}^{[k]}(1)\ ,$$

où $S_{n+1}^{[k]}(x)$ est la dérivée k-ième divisée par $k!$, qui se calcule facilement :

$$S_{n+1}^{[k]}(x) = \sum_{j=k}^{n}\binom{j}{k}x^{j-k}\ ,$$

d'où $S_{n+1}^{[k]}(1) = \sum_{j=k}^{n}\binom{j}{k} = \binom{n+1}{k+1}$. Par conséquent, on obtient :

$$(n+1)!B_{n+1}(a) = n!B_n(a)S_{n+1}(a^{n!}) = n!B_n(a)\sum_{k=0}^{n}\binom{n+1}{k+1}(a^{n!}-1)^k\ .$$

Comme $a^{n!} - 1 = n!A_n(a)$, on obtient

$$(n+1)!B_{n+1}(a) = n!B_n(a)\sum_{k=0}^{n}\binom{n+1}{k+1}n!^kA_n(a)^k\ . \tag{V.2}$$

Le terme $k = 0$ dans cette dernière sommation est simplement $(n+1)!B_n(a)$. Le terme de rang $k = 1$ est $n!^2\binom{n+1}{2}B_n(a)A_n(a) = (n+1)!\binom{n}{2}(n-2)!nB_n(a)A_n(a)$. Le terme de rang $k \geqslant 2$ est, en posant $d_n = n!/(n+1)$, égal à $(n+1)!B_n(a)\binom{n+1}{k+1}n!^{k-1}d_nA_n(a)^k$. D'où l'expression cherchée d'après la proposition II.3.4. □

Proposition V.3.6. *Si $n+1$ est premier ou égal à 4, il existe un élément $D_n(a) \in \widehat{\mathbb{Z}}$ tel que*

$A_n(a) = (n+1)D_n(a)$, et on a alors

$$B_{n+1}(a) = B_n(a) + n!B_n(a)D_n(a)\sum_{k=1}^{n}\binom{n+1}{k+1}n!^{k-1}A_n(a)^{k-1}\ .$$

Démonstration. L'existence de $D_n(a)$ résulte des lemmes V.2.6 et V.2.7. Le calcul est identique à celui utilisé pour la démonstration de la proposition V.3.5 jusqu'à la formule (V.2). Ensuite on remplace $A_n(a)^k$, avec $k \geqslant 1$, par $A_n(a)^{k-1}D_n(a)(n+1)$, faisant apparaître un $(n+1)!$ en facteur dans le membre de droite, d'où le résultat par utilisation de la proposition II.3.4. □

V.3.3 Convergence de la suite B_n

Proposition V.3.7. *La suite de fonctions $(B_n)_{n\in\mathbb{N}}$ est de Cauchy uniformément sur $\widehat{\mathbb{Z}}^*$.*

Démonstration. D'après les propositions V.3.5 et V.3.6, pour tout $a \in \widehat{\mathbb{Z}}^*$ et pour tout entier naturel $n \geqslant 2$, on peut affirmer que $B_{n+1}(a) - B_n(a)$ est élément de $(n-2)!\widehat{\mathbb{Z}}$; donc, par le lemme II.3.3, on a $\varphi(B_{n+1}(a) - B_n(a)) \geqslant n-3$ uniformément sur $\widehat{\mathbb{Z}}^*$. □

On déduit de la proposition V.3.7 que la suite de fonctions $(B_n)_{n\in\mathbb{N}}$ converge uniformément sur $\widehat{\mathbb{Z}}^*$ vers une limite ψ. Comme chaque B_n est continue sur $\widehat{\mathbb{Z}}^*$ (proposition V.3.4), on voit que $\psi : \widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$ est une fonction continue.

Proposition V.3.8. *Pour tout couple (a, a_0) d'éléments inversibles de $\widehat{\mathbb{Z}}$, on a*

$$\log a - \log a_0 = (a - a_0)a_0^{-1}\psi(aa_0^{-1})\ .$$

Démonstration. D'après les propriétés de la fonction logarithme (proposition V.2.13), on sait que $\log a - \log a_0 = \log(aa_0^{-1})$. Or

$$\log(aa_0^{-1}) = \lim_{n\to\infty} A_n(aa_0^{-1}) = \lim_{n\to\infty}(aa_0^{-1} - 1)B_n(aa_0^{-1}) = (aa_0^{-1} - 1)\psi(aa_0^{-1})\ ,$$

ce qui achève la démonstration. □

Proposition V.3.9. *La fonction $\log : \widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$ est dérivable au sens de Novoselov en tout point a_0 de $\widehat{\mathbb{Z}}^*$, de dérivée a_0^{-1}.*

Démonstration. En effet, par la proposition V.3.8, on peut écrire $\log a - \log a_0 = (a - a_0)g(a)$ avec $g(a) = a_0^{-1}\psi(aa_0^{-1})$. Or, puisque nous avons remarqué que la fonction ψ est

continue, nous avons $\lim_{a\to a_0} a_0^{-1}\psi(aa_0^{-1}) = a_0^{-1}\psi(1)$. Puisque $B_n(1) = 1$, le résultat est démontré. □

V.4 Exponentielle

V.4.1 Quelques lemmes

Rappelons d'abord la définition [1] du *coefficient de Faà di Bruno* attaché à un couple (n,k) d'entiers naturels

$$\mathrm{Faa}(k,n) = \frac{(kn)!}{n!^k k!}\,.$$

On sait [24] que ce coefficient s'exprime aussi sous la forme

$$\mathrm{Faa}(k,n) = \prod_{j=1}^{k}\binom{jn-1}{n-1}$$

qui fait voir que ce coefficient a pour valeur un entier naturel. De plus, cette expression rend apparent le fait que, si q est un nombre premier, alors le coefficient $\mathrm{Faa}(k,q)$ est premier à q quelque soit la valeur de l'entier naturel k.

Lemme V.4.1. *Pour tout entier naturel $r \geqslant 1$, soit $P(r)$ l'ensemble des nombres premiers $\leqslant r$ et φ la filtration factorielle. Soit n un nombre entier naturel, on note m la partie entière de $\frac{n}{2}$ et $\epsilon = n - 2m \in \{0,1\}$; on a alors :*

$$\varphi\left(2^{m+\epsilon}\left(\prod_{q\in P(n+1)} q\right)^m\right) \geqslant n\,.$$

Démonstration. Soit n la plus petite valeur possible ne vérifiant pas cette assertion. On a alors $n > 1$ car l'assertion est visiblement satisfaite pour $n = 0$ (avec $P(1)$ vide) ou $n = 1$ (avec $P(2) = \{2\}$). Par définition de φ, on a donc $(n+1)!$ qui ne divise pas le nombre entier $x = 2^{m+\epsilon}\left(\prod_{q\in P(n+1)} q\right)^m$. Comme les diviseurs premiers de $(n+1)!$ sont exactement les éléments de $P(n+1)$, ceci signifie qu'il existe un couple $(q,\nu) \in P(n+1)\times\mathbb{N}$ tel que q^ν divise $(n+1)!$ mais pas x. On fait alors la division euclidienne de $n+1$ par q, écrivant $n+1 = aq+r$, où $0 \leqslant r < q$. On a alors

$$(n+1)! = \binom{n+1}{r}(aq)!r! = \binom{aq+r}{r}\mathrm{Faa}(a,q)q!^a a!r!\,.$$

Puisque $a-1 < n$, on sait que notré énoncé est vérifié pour l'entier $a-1$, de sorte que $a!$ est un diviseur de $y = 2^{b+\eta}\left(\prod_{q\in P(a)} q\right)^b$, où b est la partie entière de $\frac{a-1}{2}$ et $\eta = a-1-2b$. Comme $q! = q(q-1)!$, où la factorielle $(q-1)!$ est un entier premier à q, que le coefficient de Faà di Bruno $\mathrm{Faa}(a,q)$ est premier à q et que le coefficient du binôme $\binom{aq+r}{r}$ l'est aussi, ainsi que $r!$, nous concluons que q^ν doit diviser $q^a y$. Si $q = 2$, de sorte que $n = 2a+r-1 \geqslant 2a-1$, ceci montre que $\nu \leqslant a+b+\eta+b = 2a-1$; or 2^{2a-1} divise $2^n = 2^{2m+\epsilon}$ qui divise x, ce qui contredit la définition de q. D'un autre côté, si q est un nombre premier impair, alors on a $n = qa+r-1 \geqslant qa-1$ et $\nu \leqslant a+b = \frac{3a-1-\eta}{2} \leqslant \frac{3a-1}{2} \leqslant \frac{qa-1}{2} \leqslant \frac{n}{2}$, donc on a $\nu \leqslant m$, alors que q^m divise x, et cette contradiction achève la démonstration. □

Lemme V.4.2. *Pour tout entier naturel n, $(2^n)!$ est un multiple de 2^{2^n-1}.*

Démonstration. La démonstration se fait par récurrence sur n en utilisant la formule

$$(2^{n+1})! = \mathrm{Faa}(2^n,2)\ 2^{2^n}\ (2^n)!\ .$$

□

Lemme V.4.3. *Soit $m_1, m_2, \ldots, m_d$ une suite finie d'entiers rationnels deux à deux premiers entre eux et A un anneau commutatif unifère. Alors*

$$\bigcap_{j=1}^{d} m_j A = (\prod_{j=1}^{d} m_j)A\ .$$

Démonstration. Soit $x \in \cap_{j=1}^d m_j A$. Il existe, pour tout entier $j, 1 \leqslant j \leqslant d$, des éléments $y_j \in A$ tels que $x = m_j y_j$. Montrons par récurrence sur j que x est élément de $\left(\prod_{k=1}^j m_k\right) A$. Si $j = 1$, il n'y a rien à montrer. Si on suppose que x est élément de $\left(\prod_{k=1}^j m_k\right) A$, il existe $z \in A$ tel que $x = \left(\prod_{k=1}^j m_k\right) z$; on sait qu'il existe des entiers $u, v \in \mathbb{Z}$ tels que $m_{j+1}u + \left(\prod_{k=1}^j m_k\right) v = 1$, donc $z = um_{j+1}z + v\left(\prod_{k=1}^j m_k\right) z = m_{j+1}uz + vx = m_{j+1}(uz + vy_{j+1}) \in m_{j+1}A$, et donc on a bien $x \in \left(\prod_{k=1}^{j+1} m_k\right) A$. □

Soit A un anneau commutatif unifère. On rappelle que le radical de Jacobson de l'anneau A est l'intersection de tous les idéaux maximaux de A. Par un résultat connu d'algèbre commutative [28], cet idéal J est l'ensemble des éléments $a \in A$ tels que $1+ab$ est inversible dans A pour tout élément $b \in A$. La caractérisation suivante du radical de Jacobson nous sera utile.

Lemme V.4.4. *Le radical de Jacobson J d'un anneau unifère A est le plus grand idéal I de A tel que $1 + I \subseteq A^*$, où A^* est le groupe des éléments inversibles de A.*

Démonstration. D'une part, pour tout élément a de J, l'élément $1 + a = 1 + a \cdot 1$ est élément de A^* en vertu de la caractérisation connue du radical de Jacobson citée ci-dessus. On a donc $1 + J \subseteq A^*$.

D'autre part, si I est un idéal tel que $1 + I \subseteq A^*$, alors, pour tout $a \in I$ et tout $b \in A$, le produit ab est élément de I, de sorte que $1 + ab \in A^*$; ceci signifie bien que $a \in J$, on a donc l'inclusion $I \subseteq J$. □

Lemme V.4.5. *Si A et B sont deux anneaux commutatifs unifères, si $\varpi : A \to B$ est un morphisme d'anneaux surjectif, et si a est un élément du radical de Jacobson de A, alors $\varpi(a)$ appartient au radical de Jacobson de B.*

Démonstration. Soit $b \in B$; puisque par hypothèse ϖ est une surjection, il existe $a' \in A$ tel que $\varpi(a') = b$. Alors, puisque a est supposé appartenir au radical de Jacobson de A, l'élément $1 + aa'$ est inversible dans A et donc $\varpi(1 + aa') = 1 + \varpi(a)b$ est inversible dans B. Ceci montre que $\varpi(a)$ est bien élément du radical de Jacobson de B. □

V.4.2 Le radical de Jacobson de l'anneau des entiers polyadiques

Soit J le radical de Jacobson de l'anneau $\widehat{\mathbb{Z}}$ et Γ le plus grand idéal de $\widehat{\mathbb{Z}}$ où l'on peut définir un système de puissances divisées pour Γ, c'est-à-dire :

$$\Gamma = \{x \in \widehat{\mathbb{Z}}, \forall n \geqslant 1, x^n \in n!\widehat{\mathbb{Z}}\} .$$

Nous avons la caractérisation suivante du radical de Jacobson J.

Proposition V.4.6. *Soit x un entier polyadique. Les quatre assertions suivantes sont équivalentes.*

(i) Pour tout nombre premier q, $x \in q\widehat{\mathbb{Z}}$;

(ii) $x \in \Gamma$;

(iii) x est topologiquement nilpotent, c'est-à-dire que $\lim_{n\to+\infty} x^n = 0$;

(iv) $x \in J$.

Démonstration. Montrons successivement le cycle d'implications $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.

Commençons par supposer que x est élément de $q\widehat{\mathbb{Z}}$ pour tout nombre premier q, et soit n un entier $\geqslant 1$. Alors $x \in \cap_{q\in P(n)} q\widehat{\mathbb{Z}}$, c'est-à-dire d'après le lemme V.4.3 que $x \in \left(\prod_{q\in P(n)} q\right)\widehat{\mathbb{Z}}$, de sorte que $x^n \in \left(\prod_{q\in P(n)} q\right)^n \widehat{\mathbb{Z}}$. Or le lemme V.4.1 montre que $\left(\prod_{q\in P(n)} q\right)^n \widehat{\mathbb{Z}}$ est contenu dans $n!\widehat{\mathbb{Z}}$. Ceci étant vrai pour tout entier naturel $n \geqslant 1$ prouve que $x \in \Gamma$.

Supposons que $x \in \Gamma$, alors par le lemme II.3.3, on a pour tout entier naturel $n \geqslant 1$ l'inégalité $\varphi(x^n) \geqslant n-1$, d'où la convergence vers 0 de la suite $(x^n)_{n\in\mathbb{N}}$.

Supposons que x est topologiquement nilpotent. Alors soit $y \in \widehat{\mathbb{Z}}$; la suite $x^n y^n$ converge vers 0 car $\varphi(x^n y^n) \geqslant \max(\varphi(x^n), \varphi(y^n))$. Donc la série $\sum_{n=0}^{+\infty}(-1)^n x^n y^n$ converge dans l'espace complet $\widehat{\mathbb{Z}}$. Comme le produit de la somme partielle $\sum_{n=0}^{N}(-1)^n x^n y^n$ par $1+xy$ est $1-(-1)^{N+1}x^{N+1}y^{N+1}$, on voit par passage à la limite que la somme de cette série est un inverse dans $\widehat{\mathbb{Z}}$ de $1+xy$. Puisqu'on a ainsi montré que $1+xy$ était inversible pour tout y de $\widehat{\mathbb{Z}}$, il en résulte que $x \in J$.

Supposons que $x = (p_n(x_n))_{n\geqslant 1} \in J$, et soit q un nombre premier. On considère le morphisme d'anneaux $\varpi : \widehat{\mathbb{Z}} \to \mathbb{Z}/q\mathbb{Z}$ obtenu en composant la projection $\widehat{\mathbb{Z}} \to \mathbb{Z}/q!\mathbb{Z}$ avec l'application naturelle de $\mathbb{Z}/q!\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$; autrement dit, si $y = (p_n(y_n))_{n\geqslant 1}$, on a $\varpi(y) = y_q + q\mathbb{Z}$. Comme ϖ est surjective, le lemme V.4.5 assure que $\varpi(x)$ est élément du radical de Jacobson de l'anneau $\mathbb{Z}/q\mathbb{Z}$. Or, puisque ce dernier anneau est un corps, son radical de Jacobson est trivial. Ceci établit qu'on a nécessairement $x_q \in q\mathbb{Z}$, et donc, en utilisant le lemme II.3.3, on conclut que $x \in q\widehat{\mathbb{Z}}$. □

Nous avons donc montré que

$$\cap_q q\widehat{\mathbb{Z}} = J = \Gamma\ . \tag{V.3}$$

Il en résulte que J est un idéal fermé, donc principal d'après la proposition II.6.9.

Proposition V.4.7. *Un élément ω tel que $J = \omega\widehat{\mathbb{Z}}$ n'est pas diviseur de zéro dans $\widehat{\mathbb{Z}}$.*

Démonstration. Il suffit de trouver dans J un élément qui n'est pas diviseur de zéro. Soit pour tout nombre premier q l'ensemble $E_q = \bigcup_{a\in\mathbb{Z}\setminus q\mathbb{Z}} \left(aq + (2q)!\widehat{\mathbb{Z}}\right)$. Par division euclidienne (proposition II.6.4), on voit que l'ensemble E_q est en fait la réunion finie des classes fermées (proposition II.2.8) $aq + (2q)!\widehat{\mathbb{Z}}$, pour a décrivant l'ensemble des entiers premiers à q qui appartiennent à l'intervalle $[1, (2q)![$, de sorte que E_q est une partie fermée de $\widehat{\mathbb{Z}}$. On observe que toute intersection finie $\cap_{q\in F} E_q$, où F est un ensemble fini de nombres premiers, est non vide, puisqu'il contient en effet le produit $\prod_{q\in F} q$.

Puisque $\widehat{\mathbb{Z}}$ est compact, il en résulte que l'intersection de tous les E_q est non vide, soit α un élément de cette intersection.

Alors, comme on a $E_q \subset q\widehat{\mathbb{Z}}$ pour tout nombre premier q, on peut affirmer que α est élément de $J = \cap_q q\widehat{\mathbb{Z}}$. Écrivons α sous la forme $\alpha = (p_n(\alpha_n))_{n\geqslant 1}$, où les α_n sont des entiers rationnels satisfaisant la condition (II.9). Comme q^2 est un diviseur de $(2q)!$ pour tout entier premier q, on voit par le lemme II.3.3 que α_{q^2} n'est pas élément de $q^2\mathbb{Z}$. Puisque $q^2 \geqslant 2q$, en vertu des congruences (II.10), on en déduit que $\alpha_{2q} \notin q^2\mathbb{Z}$. Fixons un nombre premier q. Pour r un entier premier tel que $r \leqslant q$, les congruences (II.10) montrent que $\alpha_{2q} \notin r^2\mathbb{Z}$. En ayant recours à la décomposition multiplicative de α_{2q} en facteurs premiers, nous en déduisons que α_{2q} est produit d'un entier d sans facteurs carrés dont tous les diviseurs premiers sont au plus égaux à q et d'un entier e dont tous les diviseurs premiers sont supérieurs à q.

Montrons que α n'est pas diviseur de zéro. En effet, soit $z = (p_n(z_n))_{n\geqslant 1}$ un élément de $\widehat{\mathbb{Z}}$ tel que $z\alpha = 0$. On a alors $z_n\alpha_n \equiv 0 \bmod n!$ pour tout entier $n \geqslant 1$. En particulier, si q est un nombre premier, on a $z_{2q}\alpha_{2q} \equiv 0 \bmod (2q)!$. Or, puisque $(2q)! = \binom{2q}{q} q!^2$, on en déduit que $z_{2q}\alpha_{2q} \equiv 0 \bmod q!^2$. D'après la relation $\alpha_{2q} = de$, avec d diviseur de $q!$ et e premier à $q!$, on voit que $z_{2q} \equiv 0 \bmod q!$. D'après les congruences (II.10), on en déduit $z_q \equiv 0 \bmod q!$ pour tout nombre premier q. Si n est un entier naturel tel que $n \geqslant 1$, on peut trouver un nombre premier q tel que $q \geqslant n$, donc les congruences (II.10) montrent que $z_n \equiv 0 \bmod n!$, ce qui prouve que $z = 0$. □

Proposition V.4.8. *Soit $f : \widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$ une fonction, $a_0 \in \widehat{\mathbb{Z}}^*$. Si f est dérivable en a_0, son nombre dérivé en a_0 est unique.*

Démonstration. Il suffit pour cela de montrer que si une fonction g définie dans un voisinage $V(a_0)$ de a_0 dans $\widehat{\mathbb{Z}}^*$ vérifiant une identité $(a - a_0)g(a) = 0$ pour tout $a \in V(a_0)$ admet une limite au point a_0, alors cette limite est nulle. On peut se restreindre au cas où $V(a_0)$ est de la forme $V(a_0) = (a_0 + d!\widehat{\mathbb{Z}}) \cap \widehat{\mathbb{Z}}^*$. Soit ω un générateur du radical de Jacobson de $\widehat{\mathbb{Z}}$, qui n'est pas diviseur de zéro en vertu de la proposition V.4.7. Alors, pour tout $n \geqslant 0$, l'élément $x_n = a_0 + (d+n)!\omega = a_0(1 + (d+n)!\omega a_0^{-1})$ est inversible dans $\widehat{\mathbb{Z}}$, et appartient donc à $V(a_0)$. Par conséquent, la suite $(g(x_n))_{n\in\mathbb{N}}$ converge vers la limite de g au point a_0. Or par hypothèse nous avons pour tout entier naturel n la relation $(d+n)!\omega g(x_n) = 0$, d'où $\omega g(x_n) = 0$ par la proposition II.3.4, et puis $g(x_n) = 0$ du fait que ω n'est pas diviseur de zéro. Donc la limite de g au point a_0 est nulle, comme on voulait le montrer. □

V.4.3 Puissances divisées sur le radical de Jacobson

Nous munissons l'idéal $J = \Gamma$ de la suite d'applications $\gamma_n \quad (n \in \mathbb{N})$ de J vers $\widehat{\mathbb{Z}}$ en posant, pour tout $x \in J$, $x^n = n!\gamma_n(x)$.

Lemme V.4.9. *Pour tout $x \in J$ et pour tout entier naturel $n \geqslant 1$, la puissance divisée $\gamma_n(x)$ est élément de J.*

Démonstration. D'après la proposition V.4.6, il suffit de montrer que la suite $\left(\gamma_n(x)^k\right)_{k\in\mathbb{N}}$ converge vers zéro. Or nous avons $n!^k\gamma_n(x)^k = x^{kn} = (kn)!\gamma_{kn}(x) = n!^k k!\mathrm{Faa}(k,n)\gamma_{kn}(x)$. En utilisant la proposition II.3.4, nous en déduisons que $\gamma_n(x)^k = k!\mathrm{Faa}(k,n)\gamma_{kn}(x) \in k!\widehat{\mathbb{Z}}$, donc par le lemme II.3.3, nous avons, quelque soit les entiers naturels k et $n \geqslant 1$, l'inégalité $\varphi(\gamma_n(x)^k) \geqslant k-1$, ce qui prouve le résultat voulu. □

Il est immédiat de vérifier à partir de là que les applications $\gamma_n : J \to J \quad (n \geqslant 1)$ définissent sur le radical de Jacobson J une structure d'idéal à puissances divisées [20].

Lemme V.4.10. *Soit $x \in 2J$ et $n \neq 0$ un entier naturel. On note m la partie entière de $n/2$, et $\epsilon = n - 2m \in \{0,1\}$. Alors $\gamma_n(x)$ est élément de $2^{m+\epsilon}J^{m+1}$.*

Démonstration. Il existe un élément y de J tel que $x = 2y$. Par l'égalité (V.3), pour tout nombre premier $q \leqslant n$, on sait que y est élément de $q\widehat{\mathbb{Z}}$. En vertu de la proposition V.4.3, on en déduit l'existence de $z \in \widehat{\mathbb{Z}}$ tel que $y = \left(\prod_{q\in P(n)} q\right) z$, où $P(n)$ est l'ensemble des nombres premiers non supérieurs à n. Par le lemme V.4.1, on sait qu'il existe un entier naturel r_n tel que $2^{m_1+\epsilon_1}\left(\prod_{q\in P(n)} q\right)^{m_1} = n!r_n$, où m_1 est la partie entière de $\frac{n-1}{2}$ et $\epsilon_1 = n - 1 - 2m_1$ est le reste dans la division euclidienne de $n-1$ par 2.

On voit que

$$x^n = 2^n y^n = 2^n \left(\prod_{q\in P(n)} q\right)^n z^n = 2^{n-m_1-\epsilon_1}\left(\prod_{q\in P(n)} q\right)^{n-m_1} n!r_n z^n,$$

qu'on peut aussi écrire

$$n!\gamma_n(x) = x^n = n!r_n 2^{n-m_1-\epsilon_1}\left(\prod_{q\in P(n)} q\right)^{n-m_1} z^n.$$

Par la proposition II.3.4, on en déduit que

$$\gamma_n(x) = 2^{n-m_1-\epsilon_1}\left(\prod_{q\in P(n)} q\right)^{n-m_1} r_n z^n. \tag{V.4}$$

Or, comme n et $n-1$ sont deux entiers consécutifs, l'un est pair et l'autre est impair, par conséquent $\epsilon+\epsilon_1 = 1$ et $m+m_1 = n-1$, d'où $n-m_1 = m+1$ et $n-m_1-\epsilon_1 = m+\epsilon$. L'expression (V.4) montre donc bien que $\gamma_n(x) \in 2^{m+\epsilon}J^{m+1}$. □

Proposition V.4.11. *Soit h, j, m des entiers naturels $\geqslant 1$ et $\epsilon \in \{0,1\}$. Pour tout $x \in 2^h J^j$, la puissance divisée $\gamma_{2m+\varepsilon}(x)$ est élément de l'idéal $2^{m(2h-1)+\epsilon h}J^{m(2j-1)+\epsilon(j-1)+1}$.*

Démonstration. Comme J est un idéal fermé, il est principal en vertu de la proposition II.6.9, soit ω un générateur de J. Il existe un $y \in J$ tel que $x = 2^{h-1}\omega^{j-1}y$. Comme on a

$$\gamma_{2m+\epsilon}(x) = 2^{(h-1)(2m+\epsilon)}\omega^{(j-1)(2m+\epsilon)}\gamma_{2m+\epsilon}(y)$$

et qu'on sait par le lemme V.4.10 que $\gamma_{2m+\epsilon}(y) \in 2^{m+\epsilon}J^{m+1}$, le résultat s'en déduit. □

Proposition V.4.12. *Soient x et y deux éléments de $2J$ et $j \geqslant 1$ un entier naturel tels que soit vérifiée la congruence*

$$x \equiv y \bmod 2J^j. \tag{V.5}$$

Alors, pour tout entier naturel n, on a la congruence

$$\gamma_n(x) \equiv \gamma_n(y) \bmod 2J^{j+m}, \tag{V.6}$$

où m est la partie entière de $n/2$.

Démonstration. Il n'y a rien à montrer si $n = 0$, par conséquent on se restreint au cas où $n \geqslant 1$. On utilise l'identité suivante, où $z = x - y$:

$$\gamma_n(x) = \gamma_n(y+z) = \sum_{k=0}^{n}\gamma_k(z)\gamma_{n-k}(y) = \gamma_n(y) + \sum_{k=1}^{n}\gamma_k(z)\gamma_{n-k}(y)\ .$$

Il suffit donc de vérifier que, pour tout entier naturel k vérifiant $1 \leqslant k \leqslant n$, le produit $\gamma_k(z)\gamma_{n-k}(y)$ est élément de $2J^{j+m}$. Notons, un tel entier k étant fixé, par ℓ la partie entière de $\frac{k}{2}$ et par ℓ' la partie entière de $\frac{n-k}{2}$, et posons $\epsilon = k - 2\ell$. D'après la proposition

V.4.11, on sait que $\gamma_k(z) \in 2J^{\ell(2j-1)+\epsilon(j-1)+1}$ et que $\gamma_{n-k}(y) \in J^{\ell'+1}$ pour $1 \leqslant k < n$. On voit que, si $1 \leqslant k < n$, on a

$$\gamma_k(z)\gamma_{n-k}(y) \in 2J^{\ell(2j-1)+\epsilon(j-1)+\ell'+2} .$$

Or, par définition de l'entier m, on a $m \leqslant \ell + \ell' + 1$, donc $\ell(2j-1) + \epsilon(j-1) + \ell' + 2 \geqslant m + 2\ell(j-1) + \epsilon(j-1) + 1 \geqslant m + k(j-1) + 1 \geqslant m + j$, donc le produit $\gamma_k(z)\gamma_{n-k}(y)$ est bien élément de $2J^{k+m}$. Reste à traiter le cas où $k = n$. Dans ce cas, on a à considérer $\gamma_n(z)$ qui par la proposition V.4.11 est élément de $2J^{m(2j-1)+\epsilon(j-1)+1}$, où on a encore posé $\epsilon = n - 2m$. On vérifie alors qu'ici encore $m(2j-1) + \epsilon(j-1) + 1 = m + j + (n-1)(j-1) \geqslant m + j$. □

V.4.4 La série exponentielle

Nous commençons par comparer la topologie J-adique à la topologie de $\widehat{\mathbb{Z}}$.

Proposition V.4.13. *La topologie J-adique est plus fine que la topologie de limite projective de $\widehat{\mathbb{Z}}$.*

Démonstration. Comme les deux topologies à comparer sont toutes deux compatibles avec la structure d'anneau de $\widehat{\mathbb{Z}}$, il suffit de montrer qu'une suite $(\alpha_n)_{n\in\mathbb{N}}$ qui converge vers zéro pour la topologie J-adique converge également vers 0 pour la topologie de limite projective de $\widehat{\mathbb{Z}}$. Soit ω un générateur de l'idéal J. Si une suite $(\alpha_n)_{n\in\mathbb{N}}$ converge vers zéro pour la topologie J-adique, alors on a $\alpha_n = \omega^{k_n}\beta_n$, avec $k_n \in \mathbb{N}$, $\beta_n \in \widehat{\mathbb{Z}}$ et $\lim_{n\to+\infty} k_n = +\infty$. Comme la suite $(\omega^k)_{k\in\mathbb{N}}$ tend vers 0 ainsi qu'il résulte de la proposition V.4.6, nous voyons bien que la suite $(\alpha_n)_{n\in\mathbb{N}}$ converge vers 0 dans $\widehat{\mathbb{Z}}$. □

Corollaire V.4.14. *Soit $(f_k)_{k\in N}$ une suite d'applications d'un ensemble E dans $\widehat{\mathbb{Z}}$. Si la suite $(f_k)_{k\in\mathbb{N}}$ converge uniformément vers une fonction $f : E \to \widehat{\mathbb{Z}}$ pour la topologie J-adique, alors elle converge aussi uniformément pour la topologie de limite projective de $\widehat{\mathbb{Z}}$.*

Remarque V.4.15. On peut observer que la topologie J-adique n'est pas équivalente à la topologie de limite projective de $\widehat{\mathbb{Z}}$. Par exemple, la suite $(k!)_{k\in\mathbb{N}}$ converge vers 0 au sens de la topologie de limite projective de $\widehat{\mathbb{Z}}$, mais n'est pas de Cauchy au sens J-adique.

Nous étudions ensuite la convergence de la *série exponentielle*, c'est-à-dire de la série de terme général $\gamma_n(x)$, pour $x \in J$.

Proposition V.4.16. *Soit x un élément de J. La série exponentielle $\sum \gamma_n(x)$ converge si et seulement si x appartient à l'idéal $2J$.*

Démonstration. D'une part, supposons que x appartient à $2J$. D'après la proposition V.4.11, on voit que la suite $(\gamma_n(x))_{n\in\mathbb{N}}$ converge vers 0 au sens J-adique, donc aussi au sens de la topologie de $\widehat{\mathbb{Z}}$ d'après la proposition V.4.13. Ainsi le terme général de la série exponentielle tend vers 0, ce qui, puisque $\widehat{\mathbb{Z}}$ est un espace ultramétrique complet, entraîne la convergence de la série exponentielle.

Réciproquement, supposons que la série $\sum \gamma_n(x)$ est convergente. Ceci entraîne que la suite $(\gamma_n(x))_{n\in\mathbb{N}}$ converge vers zéro. Puisque, par hypothèse, x est élément de J, il résulte de (V.3) qu'il existe $y \in \widehat{\mathbb{Z}}$ tel que $x = 2y$. Nous allons montrer que y appartient à J. Pour cela, d'après la proposition V.4.6, il suffit de montrer que la suite $(y^n)_{n\in\mathbb{N}}$ converge vers 0 dans $\widehat{\mathbb{Z}}$, ou encore, de façon équivalente, que la suite des filtrations $(\varphi(y^n))_{n\in\mathbb{N}}$ tend vers $+\infty$. Or, il résulte de la proposition II.2.2 que cette suite $(\varphi(y^n))_{n\in\mathbb{N}}$ est croissante, de sorte qu'il suffit de montrer qu'une suite extraite tend vers $+\infty$. Nous sommes ainsi réduits à montrer que la suite $\left(y^{2^n}\right)_{n\in\mathbb{N}}$ converge vers 0. Ecrivons donc $2^{2^n}y^{2^n} = (2^n)!\gamma_{2^n}(x)$. D'après la proposition II.3.4 et le lemme V.4.2, nous en tirons que $2y^{2^n}$ est élément de $\gamma_{2^n}(x)\widehat{\mathbb{Z}}$, donc converge vers zéro, de sorte que la suite $\left(\varphi\left(2y^{2^n}\right)\right)_{n\in N}$ tend vers $+\infty$. Or le corollaire II.2.3 montre que $\varphi\left(y^{2^n}\right) \geqslant \varphi\left(2y^{2^n}\right) - 2$. □

Pour tout $x \in 2J$, nous définissons l'*exponentielle* $\exp(x)$ *de* x comme la somme de la série exponentielle :

$$\exp(x) = \sum_{n=0}^{+\infty} \gamma_n(x) \ .$$

Proposition V.4.17. *Pour tous les éléments x et y de $2J$, on a $\exp(x+y) = \exp(x)\exp(y)$. En particulier, $exp(x) \in \widehat{\mathbb{Z}}^*$ pour tout $x \in 2J$.*

Démonstration. Pour tout élément z de $2J$, notons $E_n(z)$ la somme partielle de rang n de la série exponentielle de z. En vertu de la formule du binôme et de la proposition II.3.4, nous avons pour tout entier naturel n l'identité $\gamma_n(x+y) = \sum_{j=0}^{n} \gamma_j(x)\gamma_{n-j}(y)$. Il en résulte que

$$E_n(x)E_n(y) = \left(\sum_{j=0}^{n} \gamma_j(x)\right)\left(\sum_{\ell=0}^{n} \gamma_\ell(y)\right) = E_n(x+y) + \sum_{j+\ell>n, j\leqslant n, \ell\leqslant n} \gamma_j(x)\gamma_\ell(y) \ .$$

Par la proposition V.4.11, on sait que, pour tout couple (j,ℓ) d'entiers naturels tel que $j+\ell > n, j \leqslant n$ et $\ell \leqslant n$, on a $\gamma_j(x)\gamma_\ell(y) \in j!\ell!\widehat{\mathbb{Z}} \subseteq N!\widehat{\mathbb{Z}}$, où N est le plus petit entier $\geqslant \frac{n}{2}$. La filtration factorielle de $\gamma_j(x)\gamma_\ell(y)$ vérifie donc $\varphi\left(\gamma_j(x)\gamma_\ell(y)\right) \geqslant N-1 \geqslant \frac{n}{2}-1$. Par conséquent, on a $\lim_{n\to+\infty} E_n(x)E_n(y) - E_n(x+y) = 0$. Comme $E_n(x), E_n(y), E_n(x+y)$ convergent respectivement vers $\exp(x), \exp(y), \exp(x+y)$, le résultat s'en déduit. En particulier, lorsque $y=-x$, on obtient $\exp(x)\exp(-x) = 1$. □

Proposition V.4.18. *Pour tout $x \in 2J$, on a $\log(\exp(x)) = x$.*

Démonstration. Par définition, $\log(\exp(x))$ est la limite de la suite $(A_n(\exp(x)))_{n\geqslant 1}$ définie par les égalités $(\exp(x))^{n!} - 1 = n!A_n(\exp(x))$. Par la proposition V.4.17, on sait que $n!A_n(\exp(x)) = \exp(n!x) - 1 = \sum_{j=1}^{+\infty} \gamma_j(n!x) = \sum_{j=1}^{+\infty} n!^j\gamma_j(x) = n!\sum_{j=1}^{+\infty} n!^{j-1}\gamma_j(x)$. Par la proposition II.3.4, on en tire l'égalité $A_n(\exp(x)) = \sum_{j=1}^{+\infty} n!^{j-1}\gamma_j(x) = x + n!\sum_{j=2}^{+\infty} n!^{j-2}\gamma_j(x)$. On a donc

$$\varphi\left(A_n(\exp(x)) - x\right) \geqslant n-1,$$

ce qui montre bien que la limite de la suite $(A_n(\exp(x)))_{n\geqslant 1}$ est égale à x. □

V.4.5 La fonction exponentielle

La *fonction exponentielle* est l'application exp de $2J$ dans $\widehat{\mathbb{Z}}$ qui à tout $x \in 2J$ associe $\exp(x) \in \widehat{\mathbb{Z}}$. Cette application est injective d'après la proposition V.4.18. Puisque la convergence de la suite γ_n vers 0 est uniforme au sens J-adique, le corollaire V.4.14 montre que la convergence de la série de fonctions qui définit la fonction exponentielle est uniforme. Comme de plus les applications $\gamma_n : 2J \to \widehat{\mathbb{Z}}$ sont continues d'après la proposition V.2.5, la fonction exponentielle est continue. Nous allons maintenant déterminer l'image de cette fonction en démontrant d'abord une espèce de lemme de Hensel pour les séries de Hurwitz.

Proposition V.4.19. *Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\widehat{\mathbb{Z}}$ et $f : 2J \to \widehat{\mathbb{Z}}$ l'application définie par*

$$\forall x \in 2J, \qquad f(x) = \sum_{j=0}^{+\infty} a_j\gamma_j(x)\ .$$

On suppose que $a_0 \in 2J$ et $a_1 \in \widehat{\mathbb{Z}}^*$. Alors il existe un élément x de $2J$ tel que $f(x) = 0$.

Démonstration. La série de fonctions $f(x)$ converge pour tout $x \in 2J$ puisqu'on a vu que, pour de tels x la suite $\big(\gamma_j(x)\big)_{j\in\mathbb{N}}$ converge vers zéro. D'autre part, la somme $f(x)$ est élément de $2J$ car tous les $\gamma_j(x) \in 2J$ et $a_0 \in 2J$. Avec cette série nous considérons la dérivée formelle $f'(x) = \sum_{j=1}^{+\infty} a_j\gamma_{j-1}(x)$ qui converge pour une raison analogue, avec cette fois, puisque $a_1 \in \widehat{\mathbb{Z}}^*$, la propriété que

$$a_1^{-1}f'(x) = 1 + \sum_{j=2}^{+\infty} a_j\gamma_{j-1}(x) \in 1 + 2J \subset \widehat{\mathbb{Z}}^*$$

donc $f'(x) \in \widehat{\mathbb{Z}}^*$ pour tout $x \in 2J$. Observons que les fonctions $f : 2J \to 2J \subset \widehat{\mathbb{Z}}$ et $f' : 2J \to \widehat{\mathbb{Z}}^* \subset \widehat{\mathbb{Z}}$ sont continues ; en effet, les séries de fonctions qui les définissent convergent uniformément au sens J-adique d'après le lemme V.4.10, donc également uniformément au sens de la topologie de limite projective de $\widehat{\mathbb{Z}}$.

Définissons une application $g : 2J \to 2J$ en posant $g(x) = x - f'(x)^{-1}f(x)$. Nous remarquons que $f'(x)g(x) = \sum_{j=0}^{+\infty}(j-1)a_j\gamma_j(x) = -a_0 + \sum_{j=2}^{+\infty}(j-1)a_j\gamma_j(x)$, ce qui implique en vertu de la proposition V.4.12 que la congruence $x \equiv y \pmod{2J^k}$ entraîne que $f'(x)g(x) \equiv f'(y)g(y) \pmod{2J^{k+1}}$ et $f'(y) - f'(x) = \sum_{j=2}^{+\infty} a_j(\gamma_{j-1}(x) - \gamma_{j-1}(y)) \in 2J^k$. Or nous avons aussi

$$f'(x)(g(x) - g(y)) = f'(x)g(x) - f'(y)g(y) + (f'(y) - f'(x))g(y),$$

ce qui, puisque $g(y) \in 2J$, entraîne que $f'(x)(g(x) - g(y))$ est alors élément de $2J^{k+1}$. Puisque $f'(x)$ est inversible, on a montré que la congruence $x \equiv y \pmod{2J^k}$ entraîne que $g(x) \equiv g(y) \pmod{2J^{k+1}}$.

Soit maintenant la suite $(x_k)_{k\in\mathbb{N}}$ d'éléments de $2J$ définie par récurrence en posant $x_0 = 0$ et $x_{k+1} = g(x_k)$ pour tout entier naturel k. Comme $x_1 = -a_1^{-1}a_0$ vérifie la congruence $x_1 \equiv x_0 \pmod{2J}$, on a par une récurrence immédiate $x_{k+1} \equiv x_k \pmod{2J^{k+1}}$. La suite $(x_{k+1} - x_k)_{k\in\mathbb{N}}$ tend ainsi vers 0 au sens J-adique et, par la proposition V.4.13, on en tire que la suite $(x_k)_{k\in\mathbb{N}}$ est une suite de Cauchy pour la topologie de limite projective de $\widehat{\mathbb{Z}}$. Donc elle converge vers une limite x_∞ qui, puisque g est continue, est un point fixe de $g : 2J \to 2J$ et donc un zéro de la fonction f. □

Proposition V.4.20. *Un élément y de $\widehat{\mathbb{Z}}$ est l'image d'un élément x de $2J$ par l'application* exp *si et seulement si $y - 1$ est élément de $2J$.*

Démonstration. Soit $x \in 2J$ tel que $y = \exp(x)$. Du lemme V.4.10, résulte le fait que

$\gamma_n(x) \in 2J$ pour tout entier naturel $n \geqslant 1$. Comme $2J$ est un idéal fermé, on voit donc que $y - 1 = \exp(x) - \gamma_0(x) = \sum_{n=1}^{+\infty} \gamma_n(x)$ appartient à $2J$.

Réciproquement, soit y tel que $y - 1 \in 2J$. On considère la série de Hurwitz $f(x) = 1 - y + \sum_{j=1}^{+\infty} \gamma_j(x)$. La proposition V.4.19 montre l'existence d'un zéro de cette série, c'est donc un élément x de $2J$ tel que $\exp(x) = y$. □

Proposition V.4.21. *Pout tout élément a de $1 + 2J$, on a $\exp(\log(a)) = a$.*

Démonstration. On sait par la proposition V.4.20 qu'il existe un élément x de $2J$ tel que $\exp(x) = a$. On en déduit par utilisation de la proposition V.4.18 :

$$\exp(\log(a)) = \exp(\log(\exp(x))) = \exp(x) = a \ .$$

□

VI

Solutions rationnelles d'équations linéaires aux différences

VI.1 Introduction

Dans ce chapitre, nous considérons le problème de la recherche des solutions rationnelles d'équations linéaires aux différences à coefficients polynomiaux. Les solutions rationnelles peuvent être fondamentales pour la construction d'autres types de solutions, plus généralement, de tels algorithmes peuvent faire partie de divers algorithmes de calcul formel (voir Abramov, van Hoeij, Levy, Petkovšek [45; 11; 12; 53], etc.). L'exploration de nouvelles façons pour construire de telles solutions est très bénéfique pour le calcul formel.

Soit k un corps de caractéristique nulle. Nous considérons le système linéaire suivant

$$Y(x+1) = A(x)Y(x), \tag{VI.1}$$

avec $Y(x) = (Y_1(x), Y_2(x), \cdots, Y_n(x))^T$, la matrice $A(x) = (a_{ij}(x)) \in \mathrm{Mat}_n(k(x))$ carrée d'ordre n à coefficients dans $k(x)$ est supposée inversible, notons par $A^{-1}(x) = (\tilde{a}_{ij}(x))$

élément de $\mathrm{Mat}_n(k(x))$ son inverse. Si nous avons un système non homogène écrit sous la forme $Y(x+1) = A(x)Y(x) + G(x)$ avec $A(x) \in \mathrm{Mat}_n(k(x))$ inversible et le vecteur $G(x)$ dans $(k(x))^n$, on peut le transformer en un système homogène en ajoutant une $(n+1)$ième ligne de valeur 1 au vecteur $Y(x)$. On obtient ainsi un système homogène de matrice inversible notée $B(x) \in \mathrm{Mat}_{n+1}(k(x))$ (cf, [52, Sect. 2.2]). Dans la suite on peut se restreindre au cas des équations homogènes.

De même, pour tout $n \geqslant 1$, on considère l'équation scalaire suivante

$$y(x+n) + a_{n-1}(x)y(x+n-1) + \cdots + a_1(x)y(x+1) + a_0(x)y(x) = \varphi(x), \qquad \text{(VI.2)}$$

avec $\varphi(x), a_1(x), \cdots, a_{n-1}(x) \in k(x), a_0(x) \in k(x) \setminus \{0\}$. Une telle équation est dite non-homogène, si la fraction rationnelle φ est non nulle.

Par élimination du dénominateur de l'équation (VI.2), on obtient l'équation

$$b_n(x)y(x+n) + b_{n-1}(x)y(x+n-1) + \cdots + b_1(x)y(x+1) + b_0(x)y(x) = \psi(x), \quad \text{(VI.3)}$$

avec $\psi(x), b_1(x), \cdots, b_{n-1}(x) \in k[x], b_0(x), b_n(x) \in k[x] \setminus \{0\}$. De façon équivalente, les équations (VI.2) et (VI.3) peuvent être représentées à l'aide d'un opérateur L, qui s'écrit comme polynôme en ϕ (avec ϕ l'opérateur de translation) à coefficients dans $k[x]$. Par exemple (VI.3) s'écrit sous forme $L(y) = \psi(x)$ où l'opérateur

$$L = b_n(x)\phi^n + \cdots + b_1(x)\phi + b_0(x), \quad \phi(y(x)) = y(x+1), \qquad \text{(VI.4)}$$

Du point de vue algorithmique, actuellement il existe quelques algorithmes qui trouvent des solutions rationnelles (i,e fractions rationnelles) des équations scalaires (VI.2), (VI.3) et du système (VI.1). L'algorithme dû à Abramov et Barkatou [4; 6; 18] commence d'abord par construire le « dénominateur universel », c'est-à-dire un polynôme $U(x)$ de sorte qu'une solution rationnelle $y(x) \in k(x)$ de l'équation (VI.2) ou celle de (VI.3) s'écrit sous la forme

$$y(x) = \frac{z(x)}{U(x)}, \qquad \text{(VI.5)}$$

avec $z(x)$ dans $k[x]$ (autrement dit, si par exemple l'équation (VI.2) a une solution rationnelle qui s'écrit sous la forme $\frac{f(x)}{g(x)}$ alors $g(x)|U(x)$).

Dans le cas du système linéaire qui s'écrit sous la forme (VI.1), chaque composante

du vecteur solution est de la forme

$$Y_i(x) = \frac{Z_i(x)}{U(x)}, \quad i = 1, 2, \ldots, n, \tag{VI.6}$$

où $Z_1(x), Z_2(x), \ldots, Z_n(x) \in k[x]$.

Dans la section VI.4.3, nous décrivons l'algorithme [52], appliqué sur le corps des nombres complexes ($k = \mathbb{C}$) pour résoudre le système (VI.1). Il trouve n solutions rationnelles $R_1(x), R_2(x), \ldots, R_n(x) \in \mathbb{C}(x)$ appelées « bornes à dénominateur » (denominator bounds) de sorte que, pour toute solution rationnelle du système (VI.1) on a

$$Y_i(x) = Z_i(x)R_i(x), \quad i = 1, 2, \ldots, n, \tag{VI.7}$$

avec $Z_1(x), Z_2(x), \ldots, Z_n(x) \in \mathbb{C}[x]$, pour tout $i = 1, 2, \ldots, n$, le numérateur de $R_i(x)$ est un facteur du numérateur de la $i$ème entrée $Y_i(x)$ de la solution $Y(x)$. La substitution (VI.7) est utilisée au lieu de (VI.5) et (VI.6). Dans la section VI.5, nous proposons une version améliorée à cet algorithme (algorithme $\mathbf{A}_B$) appliquée dans un corps de caractéristique nulle, et sur des équations scalaires de la forme (VI.2) et (VI.3).

VI.2 Préliminaires

Du fait, qu'on utilise les polynômes et les fractions rationnelles sur un corps k, nous indiquerons que les deux polynômes $f(x), g(x) \in k[x]$, sont étrangers (co-premiers) par l'écriture $f(x) \perp g(x)$. Si $F(x)$ est une fraction rationnelle à coefficients dans k, alors son dénominateur $\operatorname{den} F(x)$ est un polynôme unitaire à coefficients dans le corps k tels que

$$F(x) = \frac{f(x)}{\operatorname{den} F(x)}$$

pour tout $f(x) \in k[x], f(x) \perp \operatorname{den} F(x)$. Dans ce cas, le numérateur de $F(x)$ est noté par $\operatorname{num} F(x)$.

L'ensemble des polynômes irréductibles de $k[x]$ est noté par $\operatorname{Irr}(k[x])$. Soit $p(x)$ un polynôme dans $\operatorname{Irr}(k[x])$, alors l'application $\operatorname{val}_{p(x)} : k[x] \to \mathbb{N} \cup \{\infty\}$ qui associe à un polynôme $f(x)$ dans $k[x]$ la valeur

$$\operatorname{val}_{p(x)} f(x) = \max\{m \in \mathbb{N}, \quad p^m(x) | f(x)\}, \quad \text{et} \ \operatorname{val}_{p(x)} 0 = \infty,$$

est appelée la valuation en $p(x)$ de $f(x)$. Si $F(x) \in k(x)$

$$\mathrm{val}_{p(x)}F(x) = \mathrm{val}_{p(x)}(\mathrm{num}\, F(x)) - \mathrm{val}_{p(x)}(\mathrm{den}\, F(x)).$$

Soit $p(x) \in \mathrm{Irr}(k[x])$ et $f(x)$ un polynôme non nul à coefficients dans k, soit l'ensemble fini

$$\mathcal{N}_{p(x)}(f(x)) = \{m \in \mathbb{Z} : p(x+m) | f(x)\}. \tag{VI.8}$$

Remarque VI.2.1. *Si l'ensemble $\mathcal{N}_{p(x)}(f(x))$ est vide, alors*

$$\max \mathcal{N}_{p(x)}(f(x)) = -\infty \ \ et \quad \min \mathcal{N}_{p(x)}(f(x)) = \infty\,.$$

Soit $A(x)$ la matrice carrée d'ordre n, définie comme dans le système (VI.1), alors son dénominateur

$$\mathrm{den}\, A(x) = \mathrm{ppcm}_{i=1}^{n}\mathrm{ppcm}_{j=1}^{n}\, \mathrm{den}\, a_{ij}(x),$$

et celui de sa matrice inverse

$$\mathrm{den}\, A^{-1}(x) = \mathrm{ppcm}_{i=1}^{n}\mathrm{ppcm}_{j=1}^{n}\, \mathrm{den}\, \tilde{a}_{ij}(x).$$

Si $F(x) = (F_1(x), F_2(x), \ldots, F_n(x))^T \in k(x)^n$, alors

$$\mathrm{den}\, F(x) = \mathrm{ppcm}_{i=1}^{n}\, \mathrm{den}\, F_i(x), \quad \text{et } \mathrm{val}_{p(x)}F(x) = \min_{1\leqslant i\leqslant n}(\mathrm{val}_{p(x)}F_i(x)).$$

Si $F(x) = (F_1(x), F_2(x), \ldots, F_n(x))^T \in k(x)^n$ est une vecteur solution du système (VI.1), ($F(x) \in k(x)$ une solution d'une des équations scalaires (VI.2) ou (VI.3) respectivement) est une *solution rationnelle*. Alors si de plus $\mathrm{den}\, F(x) \neq 1$, on dit que cette solution est *non-polynomiale*, elle est *polynomiale* ailleurs.

Le premier algorithme de calcul formel qui recherche les solutions rationnelles à coefficients dans un corps k, de l'équation (VI.3) est dû à Abramov [3]. En utilisant l'ensemble (VI.8), on peut reformuler quelques propriétés prouvées dans [3] comme suit.

Proposition VI.2.2. *(* [3]) *Soit $F(x)$ une solution rationnelle de l'équation (VI.3), soit $p(x)$ un polynôme irréductible dans* $\mathrm{Irr}(k[x])$*, tel que $p(x)|\,\mathrm{den}\, F(x)$ (c'est-à-dire 0 est un élément de $\mathcal{N}_{p(x)}(\mathrm{den}\, F(x))$). Posons*

$$l = \max \mathcal{N}_{p(x)}(\mathrm{den}\, F(x)), \ \ et \ \ m = \min \mathcal{N}_{p(x)}(\mathrm{den}\, F(x)).$$

Alors $p(x+l)|b_n(x-n)$ *et* $p(x+m)|b_0(x)$.

Par conséquent, si l'équation (VI.3) a une solution rationnelle non-polynomiale, alors pour tout entier $d \in \mathbb{N}$

$$\deg \operatorname{pgcd}(b_0(x+d), b_n(x-n)) > 0.$$

En effet, soit $p(x)$ le polynôme définit par la proposition VI.2.2. Posons $d = l - m$, alors $p(x+l) = p(x+m+d)$. Donc on a $p(x+m)|b_0(x)$ et $p(x+m+d)|b_n(x-n)$.

Dans [6], ceci a été généralisé pour les systèmes (VI.1).

Proposition VI.2.3. ([6]) *Soit* $F(x) = (F_1(x), F_2(x), \ldots, F_n(x))^T \in k(x)^n$ *le vecteur solution du système (VI.1), soit* $p(x)$ *un polynôme irréductible dans* $\operatorname{Irr}(k[x])$, *tel que* $p(x)|\operatorname{den} F(x)$. *Posons*

$$l = \max \mathcal{N}_{p(x)}(\operatorname{den} F(x)), \quad m = \min \mathcal{N}_{p(x)}(\operatorname{den} F(x)),$$

$$u_0(x) = \operatorname{den} A^{-1}(x), \quad u_1(x) = \operatorname{den} A(x).$$

Alors $p(x+l)|u_1(x-1)$ *et* $p(x+m)|u_0(x)$.

Par conséquent, si le système (VI.1) a une solution rationnelle non-polynomiale, alors pour tout $d \in \mathbb{N}$,

$$\deg \operatorname{pgcd}(u_1(x-1), u_0(x+d)) > 0.$$

Concernant les dénominateurs, l'algorithme [6] appliqué sur les systèmes est une généralisation de l'algorithme [4] appliqué sur le cas scalaire.

VI.3 Les ensembles $\mathcal{M}$, $\mathcal{S}$, $\mathcal{S}_{k[x]}$ et $\mathcal{D}$

VI.3.1 L'ensemble $\mathcal{M}$

On pose $\mathcal{M}$ l'ensemble fini, constitué des polynômes irréductibles $p(x) \in \operatorname{Irr}(k[x])$ de sorte, que si une équation scalaire, ou un système donné a une solution rationnelle non-polynomiale, le polynôme $p(x)$ divise le dénominateur de la solution. L'ensemble $\mathcal{M}$ dépend de l'équation ou du système d'origine.

Commençons, par traiter le cas d'un système représenté par la formule (VI.1). Posons

$$u_0(x) = \operatorname{den} A^{-1}(x), \quad \text{et} \quad u_1(x) = \operatorname{den} A(x).$$

Soit la donnée de l'ensemble fini (avec $s \geqslant 1$)

$$Q = \{q_1(x), q_2(x), \ldots, q_s(x)\}, \tag{VI.9}$$

constitué de tous les polynômes de $\operatorname{Irr}(k[x])$ vérifiant, pour tout $t = 1, 2, \ldots, s$

$$\min \mathcal{N}_{q_t(x)}(u_0(x)) = 0, \quad \max \mathcal{N}_{q_t(x)}(u_1(x-1)) \geqslant 0. \tag{VI.10}$$

Pour tout $t = 1, 2, \ldots, s$, et tout polynôme $q_t(x) \in Q$, on considère l'ensemble

$$\mathcal{M}_{q_t(x)} = \{q_t(x), q_t(x+1), \ldots, q_t(x+d_t)\}, \tag{VI.11}$$

avec

$$d_t = \max \mathcal{N}_{q_t(x)}(u_1(x-1)). \tag{VI.12}$$

On définit l'ensemble $\mathcal{M}$ par

$$\mathcal{M} = \bigcup_{t=1}^{s} \mathcal{M}_{q_t(x)}. \tag{VI.13}$$

Proposition VI.3.1. *Soit $F(x) \in k(x)^n$ un vecteur solution du système (VI.1), soit $p(x)$ dans $\operatorname{Irr}(k[x])$ de sorte que $p(x) | \operatorname{den} F(x)$. Alors $p(x) \in \mathcal{M}$.*

Démonstration. De la proposition VI.2.3, on déduit que les deux ensembles ne sont pas vide

$$\mathcal{N}_{p(x)}(u_0(x)) \neq \varnothing \neq \mathcal{N}_{p(x)}(u_1(x-1)).$$

Avec $l = \max \mathcal{N}_{p(x)}(u_1(x-1))$ et $m = \min \mathcal{N}_{p(x)}(u_0(x))$.
Évidemment, l'entier m est négatif et l'entier l est positif. En effet, posons le polynôme $q(x) = p(x+m)$, et l'entier rationnel $d = l - m$. Alors

$$\min \mathcal{N}_{q(x)}(u_0(x)) = 0\,,\ \max \mathcal{N}_{q(x)}(u_1(x-1)) = d\,,\ \ p(x) = q(x-m)$$

et aussi $0 \leqslant -m \leqslant d$. □

VI.3.2 Les ensembles $\mathcal{S}$ et $\mathcal{S}_{k[x]}$

L'algorithme de van Hoeij [52] commence par la construction de l'ensemble S constitué des éléments $c \in \mathbb{C}$ de sorte que c est soit un pôle de la matrice A, soit une racine du déterminant de la matrice A c'est-à-dire $\det A(c) = 0$. Comme il est prouvé dans [52], l'ensemble fini

$$\mathcal{S} = \{c \in \mathbb{C} : \exists_{c_1,c_2 \in S},\ c - c_1 - 1 \in \mathbb{N},\ c_2 - c \in \mathbb{N}\}. \tag{VI.14}$$

vérifie que si une solution rationnelle du système a un pôle en $c \in \mathbb{C}$ alors $c \in \mathcal{S}$.

Pour avoir une analogie avec l'algorithme [52], et en particulier avec la formule (VI.14) donnée ci-dessus, on définit l'ensemble $S_{k[x]}$ des polynômes $p(x) \in \mathrm{Irr}(k[x])$ tels que $p(x) | \operatorname{den} A(x)$ ou bien $p(x) | \operatorname{num}(\det A(x))$ et l'ensemble analogue à $\mathcal{S}$

$$\mathcal{S}_{k[x]} = \{p \in \mathrm{Irr}(k[x]) : \exists_{p_1,p_2 \in S_{k[x]},\, l,m \in \mathbb{N}}\ p(x+l+1) = p_1(x), p(x-m) = p_2(x)\}$$

On remarque que si $k = \mathbb{C}$ et $\mathcal{S} = \{c_1, c_2, \ldots\}$ alors $\mathcal{S}_{\mathbb{C}[x]} = \{x - c_1, x - c_2, \ldots\}$.
De la même manière que [52], on prouve que si $F(x) \in k(x)^n$ est une solution du système (VI.1) et $p(x) \in \mathrm{Irr}(k[x])$ tel que $p(x) | \operatorname{den} F(x)$ alors $p(x) \in \mathcal{S}_{k[x]}$. Maintenant on compare les ensembles $\mathcal{S}_{k[x]}$ et $\mathcal{M}$.

Proposition VI.3.2. $\mathcal{M} \subseteq \mathcal{S}_{k[x]}$.

Démonstration. Soit l'ensemble $\mathcal{M}_{q_t(x)}$ donné par la formule (VI.11) est l'un des ensembles donnés dans la partie droite de l'ensemble (VI.13). Il suffit de montrer que

$$q_t(x), q_t(x+1), \ldots, q_t(x+d_t) \in \mathcal{S}_{k[x]}. \tag{VI.15}$$

De la formule (VI.10) et (VI.12), nous avons

$$q_t(x) | \operatorname{den} A^{-1}(x), \tag{VI.16}$$

et

$$q_t(x + d_t + 1) | \operatorname{den} A(x). \tag{VI.17}$$

La relation (VI.17) implique que $q_t(x + d_t + 1) \in S_{k[x]}$.

On considère la relation (VI.16), on sait que

$$A^{-1}(x) = \frac{1}{\det A(x)} \cdot C^T(x),$$

où $C(x)$ est la matrice des cofacteurs. Chaque cofacteur a un déterminant d'ordre $n-1$, dont ses composantes sont les mêmes que quelques composantes de la matrice $A(x)$. Donc le dénominateur de chaque cofacteur divise $(\operatorname{den} A(x))^{n-1}$. Ceci implique que le dénominateur de chaque entrée de $A^{-1}(x)$ divise le produit

$$(\operatorname{num} \det A(x)) \cdot (\operatorname{den} A(x))^{n-1}.$$

Comme $q_t(x)$ est irréductible, de (VI.16) on déduit qu'au moins une des relations

$$q_t(x) | \operatorname{num}(\det A(x)), \quad q_t(x) | \operatorname{den} A(x)$$

est vérifiée (dans le cas où $n = 1$ la première relation est vraie). Ceci donne $q_t(x) \in S_{k[x]}$. Donc $q_t(x), q_t(x + d_t + 1) \in S_{k[x]}$, et par suite (VI.15) est prouvée. □

Cependant $\mathcal{M}$ et $\mathcal{S}_{k[x]}$ ne coïncide pas dans certains cas.

Exemple VI.3.3. *Soit m un entier positif, $k = \mathbf{C}$ et la matrice*

$$A(x) = \begin{pmatrix} \frac{x+m}{x(x-m)} & 0 \\ 0 & \frac{x+m}{x(x-m)} \end{pmatrix}.$$

Dans ce cas, son inverse est

$$A^{-1}(x) = \begin{pmatrix} \frac{x(x-m)}{x+m} & 0 \\ 0 & \frac{x(x-m)}{x+m} \end{pmatrix},$$

Le calcul des déterminants $\det A(x) = \frac{(x+m)^2}{x^2(x-m)^2}$, $\operatorname{den} A(x) = x(x-m)$, $\operatorname{den} A^{-1}(x) = x + m$ *et aussi*

$$S = \{-m, 0, m\}, \quad \mathcal{S} = \{-m+1, -m+2, \ldots, 0, 1, \ldots, m\},$$

$$S_{k[x]} = \{x+m, x, x-m\}, \quad \mathcal{S}_{k[x]} = \{x+m-1, x+m-2, \ldots, x, x-1, \ldots, x-m\}.$$

Mais $\mathcal{M} = \varnothing$ et par la proposition VI.3.1 le système a une solution rationnelle non-polynomiale.

Nous n'avons pas besoin de faire la substitution définie par (VI.7).

Dans le cas scalaire, on prend $b_0(x), b_n(x-n)$ au lieu de $u_0(x), u_1(x-1)$, l'ensemble $\mathcal{M}$ peut être construit de la même manière.

VI.3.3 L'ensemble de dispersion $\mathcal{D}$

Pour tous polynômes (non nuls) $f(x)$ et $g(x)$ à coefficients dans k, on définit leur *ensemble de dispersion*

$$\mathbf{ds}(f(x), g(x)) = \{d \in \mathbb{N} \ : \ \deg \operatorname{pgcd}(f(x), g(x+d)) > 0\}$$

et leur *dispersion* :

$$\operatorname{dis}(f(x), g(x)) = \max(\mathbf{ds}(f(x), g(x)) \cup \{-\infty\}).$$

La dispersion vaut $-\infty$, si et seulement si, pour tout entier $d \in \mathbb{N}$ on a $\deg \operatorname{pgcd}(f(x), g(x+d)) = 0$. L'ensemble $\mathbf{ds}(f(x), g(x))$ peut être vu (obtenu) comme l'ensemble de toutes les racines entières non nulles du polynôme

$$\operatorname{Res}_x(f(x), g(x+d)) \in k[d].$$

Cependant on peut avoir rapidement cet ensemble, si on fait recourt à l'approche de Man et Wright [40] basée sur la décomposition irréductible (factorisation polynomiale) de $f(x)$ et $g(x)$.

Remarque VI.3.4. *Si une solution rationnelle non-polynomiale existe alors* $\mathbf{ds}(V(x), W(x))$ *est non vide. (voir Propositions VI.2.2, VI.2.3)*

VI.4 Algorithmes de construction du dénominateur universel et des bornes à dénominateur

Dans les sections VI.4.1, VI.4.2, VI.6.1, VI.6.2, on revoit les algorithmes de construction du polynôme universel [4; 6; 18]. Nous considérons l'algorithme de construction des bornes à dénominateur [52] dans la section VI.4.3. Dorénavant, nous utiliserons les notations suivantes :

$$V(x) = b_n(x-n), \quad W(x) = b_0(x)$$

pour l'équation (VI.3). Et les notations

$$V(x) = u_1(x-1), \quad W(x) = u_0(x),$$

où $u_1(x) = \operatorname{den} A(x)$, $u_0(x) = \operatorname{den} A^{-1}(x)$, pour le système (VI.1).

VI.4.1 L'algorithme de Abramov

L'algorithme [4; 6] est comme suit :

Find $\mathcal{D} = \mathbf{ds}(V(x), W(x))$. If $\mathcal{D} = \varnothing$ alors l'algorithme se termine et le résultat est $U(x) = 1$. (ci-dessous, nous supposerons que l'ensemble $\mathcal{D}$ à s éléments et s'écrit sous la forme $\mathcal{D} = \{d_1, d_2, \ldots, d_s\}$ sous la condition $d_1 > d_2 > \cdots > d_s$ pour tout $s \geqslant 1$.)
Poser $U(x) = 1$ puis exécuter successivement pour $m = 1, 2, \ldots, s$ les commandes suivantes :

$P(x) = \gcd(V(x), W(x + d_m))$
$V(x) = V(x)/P(x)$
$W(x) = W(x)/P(x - d_m)$
$U(x) = U(x) \prod_{i=0}^{d_m} P(x - i)$.

La valeur finale (sortie) $U(x)$ est le dénominateur universel des équations (VI.2),(VI.3) ou respectivement du système (VI.1). Nous nous référerons à cet algorithme par $\mathbf{A}_D$. Ce dernier est exploité dans les versions actuelles de Maple [44] :

LREtools[ratpolysols], LinearFunctionSystems[UniversalDenominator].

VI.4.2 L'algorithme de Barkatou

Dans Barkatou [18] le problème le plus général de recherche des solutions rationnelles du système (VI.1) a été résolu. Cependant, l'algorithme de [18, Prop. 3] peut être utilisé pour calculer le dénominateur universel $u(x)$ du système (VI.1). En utilisant notre notation (la mise en plus $d = \operatorname{dis}(V(x), W(x))$) cet algorithme peut être représenté comme suit.

On considère la suite des polynômes $\{(V_j(x), W_j(x), P_j(x))\}$ définie par :

$$V_0(x) = V(x), \quad W_0(x) = W(x), \quad P_0(x) = \operatorname{pgcd}(V(x), W(x+d)),$$

pour tout $j = 1, 2, \ldots, d$,

$V_j(x) = V_{j-1}(x)/P_{j-1}(x)$,

$W_j(x) = W_{j-1}(x)/P_{j-1}(x-d+j-1)$,

$P_j(x) = \text{pgcd}(V_j(x), W_j(x+d-j))$.

Alors $u(x) = \prod_{j=0}^{d} \prod_{i=0}^{d-j} P_j(x-i)$.

Nous nous référerons à cet algorithme par $\mathbf{A}_G$.

VI.4.3 L'algorithme de van Hoeij

Dans le cas d'un système, suite à l'algorithme de van Hoeij [52], on définit pour tout entier naturel N

$$A_N(x) = A(x-1)A(x-2)\ldots A(x-N). \tag{VI.18}$$

Alors chaque solution $Y(x)$ du système (VI.1) vérifie

$$Y(x) = A_N(x)Y(x-N). \tag{VI.19}$$

Comme nous l'avons déjà mentionné dans la section VI.1, si $k = \mathbb{C}$ l'algorithme de [52] s'applique au système (VI.1). Soit l'ensemble $\mathcal{S}$ défini par la formule (VI.14), pour tout élément c de $\mathcal{S}$, l'algorithme prend une valeur $N \in \mathbb{N}$ de sorte que $c - N \notin \mathcal{S}$.

On suppose que $Y(x) = (Y_1(x), Y_2(x), \ldots, Y_n(x))^T$ est une solution rationnelle du système (VI.1), alors, pour tout $i = 1, 2, \ldots, n$, on a $\text{val}_{x-c} Y_i(x-N) \geqslant 0$. Les valuations en $x - c$ des entrées (composantes) de $A_N(x)$, donne des bornes (bornes à gauche)

$$i = 1, 2, \ldots, n, \quad \text{val}_{x-c} Y_i(x). \tag{VI.20}$$

Cette fois-ci, on prend N de sorte que $c + N \notin \mathcal{S}$. Puisque la matrice A est inversible, nous avons

$$Y(x) = A_{-N}(x)Y(x+N), \tag{VI.21}$$

avec

$$A_{-N} = A^{-1}(x)A^{-1}(x+1)\ldots A^{-1}(x+N-1). \tag{VI.22}$$

Ceci aussi donne des bornes, il s'agit des bornes (à droite) de (VI.20). Pour tout i l'algorithme prend le maximum.

VI.5 Versions modifiées de l'algorithme de construction des bornes à dénominateur (algorithm A_B)

Dans ce paragraphe, nous décrivons une généralisation de l'algorithme de [52] dans un corps de caractéristique nulle. Nous utiliserons aussi l'ensemble $\mathcal{M}$ au lieu de $\mathcal{S}$,$\mathcal{S}_{k[x]}$.

Soit $p(x) \in \mathrm{Irr}(k[x])$, N un entier positif, $1 \leqslant i \leqslant n$. On définit $B(p(x), N, i)$ par le minimum des valuations en $p(x)$ des composantes (entrées) de la i-ème ligne de la matrice $A_N(x)$. Alors $\mathrm{val}_{p(x)} Y_i(x - N) \geqslant 0$, pour $i = 1, 2, \ldots, n$, implique

$$\mathrm{val}_{p(x)} Y_i(x) \geqslant B(p(x), N, i), \quad i = 1, 2, \ldots, n. \tag{VI.23}$$

De la même manière, on peut utiliser la matrice de la forme $A_{-N}(x)$ (voir (VI.21)). Pour un entier naturel N, la valeur $B(p(x), -N, i)$ est définie par le minimum des valuations en $p(x)$ des composantes de la i-ème ligne de la matrice $A_{-N}(x)$. Si l'entier N est de sorte que $\mathrm{val}_{p(x)} Y_i(x + N) \geqslant 0$, pour $i = 1, 2, \ldots, n$ alors

$$\mathrm{val}_{p(x)} Y_i(x) \geqslant B(p(x), -N, i), \quad i = 1, 2, \ldots, n. \tag{VI.24}$$

De la même manière que [52], les bornes (VI.23) sont des bornes à gauche, alors que celles de (VI.24) sont des des bornes à droite.

Maintenant, soit l'ensemble Q défini par (VI.9) et $\mathcal{M}_{q_t(x)}$ défini par (VI.11), $t = 1, 2, \ldots, s$. Soit

$$d = \max\{d_1, d_2, \ldots, d_t\} = \mathrm{dis}(V(x), W(x)). \tag{VI.25}$$

L'algorithme est défini comme suit. En calculant successivement les matrices $A_N(x)$, pour $N = 1, 2, \ldots, d + 1$, on trouve pour tout t tels que $1 \leqslant t \leqslant s$ et $d_t \geqslant N - 1$, les valeurs

$$B(q_t(x + d_t - N + 1), N, i), \quad i = 1, 2, \ldots, n,$$

Ceci nous donne une borne à gauche de $\mathrm{val}_{q_t(x+d_t-N+1)} Y_i(x)$, pour $i = 1, 2, \ldots, n$.

De même, en calculant successivement les matrices $A_{-N}(x)$, pour $N = 1, 2, \ldots, d + 1$, on trouve pour tout t tels que $1 \leqslant t \leqslant s$ et $d_t \geqslant N - 1$, les valeurs

$$B(q_t(x + N - 1), -N, i), \quad i = 1, 2, \ldots, n,$$

Ceci nous donne une borne à droite de $\mathrm{val}_{q_t(x+N-1)}Y_i(x)$, $i = 1, 2, \ldots, n$. Ainsi toutes les valuations $\mathrm{val}_{q_t(x+j)}Y_i(x)$, pour tout $i = 1, 2, \ldots, n$, $t = 1, 2, \ldots, s$ et $j = 0, 1, \ldots, d_t$ sont bornées. Notons par $\alpha_{i,j,t}$ leurs maximum. Les fractions rationnelles suivantes

$$R_i(x) = \prod_{\substack{1\leqslant t\leqslant s\\ 0\leqslant j\leqslant d_t}} q_t^{\alpha_{i,j,t}}(x+j), \quad i = 1, 2, \ldots, n,$$

sont utilisées dans la substitution (VI.7).

L'algorithme [52] est décrit que dans le cas d'un système (VI.1). Le cas des équations scalaires, homogènes (VI.2) et (VI.3) ont été considéré ([52, Sect. 3]) par leurs interprétations matricielles, c'est-à-dire un système où $A(x)$ est la matrice compagnon de l'équation scalaire. Mais le produit matricielle est une opération coûteuse. En outre, il n'est pas difficile de donner une version scalaire de l'algorithme ; nous décrivons cette version sur un corps quelconque de caractéristique nulle. Montrons d'abord, qu'on peut construire, pour tout entier positif N, l'équation

$$y(x) = v_{N,\,n-1}(x)y(x-N) + \cdots + v_{N,\,0}(x)y(x-N-n+1) + v_{N,\,-1}(x) \tag{VI.26}$$

où $v_{N,\,-1}(x), v_{N,0}(x), \ldots, v_{N,n-1}(x) \in k(x)$, qui admet comme solutions toutes les solutions rationnelles de (VI.2) et (VI.3). En effet, on procède par récurrence.

Pour $N = 1$ l'équation suivante

$$y(x) = -a_{n-1}(x-n)y(x-1) - \cdots - a_0(x-n)y(x-n) + \varphi(x-n), \tag{VI.27}$$

est une conséquence de (VI.2).
Il suffit de prendre $v_{1,\,-1}(x) = \varphi(x-n)$ et $v_{1,i}(x) = -a_i(x-n)$, $i = 0, 1, \ldots, n-1$. On suppose que l'équation(VI.27) est construite pour tout entier $N \geqslant 1$, nous montrons qu'on peut en construire une pour $N+1$. En utilisant l'égalité

$$\begin{aligned} y(x-N) \;=\; & -a_{n-1}(x-N-n)y(x-N-1) - \ldots \\ & \cdots - a_0(x-N-n)y(x-N-n) + \varphi(x-N-n) \end{aligned} \tag{VI.28}$$

pour éliminer $y(x-N)$ de (VI.26).

Pour tout N, de la même manière que (VI.26), on construit une équation

$$y(x) = w_{N,\,n-1}(x)y(x+N) + \cdots + w_{N,\,0}(x)y(x+N+n-1) + w_{N,\,-1}(x) \qquad \text{(VI.29)}$$

avec $w_{N,\,-1}(x), w_{N,0}(x), \ldots, w_{N,n-1}(x) \in k(x)$, de sorte qu'elle soit satisfaite par toutes les solutions rationnelles de (VI.2) et (VI.3). Si le coefficients $a_0(x)$ de l'équation (VI.2) est non nul, on peut l'écrire sous la forme suivante

$$y(x) = c_1(x)y(x+1) + c_2(x)y(x+2) + \cdots + c_n(x)y(x+n) + \chi(x),$$

avec $c_1(x), c_2(x), \ldots, c_n(x), \chi(x) \in k(x)$.
Donc pour $N = 1$, on pose $w_{1,\,-1}(x) = \chi(x)$ et $w_{1,i}(x) = c_{n-i}(x)$, $i = 0, 1, \ldots, n-1$. On suppose que l'équation (VI.29) est construite pour un certain entier $N \geqslant 1$. alors on peut obtenir l'équation correspondante à $N+1$ en utilisant l'égalité suivante

$$y(x+N) = c_1(x+N)y(x+N+1) + \cdots + c_n(x+N)y(x+N+n) + \chi(x+N)$$

par elimination de $y(x+N)$ dans (VI.29). Les équations (VI.26), (VI.29) sont équivalentes aux équations (VI.19), (VI.21). Soit $p(x) \in \mathrm{Irr}(k[x])$, soit N un entier positif. On note le minimum des valuations des coefficients $v_{N,\,-1}(x), v_{N,\,0}(x), \ldots, v_{N,n-1}(x)$ en $p(x)$ de l'équation (VI.26) par $B(p(x), N)$. Et par $B(p(x), -N)$, le minimum des valuations des coefficients $w_{N,\,-1}(x), w_{N,\,0}(x), \ldots, w_{N,n-1}(x)$ en $p(x)$ de l'équation (VI.29).

Nous considérons l'ensemble $\mathcal{M}$ donné par la formule (VI.13) pour l'équation (VI.2). Les égalités (VI.9), (VI.11) et (VI.25) sont vraies. L'algorithme dans le cas scalaire est comme suit.
Une construction successive, pour tout $N = 1, 2, \ldots, d+1$, des équations (VI.26) donne tout t vérifiant $1 \leqslant t \leqslant s$ et $d_t \geqslant N-1$ la valeur $B(q_t(x+d_t-N+1), N)$; ce qui nous donne une borne à gauche de la valuation $\mathrm{val}_{q_t(x+d_t-N+1)}y(x)$. De même, pour tout $N = 1, 2, \ldots, d+1$, par la construction successive des équations (VI.29), on calcule pour tout t vérifiant $1 \leqslant t \leqslant s$ et $d_t \geqslant N-1$ la valeur $B(q_t(x+N-1), -N)$, ce qui nous donne un borne à droite de la valuation $\mathrm{val}_{q_t(x+N-1)}y(x)$.

Ainsi, pour tout $t = 1, 2, \ldots, s$, $j = 0, 1, \ldots, d_t$, la valuation $\mathrm{val}_{q_t(x+j)}y(x)$ est bornée, il suffit de prendre le maximum de chaque, qu'on notera $\beta_{j,t}$. La fraction rationnelle

$$R(x) = \prod_{\substack{1 \leqslant t \leqslant s \\ 0 \leqslant j \leqslant d_t}} q_t^{\beta_{j,t}}(x+j) \qquad \text{(VI.30)}$$

serait utilisée pour la substitution $y(x) = z(x)R(x)$ dans (VI.2).

Nous nous référons à cette modification (dans les deux cas : système et scalaire) de l'algorithme [52] par $\mathbf{A}_B$. En le comparant cet algorithme avec [52], la nouveauté consiste à considérer les polynômes irréductibles sur un corps de caractéristique nulle au lieu des nombres complexes, et de l'ensemble $\mathcal{M}$ au lieu de $\mathcal{S}$, $\mathcal{S}_{k[x]}$.

VI.6 Nouveaux algorithmes de construction de dénominateur universel

VI.6.1 L'algorithme $\mathbf{A}_U$

Les algorithmes [4; 6; 18] de construction du dénominateur universel utilisent le calcul du pgcd au lieu de la décomposition irréductible de polynômes, mais ils utilisent le calcul de dispersion de polynômes *polynomial dispersion computation* ; nous avons déjà mentionné dans la section VI.2 que la version récente de Maple utilise la factorisation polynomiale pour le calcul de dispersion. L'algorithme que nous présentons dans la suite a le même style que l'algorithme $\mathbf{A}_B$.

Théorème VI.6.1. *Soit une équation donnée par la formule (VI.3), on pose $V(x) = b_n(x-n)$, $W(x) = b_0(x)$. Dans le cas d'un système (VI.1), nous posons $V(x) = u_1(x-1)$, $W(x) = u_0(x)$ avec $u_1(x) = \operatorname{den} A(x)$, $u_0(x) = \operatorname{den} A^{-1}(x)$. Soit $F(x)$ une solution rationnelle de l'équation (VI.3) ou du système (VI.1). Alors pour tout polynôme irréductible $p(x) \in \operatorname{Irr}(k[x])$ nous avons*

$$\operatorname{val}_{p(x)} F(x) \geqslant -\gamma_{p(x)}, \tag{VI.31}$$

où

$$\gamma_{p(x)} = \min\left\{ \sum_{l\in\mathbb{N}} \operatorname{val}_{p(x+l)} V(x), \sum_{l\in\mathbb{N}} \operatorname{val}_{p(x-l)} W(x) \right\}. \tag{VI.32}$$

Démonstration. Posons $d = \operatorname{dis}(V(x), W(x))$ et $N = d+1$ dans (VI.19) et (VI.21). Les deux polynômes $\operatorname{den} A_{d+1}(x)$ et $\operatorname{den} A_{-d-1}(x))$ (voir (VI.18), (VI.22)) sont des dénominateurs universels pour le système (VI.1). En effet $\operatorname{den} A_{d+1}(x) \mid W(x)W(x+1)\dots W(x+d)$ et $\operatorname{den} A_{-d-1}(x) \mid V(x)V(x-1)\dots V(x-d)$. Donc $\operatorname{den} F(x) \mid V(x)V(x-1)\dots V(x-d)$ et $\operatorname{den} F(x) \mid W(x)W(x+1)\dots W(x+d)$. (Dans le cas scalaire, on obtient des relations similaires, il suffira de prendre $A(x)$ la matrice compagnon pour obtenir un système de type $Y(x+1) = A(x)Y(x)$.) Reste à montrer l'inégalité (VI.31), cette

dernière provient des égalités suivantes

$$\mathrm{val}_{p(x)} \prod_{i=0}^{d} V(x-i) = \sum_{i\in\mathbb{N}} \mathrm{val}_{p(x)} V(x-i),$$

$$\mathrm{val}_{p(x)} \prod_{i=0}^{d} W(x+i) = \sum_{i\in\mathbb{N}} \mathrm{val}_{p(x)} W(x+i).$$

□

Si pour tout $q_t(x+j) \in \mathcal{M}$ (section VI.3.2), nous calculons la valeur

$$\gamma_{j,t} = \min\left\{ \sum_{i\in\mathbb{N}} \mathrm{val}_{q_t(x+j+i)} V(x),\ \sum_{i\in\mathbb{N}} \mathrm{val}_{q_t(x+j-i)} W(x) \right\}$$

ceci nous permet d'avoir le dénominateur universel

$$\prod_{\substack{1\leqslant t\leqslant s \\ 0\leqslant j\leqslant d_t}} q_t^{\gamma_{j,t}}(x+j). \tag{VI.33}$$

Nous nus référons à cet algorithme par l'algorithme $\mathbf{A}_U$. En comparant cet algorithme avec [4; 6; 18] , la nouveauté est de considérer l'ensemble $\mathcal{M}$ et la valuation en ses éléments au lieu de la dispersion et les pgcd.

Remarque VI.6.2. *Soit la matrice $A(x)$, pour tout $i = 1, 2, \ldots, n$, notons par $a_i(x)$ la ième ligne de la matrice $A(x)$. Posons $h_i(x) = \mathrm{den}\, a_i(x)$. Soit*

$$D(x) = \mathrm{diag}(h_1(x), h_2(x), \ldots, h_n(x)). \tag{VI.34}$$

Pour la construction du dénominateur universel (cas d'un système (VI.1)), les polynômes $\det D(x)$ et $\det(D(x)A(x))$ sont utilisés dans $\mathbf{A}_G$ au lieu des dénominateurs $\mathrm{den}\, A(x)$ et $\mathrm{den}\, A^{-1}(x)$. Soit $v_0(x) = \det(D(x)A(x))$ et $v_1(x) = \det D(x)$, avec $D(x)$ est défini par la formule(VI.34). Il a été démontré dans l'article de Barkatou [18] que le $\mathrm{pgcd}\left(\prod_{i=0}^{h} v_0(x-i), \prod_{i=0}^{h} v_1(x+i)\right)$ est le dénominateur universel. Ceci peut être utilisé pour une deuxième preuve du théorème VI.6.1. De même, le cas scalaire du théorème VI.6.1 résulte de [4, Th. 2].

Dans [18] les deux cas suivant sont prouvés

1. *Si l'équation (VI.3) a une solution rationnelle* $F(x) \in k(x)$, *soit l'entier* $m \in \mathbb{N}$ *tel que* $b_n(x-n) \perp b_0(x+l)$ *pour tout entier* $l > m$. *Alors* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} b_n(x-n-i)$ *et aussi* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} b_0(x+i)$.

2. *Si le système (VI.1) a une solution rationnelle* $F(x) \in k(x)^n$, $v_0(x) = \det(D(x)A(x))$, $v_1(x) = \det D(x)$, *où la matrice* $D(x)$ *est définie par la formule (VI.34), soit* m *un entier naturel, de sorte que* $v_1(x-1-l) \perp v_0(x)$ *pour tout entier* $l > m$. *Alors* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} v_1(x-1-i)$ *et* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} v_0(x+i)$.

Proposition VI.6.3. *On suppose que le système (VI.1) a une solution rationnelle* $F(x) \in k(x)^n$. *Soit* $u_0(x) = \operatorname{den} A^{-1}(x)$ *et* $u_1(x) = \operatorname{den} A(x)$, *soit* m *un entier naturel de sorte que* $u_1(x-1) \perp u_0(x+l)$ *pour tout entier* $l > m$. *Alors on a* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} u_1(x-1-i)$ *et* $\operatorname{den} F(x) \mid \prod_{i=0}^{m} u_0(x+i)$.

Démonstration. Résulte du théorème VI.6.1. □

Dans le cas d'un système différentiel $Y'(x) = A(x)Y(x)$ avec $A(x) \in \mathrm{Mat}_n(k(x))$. Si le système admet une solution rationnelle $F(x)$, alors on sait que pour tout m entier assez grand on a $\operatorname{den} F(x) \mid (\operatorname{den} A(x))^m$. La proposition VI.6.3 donne une analogie.

Il est facile de montrer que $\operatorname{den} A(x) \mid \det D(x)$ et que $\operatorname{den} A^{-1}(x) \mid \det(D(x)A(x))$ avec la matrice $D(x)$ définie par (VI.34). Dans certain cas, les inégalités $\deg(\operatorname{den} A(x)) < \deg(\det D(x))$, $\deg(\operatorname{den} A^{-1}(x)) < \deg(\det(D(x)A(x)))$ sont vraies, car le déterminant $\det D(x) = h_1(x)h_2(x)\dots h_n(x)$ et $\det A(x) = \operatorname{ppcm}(h_1(x), h_2(x), \dots h_n(x))$.
Si par exemple, $A(x)$ la matrice carrée d'ordre n est donné par

$$A(x) = \operatorname{diag}\left(\frac{x(x+1)}{(x+3)(x+4)}, \frac{x(x+1)}{(x+3)(x+4)}, \cdots, \frac{x(x+1)}{(x+3)(x+4)}\right), \tag{VI.35}$$

alors

$$D(x) = \operatorname{diag}((x+3)(x+4), (x+3)(x+4), \dots, (x+3)(x+4)),$$

$$\det D(x) = (x+3)^n(x+4)^n, \quad \text{et} \quad \operatorname{den} A(x) = (x+3)(x+4);$$

de même $\det(D(x)A(x)) = x^n(x+1)^n$ avec $\operatorname{den} A^{-1}(x) = x(x+1)$. Soit le système $Y(x+1) = A(x)Y(x)$ où la matrice $A(x)$ est donnée par la formule (VI.35). En utilisant l'algorithme [6] et $\mathbf{A}_U$, on obtient le dénominateur universel $x(x+1)^2(x+2)^2(x+3)$. Cependant, par $\mathbf{A}_G$ on a le dénominateur universel $x^n(x+1)^{2n}(x+2)^{2n}(x+3)^n$. Une modification de $\mathbf{A}_G$ permettra d'éviter cet excès.

VI.6.2 Une version améliorée de l'algorithme $\mathbf{A}_U$ (l'algorithme $\mathbf{A}'_U$)

Comme il a été décrit précédemment, l'algorithme $\mathbf{A}_U$ a deux étapes. La construction de l'ensemble $\mathcal{M}$, puis pour tout polynôme $p(x) \in \mathcal{M}$ le calcul de la valeur $\gamma_{p(x)}$ donnée par la formule (VI.32) qui résulte dans le dénominateur universel. La formule (VI.32) contient des sommes sur $l \in \mathbb{N}$. En dépit, du fait que l'ensemble des entiers naturels $\mathbb{N}$ ne soit pas fini, les sommes sont finies. En effet, les termes de la somme correspondent aux facteurs irréductibles des polynômes $V(x)$ et $W(x)$ (la valuation correspondante est égale à l'exposant de chaque facteur de la décomposition en produits de polynômes irréductibles des $V(x)$ et $W(x)$). Le calcul de $\gamma_{p(x)}$ (VI.32) avec $p(x) = q_i(x+j) \in \mathcal{M}_{q_i(x)}$ (l'ensemble $\mathcal{M}_{q_i(x)}$ est donné par la formule (VI.11)), la valeur correspondante $\gamma_{q_i(x+j)}$ eut être être la même valeur pour plusieurs entiers successifs j. En effet, si par exemple on calcule $\gamma_{q_i(x)}$, puis pour tout j de 1 à d_i, on calcule $\gamma_{q_i(x+j)}$, alors la valeur peut être changée seulement que pour certains j de sorte $q_i(x+j)$ est un facteur irréductible de $V(x)$ ou $W(x)$ (tels points *critiques* peuvent être calculés en même temps que l'ensemble $\mathcal{M}$). Comme le lecteur peut le constater, le point clé ici est basé sur la correction de l'algorithme $\mathbf{A}_U$. Nous nous référons à cette version par $\mathbf{A}'_U$.

VI.7 Analyse des algorithmes $\mathbf{A}_D$, $\mathbf{A}_G$, $\mathbf{A}_U$ and $\mathbf{A}'_U$

VI.7.1 Equivalence des résultats

Théorème VI.7.1. *Les dénominateurs universels calculés par les algorithmes $\mathbf{A}_D$, $\mathbf{A}_G$ décrits dans la section VI.4.2 coïncident pour tout $V(x)$ et $W(x)$. Les polynômes intermédiaires calculés par $\mathbf{A}_D$ sont exactement les mêmes calculés par $\mathbf{A}_G$.*

Démonstration. Tout d'abord, on commence par montrer que l'algorithme $\mathbf{A}_G$ donne le même résultat et calcule les mêmes polynômes intermédiaires que $\mathbf{A}_D$. En effet, on remplace $\mathcal{D}$ par

$$\bar{\mathcal{D}} = \{d, d-1, \ldots, 0\},$$

$d = d_1 = \mathrm{dis}(V(x), W(x))$. Cette extension de $\mathcal{D}$ ne va pas changer le résultat (de plus, les pgcd seraient égaux à 1). En énumérant aussi les valeurs $V(x), W(x), P(x), U(x)$ dans $\mathbf{A}_D$.
On fixe $U_0(x) = 1, V_0(x) = V(x), W_0(x) = W(x)$, pour tout $j = 0, 1, \ldots, d-1$, nous exécutons successivement les relations suivantes

$P_{j+1}(x) = \mathrm{pgcd}(V_j(x), W(x+d-j))$
$V_{j+1}(x) = V_j(x)/P_{j+1}(x)$
$W_{j+1}(x) = W_j(x)/P_{j+1}(x-d+j)$
$U_{j+1}(x) = U_j(x)\prod_{i=0}^{d-j} P_{j+1}(x-i)$.

On constate pour tout $t = 0, 1, \ldots d$ que les triplets $(V_t(x), W_t(x), P_t(x))$ coïncident pour les deux algorithmes et $u(x) = U_d(x)$.

Il a été démontré dans [18] que si $d = \mathrm{dis}(V(x), W(x))$ alors

$$u(x) = \mathrm{pgcd}\left(\prod_{i=0}^{d} V(x-i),\ \prod_{i=0}^{d} W(x+i)\right).$$

Donc, pour tout $p(x) \in \mathrm{Irr}(k[x])$ la valeur $\mathrm{val}_{p(x)}u(x)$ est égale à $\gamma_{p(x)}$ de (VI.32). Ceci implique que les résultats (sorties) $\mathbf{A}_G$ et $\mathbf{A}_U$ coïncident. Donc, les sorties de $\mathbf{A}_D$ et, resp $\mathbf{A}_U$ coïncident aussi bien. Par conséquent il est évident que les sorties de $\mathbf{A}_U$ et $\mathbf{A}'_U$ coïncident aussi. □

Notons bien que le résultat similaire au Théorème VI.7.1 a été présenté dans [25].

VI.7.2 Comparaison de complexité de $\mathbf{A}_D$ et $\mathbf{A}'_U$

Soit $l = \max\{\deg V(x), \deg W(x)\}$ et $d = \mathrm{dis}(V(x), W(x))$ et $T_{\mathrm{gcd}}(l)$ la complexité du calcul de pgcd de deux polynômes (de degré au plus vaut l). On compare les complexités $T_{\mathbf{A}_D}(l,d)$ et $T_{\mathbf{A}'_U}(l,d)$ des deux algorithmes $\mathbf{A}_D$ et $\mathbf{A}'_U$ respectivement. Dans ce contexte, la complexité est le nombre d'opération sur un corps k dans le pire cas . Le lecteur peut observer qu'il en résulte du Théorème VI.7.1 que $T_{\mathbf{A}_D}(l,d) \leqslant T_{\mathbf{A}_G}(l,d)$.

Les deux algorithmes effectuent la multiplication polynomiale pour obtenir le dénominateur universel $U(x)$. On ne spécifie pas l'utilisation de l'algorithme de multiplication polynomiale, mais on supposera que le pire des cas est quand il est nécessaire de multiplier un nombre très grand (il s'agit de $\deg U(x)$) de polynômes de premier degré.

Les deux algorithmes trouvent la décomposition en produit d'irréductibles (factorisation polynomiale complète) de $V(x)$ et $W(x)$ et calculent leur ensemble de dispersion en même temps. De plus, $\mathbf{A}'_U$ construit l'ensemble Q (cf. (VI.9)), l'ensemble des valeurs d_t (voir (VI.12)), l'ensemble des points critiques et l'ensemble des valuations correspondantes. Le coût de ce calcul (au pire des cas) vaut $O(l)$, plus le coût de sortie des points critiques. Ceci donne le coût total $O(l \log l)$. D'autre part, $\mathbf{A}_D$ calcule les pgcd ; si $d \geqslant l$, alors au pire des cas ,le coût de ce calcul est $\sum_{i=0}^{l} T_{\mathrm{gcd}}(l-i)$ avec $T_{\mathrm{gcd}}(l)$ la complexité

de calcul du pgcd de deux polynômes (de degré ne dépassant pas l). Si $0 < d < l$ alors le coût au pire des cas est $\sum_{i=0}^{d} T_{\gcd}(l-i)$. Evidemment, $\sum_{i=0}^{l} T_{\gcd}(l-i) = \sum_{i=0}^{l} T_{\gcd}(i)$, $\sum_{i=0}^{d} T_{\gcd}(l-i) = \sum_{i=l-d}^{l} T_{\gcd}(i)$. Il en résulte la proposition suivante

Proposition VI.7.2. *Si* $T_{\gcd}(l)/(l\log l) \to \infty$ *alors pour tout* $l, d \in \mathbb{N} \setminus \{0\}$, *la différence* $T_D(l,d) - T_U(l,d)$ *est positive. Et on a*

$$T_D(l,d) - T_U(l,d) = \begin{cases} \sum_{i=0}^{l} T_{\gcd}(i) + O(l\log l), & \text{si } d \geqslant l, \\ \\ \sum_{i=l-d}^{l} T_{\gcd}(i) + O(l\log l), & \text{si } d < l. \end{cases} \tag{VI.36}$$

Dans le théorème suivant, on utilise la notation Ω qui est souvent la même en théorie de complexité ([36]). Contrairement à la notation O qui est utilisé pour décrire une borne asymptotique supérieure, la notation Ω est utilisé pour écrire une borne asymptotique inférieure.

Théorème VI.7.3. *Soit* $T_{\gcd}(l) = \Omega(l^\tau)$, $\tau > 1$. *Alors pour presque tout* $l, d \in \mathbb{N} \setminus \{0\}$ *la différence* $T_D(l,d) - T_U(l,d)$ *est positive et vaut* $\Omega(R(l,d))$, *avec*

$$R(l,d) = \begin{cases} l^{\tau+1}, & \text{si } d \geqslant l, \\ \\ dl^\tau, & \text{si } d < l. \end{cases}$$

Démonstration. Si $d \geqslant l$, le résultat provient de la formule (VI.36) et du fait que $\tau > 1$. Dans l'autre cas, c'est à dire si $d < l$ on peut utiliser l'inégalité suivante

$$\sum_{i=m}^{l} i^\tau > \frac{l^\tau(l-m)}{\tau+1} \tag{VI.37}$$

qui est vérifié pour tout entier $0 < m \leqslant l$ et tout réel $\tau \geqslant 1$. Posons $m = l - d$ ainsi on obtient ce qui a été demandé. Maintenant reste à prouver l'inégalité (VI.37), pour tout réels $x \geqslant 0$ et $\tau \geqslant 1$ la fonction x^τ est croissante. Ceci donne pour $m < l$ (le cas $m = l$ est trivial)

$$\sum_{i=m}^{l} i^\tau > \sum_{i=m+1}^{l} i^\tau > \sum_{i=m+1}^{l} \int_{i-1}^{i} x^\tau \,\mathrm{d}x = \int_{m}^{l} x^\tau \,\mathrm{d}x = \frac{l^{\tau+1}}{\tau+1}\left(1 - \left(\frac{m}{l}\right)^{\tau+1}\right).$$

Comme dans notre cas $1 - \left(\frac{m}{l}\right)^{\tau+1} \geqslant 1 - \frac{m}{l}$, d'où le résultat. □

Alors l'algorithme $\mathbf{A}_G$ et les algorithmes $\mathbf{A}_D, \mathbf{A}'_U$donne le même dénominateur universel, bien que parmi les trois $\mathbf{A}'_U$ a la complexité la plus basse.

Actuellement, selon la connaissance de l'auteur $T_{\gcd}(l) = \Omega(l^\tau)$, $\tau > 1$, de l'utilisation des algorithmes qui calculent les pgcd.

L'algorithme d'Euclide rapide (fast Euclidean algorithm ; FEA) [29, Ch. 11] a une complexité qui vaut $O(l \log^2 l \log\log l)$ si le transformée de Fourier rapide (Fast Fourier Transform, FFT) est utilisé pour la multiplication polynomiale. Mais, comme il y a un très grand nombre caché dans O ; il n'est pas possible, sur le plan pratique, d'utiliser cette version d'algorithme d'Euclide rapide. Néanmoins, si on suppose que FEA (fast Euclidean algorithm) est utilisé, alors l'estimation de la complexité pour cet algorithme est $\Omega(l \log^2 l \log\log l)$ (ou encore $\Omega(l \log^2 l)$). Alors suite à la Proposition VI.7.2 la valeur $T_D(l,d) - T_U(l,d)$ est positive (i.e., $T_U(l,d) < T_D(l,d)$) pour presque tout $l, d \in \mathbb{N} \setminus \{0\}$.

VI.8 Complexité de $\langle \mathbf{A}_B \rangle$ et $\langle \mathbf{A}'_U \rangle$

VI.8.1 Le schéma RS

Il est possible de montrer que la complexité de $\mathbf{A}_B$ est plus grande que celle de $\mathbf{A}_U$, et par suite plus grande que la complexité de $\mathbf{A}'_U$. Cependant l'algorithme $\mathbf{A}_B$ donne une bonne minoration. Une combinaison d'algorithmes $\mathbf{A}'_U, \mathbf{A}_B$ (l'un avec l'autre) pour trouver toutes les solutions polynomiales donne les algorithmes de construction des solutions rationnelles $\langle \mathbf{A}'_U \rangle$, $\langle \mathbf{A}_B \rangle$. dans la suite on compare leurs complexités.

On considère le cas scalaire. Dans la suite, on donne le schéma, des algorithmes décrits dans la Section VI.1 qui trouvent les solutions rationnelles des équations aux différences linéaires scalaires. Ce Schéma est appelé RS

RS1 : Construction d'unefraction rationnelle $R(x)$ de sorte que toute solution rationnelle de l'équation d'origine peut être représentée sous la forme $R(x)f(x)$ où $f(x)$ est un polynôme.

RS2 : Transformer l'équation d'origine en une équation qui admet $f(x)$ comme solution polynomiale si et seulement si $R(x)f(x)$ est une solution de l'équation d'origine.

RS3 : Construire toutes les solutions polynomiales de la nouvelle équation (l'équation transformée)

Certaines hypothèses de l'utilisation de l'algorithme décrit (qui trouve toutes les solutions polynomiales) dans l'étape RS3, permettront de montrer que la complexité de $\langle \mathbf{A}'_U \rangle$ est plus faible que celle de $\langle \mathbf{A}_B \rangle$ (selon la Section VI.7.2 la complexité est le nombre d'opérations sur le corps k au pire des cas).

Pour cet investissement, dans la suite, on a besoin des notions suivantes, à savoir l'équation indicielle (indicial equation) et aussi la hauteur d'une équation aux différences donnée par la formule (VI.3).

VI.8.2 Équation indicielle à l'infini

Soit L un opérateur de la forme (VI.4), alors on peut construire *l'équation indicielle* à l'infini (une équation algébrique) notée $I_L(\lambda) = 0$. L'entier μ est appelé *l'incrément* de l'opérateur L. L). On rappelle, qu'on obtient l'équation $I_L(\lambda)$ et l'entier μ, en écrivant la formule (VI.4) en fonction de l'opérateur $\Delta = \phi - 1$ au lieu de l'opérateur de translation ϕ, c'est à dire $L = c_n(x)\Delta^n + \cdots + c_1(x)\Delta + c_0(x)$. Alors

$$\mu = \max_{0 \leqslant j \leqslant n} (\deg c_j - j), \quad I_L(\lambda) = \sum_{\substack{0 \leqslant j \leqslant n \\ \deg a_j - j = \mu}} \mathrm{lc}(c_j)\lambda(\lambda-1)\ldots(\lambda-j+1).$$

Toute solution polynomiale de l'équation $L(y) = \psi(x)$ de la forme (VI.4) a un degré ne dépassant pas la hauteur de $L(y) = \psi(x)$:

$$h = \max\{\deg \psi - \mu,\ \tilde{\lambda}\}, \tag{VI.38}$$

où

$$\tilde{\lambda} = \max(\{\lambda \in \mathbb{N} \ :\ I_L(\lambda) = 0\} \cup \{-\infty\}). \tag{VI.39}$$

Les algorithmes connus utilisent l'équation indicielle à l'infini pour trouver une borne des degrés des solutions polynomiales de $L(y) = \psi$ et trouvent toutes les solutions en utilisant la valeur h ([2], [7], [45], [17] etc). Cependant l'équation indicielle donne plusieurs informations sur l'opérateur L alors que pour les solutions polynomiales donne juste une borne de degré. Le fait que si l'équation $L(y) = 0$ a une solution rationnelle $S(x) = \frac{s_1(x)}{s_2(x)}$, $s_1(x), s_2(x) \in k[x]$, alors l'entier rationnel

$$\mathrm{val}_\infty S(x) = \deg s_1(x) - \deg s_2(x)$$

(la *valuation* de $S(x)$ à l'infini) est la racine de l'équation indicielle. Le cas d'une équation différentielle a été fait dans [19, Lemma 1]. Cependant, malgré notre tentative nous n avons pas trouvé une référence dans le cas d'une équation aux différence, Il est possible qu'une analogie à ce cas soit bien connu. C'est la raison pour laquelle, nous donnons dans la Section VI.8.3 une preuve de cette propriété dans le cas aux différences. Dans le concept de notre investissement il s'agit d'une propriété principale de l'équation indicielle. En effet, si $f(x)$ est une solution polynomiale de l'équation $L(y) = 0$ alors d'après cette propriété dés que $\mathrm{val}_\infty f(x) = \deg f(x)$ on a $\deg f(x)$ est une racine de l'équation indicielle. De plus, cette propriété nous permettra d'améliorer (dans la section VI.10.1) le schéma traditionnel RS donné dans la Section VI.8.1. Dans la Section VI.10.2 on propose quelques changements de ce schéma.

Notons aussi que si on multiplie l'opérateur par un polynôme non nul $u(x)$, ceci augmente l'incrément de cet opérateur par le degré du polynôme $u(x)$. Alors que la hauteur de l'équation reste inchangée.

VI.8.3 Certaines propriétés de l'équation indicielle à l'infini

On suppose que l'opérateur s'écrit sous la forme

$$r_n(x)\Delta^n + \cdots + r_1(x)\Delta + r_0(x), \tag{VI.40}$$

avec $r_1(x), \ldots, r_{n-1}(x) \in k(x), r_0(x), r_n(x) \in k(x) \setminus \{0\}$ et $\Delta(y(x)) = y(x+1) - y(x)$. Si une fraction rationnelle $F(x) \in k(x)$

$$F(x) = c\,\frac{f(x)}{g(x)}, \tag{VI.41}$$

avec $c \in k$ et $f(x), g(x)$ sont des polynômes unitaires, alors on écrit $c = \mathrm{lc}\, F(x)$.

Proposition VI.8.1. *Soit l'opérateur L de la forme (VI.40). Soit le nombre μ et le polynôme $I_L(\lambda)$*

$$\mu = \max_{0 \leqslant j \leqslant n} (\mathrm{val}_\infty r_j - j), \quad I(\lambda) = \sum_{\substack{0 \leqslant j \leqslant n \\ \mathrm{val}_\infty r_j - j = \mu}} \mathrm{lc}(r_j)\lambda^{\underline{j}} \tag{VI.42}$$

($\lambda^{\underline{j}} = \lambda(\lambda-1)\ldots(\lambda-j+1)$), Alors $\mathrm{val}_\infty L(F) \leqslant \mathrm{val}_\infty F(x) + \mu$ pour tout $F(x) \in k(x) \setminus \{0\}$, on a l'inégalité stricte si et seulement si $I(\mathrm{val}_\infty F(x)) = 0$.

Démonstration. Soit la fraction rationnelle $F(x)$ donné par (VI.41) et $\deg f = u$,

$\deg g = v$, $m = u - v$. Par induction sur j on a que

$$\Delta^j(F(x)) = c\,\frac{m^{\underline{j}}\,x^{u+j(v-1)} + \dots}{g(x)g(x+1)\dots g(x+j)} = c\,\frac{m^{\underline{j}}\,x^{u+nv-j} + \dots}{g(x)g(x+1)\dots g(x+n)},$$

pour tout $j = 0, 1, \dots$ (in the numerators hide lower terms). On suppose que tout les $r_j(x)$ sont des polynômes. Pour tout $j = 0, 1, \dots, n$ on a alors :

$$r_j(x)\Delta^j(F(x)) = c\,\frac{\mathrm{lc}(r_j)m^{\underline{j}}\,x^{u+nv+\deg r_j - j} + \dots}{g(x)g(x+1)\dots g(x+n)}.$$

Le numérateur de l'expression correspondante à $L(F(x))$ est : $cI(m)x^{u+nv+\mu} + \dots$.
Ceci prouve le cas des coefficients polynomiaux. Soit $r_j(x) = \frac{\tilde{a}_j(x)}{w(x)}$, où $w(x)$ et tous les $\tilde{a}_j(x)$ sont polynômes, $w(x)$ est un polynôme unitaire, $\tilde{L} = \tilde{a}_n(x)\Delta^n + \dots + \tilde{a}_1(x)\Delta + \tilde{a}_0(x)$ avec $\tilde{\mu}, \tilde{I}(\lambda)$ correspondent à l'opérateur $\tilde{L}$. La propriété est vraie pour $\tilde{L}, \tilde{\mu}, \tilde{I}(\lambda)$. Comme

$$\mathrm{val}_\infty L(F(x)) = \mathrm{val}_\infty \tilde{L}(F(x)) - \deg w(x) \leqslant \mathrm{val}_\infty F(x) + \tilde{\mu} - \deg w(x) = \mathrm{val}_\infty F(x) + \mu$$

et aussi $I_L(\lambda) = \tilde{I}(\lambda)$, reste vraie aussi pour $L, \mu, I_L(\lambda)$. □

Soit la fraction rationnelle $S(x) \in k(x)$. Alors $S(x)$ est non nulle si et seulement si $\mathrm{val}_\infty S(x) \in \mathbb{Z}$ (par convention $\mathrm{val}_\infty 0 = -\infty$). Donc $L(F(x)) = 0$ si et seulement si $\mathrm{val}_\infty L(F(x)) \notin \mathbb{Z}$. Il en résulte de la proposition précedente

Proposition VI.8.2. *Soit l'opérateur L donné par la formule (VI.40), $F(x)$ une fraction rationnelle non nulle à coefficients dans le corps k et $L(F(x)) = 0$. Soit $I_L(\lambda) = 0$ l'équation indicielle à l'infini de l'opérateur L. Alors on a $I(\mathrm{val}_\infty F) = 0$.*

Remarque VI.8.3. *Soit $K = LF$, avec F une fraction rationnelle non nulle et $I_L(\lambda) = 0, I_K(\lambda) = 0$ sont les équations indicielles des deux opérateurs L et K. Alors on peut prouver qu'il existe un coefficient (autre que le coefficient constant) non nul,*

$$I_L(\lambda + \mathrm{val}_\infty F(x)) = I_K(\lambda). \tag{VI.43}$$

La preuve découle de la loi de Leibniz ([38, Ch.1, §6]) et l'égalité $(\lambda + \varkappa)^{\underline{n}} = \sum_{i=0}^{n} \binom{n}{i} \lambda^{\underline{i}}\, \varkappa^{\underline{n-i}}$. Evidemment $L(F) = 0$ si et seulement si $K(1) = 0$. Si $L(F) = 0$ alors l'équation $K(y) = 0$ a une solution polynomiale de degré zéro, donc $I_K(0) = 0$. D'après (VI.43) on a $I_L(\mathrm{val}_\infty F(x)) = 0$. Ceci est une autre preuve de la Proposition VI.8.2.

Exemple VI.8.4. *Soit* $L = (x+2)\phi - x$. *On a* $I_L(\lambda) = \lambda + 2$. *Si* L *a une solution* $y(x)$ *rationnelle non nulle alors* $\mathrm{val}_\infty y(x) = -2$. *Ceci donne que toute fraction rationnelle* $\frac{C}{x(x+1)}$ *(*C *est une constante) est une solution de* L. *Comme* $\operatorname{ord} L = 1$ *cet opérateur n'a pas de solution rationnelle.*

VI.8.4 Comparaison de complexité

On suppose que les solutions polynomiales sont obtenues par un algorithme. En utilisant les algorithmes $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$ qui calculent en premier la hauteur (VI.38), puis calculent les solutions polynomiales (en utilisant la hauteur comme borne supérieur de leurs degré).

Soit l'équation $L(y) = \psi(x)$ écrite sous la forme (VI.3), on fixe

$l = \max\{\deg b_0(x), \deg b_1(x), \ldots, \deg b_n(x)\}$,

$d = \operatorname{dis}(b_n(x-n), b_0(x))$,

$n = \operatorname{ord} L$,

$h =$ la hauteur de l'équation.

Le quadruplet (l, d, n, h) The quadruple (l, d, n, h) est la *taille* (*combined size*) de l'équation $L(y) = \psi(x)$. Notons par $T_{\langle \mathbf{A}'_U \rangle}(l, d, n, h)$, $T_{\langle \mathbf{A}_B \rangle}(l, d, n, h)$ les complexités des algorithmes $\langle \mathbf{A}'_U \rangle$ and $\langle \mathbf{A}_B \rangle$ respectivement.

En utilisant l'algorithme $\mathbf{A}'_U$ (respectivement., $\mathbf{A}_B$), Après avoir fait la substitution et l'élimination des dénominateurs on obtient une équation à coefficients polynomiaux Dans la première étape, l'utilisation de l'algorithme $\mathbf{A}'_U$ (respectivement., $\mathbf{A}_B$) pour l'élimination du dénominateur après substitution correspondante on obtient une équation à coefficients polynomiaux. Cette équation sera appelée U-image (respectivement. B-image) de l'équation d'origine.

Le lemme suivant est une conséquence de la remarque VI.8.3

Lemme VI.8.5. *Soit* $F(x) \in k(x) \setminus \{0\}$. *Soit* $K(z) = \chi(x)$ *est l'équation obtenue la substitution* $y(x) = z(x)F(x)$ *et l'élimination des dénominateurs de l'équation originale* $L(y) = \psi(x)$. *Soit* $I_L(\lambda) = 0$ *et* $I_K(\lambda) = 0$ *est l'équation indicielle de* $L(y) = \psi(x)$ *et respectivement pour* $K(z) = \chi(x)$. *Alors* $I_K(\lambda) = I_L(\lambda + \deg \operatorname{num} F(x) - \deg \operatorname{den} F(x))$.

Soit (l, d, n, h) la taille de l'équation d'origine. On note par (l_U, d_U, n_U, h_U) la taille de l'équation U-image (on n a $n_U = n$). De plus, on note par r_U le degré du polynôme du membre de droite de l'équation U-image.

Lemme VI.8.6. *Soit l'équation $L(y) = \psi(x)$ de taille (l, d, n, h). Alors*

(i) l'ensemble $\mathcal{M}$ de cette équation contient au plus $l(d+1)$ éléments (polynômes irréductibles) et

$$l_U \leqslant l(n-1), \quad h_U \leqslant h + l(d+1), \quad r_U \leqslant h + l(d+n);$$

(ii) la hauteur de l'équation

$$\begin{aligned} &f(x+n+d)y(x+n) + (x+1)^l y(x+n-1) + \dots \\ &\quad \cdots + (x+1)^l y(x+1) + f(x)y(x) = (x+1)^{h+l}, \end{aligned} \tag{VI.44}$$

où

$$f(x) = \prod_{t=1}^{l} \left(x + \frac{1}{t+1} \right),$$

est égal à h (donc la taille de cette équation est (l, d, n, h)), et l'ensemble $\mathcal{M}$ a $l(d+1)$ éléments, l'algorithme $\mathbf{A}'_U$ donne le dénominateur universel de cette équation de degré $l(d+1)$, et

$$h_U = h + l(d+1), \quad r_U = h + l(d+n)$$

le degré de chaque polynôme du membre de droite de l'équation U-image de $L(y) = \psi$ est égal à $l(n-1)$ (d'après (i) pour les équations de taille (l, d, n, h) ces valeurs sont les plus grandes possible).

Démonstration. (i) D'après la structure (VI.13) l'ensemble $\mathcal{M}$ a au plus $l(d+1)$ éléments. Soit le polynôme $G(x)$ le plus petit commun multiple des coefficients de l'opérateur L tel que L est sous la forme (VI.3). Soit

$$s = \min\{\deg \operatorname{pgcd}(U(x), b_0(x)), \ \deg \operatorname{pgcd}(U(x), b_n(x-n))\}.$$

Alors,

$$\deg \operatorname{den} \frac{b_0(x)}{U(x)} \leqslant \deg U(x) - s, \quad \deg \operatorname{den} \frac{b_n(x)}{U(x+n)} \leqslant \deg U(x) - s$$

et $\deg U(x) \leqslant s(d+1)$. Donc, $\deg G(x) \leqslant \deg U(x) + ns - 2s \leqslant s(d+n-1) \leqslant l(d+n-1)$, et on obtient $l_U \leqslant l + \deg G(x) - \deg U(x) \leqslant l(n-1)$.

Ceci peut se déduire de la définition de la hauteur de l'équation $L(y) = \psi(x)$ que

$$\deg \psi(x) \leqslant h + \mu \leqslant h + l. \tag{VI.45}$$

De cette inégalité et $\deg G(x) \leqslant l(d+n-1)$, ceci implique que $r_U \leqslant h + l(d+n)$.

Après élimination du dénominateur dans l'équation $\left(L_{\frac{1}{U(x)}}\right)(y) = \psi(x)$, on peut commencer par multiplier les deux types de cette équation par $G(x)$. Ceci donne l'équation $L'(y) = \psi'(x)$, $\deg \psi'(x) = \deg \psi(x) + \deg G(x)$. L'incrément μ' de l'opérateur L' est égal à $\mu + \deg G(x) - \deg U(x)$. D'après le lemme VI.8.5 le polynôme $I'(\lambda)$ construit par l'opérateur L' coïncide à un facteur (scalaire) non nul avec $I(\lambda + \mathrm{val}_\infty \frac{1}{U(x)})$, i.e., avec $I(\lambda - \deg U(x))$. Donc,

$$\mu' = \mu + \deg G(x) - \deg U(x), \quad \deg \psi'(x) = \deg \psi(x) + \deg G(x),$$

$$\tilde{\lambda}' = \tilde{\lambda} + \deg U(x),$$

avec $\tilde{\lambda}' = \max(\{d \in \mathbb{N} \,:\, I'(d) = 0\} \cup \{-\infty\})$. La hauteur de l'équation $L'(y) = \psi'(x)$ est égale à

$$\max\{\deg \psi'(x) - \mu', \;\; \tilde{\lambda}'\} = h + \deg U(x)$$

et, donc ne peut pas dépasser la valeur $h + l(d+1)$. Notons que l'équation $L'(y) = \psi'(x)$ peut différer de l'équation U-image de $L(y) = \psi(x)$ par des facteurs polynomiaux non nul. Comme on l'a déjà évoqué, à la fin de la Section **??**, la multiplication par un tel facteur ne change pas valeur de la hauteur de l'équation. Donc, $d_U \leqslant h + l(d+1)$.

(ii) Il est évident de voir, que pour l'équation (VI.44), l'ensemble $\mathcal{M}$ a $l(d+1)$ éléments, et le degré du dénominateur universel $U(x)$ obtenu par l'algorithme $\mathbf{A}'_U$ est égal à $l(d+1)$. On peut vérifier directement les assertions de la partie qui reste. □

Dans la suite, on considère la complexité des algorithmes $\langle \mathbf{A}_B \rangle$, $\langle \mathbf{A}'_U \rangle$ comme le nombre des opérations dans le corps k effectué au pire cas. Il est facile de voir que si on supprime h des composantes de la taille (combined size) (en gardant que l, d et n), alors la complexité de chaque algorithme serait égale à l'infini, dés qu'on donne les valeurs l, d et n, l'équation peut avoir une hauteur arbitraire, donc aboutisse à des grosses dépenses arbitraires par l'étape RS3. La présence de la composante h exclue cette possibilité. Nous remarquons aussi que le membre de droite $\psi(x)$ satisfait (VI.45). Donc si la taille de l'équation d'origine est fixée, les dépenses nécessaires pour la construction de chaque équation de la forme (VI.26) ainsi que (VI.29) sont délimitées (bornées).

Notons par $\mathcal{T}_{l,d,n,h}$ l'ensemble des équations de taille (size) (l,d,n,h) et par $\mathcal{U}_{l,d,n,h}$ le sous-ensemble de $\mathcal{T}_{l,d,n,h}$ constitué des équations de sorte que le coût de trouver des solutions polynomiales de toutes les équations de U-image est maximal parmi toutes les équations de $\mathcal{T}_{l,d,n,h}$. L'ensemble $\mathcal{U}_{l,d,n,h}$ peut contenir plus d'une équation.

Théorème VI.8.7. *Soit une équation de la forme (VI.44) appartenant à l'ensemble $\mathcal{U}_{l,d,n,h}$ pour tout l,d,n,h. Soit l'algorithme utilisé pour trouver les solutions polynomiales de telles équations. Alors on a $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) > T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h)$, et $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) - T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h) = \Omega(dln)$.*

Avant de prouver le théorème, on rappelle que l'hypothèse sur l'équation est tout à fait naturel. Cette hypothèse, veut dire aussi, que l'exécution de l'étape RS3 de l'algorithme $\langle \mathbf{A}'_U \rangle$ appliqué à cette équation nécessite des dépenses maximales. On n'utilise pas (on ne le fait pas) pour l'algorithme spécifique qui trouve les solutions polynomiales, mais on suppose que l'algorithme utilise la taille de l'équation afin de borner les degrés des solutions polynomiales. Par le lemme VI.8.6 la taille de U-image de l'équation (VI.44) est maximale, et l'équation U-image (elle même) est un maximum (combersome) parme toutes les U-images des équations de l'ensemble $\mathcal{T}_{l,d,n,h}$.

Démonstration. L'ensemble $\mathcal{M}$ de l'équation de la forme (VI.44) a le plus grand nombre possible d'éléments. Le cardinal de l'ensemble $\mathcal{M}$ est un diviseur de $V(x)$ et $W(x)$, il est égal à $2l$; autrement dit, il atteint également la plus grande valeur possible. Par conséquent, les dépenses (expenditures) de l'algorithme à l'étape RS1 appliqué sur l'équation (VI.44), atteint aussi la plus grande valeur possible. On déduit, de cette propriété de l'ensemble $\mathcal{M}$ et de l'hypothèse sur l'équation (VI.44) considérée(c'est à dire elle appartient à l'ensemble $\mathcal{U}_{l,d,n,h}$) que l'entrée de l'algorithme correspond au pire des cas.

La différence $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) - T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h)$ n'est pas inférieure à la différence des dépenses (expenditures) nécessaires pour la construction de toutes les solutions rationnelles de l'équation (VI.44) par les algorithmes $\langle \mathbf{A}_B \rangle$ et $\langle \mathbf{A}'_U \rangle$. L'application de $\mathbf{A}_B$ sur l'équation (VI.44) donne $R(x) = \frac{1}{U}$, où $U(x)$ est le dénominateur universel obtenu par l'algorithme $\mathbf{A}'_U$. Ceci, en effet du fait que

$$v_{N,-1}(x) = \frac{(x-n-N+2)^{h+2}}{f(x+d-N+1)}$$

dans (VI.26) et aussi de la relation pour tout $p(x) \in \mathcal{M}$

$$\mathrm{val}_{p(x+d-N+1)} v_{N,-1}(x) = -1.$$

Par conséquent, les dépenses des deux algorithme à l'étape RS3 appliqués à l'équation (VI.44) sont les mêmes. On considère que la construction du polynôme $U(x)$ par le moyen $\langle \mathbf{A}'_U \rangle$ et la fraction rationnelle $\frac{1}{U(x)}$ via $\langle \mathbf{A}_B \rangle$. Dans le but de simplifier, on suppose que les dépenses requis pour le calcul des $\gamma_{j,t}$ dans (VI.33) coïncident avec les dépenses requis pour le calcul des $\beta_{j,t}$ dans (VI.30), aussi (VI.26), (VI.29) requis pour l'algorithme $\langle \mathbf{A}_B \rangle$ ont déjà été construites (pour la démonstration [8], les dépenses de l'algorithme pour le calcul des exposants sont très petites). En écrivant l'équation (VI.44) sous la forme de (VI.2) tous les $r_i(x)$ et $\varphi(x)$ ont des numérateurs et les dénominateurs de degré l. Pour tout $1 \leqslant N \leqslant d+1$, on trouve que si par exemple (VI.26). En construisant une équation semblable (similaire) pour tout $1 \leqslant N \leqslant d+1$.

Seulement, le changement actuel de (VI.2) exigera $\Omega(nl)$ des opérations sur le corps k. Pour $N = 1, 2, \ldots, d+1$, l'algorithme $\mathbf{A}_B$ construit de telles équations, qui prouve le théorème. □

Remarque VI.8.8. *La démonstration du théorème ci-dessus sur la différence $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) - T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h)$, peut probablement être considérablement renforcée. Lors de l'estimation de $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h)$, nous n'avons pas pris en compte des coefficients "Welling" d'équations (VI.26), (VI.29) lorsque N croît. En effet, pour un entier fixé n et l avec l'entier d qui augmente. La différence $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) - T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h)$ augmente plus rapidement que d. Notre but était seulement de montrer que la différence $T_{\langle \mathbf{A}_B \rangle}(l,d,n,h) - T_{\langle \mathbf{A}'_U \rangle}(l,d,n,h)$ est positive et qu'elle croît en fonction de la croissance des composantes n, l et d la taille de l'échantillon.*

Dans le cas d'un système, l'algorithme $\langle \mathbf{A}_B \rangle$ nécessite la construction de la matrice A_N, ce qui est encore plus coûteux que de construire l'équation (VI.26).

VI.9 Expérimentations

L'algorithme $\mathbf{A}_D$ a été implémenté et est disponible sur Maple, sous forme de procédure interne du package LREtools. L'algorithme $\mathbf{A}'_U$ est implémenté pour réaliser l'expérimentation de comparaison. [1] On rappelle que $\mathbf{A}'_U$ est basé sur la factorisation complète (décomposition en produit de polynômes irréductibles) des polynômes donnés

1. L'algorithme a été implémenté par D.Khmelnov.

$V(x)$ et $W(x)$. L'implémentation utilise le résultat de la factorisation polynomiale (décomposition en produit d'irréductibles)non seulement pour construire l'ensemble des polynômes irréductibles $\mathcal{M}$, mais l'utilise aussi pour calculer la valeur (VI.32). Ce n'est pas le cas pour l'implémentation de $\mathbf{A}_D$ sur Maple. En effet, elle utilise la procédure LREtools[dispersion] pour calculer la dispersion de polynômes qui l'implémentent [40], c'est-à-dire elle utilise la décomposition en produit d'irréductibles. Mais, les étapes suivantes sont implémentées comme dans la section VI.4.1 sans exploiter le résultat de la décomposition en produit d'irréductibles de l'étape précédente.

Nous avons aussi réalisé des expériences de comparaison pour $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$. L'algorithme $\langle \mathbf{A}'_U \rangle$ est implémenté en combinant l'implémentation de $\mathbf{A}'_U$ et LREtools[polysols] de Maple (cas scalaire) et LinearFunctionalSystems[PolynomialSolution] (cas système) pour la recherche de toutes les solutions polynomiales.

Nous avons aussi implémenté $\mathbf{A}_B$ (dans les deux cas scalaire et système) ; $\langle \mathbf{A}_B \rangle$ a été implémenté en combinant l'implémentation de $\mathbf{A}_B$ et LREtools[polysols] de Maple (dans le cas scalaire) et LinearFunctionalSystems[PolynomialSolution] (cas système) pour la recherche de toutes les solutions polynomiales.

VI.9.1 Comparaison de $\mathbf{A}'_U$ avec $\mathbf{A}_D$

Nous avons réalisé plusieurs expérimentation pour comparer entre $\mathbf{A}'_U$ et $\mathbf{A}_D$. Le résultat de l'expérimentation est présenté ci-dessous.

Les deux algorithmes ont été appliqués à l'ensemble des données suivantes (et entrées)

$$V(x) = W(x) = \prod_{i=1}^{l} (x + m + i + 1/i)(x - m - i + 1/i)$$

pour $m = 20, 100, 500, 2500$, $l = 1, 15, 30, 45, 60$. Les dénominateurs universels correspondants trouvés sont : $\prod_{i=1}^{l} \prod_{j=-m-i}^{m+i} (x - j + 1/i)$. Les résultats pour l'ensemble d'entrées est donné en secondes :

L'ensemble des données est proche au pire des cas pour les deux algorithmes $\mathbf{A}'_U$ et $\mathbf{A}_D$, et à l'avantage de $\mathbf{A}'_U$ est évident.

Les résultats d'autres expérimentations pour comparer $\mathbf{A}'_U$ et $\mathbf{A}_D$ sont présentés dans [8]. Toutes les expérimentations ont été à l'avantage d'appliquer l'algorithme $\mathbf{A}'_U$.

	m=20		m=100		m=500		m=2500	
	$\mathbf{A}'_U$	$\mathbf{A}_D$	$\mathbf{A}'_U$	$\mathbf{A}_D$	$\mathbf{A}'_U$	$\mathbf{A}_D$	$\mathbf{A}'_U$	$\mathbf{A}_D$
l=1	0.016	0.015	0.000	0.000	0.000	0.016	0.031	0.031
l=15	0.078	0.375	0.109	0.422	0.172	0.531	0.578	1.032
l=30	0.359	2.890	0.407	3.063	0.531	3.484	1.266	5.344
l=45	0.860	10.641	0.796	11.547	1.516	13.234	3.078	17.656
l=60	2.406	31.187	2.719	33.484	2.657	37.125	4.766	44.797

VI.9.2 Comparaison de $\langle \mathbf{A}'_U \rangle$ avec $\langle \mathbf{A}_B \rangle$ (cas scalaire)

Nous avons réalisé plusieurs expérimentations pour comparer entre $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$. Le résultat d'une expérimentations est présenté ci-dessous.

Les deux algorithmes $\langle \mathbf{A}'_U \rangle$ and $\langle \mathbf{A}_B \rangle$ ont été appliqués sur 27 équations (VI.44) du lemme VI.8.6 : $h = 6$ pour chacun d'entre eux, $n = 3, 6, 9$, $l = 2, 4, 6$, $d = 5, 10, 15$. La différence du temps qui en résulte pour $\langle \mathbf{A}_B \rangle$ et $\langle \mathbf{A}'_U \rangle$ en secondes :

n	l	d=5	d=10	d=15
3	2	0.546 - 0.141 = 0.405	1.438 - 0.125 = 1.313	2.796 - 0.203 = 2.593
3	4	1.359 - 0.235 = 1.124	4.188 - 0.375 = 3.813	9.594 - 0.812 = 8.782
3	6	2.703 - 0.375 = 2.328	10.172 - 0.969 = 9.203	24.937 - 1.734 = 23.203
6	2	0.813 - 0.234 = 0.579	2.015 - 0.328 = 1.687	4.625 - 0.453 = 4.172
6	4	2.313 - 0.672 = 1.641	7.515 - 1.063 = 6.452	17.235 - 2.140 = 15.095
6	6	5.094 - 1.547 = 3.547	18.484 - 3.156 = 15.328	45.656 - 6.094 = 39.562
9	2	1.047 - 0.563 = 0.484	3.062 - 0.671 = 2.391	6.610 - 1.063 = 5.547
9	4	3.687 - 1.328 = 2.359	11.063 - 2.516 = 8.547	25.484 - 4.265 = 21.219
9	6	8.281 - 3.172 = 5.109	28.453 - 6.875 = 21.578	69.672 - 13.328 = 56.344

Les résultats correspondent à la proposition VI.8.7, en outre, pour n, l fixé, la différence croît plus vite que d.

Rappelons, que si h ne figure pas dans le tableau : $h = 6$ pour toutes les équations. Des expérimentations supplémentaires pour $h = 2, 4$, montrent que les résultats sont quasiment indépendants de la valeur de h. La croissance de h en 3 fois de 2 à 6 provoque le changement de la différence de temps plus petit à 3% pour l, d et n fixés.

Les résultats d'autres expérimentations de comparaison entre $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$ sont présentés dans [10]. tous les résultats des expériences correspondent à la proposition VI.8.7.

VI.9.3 Comparaison de $\langle \mathbf{A}'_U \rangle$ avec $\langle \mathbf{A}_B \rangle$ (cas d'un système)

Dans l'expérimentation de comparaison entre $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$ ont été appliqués sur 3 ensembles d'entrées. Chaque ensemble contient 20 équations d'ordre $n = 2, 3, 4$. Chaque système possède un système fondamental de solutions formé des fonctions rationnelles qui l'engendrent de façon aléatoire. Notons que, ces données en entrées ont été plus commode pour $\langle \mathbf{A}_B \rangle$. Puisque$\mathbf{A}_B$ construit des bornes exactes (sans la possibilité de réduction)de ces données en conformité avec [52, Theorem 1].

Résultats de l'expérimentions :

n	deg $U(x)$ $\mathbf{A}'_U$	deg den $R_i(x)$ $\mathbf{A}_B$	Time $\langle \mathbf{A}'_U \rangle$	Time $\langle \mathbf{A}_B \rangle$
2	7-39	2-8	7.216	22.922
3	18-49	3-21	38.859	169.906
4	36-74	5-28	176.829	836.172

Chaque ligne du tableau correspond à l'ensemble d'entrées de paramètre n. Les autres colonnes présentent une gamme de degrés des dénominateurs trouvés par $\mathbf{A}'_U$ et $\mathbf{A}_B$ pour les systèmes de l'ensemble de données correspondant, ainsi que le temps total pour la recherche des solutions rationnelles de les systèmes sur l'ensemble de données correspondant pris par $\langle \mathbf{A}'_U \rangle$ et $\langle \mathbf{A}_B \rangle$.

Le temps de $\langle \mathbf{A}_B \rangle$ était supérieur à celui de $\langle \mathbf{A}'_U \rangle$ pour tout les données en entrée, malgré les bornes exactes trouvées par $\mathbf{A}_B$ (on note que $\mathbf{A}'_U$ a trouvé moins de bornes exactes comme on le voit dans la gamme de degrés des dominateurs sur le tableau).

VI.10 Équations scalaires homogènes

De nombreuses équations n'ont pas de solutions rationnelles (non nulles). Cependant, si l'ont utilise des algorithmes tel que l'algorithme $\langle \mathbf{A}'_U \rangle$ ou bien $\langle \mathbf{A}_B \rangle$, l'absence de telles solutions ne sera reconnu que dans la dernière étape du calcul, lorsque U-image, respectivement. B-image de l'équation d'origine est construite. Dans le cas d'une équation scalaire homogène $L(y) = 0$, nous supposons quelques changements dans les schémas RS (voir section VI.8.1). Ces changements n'augmentent pas le coût de calcul, mais permettent assez souvent de prévoir, par exemple, l'absence d'une solution rationnelle non nulle dans une première étape de calcul.

VI.10.1 Un nouveau Schéma

L'étape RS2 résulte dans l'équation avec l'opérateur $M = LR$ (le produit de L et de l'opérateur d'ordre zéro R). À l'étape RS3, les solutions polynomiales de M devraient être trouvées. Comme déjà mentionné, cette recherche est donnée dans comme suit. D'abord, en premier lieu, un majorant $d \geqslant 0$ des degrés de toutes les solutions polynomiales, doit être trouvés en utilisant l'équation indicielle de M. En second lieu, on trouve toutes les solutions polynomiales à l'aide de cette borne.

Dans la suite, nous noterons les équations indicielles à l'infinides opérateurs L et $M = LR$ par $I_L(\lambda) = 0$ et $I_M(\lambda) = 0$, respectivement.

Proposition VI.10.1. *Si l'équation $I_L(\lambda) = 0$ n'a pas de solutions entières, alors M n'a pas de solutions polynomiales, L n'a pas de solutions rationnelles. Si cette équation indicielle a des racines entières et λ_0 est supposé le maximum de ses racines entières, alors l'inégalité $\deg f(x) \leqslant \lambda_0 - \mathrm{val}_\infty R(x)$ est vérifiée pour toute solution polynomiale $f(x)$ de M (si $\lambda_0 - \mathrm{val}_\infty R(x) < 0$, alors il n y pas de solutions polynomiales).*

Démonstration. Si $I_L(\lambda) = 0$ n'a pas de solutions entières, alors d'après la propriété de l'équation indicielle, M n'a pas de solutions rationnelles et par suite pas de solutions polynomiales. On suppose que $y(x)$ est une solution rationnelle de L. Alors, il résulte de RS1 et de RS2 que $y(x) = R(x)f(x)$ pour certains polynômes $f(x)$, et aussi

$$M(f(x)) = (LR)(f(x)) = L(R(x)f(x)) = L(y(x)) = 0.$$

Mais M n' a pas de solutions polynomiales, une contradiction. On déduit que L n a pas de solutions rationnelles.

Montrons à présent la seconde partie. Si $f(x)$ n'est pas une solution polynomiale de M, alors $R(x)f(x)$ est une solution de L. Donc

$$\deg f(x) + \mathrm{val}_\infty R(x) = \mathrm{val}_\infty f(x) + \mathrm{val}_\infty R(x) = \mathrm{val}_\infty(R(x)f(x)) \leqslant \lambda_0.$$

D'où l'énégalité $\deg f(x) \leqslant \lambda_0 - \mathrm{val}_\infty R(x)$. □

Cette proposition rend possible une amélioration du schéma RS donné dans la section VI.8.1. on peut commencé par la construire l'équation indicielle $I_L(\lambda) = 0$ de l'opérateur d'origine L. On obtient le schéma RS′ :

RS′0 : Construire l'équation $I_L(\lambda) = 0$; si elle n a pas de racine entière, alors STOP , sinon, posons λ_0 sa plus grande racine entière.

RS′1 : Construire une fraction rationnelle $R(x)$ de telle sorte que toute solution rationnelle de L peut être représentée sous la forme $f(x)R(x)$ avec $f(x)$ un polynôme ; posons $\delta = \lambda_0 - \mathrm{val}_\infty R(x)$; si $\delta < 0$, alors STOP.

RS′2 : Construire $M = LR$.

RS′3 : Construire toutes les solutions polynomiales de M en prenant en considération que le degré de chacun d'entre eux est inférieur ou égal à δ.

On note qu'à l'étape RS1 du schéma RS, certains algorithmes liés au cas d'une équation différentielle à coefficients polynomiaux $L = a_n(x)\frac{d^n}{dx^n} + \cdots + a_1(x)\frac{d}{dx} + a_0(x)$ permettent de savoir que l'équation n'a pas de solutions rationnelles, en raison des racines entières de l'équation indicielle de L, c'est-à-dire, l'équation indicielle en un facteur irréductible du coefficient $a_n(x)$ ([19]). Ceci peut être combiné avec l'étape RS′1(par exemple les équations indicielles en ces facteurs irréductibles peuvent être examinées dans un ordre aléatoire).

Cependant à l'étape RS1, les algorithmes connus dans le cas des équations aux différences donnent toujours une fraction rationnelle.

Dans la section suivante, nous vous proposons une astuce supplémentaire pour les équations différentielles.

VI.10.2 Critère d'arrêt supplémentaire

Maintenant, on revient à l'étape RS′1. Dans le cas aux différences, la conclusion que l'opérateur L n'admet pas de solution rationnelle peut se faire au début de la construction d'une solution rationnelle $R(x)$. Soit l'opérateur L de la forme (VI.40), soit l'opérateur $\Delta = \phi - 1$. L'opérateur L peut être transformé sous la forme

$a'_n(x)\phi^n + \cdots + a'_1(x)\phi + a'_0(x), a'_1(x), \ldots, a'_{n-1}(x) \in k(x), a'_0(x), a'_n(x) \in k(x) \setminus \{0\}$.

En multipliant à gauche par un polynôme convenable l'opérateur L, on obtient un opérateur à coefficients polynomiaux

$$b_n(x)\phi^n + \cdots + b_1(x)\phi + b_0(x), \quad \phi(y(x)) = y(x+1).$$

De nombreux algorithmes ([3], [4], [17] etc) à l'étape préliminaire de la construction de $R(x)$ calculent la dispersion $\mathrm{dis}(b_n(x-n), b_0(x))$ des polynômes $b_n(x-n)$ et $b_0(x)$, c'est-à-dire, le plus grand entier non-négatif d de sorte que $b_n(x-n)$ et $b_0(x+d)$ ne soient pas étrangers. Si de tels entiers non-négatifs n'existent pas, alors posons $d = -\infty$. Si $d = -\infty$, alors l'opérateur L n'a pas de solution dans $k(x) \setminus k[x]$ (on peut remplacé

$R(x)$ par 1 dans RS′3). Autrement dit, il est possible de construire $R(x)$ sous la forme $\frac{1}{U(x)}$ avec $U(x)$ le dénominateur universel (mais dans certains cas, on peut considérer un autre type de fonction).

Théorème VI.10.2. *Soit $d = \operatorname{dis}(b_n(x-n), b_0(x)) \geqslant 0$, et soit λ_0 l'entier donné dans la proposition VI.10.1. Dans ce cas, si on a l'inégalité*

$$\lambda_0 + (d+1)\min\{\deg b_0(x), \deg b_n(x)\} < 0, \tag{VI.46}$$

alors L n'a pas de solutions rationnelles.

Démonstration. En considérant, par exemple, l'algorithme $\mathbf{A}_D$ (section VI.4.1) il est facile de voir que cet algorithme conduit au dénominateur universel $U(x)$ de sorte que $\deg U(x) \leqslant (d+1)\min\{\deg b_0(x), \deg b_n(x)\}$. On suppose que l'algorithme [4] a calculé $R(x)$. Mais, néanmoins la fraction rationnelle $R(x) = \frac{1}{U(x)}$ peut être utilisée à l'étape RS′2. Par la proposition VI.10.1 l'inégalité (VI.46) est vraie, si L a une solution rationnelle. □

Par conséquent, dans le cas aux différences l'étape
RS′1 peut être utilisée comme ci-dessous :

RS′1 : Exécuter l'étape préliminaire de construction de $R(x)$ qui consiste par le calcul de la dispersion $d = \operatorname{dis}(b_n(x-n), b_0(x))$; si $d = -\infty$ et $\lambda_0 \geqslant 0$ alors posons $M = L$, $d = \lambda_0$ et on va directement à l'étape RS′3 ; si $d = -\infty$ et $\lambda_0 < 0$ alors STOP ; si (VI.46) n'est pas vraie, alors STOP ; terminer la construction de $R(x)$; on pose $\delta = \lambda_0 - \operatorname{val}_\infty R(x)$; si $\delta < 0$ alors STOP.

Exemple VI.10.3. *Pour $L = 2(x+2)\phi + (2x+3)$, l'équation indicielle $2\lambda + 1 = 0$ n a pas de racine entière. Alors L n'a pas de solution rationnelle.*

Pour $L = (x+1)(x^2+1)\phi - x(x^2-4x+1)$, l'équation indicielle est $\lambda + 5 = 0$. On a $\lambda_0 = -5$, $d = 0$. L'inégalité (VI.46) n'est pas vraie. Donc L n'a pas de solution rationnelle.

Pour $L = (x+2)\phi - x$ (le même opérateur que dans l'exemple VI.8.4), on a $\lambda + 2 = 0$, $\lambda_0 = -2$, $d = 1$. L'inégalité (VI.46) est vraie. Si l'algorithme de [4] est utilisé, on obtient $R(x) = \frac{1}{x(x+1)}$. On a $-2 - \operatorname{val}_\infty R(x) = 0$. Donc 0 est une borne supérieure du degré du polynôme solution de $LR = \frac{1}{x+1}\phi - \frac{1}{x+1}$. Toutes les constantes sont solutions polynomiales de cet opérateur.

Bibliographie

[1] S. A. Joni and G. C. Rota. Coalgebras and bialgebras in combinatorics. *Studies in Applied Math*, 61 :93–139, 1979.

[2] S. Abramov. Problems in computer algebra that are connected with a search for polynomial solutions of linear differential and difference equations. *Vestnik Moskov. Univ. Ser. XV Vychisl. Mat. Kibernet.*, 3 :56–60, 1989.

[3] S. Abramov. Rational solutions of linear differential and difference equations with polynomial coefficients. *Zh. Vychisl. Mat. i Mat. Fiz.*, 29(11) :1611–1620, 1757, 1989.

[4] S. Abramov. Rational solutions of linear difference and q-difference equations with polynomial coefficients. *Programmirovanie*, 6 :3–11, 1995.

[5] S. Abramov. Rational solutions of linear difference and q-difference equations with polynomial coefficients. In *ISSAC'98 Proceedings*, pages 303–308. ACM Press, 1995.

[6] S. Abramov and M. Barkatou. Rational solutions of first order linear difference systems. In *ISSAC'98 Proceedings*, pages 124–131. ACM Press, 1998.

[7] S. Abramov, M. Bronstein, and M. Petkovšek. On polynomial solutions of linear operator equations. In *ISSAC'95 Proceedings*, pages 290–295. ACM Press, 1995.

[8] S. Abramov, A. Gheffar, and D. E. Khmelnov. Factorization of polynomials and gcd computations for finding universal denominators. In *Programming and Computer Software*, pages 4–18, 2010.

[9] S. Abramov, A. Gheffar, and D. E. Khmelnov. Rational solutions of linear difference equations revisited. In *Computer Algebra Systems in Teaching and Research, CASTR*, pages 5–19, 2011.

[10] S. Abramov, A. Gheffar, and D. E. Khmelnov. Rational solutions of linear difference equations : universal denominators and denominator bounds. In *CASC'2010 Proceedings*, pages 78–86, 2011.

[11] S. Abramov and M. van Hoeij. A method for the integration of solutions of ore equations. In *ISSAC'97 Proceedings*, pages 172–175. ACM Press, 1997.

[12] S. Abramov and M. van Hoeij. Integration of solutions of linear functional equations. *Integral Transform. Spec. Funct.*, 8(1-2) :3–12, 1999.

[13] S. Albeverio and V. Polischook. Prüfer's ideal numbers as gelfand's maximal ideals. *p-Adic Numbers, Ultrametric Analysis, and Applications*, 2 :35–45, Feb 2010.

[14] Y. Amice. *Les nombres p-adiques*. Presses Universitaires de France, Paris, 1975. Préface de Ch. Pisot, Collection SUP : Le Mathématicien, No. 14.

[15] F. Arnault. *Sur quelques tests probabilistes de primalité*. PhD thesis, Université de Poitiers, 1993.

[16] M. Artin, A. Grothendieck, and J. L, Verdier. *Théorie des topos et cohomologie étale des schémas, Tome 3*, volume 305 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4). Avec la collaboration de P. Deligne et B. Saint-Donat.

[17] M. Barkatou. On rational solutions of systems of linear difference equations. *J. Symbolic Comput.*, 28 :547–567, 1999.

[18] M. Barkatou. Rational solutions of matrix difference equations : problem of equivalence and factorization. In *ISSAC'99 Proceedings*, pages 277–282. ACM Press, 1999.

[19] M. Barkatou. A fast algorithm to compute the rational solutions of systems of linear differential equations. In *The title of the book*. IMAG-LCM, 3 19997. RR 973.

[20] P. Berthelot and A. Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J., 1978.

[21] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean Analysis*. Springer, 1984.

[22] N. Bourbaki. *Algèbre Commutative,chapitre 3,4*. Hermann, 1967.

[23] N. Bourbaki. *Topologie Générale, chapitres I-IV*. Hermann, 1967.

[24] H. Cartan. Puissances divisées. *Séminaire H. Cartan,E.N.S, Numdam*, pages 1–11, Janv 1955.

[25] W. Y. C. Chen, P. Paule, and H. L. Saad. Converging to Gosper's algorithm. *Adv. in Appl. Math.*, 41(3) :351–364, 2008.

[26] S. De Smedt. The van der Put base for C^n-functions. *Bull. Belg. Math. Soc. Simon Stevin*, 1(1) :85–98, 1994.

[27] B. Diarra. *Analyse p-adique*. Mali, 2000. Cours de DEA-Algèbre Commutative.

[28] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. GTM. Springer, 1995.

[29] J. Von Zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2 edition, 2003.

[30] A. Gheffar. Linear differential, difference and q-difference homogeneous equations having no rational solutions. *ACM Commun. Comput. Algebra*, 44(3-4) :78–83, 2010.

[31] A. Gheffar and S. Abramov. Valuations of rational solutions of linear difference equations at irreducible polynomials. *Adv. in Appl. Math.*, 47(2) :352–364, 2011.

[32] H. Herrlich and G. E. Strecker. *Category Theory*, volume 1 of *Sigma series in pure mathematics*. Heldermann-Verlag, Berlin, 1979. second edition.

[33] E. Hewitt and K. A. Ross. *Abstract Harmonic Analysis : Volume 1*. Springer, 1994.

[34] J. L. Kelley. *General Topology*. Springer, 1975.

[35] D. E. Khmelnov. Search for polynomial solutions of linear functional systems by means of induced recurrences. *Programming and Computer Software*, 30(2) :61–67, 2004.

[36] D. E. Knuth. Big omicron and big omega and big theta. *SIGACT News*, 8(2) :18–24, 1976.

[37] H. W. Lenstra. Profinite Fibonacci numbers. *Nieuw Arch. Wiskd. (5)*, 6(4) :297–300, 2005.

[38] H. Levy and F. Lessman. *Finite difference equations*. Dover Publications Inc., New York, 1992. Reprint of the 1961 edition.

[39] S. Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[40] Y. K. Man and F. J. Wright. Fast polynomial dispersion computation and its application to indefinite summation. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, pages 175–180, New York, NY, USA, 1994. ACM.

[41] A. Necer. *Suites récurrentes linéaires et séries formelles en plusieurs variables*. PhD thesis, Université de Limoges, 1998.

[42] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[43] E. V. Novoselov. *Vvedenie v poliadicheskii analiz [Introduction to polyadic analysis]*. Petrozavodsk. Gos. Univ., Petrozavodsk, 1982. [Russian].

[44] Maple online help. http://maplesoft.com/support/help/.

[45] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symbolic Comput.*, 14(2-3) :243–264, 1992.

[46] H. Prüfer. Neue Begründung der algebraischen Zahlentheorie. *Math. Ann.*, 94(1) :198–243, 1925.

[47] M. Renault. The fibonacci sequence under various moduli. Master's thesis, Wake Forest University, May 1996.

[48] L. Ribes and P. Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.

[49] Alain.M Robert. *A Course in p-adic Analysis*. GTM. Springer, 2000.

[50] L. Schwartz. *Topologie Générale et Analyse Fonctionnelle*. Hermann, 1970.

[51] D. M. van Dantzig. Nombres universels v!-adiques avec une introduction sur l'algèbre topologique. *Annales scientifiques de l'École normale supérieure*, 53 :275–307, 1936.

[52] M. van Hoeij. Rational solutions of linear difference equations. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*, pages 120–123 (electronic), New York, 1998. ACM.

[53] M. van Hoeij and G. Levy. Liouvillian solutions of irreducible second order linear difference equations. In Wolfram Koepf, editor, *ISSAC*, pages 297–301. ACM, 2010.

[54] J. von Neumann. Zur proüferschen theorie der idealen zahlen. *Acta Litterarum ac Scientiarum Szeged*, 2 :193–227, 1926.

[55] D. D. Wall. Fibonacci series modulo m. *Amer. Math. Monthly*, 67 :525–532, 1960.