Académie Universitaire Wallonie-Europe

Université de Liège

Faculté des Sciences

Département de Mathématiques

Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini

Laurent Waxweiler

Dissertation originale
présentée en vue de l'obtention
du grade académique de
Docteur en sciences

Décembre 2009

Qu'il me soit permis de témoigner de ma reconnaissance à Monsieur le Professeur Michel Rigo *pour m'avoir guidé tout au long de ma thèse de doctorat et pour m'avoir été d'une aide précieuse à plusieurs reprises.*

Qu'il me soit également permis de remercier tous mes collègues, non seulement pour les conversations mathématiques intéressantes que nous avons eues, mais également pour l'ambiance amicale qui règne entre nous. Je remercie particulièrement Rémi Lambert *pour sa disponibilité et ses conseils avisés concernant le langage* LaTeX*, Jacqueline* Crasborn *pour m'avoir gentiment proposé de reprendre des centaines d'interrogations à corriger à un moment crucial, et Bruno* Teheux *pour les longs débats que nous avons eus sur les mathématiques et la logique.*

Qu'il me soit finalement permis de remercier tout particulièrement ma compagne, Irina Mahmudova*, pour son soutien et ses encouragements tout au long de ces dix-huit derniers mois, ainsi que tous mes amis et toute ma famille.*

Table des matières

I Logique mathématique **1**

1 Théorie du premier ordre **3**
1.1 Formule d'une structure syntaxique 3
1.1.1 Structure syntaxique 3
1.1.2 Termes 3
1.1.3 Formules 4
1.2 Déductibilité syntaxique 5
1.2.1 Théorie 6
1.2.2 Récursivité 6
1.3 Vérité sémantique 7
1.3.1 Interprétation 7
1.3.2 Connecteurs principaux 10
1.3.3 Quantificateurs principaux 12
1.4 Correction, complétude et cohérence 13
1.4.1 Théorie correcte et complète 13
1.4.2 Théorie cohérente 14

2 Théorie classique du premier ordre **15**
2.1 Théorie classique 15
2.1.1 Axiomes classiques 15
2.1.2 Règles d'inférence classiques 16
2.1.3 Théories classiques 17
2.1.4 Complétude 19
2.2 Théories relatives à $\mathbb{N}$ 19
2.2.1 Théorie **Z** 19
2.2.2 Définition de $\mathbb{N}$ 20
2.3 Arithmétiques de Presburger et de Peano 22
2.3.1 Arithmétique de Presburger 22
2.3.2 Arithmétique de Peano 23
2.4 Indécidabilité 24
2.4.1 Indécidabilité 24
2.4.2 Théorème de Gödel-Rosser 25
2.5 Corps et Anneau 26

2.5.1 Corps fini 26
2.5.2 Anneau de polynômes sur un corps fini 31

II Ensembles définissables et ensembles reconnaissables 32

3 Ensemble définissable 35
3.1 Ensemble reconnaissable dans une base 35
3.1.1 Cas de $\mathbb{N}$ 35
3.1.2 Cas de $\mathbb{F}[X]$ 36
3.2 Développement 38
3.2.1 Cas de $\mathbb{N}$ 38
3.2.2 Cas de $\mathbb{F}[X]$ 39

4 Automate et ensemble reconnaissable 40
4.1 Automate fini (déterministe) 40
4.2 Ensemble reconnaissable dans une base 44
4.2.1 Cas de $\mathbb{N}^n$ 44
4.2.2 Cas de $(\mathbb{F}[X])^n$ 45
4.3 Premiers exemples et contre-exemples 46
4.3.1 Cas de $\mathbb{N}$ 46
4.3.2 Cas de $\mathbb{F}[X]$ 47
4.4 Relations reconnaissables dans une base 49
4.4.1 Cas de $\mathbb{N}$ 49
4.4.2 Cas de $\mathbb{F}[X]$ 54

5 Théorème de Büchi-Bruyère 60
5.1 Énoncé dans $\mathbb{N}$ 60
5.2 Énoncé et preuve dans $\mathbb{F}[X]$ 60

6 Ensemble définissable, reconnaissable 66
6.1 Ensembles reconnaissables de type 1,2,3 et combinaisons booléennes 66
6.1.1 Cas de $\mathbb{N}$ 66
6.1.2 Cas de $\mathbb{F}[X]$ 68
6.2 Point de vue de la logique 73
6.2.1 Cas de $\mathbb{N}$ 73
6.2.2 Cas de $\mathbb{F}[X]$ 74
6.3 Stabilité 76
6.3.1 Cas de $\mathbb{N}$ 76
6.3.2 Cas de $\mathbb{F}[X]$ 76
6.4 Bases dépendantes 77
6.4.1 Cas de $\mathbb{N}$ 77
6.4.2 Cas de $\mathbb{F}[X]$ 78

7 Théorème de Cobham **79**
7.1 Ensembles syndétiques 79
7.2 Noyau 83
7.2.1 Cas de $\mathbb{N}$ 84
7.2.2 Cas de $\mathbb{F}[X]$ 86
7.3 Suite automatique 88
7.3.1 Cas de $\mathbb{N}$ 89
7.3.2 Cas de $\mathbb{F}[X]$ 90
7.4 Fonction de complexité 91
7.4.1 Cas de $\mathbb{N}$ 91
7.4.2 Cas de $\mathbb{F}[X]$ 92
7.5 Preuve dans $\mathbb{N}$ 93

III Définissabilité de la multiplication **98**

8 Partition de $P^{\mathbb{N}}$ **100**
8.1 Définitions de base 100
8.2 Premier cas particulier 101
8.3 Second cas particulier 105
8.4 Cas général 109
8.5 Compléments 110
8.5.1 Premier complément 110
8.5.2 Second complément 111

9 La multiplication est $\mathcal{P}$-définissable **112**
9.1 Définitions de base 112
9.2 Quelques fonctions $\mathcal{P}$-définissables utiles 113
9.3 La multiplication est $\mathcal{P}$-définissable. 116

10 La multiplication est (S,T)-définissable **120**
10.1 La multiplication est (S,T)-définissable 120

IV Perspectives **122**

Introduction

Depuis les travaux d'Alan Cobham [18] sur la dépendance du caractère reconnaissable d'un ensemble de nombres entiers par rapport à la base considérée, les systèmes de numération et les ensembles reconnaissables correspondants ont largement été étudiés ; citons, par exemple, les articles [26], [11] et [36]. Dans le cadre classique de la numération en base entière $p \geq 2$, un ensemble $\mathcal{N}$ de nombres entiers naturels est dit *p-reconnaissable*, si les représentations en base p des éléments de $\mathcal{N}$ forment un langage régulier, c'est-à-dire accepté par un automate fini déterministe. D'un point de vue algorithmique, il s'agit donc des ensembles dont les éléments possèdent les représentations en base k les plus simples syntaxiquement. A. Cobham a montré dans son article [18] de 1969 que les seuls ensembles de nombres entiers naturels simultanément reconnaissables dans deux bases multiplicativement indépendantes sont exactement les unions finies de progressions arithmétiques.

Il existe plusieurs caractérisations des ensembles p-reconnaissables, par exemple en termes de suites p-automatiques [19], de séries algébriques quand p est premier [17], ou de formules du premier ordre dans l'arithmétique de Presburger $\langle \mathbb{N}, + \rangle$ étendue par une fonction V_p spécifique à la base retenue. Nous pouvons par exemple consulter les excellents survols [11] et [8].

Il est bien connu que l'anneau $\mathbb{Z}$ des entiers relatifs et l'anneau $\mathbb{F}[X]$ des polynômes sur un corps $\mathbb{F}$ possèdent de nombreuses propriétés communes. Si $\mathbb{F}$ est un corps fini, il est alors naturel de définir les représentations en base P des éléments de $\mathbb{F}[X]$ où P est un polynôme de degré au moins 1. Dans un tel contexte et disposant d'un corps fini, tout polynôme $Q \in \mathbb{F}[X]$ se décompose de manière unique sous la forme d'une combinaison linéaire $\sum_{i=0}^{n} A_i P^i$ de puissances de P, dont les coefficients A_i $(i = 0, 1, \ldots, n)$ sont pris dans l'ensemble Σ_P des polynômes de degré strictement inférieur à celui de P. À une telle décomposition, on peut alors associer un mot sur l'alphabet fini Σ_P. Disposant pour tout polynôme Q d'une unique P-représentation, il est alors licite d'introduire, comme dans [49], la notion d'ensemble *P-reconnaissable* de polynômes.

Bien sûr la grande question dans ce cadre réside dans la formulation correcte d'un hypothétique théorème de Cobham : si P et Q sont deux polynômes multiplicativement indépendants, quelles sont les parties de $\mathbb{F}[X]$ simultanément P-reconnaissables et Q-reconnaissables ? Dans cette thèse, nous donnons quelques réponses partielles dans cette direction. Au cours des différentes sections, une très forte analogie est établie entre ce qui se passe dans $\mathbb{F}[X]$ et dans $\mathbb{Z}$ (ou $\mathbb{N}$). Nous y étudions plus particulièrement la caractérisation logique des parties P-reconnaissables.

Dans la première partie, nous rappelons les notions de base de la logique mathématique. Le chapitre 1 est consacré aux théories du premier ordre sans restriction sur les axiomes et les règles d'inférence. Nous y mettons essentiellement l'accent sur la différence entre l'aspect syntaxique et l'aspect sémantiques des théories. Dans le chapitre 2, nous nous plaçons dans le cadre de la logique classique du premier ordre et nous rappelons le théorème de complétude de Gödel, théorème qui montre que les théories sont un bon moyen syntaxique d'étudier les modèles qu'elles représentent. Ensuite, nous nous plaçons dans une théorie des ensembles pour définir rigoureusement l'ensemble des entiers naturels qui, muni des relations, fonctions et constantes adéquates, est un modèle de deux célèbres théories classiques : celle de Presburger et celle de Peano. Nous citons ensuite le théorème de Gödel-Rosser dans une section sur l'indécidabilité. Dans une dernière section, nous démontrons quelques résultats connus de la théorie des corps finis et nous considérons l'anneau $\mathbb{F}[X]$ des polynômes sur des corps fini $\mathbb{F}$.

Dans la seconde partie, nous étudions les ensembles reconnaissables dans une base donnée, ainsi que leurs caractérisations logique et automatique. Nous avons décidé de présenter chaque notion en parallèle avec son analogue dans le cadre des entiers naturels, même si certaines preuves sont presque des redites. Afin de ne pas le lasser, nous prévenons le lecteur habitué à ces notions dans le cadre des entiers qu'il peut directement se concentrer sur $\mathbb{F}[X]$. Dans le chapitre 3, nous mettons en évidence une fonction importante $\mathrm{V_P}$ jouant un rôle dans le développement en base P des polynômes. Dans le chapitre 4, nous donnons la définition des automates finis déterministes et des ensembles reconnaissables dans une base P. Quelques exemples sont donnés, puis nous démontrons que l'addition, la fonction $\mathrm{V_P}$ et d'autres relations sont P-reconnaissables. Le chapitre 5 est consacré au théorème de Büchi-Bruyère qui fournit une caractérisation logique des ensembles P-reconnaissables : il est possible d'identifier le caractère P-reconnaissable au fait d'être définissable par une formule du premier ordre dans une structure particulière basée sur la fonction $\mathrm{V_P}$. Déterminer la structure adéquate pour adapter le théorème dans le cadre des polynômes est une de nos contributions personnelles. Le chapitre 6 est réservé aux ensembles reconnaissables, c'est-à-dire à ceux qui le sont simultanément dans toutes les bases. Deux types élémentaires

d'ensembles reconnaissables avaient déjà été abordées par Michel Rigo dans l'article [49] :
- les ensembles $\{A \cdot C + B : C \in \mathbb{F}[X]\}$ de $\mathbb{F}[X]$, qui constituent l'analogue des progressions arithmétiques de $\mathbb{N}$, où $A, B \in \mathbb{F}[X]$,
- les ensembles $\{C \in \mathbb{F}[X] : \deg(C) \equiv a \pmod{b}\}$ où $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$.
Nous avons découvert un troisième type élémentaire d'ensembles reconnaissables : les ensembles $\{X^n \cdot C + R : n \in \mathbb{N},\ R \in \mathbb{F}[X] \text{ et } \deg(R) < n\}$ où $C \in \mathbb{F}[X] \setminus \{0\}$.
Il s'agit des ensembles de polynômes qui, exprimés en base X, commencent tous par un même préfixe. Nous conjecturons dans cette thèse que tous les ensembles reconnaissables sont des combinaisons booléennes d'ensembles pris dans ces trois catégories élémentaires. Bien entendu, nous ne manquons pas d'examiner aussi cet aspect dans le cadre de la logique. Nous montrons ensuite la stabilité des ensembles reconnaissables par combinaisons linéaires et nous prouvons que si deux bases P et Q sont des puissances d'un même polynôme, alors une partie de $\mathbb{F}[X]$ est P-reconnaissable si et seulement si elle est Q-reconnaissable. Le chapitre 7 est consacré au théorème de Cobham. Nous étudions successivement le caractère syndétique, le noyau, le p-noyau, la complexité et le caractère p-automatique des parties de $\mathbb{N}$. Le théorème de Cobham est ensuite prouvé au moyen de certains de ces outils. Les notions de p-noyau et de suite p-automatique s'adaptent aisément au cadre de $\mathbb{F}[X]$. Par contre, nous ne pouvons que définir et poser des conjectures pour les autres notions, et cela nous empêche de démontrer le théorème de Cobham dans le cadre des polynômes. Cependant, nous donnons une nouvelle preuve, très élégante, qu'un ensemble infini d'entiers naturels qui est p-reconnaissable et q-reconnaissable est syndétique dans $\mathbb{N}$. Ce dernier point est une contribution personnelle et est motivée par la nécessité de combler un trou dans une preuve simplifiée (*confer* [45] et [3]) qui était basée sur un lemme erroné. Il est en effet faux (voir [50] pour un contre-exemple) qu'en toute généralité un ensemble infini dense à droite et p-reconnaissable est syndétique dans $\mathbb{N}$.

Dans la troisième partie, nous montrons que la multiplication est définissable dans une structure $\mathcal{S}_{R,S}$ basée sur deux fonctions $\mathrm{V_R}$ et $\mathrm{V_S}$ dépendant de deux polynômes R et S de degré au moins 1 et multiplicativement indépendants. Tout se passe de façon analogue à ce qui a été prouvé pour les nombres entiers par Roger Villemaire dans l'article [59]. La démarche est nettement inspirée de celle qu'il a adoptée, mais nous avons cependant dû la modifier substantiellement car celle-ci est en fait incomplète. Ce résultat est très encourageant pour se conforter dans l'idée que la notion de polynômes multiplicativement indépendants est la bonne pour donner lieu à un éventuel théorème de Cobham. Dans le chapitre 8, nous mettons en évidence des objets définissables dans une structure basée sur deux fonctions $\mathrm{V_P}$ et $\mathrm{V_Q}$ où $P, Q \in \mathbb{F}[X]_{>0}$ sont certaines puissances de n'importe quels polynômes $R, S \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants. Nous clôturons le chapitre

en mettant en évidence les deux failles que nous avons trouvées dans l'article [59]. Dans le chapitre 9, nous exploitons les objets définis au chapitre précédent pour définir la multiplication. Dans chapitre 10, nous prouvons que la multiplication est définissable dans la structure $\mathcal{S}_{R,S}$ pour n'importe quels polynômes R, S de degré au moins 1 et multiplicativement indépendants.

Finalement, quelques perspectives intéressantes sont données en quatrième partie.

Introduction (English version)

Since Alan Cobham's seminal work [18] on the dependence of recognizability of a set of integers with respect to the considered base, numeration systems and the corresponding recognizable sets have been widely studied. For instance, let us cite [26], [11] and [36]. In the classical framework of the integer base $p \geq 2$ numeration system, a set $\mathcal{N}$ of non-negative integers is said to be *p-recognizable*, if the p-ary representations of the elements in $\mathcal{N}$ give a regular language, that is, a language accepted by a deterministic finite automaton. From an algorithmic point of view, these sets are the ones whose elements have the simplest syntactic k-ary representations. A. Cobham shows in his famous paper [18] from 1969 that the only sets of natural numbers simultaneous recognizable for two multiplicatively independent bases are exactly the finite unions of arithmetic progressions.

There are several well-known characterizations of the p-recognizable sets, for instance, using p-automatic sequences [19], algebraic series for p being a prime number [17], or through first order formulas in the Presburger arithmetic $\langle \mathbb{N}, + \rangle$ extended with a specific function V_p depending on the chosen base. For instance one can consider the excellent surveys [11] and [8].

It is well known that the ring $\mathbb{Z}$ of integers and the polynomial ring $\mathbb{F}[X]$ over a field $\mathbb{F}$ share a lot of common properties. Let $\mathbb{F}$ be a finite field a P be a polynomial of degree at least 1. Representations in base P of the elements in $\mathbb{F}[X]$ are naturally considered. In this framework, having a finite field at our disposal, any polynomial $Q \in \mathbb{F}[X]$ can be uniquely written as a linear combination $\sum_{i=0}^{n} A_i P^i$ of powers of P, where the coefficients A_i $(i = 0, 1, \ldots, n)$ belong to the set Σ_P of polynomials of degree (strictly) less than the one of P. With such a decomposition, one can associate a finite word over the finite alphabet Σ_P. Having for all polynomials Q a unique P-representation, it is permitted to introduce, as in [49], the notion of *P-recognizable* set of polynomials.

To that respect a major question is of course about the correct way to state a possible Cobham's theorem : if P and Q are two multiplicatively independent polynomials, which subsets of $\mathbb{F}[X]$ are simultaneously P-

recognizable and Q-recognizable ? In this thesis, we give partial answers in that direction. Along the different sections, a strong analogy is made between what is going on in $\mathbb{F}[X]$ and in $\mathbb{Z}$ (or $\mathbb{N}$). In particular we study the logical characterization of the P-recognizable sets.

In the first part of this thesis, we recall basic notions in mathematical logic. Chapter 1 is dedicated to first order theories without any restriction on the axioms and inference rules. Mainly we focus on the differences existing between syntactic and semantic aspects of the theories. In Chapter 2 the framework of the classical first order logic is considered and we recall Gödel's completeness theorem. This latter result shows that theories are a good syntactic way to study the models that they represent. Next we consider a set theory to properly define the set of natural numbers which, equipped with properly chosen relations, functions and constants is a model of two famous classical theories : the ones of Presburger and Peano. Next we state Gödel-Rosser in a section about undecidability. In a last section, we prove some well-known results on finite fields and we consider the ring $\mathbb{F}[X]$ of polynomials over a finite field $\mathbb{F}$.

In the second part, we study sets which are recognizable in a given base as well as their logical and automatic characterizations. We have decided to present each notion in parallel with its counterpart in the framework of integers, even if some proofs are the same. The knowledgeable reader can only focus on the case of $\mathbb{F}[X]$. In Chapter 3, we shed some light on an important function $\mathrm{V_P}$ playing a role in the base P developments of polynomials. In Chapter 4 we define deterministic finite automata and sets which are recognizable in a base P. Some examples are given. Next we prove that addition, the map $\mathrm{V_P}$ and some other useful relations are P-recognizable. Chapter 5 is dedicated to Büchi-Bruyère's theorem giving a logical characterization of P-recognizable sets : one may provide such a characterization in terms of a first order formulas in a specific structure based on the function $\mathrm{V_P}$. Determining the right structure to adapt this theorem in the framework of polynomials is one of our personal contributions. Recognizable sets, that is, sets which are simultaneously recognizable in all bases, are presented in Chapter 6. Two kinds of such sets have been presented by Michel Rigo in [49] :
- subsets $\{A \cdot C + B : C \in \mathbb{F}[X]\}$ of $\mathbb{F}[X]$, which play a role similar to the arithmetic progressions in $\mathbb{N}$, where $A, B \in \mathbb{F}[X]$;
- subsets $\{C \in \mathbb{F}[X] : \deg(C) \equiv a \pmod{b}\}$ where $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$.
We have found a third elementary kind of recognizable sets : the sets $\{X^n \cdot C + R : n \in \mathbb{N},\ R \in \mathbb{F}[X] \text{ and } \deg(R) < n\}$ with $C \in \mathbb{F}[X] \setminus \{0\}$.
These are sets of polynomials which expressed in base X have all the same prefix. We make the following conjecture : any recognizable set is a Boolean combination of sets belonging these three elementary classes. Naturally we study these questions in the logical framework. We show the stability of re-

cognizable sets by Boolean combinations and we prove that if P and Q are two bases which are powers of a same polynomial, then a subset of $\mathbb{F}[X]$ is P-recognizable if and only if it is Q-recognizable. Chapter 7 is dedicated to Cobham's theorem. We study syndeticity, kernel, p-kernel, complexity and p-automaticity of subsets of $\mathbb{N}$. Cobham's theorem is proved using some of these tools. Notions of p-kernel and p-automatic sequences are adapted accordingly to $\mathbb{F}[X]$. On the other hand we are only able to define some notions and propose some conjectures in the polynomial framework. Nevertheless we give a new and quite elegant proof that an infinite set of non-negative integers which is simultaneously p-recognizable and q-recognizable is syndetic inside $\mathbb{N}$. This last point is a personal contribution motivated by the necessity to correct a simplified approach (*confer* [45] et [3]) based on a false lemma. It is not correct (for instance, see [50] for a counter-example) that an infinite right-dense p-recognizable set is always syndetic inside $\mathbb{N}$.

In the third part, we show that multiplication is definable in a structure $\mathcal{S}_{R,S}$ based on two maps $\mathrm{V_R}$ and $\mathrm{V_S}$ depending on two polynomials R and S of degree at least 1 and multiplicatively independent. The scheme is analogous to the integer case provided by Roger Villemaire in [59]. The path is inspired by Villemaire's methods but has been substantially modified because first it was incomplete. This result is a positive hope for the idea that multiplicatively independent polynomials is the right notion to give rise to some Cobham's theorem. In Chapter 8 we exhibit objects which are definable in a structure based on two maps $\mathrm{V_P}$ and $\mathrm{V_Q}$ where $P, Q \in \mathbb{F}[X]_{>0}$ are powers of some multiplicatively independent polynomials $R, S \in \mathbb{F}[X]_{>0}$. We conclude the chapter by exhibiting two flaws in the paper [59]. In Chapter 9, we make use of previously defined objects to define multiplication. In Chapter 10, we prove that multiplication is definable in the structure $\mathcal{S}_{R,S}$ for any multiplicatively independent polynomials R, S of degree at least 1.

Finally, some perspectives are presented at the fourth part.

Première partie

Logique mathématique

Dans cette première partie, nous posons les bases rigoureuses de la logique mathématique du premier ordre. Il est délicat[1] de bien définir celles-ci car c'est un domaine qui touche aux limites des mathématiques et qui à tendance à parler de lui-même, voire à se contredire à la première mauvaise porte ouverte. Nous avons eu une approche réfléchie et nous avons volontairement voulu nous poser nos propres questions en essayant d'y apporter nos propres réponses et nos propres constructions. En général, le cadre de la logique classique du premier ordre est vite abordé et c'est seulement ensuite qu'apparaît la notion de modèle. Nous avons préféré faire l'inverse, quitte à ne pas avoir la définition habituelle de modèle, faute d'avoir une distinction assez tôt entre les axiomes purs et les autres. Bien entendu, grâce au sens le plus simple (que nous démontrons) du premier théorème de complétude de Gödel (que nous ne démontrons pas) cette définition se confond avec la définition habituelle. Nous posons au lecteur une question sur les quantificateurs dans la remarque 1.3.24. Sans entrer dans les détails, précisons que nous construisons $\mathbb{N}$ rigoureusement avec des structures de Dedekind-Peano, que nous définissons les arithmétiques de Peano et Presburger et que nous démontrons certains théorèmes classiques sur les corps finis. Pour une référence générale sur la logique mathématique, nous renvoyons le lecteur au livre [23].

[1] De nos jours, cela n'est certainement plus vrai grâce aux nombreux travaux déjà effectués dans le domaine. Mais la logique est néanmoins la branche des mathématiques qui a démandé le plus de recul aux mathématiciens avant d'être bien digérée

Chapitre 1

Théorie du premier ordre

Le but de ce chapitre est de se familiariser avec les notions de base de la logique mathématique du premier ordre et en particulier de bien séparer les notions syntaxiques des notions sémantiques. Nous sommes volontairement très général dans les notions définies (pas de contraintes sur les connecteurs, les quantificateurs, les axiomes et les règles d'inférence), même si nous restons strictement dans le cadre des théories du premier ordre et des modèles basés sur une notion de vérité à deux valeurs. Les contraintes sont posées au chapitre 2.1.

1.1 Formule d'une structure syntaxique

1.1.1 Structure syntaxique

Définition 1.1.1. Une *structure syntaxique* est la donnée d'un sextuplet

$$(V, R, R_f, R_c, C, Q)$$

pour lequel V, R, R_f, R_c, C, Q sont six ensembles disjoints. L'ensemble V est infini dénombrable et chacun de ses éléments est appelé *variable syntaxique*, tout élément de R est appelé *relation syntaxique*, tout élément de R_f est appelé *fonction syntaxique*, tout élément de R_c est appelé *constante syntaxique*, tout élément de C est appelé *connecteur syntaxique* et tout élément de Q est appelé *quantificateur syntaxique*. À chaque relation syntaxique, à chaque fonction syntaxique et à chaque connecteur syntaxique est associé un nombre entier strictement positif appelé *arité*. Une relation syntaxique, une fonction syntaxique ou un connecteur syntaxique d'arité 1, 2, 3 est respectivement qualifié de *unaire*, *binaire*, *ternaire*.

1.1.2 Termes

Les définitions 1.1.2 et 1.1.3 nous donnent récursivement les termes d'une structure syntaxique et un niveau pour chacun d'eux.

Définition 1.1.2. Un *terme de niveau 0*, aussi appelé *terme élémentaire*, d'une structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ est une variable syntaxique ou une constante syntaxique.

Définition 1.1.3. Soit k un entier strictement positif. Un *terme de niveau* k d'une structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ est une expression syntaxique de la forme $f(t_1, \ldots, t_n)$ où $t_1, \ldots, t_n$ sont des termes de $\mathcal{S}$ de niveau au plus $(k-1)$ dont l'un au moins est de niveau $(k-1)$ et f est une fonction syntaxique d'arité n.

1.1.3 Formules

Les définitions 1.1.4 et 1.1.5 nous donnent récursivement les formules d'une structure syntaxique et un niveau pour chacune d'elles.

Définition 1.1.4. Une *formule de niveau 0*, appelée aussi *formule atomique*, d'une structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ est une expression syntaxique de la forme $r(t_1, \ldots, t_n)$ dans laquelle $t_1, \ldots, t_n$ sont des termes de $\mathcal{S}$ et r est une relation syntaxique d'arité n.

Définition 1.1.5. Soit k un entier strictement positif. Une *formule de niveau* k d'une structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ est une expression syntaxique de l'une des deux formes suivantes :
- $c(\varphi_1, \ldots, \varphi_n)$ où $\varphi_1, \ldots, \varphi_n$ sont des formules de $\mathcal{S}$ de niveau au plus $(k-1)$ dont l'une au moins est de niveau $(k-1)$ et c est un connecteur syntaxique d'arité n,
- $q(a, \varphi)$ où φ est une formule de $\mathcal{S}$ de niveau $(k-1)$, a est une variable syntaxique et q est un quantificateur syntaxique.

Si $*$ est un connecteur syntaxique binaire d'une structure syntaxique $\mathcal{S}$ et a, b, c, d sont des termes de $\mathcal{S}$, des expressions comme $*(*(a,b),*(c,d))$ et $*(*(*(a,b),c),d)$ sont syntaxiquement différentes et représentent donc deux formules différentes, même si (en anticipant sur les définitions 1.3.13 et 1.3.14, ainsi que sur la remarque 1.3.15) le connecteur syntaxique $*$ est sémantiquement associatif. Une formule n'a donc qu'un seul niveau.

Définition 1.1.6. Une formule d'une structure syntaxique est qualifiée de *quantifiée* si elle est construite avec au moins un quantificateur syntaxique. Dans le cas contraire, elle est qualifiée de *non quantifiée*.

Définition 1.1.7. Soit t un terme d'une structure syntaxique. Chaque occurence de chaque variable syntaxique de t est qualifiée de *libre dans le terme* t.

La définition 1.1.8 nous donne récursivement la notion d'occurence libre d'une variable dans une formule.

Définition 1.1.8. Soit φ une formule d'une structure syntaxique.

Si φ est atomique, alors chaque occurence de chaque variable syntaxique de φ est qualitifée de *libre dans la formule* φ.

Si φ est de la forme $c(\varphi_1, \ldots, \varphi_n)$ où $\varphi_1, \ldots, \varphi_n$ sont des formules de $\mathcal{S}$ et c est un connecteur syntaxique d'arité n, alors chaque occurence libre de chaque variable syntaxique de chacune des formules $\varphi_1, \ldots, \varphi_n$ est également qualifiée de *libre dans la formule* φ.

Si φ est de la forme $q(a, \psi)$ où ψ est une formule de $\mathcal{S}$, a est une variable syntaxique et q est un quantificateur syntaxique, alors chaque occurence libre de chaque variable syntaxique différente de a de la formule ψ est également qualifié de *libre dans la formule* φ.

Définition 1.1.9. Une formule d'une structure syntaxique est qualifiée de *close* si aucune des occurences de ses variables syntaxiques n'est libre dans elle-même.

Lorsque φ est une formule d'une structure syntaxique $\mathcal{S}$ et $a_1, \ldots, a_n$ sont des variables syntaxiques de cette structure, la notation $\varphi(a_1, \ldots, a_n)$ signifie que $a_1, \ldots, a_n$ sont n variables syntaxiques (deux à deux distinctes) ayant chacune au moins une occurence libre dans la formule φ. De plus, la notation $\varphi[a_1, \ldots, a_n]$ signifie non seulement que $a_1, \ldots, a_n$ sont n variables syntaxiques (deux à deux distinctes) ayant chacune au moins une occurence libre dans la formule φ, mais en plus qu'il n'y a pas d'autres variables syntaxiques que $a_1, \ldots, a_n$ ayant une occurence libre dans la formule φ.

Insistons sur le fait que les relations syntaxiques ne sont que des symboles syntaxiques ayant un rôle formatif pour générer des expressions syntaxiques de plus en plus grosses. Ce rôle formatif se veut arbitraire par rapport aux différents termes : en aucun cas une relation syntaxique ne doit être vue comme un vraie relation distingant certains termes ou uplets de termes. C'est la raison pour laquelle, il est nécessaire de définir les constantes syntaxiques et les fonctions syntaxiques : strictement parlant, celles-ci ne sont pas des relations syntaxiques particulières. Toutefois, dans la section 1.3, nous interprétons les variables syntaxiques par des éléments d'un ensemble, les relations syntaxiques par des relations, les fonctions syntaxiques par des fonctions et les constantes syntaxiques par des constantes. Ces constantes et ces fonctions sont évidemment des relations particulières.

1.2 Déductibilité syntaxique

Dans cette section, nous enrichissons les structures syntaxiques en distinguant certaines formules que nous considérons comme prouvables dans un

certain contexte par des moyens purement syntaxiques. En fait, nous nous donnons d'une part, un ensemble de formules considérées comme prouvées dès le départ et d'autre part, un ensemble de règles permettant de prouver de nouvelles formules à partir d'autres formules déjà prouvées.

1.2.1 Théorie

Définition 1.2.1. Une *règle d'inférence* sur une structure syntaxique $\mathcal{S}$ est une fonction qui associe une formule de $\mathcal{S}$ à certains uplets de formules de $\mathcal{S}$ (la taille de ces uplets peut varier).

Définition 1.2.2. Une formule φ d'une structure syntaxique $\mathcal{S}$ est *directement déductible* à partir d'un ensemble I de règles d'inférence sur $\mathcal{S}$ et d'un ensemble F de formules de $\mathcal{S}$ si et seulement si elle est l'image par une des règles d'inférence de I d'un uplet de formules de F.

Définition 1.2.3. Une formule φ d'une structure syntaxique $\mathcal{S}$ est *déductible* à partir d'un ensemble I de règles d'inférence sur $\mathcal{S}$ et d'un ensemble F de formules de $\mathcal{S}$ si et seulement si il existe une suite finie de formules $\varphi_1, \ldots, \varphi_n$ de $\mathcal{S}$ telle que φ est φ_n et que, pour tout $i \in \{1, \ldots, n\}$, la formule φ_i est directement déductible à partir de l'ensemble I de règles d'inférence et de l'ensemble $F \cup \{\varphi_1, \ldots, \varphi_{i-1}\}$ de formules de $\mathcal{S}$.

Définition 1.2.4. Une *théorie* est la donnée d'un triplet $\mathcal{T} = (\mathcal{S}, A, I)$ pour lequel $\mathcal{S}$ est une structure syntaxique, A un ensemble de formules de $\mathcal{S}$ et I un ensemble de règles d'inférence sur $\mathcal{S}$. Chaque élément de A est appelé *axiome* de $\mathcal{T}$. Chaque élément de I est aussi appelé *règle d'inférence* de $\mathcal{T}$.

Définition 1.2.5. Un *théorème* d'une théorie $\mathcal{T}$ est un axiome de $\mathcal{T}$ ou une formule déductible à partir des règles d'inférence de $\mathcal{T}$ et des axiomes de $\mathcal{T}$.

1.2.2 Récursivité

La définition suivante est donnée avec la notion intuitive d'algorithme. Il est possible de remplacer cette notion intuitive par n'importe quelle définition rigoureuse du concept d'algorithme (elles sont toutes équivalentes, si nous acceptons la thèse de Church-Turing), comme par exemple celles basées sur les machines de Turing (voir [44]) ou le lambda-calcul (voir [4]), mais ceci n'a pas beaucoup d'importance ici.

Définition 1.2.6. Un sous-ensemble P d'un ensemble E est *récursif* dans E s'il existe un algorithme permettant de décider si un élément arbitraire de E appartient ou n'appartient pas à P.

Définition 1.2.7. Une théorie est *récursivement axiomatisable* si l'ensemble de ses axiomes est récursif dans l'ensemble de ses formules.

Définition 1.2.8. Un *schéma* sur une structure syntaxique $\mathcal{S}$ est un ensemble de la forme

$$\{\varphi(\varphi_1, \ldots, \varphi_n) : \varphi_1, \ldots, \varphi_n \text{ sont des formules de } \mathcal{S}\}$$

où l'expression $\varphi(\varphi_1, \ldots, \varphi_n)$ représente la formule obtenue en remplaçant dans la formule $\varphi(a_1, \ldots, a_n)$ chaque occurence libre de chacune des variables syntaxiques a_i ($i \in \{1, \ldots, n\}$) par la formule φ_i d'indice correspondant.

Dans une théorie récursivement axiomatisable, les axiomes sont souvent donnés au moyen d'une liste finie de schémas d'axiomes.

1.3 Vérité sémantique

1.3.1 Interprétation

Une théorie sur une structure syntaxique étudie toutes les structures mathématiques vérifiant certaines propriétés indépendamment des structures elles-mêmes. Mais, *a priori*, rien ne garantit que tout ce qui est vrai pour ces structures est prouvable dans le cadre purement syntaxique de cette théorie. Cela est-il toujours le cas ? Il est important de développer d'abord l'aspect sémantique avec précision, ce que nous faisons dans cette section, avant de répondre à cette question dans un cadre particulier et intéressant à la fin de la section 2.1.

Dans les définitions qui suivent, le mot *interprétation* est utilisé sur des ensembles de natures différentes. Il est important de bien distinguer à chaque fois la portée de l'interprétation dont il est question.

Définition 1.3.1. Soit $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ une structure syntaxique et soit E un ensemble non vide. Une *interprétation* de R sur E est une fonction qui associe une relation d'arité n sur E à chaque relation syntaxique d'arité n. Une *interprétation* de R_f sur E est une fonction qui associe une fonction de E^n dans E à chaque fonction syntaxique d'arité n. Une *interprétation* de R_c sur E est une fonction qui associe un élément de E à chaque constante syntaxique.

Définition 1.3.2. Soit $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ une structure syntaxique. Une *structure mathématique* sur $\mathcal{S}$ est la donnée d'un quadruplet

$$(E, R^*, R_f^*, R_c^*)$$

pour lequel E est un ensemble non vide, R^* est l'image de R par une interprétation de R sur E, R_f^* est l'image de R_f par une interprétation de R_f sur E, R_c^* est l'image de R_c par une interprétation de R_c sur E.

Si $\mathcal{M} = (E, R^*, R_f^*, R_c^*)$ est une structure mathématique sur une structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ et si g est une relation syntaxique (resp. une fonction syntaxique, une constante syntaxique), alors nous désignons par g^* l'image de g par l'interprétation de R (resp. de R_f, de R_c) qui a servi à définir R^* (resp. R_f^*, R_c^*).

Définition 1.3.3. Soit $\mathcal{M} = (E, R^*, R_f^*, R_c^*)$ une structure mathématique sur la structure syntaxique $\mathcal{S}$. Une *interprétation* des variables de $\mathcal{S}$ dans $\mathcal{M}$ est une fonction τ qui associe un élément de E à chaque variable syntaxique de $\mathcal{S}$.

Dans les définitions 1.3.4 et 1.3.5, nous étendons naturellement et récursivement à tous les termes d'une structure syntaxique $\mathcal{S}$, puis à toutes ses formules atomiques, la fonction que l'interprétation des variables de $\mathcal{S}$ dans une structure mathématique $\mathcal{M}$ sur $\mathcal{S}$ est.

Définition 1.3.4. Soient $\mathcal{M}$ une structure mathématique sur une structure syntaxique $\mathcal{S}$, τ une interprétation des variables de $\mathcal{S}$ dans $\mathcal{M}$ et t un terme de $\mathcal{S}$. La valeur du terme t par l'interprétation τ est notée t_τ.

Si t est une variable syntaxique a, alors t_τ vaut $\tau(a)$.

Si t est une constante syntaxique c, alors t_τ vaut c^*.

Si t est une terme de la forme $f(t_1, \ldots, t_n)$ où $t_1, \ldots, t_n$ sont des termes de $\mathcal{S}$ et f est une fonction syntaxique d'arité n, alors l'interprétation de t vaut $f^*((t_1)_\tau, \ldots, (t_n)_\tau)$.

Définition 1.3.5. Soient $\mathcal{M}$ une structure mathématique sur une structure syntaxique $\mathcal{S}$, τ une interprétation des variables de $\mathcal{S}$ dans $\mathcal{M}$ et φ une formule de $\mathcal{S}$ de la forme $\varphi[t_1, \ldots, t_n] = r(t_1, \ldots, t_n)$ où $t_1, \ldots, t_n$ sont des termes de $\mathcal{S}$ et r est une relation syntaxique d'arité n. La valeur de la formule φ par l'interprétation τ est notée φ_τ et vaut

$$\begin{cases} 1 \text{ si } ((t_1)_\tau, \ldots, (t_n)_\tau) \in r^* \\ 0 \text{ si } ((t_1)_\tau, \ldots, (t_n)_\tau) \notin r^* \end{cases}.$$

Nous notons $\mathbb{B}$ l'ensemble $\{0, 1\}$.

Dans une structure syntaxique $\mathcal{S}$, un connecteur syntaxique d'arité n a juste le rôle d'un symbole liant n formules pour former de nouvelles formules plus grandes. Néanmoins, contrairement aux relations syntaxiques, aux fonctions syntaxiques et aux constantes syntaxiques, chaque connecteur détient lui-même son interprétation. Celle-ci est indépendante de la structure mathématique $\mathcal{M}$ choisie sur $\mathcal{S}$. Elle permet d'étendre l'interprétation par des variables de $\mathcal{S}$ dans $\mathcal{M}$ à davantage de formules de $\mathcal{S}$. En fait, l'image d'un

connecteur syntaxique c d'arité n par son interprétation est tout simplement une fonction de $\mathbb{B}^n$ dans $\mathbb{B}$.

Une remarque similaire est valable aussi pour les quantificateurs syntaxiques d'une structure syntaxique $\mathcal{S}$: dans $\mathcal{S}$, un quantificateur syntaxique a juste le rôle d'un symbole liant une formule à une variable syntaxique, mais en réalité il détient lui-même son interprétation, en ce sens que celle-ci ne dépend de la structure mathématique $\mathcal{M} = (E, R^*, R_f^*, R_c^*)$ choisie sur $\mathcal{S}$ que pour le choix de l'ensemble E. En fait, l'image d'un quantificateur par son interprétation dans $\mathcal{M}$ est une fonction de $\mathbb{B}^E$ dans $\mathbb{B}$ (la notation $\mathbb{B}^E$ représente l'ensemble des fonctions de E dans $\mathbb{B}$).

À partir de maintenant, nous parlons volontiers de *connecteur* (resp. de *quantificateur*) pour désigner à la fois un connecteur syntaxique (resp. un quantificateur syntaxique) et son image par son interprétation, et nous utilisons la même notation dans les deux cas puisque le choix du contexte, syntaxique (symbole) ou sémantique (fonction), est généralement évident.

Nous sommes maintenant armés pour étendre récursivement à toutes les formules d'une structure syntaxique, la notion d'interprétation des variables de cette structure syntaxique dans une structure mathématique sur cette structure syntaxique. C'est le but de la définition 1.3.6.

Définition 1.3.6. Soient $\mathcal{M} = (E, R^*, R_f^*, R_c^*)$ une structure mathématique sur une structure syntaxique $\mathcal{S}$, τ une interprétation des variables de $\mathcal{S}$ dans $\mathcal{M}$ et φ une formule de niveau non nul de $\mathcal{S}$. La valeur de la formule φ par l'interprétation τ est notée φ_τ.

Si la formule φ est de la forme $c(\varphi_1, \ldots, \varphi_n)$ où $\varphi_1, \ldots, \varphi_n$ sont des formules de $\mathcal{S}$ et c est un connecteur syntaxique d'arité n, alors

$$\varphi_\tau = c((\varphi_1)_\tau, \ldots, (\varphi_n)_\tau).$$

Si la formule φ est de la forme $q(a, \psi)$ où ψ est une formule de $\mathcal{S}$, a est une variable syntaxique et q est un quantificateur syntaxique, alors

$$\varphi_\tau = q\left(e \mapsto \psi_{\tau_e}\right)$$

où, pour tout $e \in E$, τ_e est l'interprétation des variables de $\mathcal{S}$ dans $\mathcal{M}$ pour laquelle $\tau_e(a) = e$ et $\tau_e(b) = \tau(b)$ pour toute variable syntaxique b différente de a, et $(e \mapsto \psi_{\tau_e}) \in \mathbb{B}^E$ est la fonction qui à e associe ψ_{τ_e}.

Définition 1.3.7. Soient $\mathcal{M}$ une structure mathématique sur une structure syntaxique $\mathcal{S}$, τ une interprétation des variables de $\mathcal{S}$ dans $\mathcal{M}$ et φ une formule de $\mathcal{S}$. La formule φ est *satisfaite par* τ dans $\mathcal{M}$ si $\varphi_\tau = 1$. La formule φ est *non satisfaite par* τ dans $\mathcal{M}$ si $\varphi_\tau = 0$.

Définition 1.3.8. Soient $\mathcal{M}$ une structure mathématique sur une structure syntaxique $\mathcal{S}$ et φ une formule de $\mathcal{S}$. La formule φ est *valide* dans $\mathcal{M}$ si elle est satisfaite par toute interprétation des variables syntaxiques de $\mathcal{S}$ dans $\mathcal{M}$. La formule φ est *non valide* dans $\mathcal{M}$ si elle est non satisfaite par toute interprétation des variables syntaxiques de $\mathcal{S}$ dans $\mathcal{M}$.

Définition 1.3.9. Soit $\mathcal{T} = (\mathcal{S}, A, I)$ une théorie. Un *modèle* de $\mathcal{T}$ est une structure mathématique $\mathcal{M}$ sur $\mathcal{S}$ pour laquelle chaque axiome de $\mathcal{T}$ est valide dans $\mathcal{M}$.

Définition 1.3.10. Soient $\mathcal{T} = (\mathcal{S}, A, I)$ une théorie et φ une formule de $\mathcal{S}$. La formule φ est *vraie* (ou encore est une *tautologie*) dans $\mathcal{T}$ si elle est valide dans tout modèle $\mathcal{M}$ de $\mathcal{T}$. La formule φ est *fausse* (ou encore est une *contradiction*) dans $\mathcal{T}$ si elle est non valide dans tout modèle $\mathcal{M}$ de $\mathcal{T}$.

1.3.2 Connecteurs principaux

Nous allons mettre en évidence certains connecteurs particuliers et montrer que nous pouvons nous restreindre à utiliser très peu de connecteurs différents sans aucune perte de généralité.

Définition 1.3.11. L'*affirmation* $\imath$ est le connecteur unaire défini par :

$$\imath : \mathbb{B} \to \mathbb{B}, \begin{cases} \imath(0) = 0 \\ \imath(1) = 1 \end{cases}.$$

Définition 1.3.12. La *négation* $\neg$ est le connecteur unaire défini par :

$$\neg : \mathbb{B} \to \mathbb{B}, \begin{cases} \neg(0) = 1 \\ \neg(1) = 0 \end{cases}.$$

Définition 1.3.13. La *disjonction* $\vee$ est le connecteur binaire défini par :

$$\vee : \mathbb{B} \to \mathbb{B}, \begin{cases} \vee(0,0) = 0 \\ \vee(0,1) = 1 \\ \vee(1,0) = 1 \\ \vee(1,1) = 1 \end{cases}.$$

Définition 1.3.14. La *conjonction* $\wedge$ est le connecteur binaire défini par :

$$\wedge : \mathbb{B} \to \mathbb{B}, \begin{cases} \wedge(0,0) = 0 \\ \wedge(0,1) = 0 \\ \wedge(1,0) = 0 \\ \wedge(1,1) = 1 \end{cases}.$$

Remarque 1.3.15. Par commodité, nous notons $(a \vee b)$, l'expression $\vee(a, b)$. De plus, comme les expressions $(a \vee (b \vee c))$ et $((a \vee b) \vee c)$ représentent la

même fonction (nous disons que le connecteur $\vee$ est *sémantiquement associatif*), nous pouvons les noter sous la forme $\vee(a, b, c)$ ou $(a \vee b \vee c)$ sans aucun risque de confusion. De façon analogue, nous utilisons aussi les notations $\vee_{i\in\{1,\dots,n\}} a_i$ ou $(a_1 \vee \cdots \vee a_n)$ pour représenter l'expression $\vee(a_1, \dots, a_n)$. Cependant, une expression de ce genre n'est plus strictement parlant une formule avec un niveau fixé, mais est une notation abrégée représentant plusieurs formules éventuellement de niveaux différents mais sémantiquement équivalentes. Les remarques de ce paragraphe s'adaptent immédiatement aux conjonctions.

Par convention, une affirmation ou une négation est prioritaire sur une disjonction ou une conjonction (au même sens qu'une multiplication est généralement prioritaire sur une addition). De plus, les parenthèses extrêmes d'une formule sont souvent omises. Ainsi,

$$\begin{aligned} \imath a \vee \imath b \quad &\text{signifie} \quad ((\imath(a)) \vee (\imath(b))), \\ \imath a \wedge \imath b \quad &\text{signifie} \quad ((\imath(a)) \wedge (\imath(b))), \\ \neg a \vee \neg b \quad &\text{signifie} \quad ((\neg(a)) \vee (\neg(b))), \\ \neg a \wedge \neg b \quad &\text{signifie} \quad ((\neg(a)) \wedge (\neg(b))). \end{aligned}$$

Proposition 1.3.16. *Tout connecteur est équivalent à une composition de connecteurs choisis parmi les quatre connecteurs $\imath$, $\neg$, $\vee$ et $\wedge$.*

Démonstration. Soit c un connecteur d'arité n. Soit f la fonction définie par

$$f : \mathbb{B} \to \{\imath, \neg\}, \begin{cases} f(0) = \neg \\ f(1) = \imath \end{cases}.$$

Avec ces notations, l'égalité suivante est évidente :

$$c(a_1, \dots, a_n) = \bigvee_{(b_1,\dots,b_n)\in c^{-1}(1)} (f(b_1)a_1 \wedge \cdots \wedge f(b_n)a_n).$$

En effet, la disjonction du second membre est satisfaite pour un n-uplet $(a_1, \dots, a_n)$ fixé dans $\mathbb{B}^n$ si et seulement si elle possède un terme pour lequel les n égalités $a_1 = b_1, \dots, a_n = b_n$ sont toutes satisfaites. Or, ce dernier point est réalisé si et seulement si $c(a_1, \dots, a_n) = 1$. □

Corollaire 1.3.17. *Tout connecteur est équivalent à une composition de connecteurs choisis parmi les deux connecteurs $\neg$ et $\vee$.*

Démonstration. Cela découle directement de l'égalité principale de la preuve de la proposition 1.3.16, du fait que le connecteur $\imath$ n'est pas utile et du fait que $a \wedge b = \neg(\neg a \vee \neg b)$ quels que soient $a, b \in \mathbb{B}$. □

Corollaire 1.3.18. *Tout connecteur est équivalent à une composition de connecteurs choisis parmi les deux connecteurs $\neg$ et $\wedge$.*

Démonstration. Cela découle directement de l'égalité principale de la preuve de la proposition 1.3.16, du fait que le connecteur $\imath$ n'est pas utile et du fait que $a \vee b = \neg(\neg a \wedge \neg b)$ quels que soient $a, b \in \mathbb{B}$. □

Mentionnons qu'il est possible de définir tous les connecteurs au moyen d'un seul connecteur binaire. Le connecteur $NAND(a, b) = \neg(a \wedge b)$ le permet. Le connecteur $NOR(a, b) = \neg(a \vee b)$ le permet également. Mais ceci ne nous est pas utile dans la suite.

Dans la définition suivante, il faut faire attention à distingueur le connecteur $\rightarrow$ du symbole identique servant à écrire l'expression $\mathbb{B} \rightarrow \mathbb{B}$. Nous nous permettons exceptionnellement cet abus de notation car il ne pose aucun soucis de compréhension.

Définition 1.3.19. L'*implication* est le connecteur binaire $\rightarrow$ défini par :

$$\rightarrow : \mathbb{B} \rightarrow \mathbb{B}, \begin{cases} \rightarrow (0,0) = 1 \\ \rightarrow (0,1) = 1 \\ \rightarrow (1,0) = 0 \\ \rightarrow (1,1) = 1 \end{cases}.$$

Par commodité, nous notons $(a \rightarrow b)$ l'expression $\rightarrow (a, b)$ et $(a \leftarrow b)$ l'expression $(b \rightarrow a)$.

Définition 1.3.20. L'*équivalence* est le connecteur binaire $\leftrightarrow$ défini par :

$$\leftrightarrow : \mathbb{B} \rightarrow \mathbb{B}, \begin{cases} \leftrightarrow (0,0) = 1 \\ \leftrightarrow (0,1) = 0 \\ \leftrightarrow (1,0) = 0 \\ \leftrightarrow (1,1) = 1 \end{cases}.$$

Par convention, une disjonction ou une conjonction est prioritaire sur une implication ou une équivalence.

Corollaire 1.3.21. *Tout connecteur est équivalent à une composition de connecteurs choisis parmi les deux connecteurs $\neg$ et $\rightarrow$.*

Démonstration. Cela découle directement du corollaire 1.3.17 et du fait que $a \vee b = \neg a \rightarrow b$ quels que soient $a, b \in \mathbb{B}$. □

1.3.3 Quantificateurs principaux

Seuls deux quantificateurs nous intéressent. Ils sont présentés dans les définitions 1.3.22 et 1.3.23. Pour ces définitions sémantiques, nous fixons un ensemble non vide E, puis nous notons $1_{\mathbb{B}^E}$ la fonction de E dans $\mathbb{B}$ pour laquelle $1_{\mathbb{B}^E}(E) = \{1\}$ et $0_{\mathbb{B}^E}$ la fonction de E dans $\mathbb{B}$ pour laquelle $0_{\mathbb{B}^E}(E) = \{0\}$.

Définition 1.3.22. Le *quantificateur universel* est le quantificateur $\forall$ défini par :

$$\forall : \mathbb{B}^E \to \mathbb{B}, \begin{cases} \forall(1_{\mathbb{B}^E}) = 1 \\ \forall(a) = 0 \text{ si } a \neq 1_{\mathbb{B}^E} \end{cases} .$$

Définition 1.3.23. Le *quantificateur existentiel* est le quantificateur $\exists$ défini par :

$$\exists : \mathbb{B}^E \to \mathbb{B}, \begin{cases} \exists(0_{\mathbb{B}^E}) = 0 \\ \exists(a) = 1 \text{ si } a \neq 0_{\mathbb{B}^E} \end{cases} .$$

Ces notations fonctionnelles ne sont presque jamais utilisées pour les quantificateurs. Quant aux notations syntaxiques $\forall(a, \varphi)$ et $\exists(a, \varphi)$, nous les remplaçons habituellement par les notations $(\forall a\varphi)$ et $(\exists a\varphi)$. Par convention, un quantificateur est prioritaire sur un connecteur.

Il y a un lien sémantique évident entre les deux quantificateurs étudiés. Ce lien est le suivant : $\neg\forall a\varphi = \exists a\neg\varphi$ ou encore $\neg\exists a\varphi = \forall a\neg\varphi$.

Remarque 1.3.24. La question ouverte qui suit sort du cadre de cette thèse, mais nous paraît intéressante. Lorsque E est infini, cela apporterait-il un plus à la logique classique de l'enrichir au moyen d'un quantificateur (voire de plusieurs quantificateurs) par lequel l'image inverse de $\{1\}$ est un ensemble infini, récursif et non cofini dans $\mathbb{B}^E$? Nous pensons que la réponse est affirmative.

1.4 Correction, complétude et cohérence

1.4.1 Théorie correcte et complète

Une théorie est sensée permettre de déduire syntaxiquement les formules valides dans tous les modèles qu'elle représente. Il est évidemment primordial de ne déduire que des théorèmes qui sont vrais. Ceci motive les définitions 1.4.1 et 1.4.2.

Définition 1.4.1. Une théorie $\mathcal{T} = (\mathcal{S}, A, I)$ est *correcte* si et seulement si toute formule de $\mathcal{S}$ qui est un théorème dans $\mathcal{T}$ est une vrai dans $\mathcal{T}$.

Vérifier qu'une théorie est correcte revient à vérifier que l'image d'un uplet arbitraire de théorèmes par une règle d'inférence est vrai dans la théorie.

Définition 1.4.2. Une théorie est *complète* si et seulement si toute formule de $\mathcal{S}$ qui est vrai dans $\mathcal{T}$ est une théorème de $\mathcal{T}$.

1.4.2 Théorie cohérente

Nous pourrions intuitivement être tenté de dire qu'une théorie correcte et complète est idéale pour étudier les modèles qu'elle représente. En fait, il n'en est rien : il reste encore un piège à éviter. Imaginons en effet que nous acceptions comme axiome d'une théorie $\mathcal{T} = (\mathcal{S}, A, I)$ une formule de $\mathcal{S}$ qui n'est valide dans aucune structure mathématique sur $\mathcal{S}$ (c'est le cas de la formule $(\varphi \wedge \neg\varphi)$, quelle que soit la formule φ, par exemple). La théorie $\mathcal{T}$ n'aurait alors aucun modèle, si bien que toutes ses formules seraient valides et non valides dans chacun de ses modèles et donc seraient toutes vraies et fausses à la fois. Une telle structure serait donc correcte par définition, mais, même si elle était aussi complète (ce serait le cas à condition d'avoir assez d'axiomes et de règles d'inférence), elle n'aurait aucun intérêt : ce serait comme étudier les propriétés des moutons à cinq pattes. Il n'est donc pas raisonnable d'étudier une théorie pour laquelle il n'existe aucune structure mathématique satisfaisant tout axiome de la théorie. De plus, une théorie sans formule n'est pas raisonnable non plus : elle serait inutile, mais en plus toutes ses formules y seraient à la fois vraies et fausses. Il est donc nécessaire de s'assurer de l'existence d'une formule atomique avec l'existence d'une relation syntaxique. Ceci motive la définition 1.4.3.

Définition 1.4.3. Une théorie $\mathcal{T} = ((V, R, R_f, R_c, C, Q), A, I)$ est *cohérente* (ou *consistante*) si elle admet un modèle sur $\mathcal{S}$ et si $R \neq \emptyset$.

Posséder au moins un modèle garantit à une théorie qu'aucune de ses formules n'est simultanément vraie et fausse.

Chapitre 2

Théorie classique du premier ordre

Les théories $\mathcal{T} = (\mathcal{S}, A, I)$ dont nous avons parlé au chapitre 1 sont toutes des théories du premier ordre, c'est-à-dire des théories pour lesquelles il n'est permis de lier à des quantificateurs que des variables syntaxiques (et pas des objets plus compliqués, tels que des ensembles, par exemple), mais elles sortent du cadre des théories classiques en ce sens que nous n'avons imposé presque aucune règle sur les connecteurs et quantificateurs présents dans $\mathcal{S}$, sur les axiomes présents dans A et sur les règles d'inférence présentes dans I.

Dans le présent chapitre, nous définissons d'abord les théories classiques du premier ordre et énonçons le théorème de complétude de Gödel sans le démontrer. Ensuite, nous sortons brièvement du cadre des théories du premier ordre pour construire un modèle de $\mathbb{N}$ et nous mettons en évidence deux théories classiques particulières : celle de Presburger et celle de Peano. Ensuite, nous énonçons, sans la démontrer, une version renforcée du premier théorème d'incomplétude de Gödel. Finalement, nous abordons les notions de corps fini et d'anneau de polynômes sur un corps fini.

2.1 Théorie classique

Le lecteur intéressé par plus de détails peut consulter l'ouvrage [23].

2.1.1 Axiomes classiques

Dans les définitions 2.1.1, 2.1.2, 2.1.3, les lettres grecques φ, ψ, ζ représentent des formules arbitraires d'une structure syntaxique comprenant au moins les connecteurs $\neg$ et $\rightarrow$.

Définition 2.1.1. L'*affirmation du conséquent* est le schéma d'axiomes

$$\varphi \rightarrow (\psi \rightarrow \varphi).$$

Définition 2.1.2. L'*autodistributivité de l'implication* est le schéma d'axiomes

$$(\varphi \to (\psi \to \zeta)) \to ((\varphi \to \psi) \to (\varphi \to \zeta)).$$

Définition 2.1.3. La *contraposition converse* est le schéma d'axiomes

$$(\neg\varphi \to \neg\psi) \to (\psi \to \varphi).$$

Les noms des schémas d'axiomes des définitions 2.1.4 et 2.1.5 ne sont pas officiels.

Définition 2.1.4. Soit $\mathcal{S}$ est une structure syntaxique comprenant au moins le connecteur $\to$ et le quantificateur universel $\forall$. La *particularité* est le schéma d'axiomes

$$\forall x\varphi \to \varphi(x := t)$$

où φ est une formule de $\mathcal{S}$, t un terme de $\mathcal{S}$ et x une variable syntaxique de $\mathcal{S}$ pour lesquels chaque occurence libre de la variable syntaxique x dans la formule φ serait encore libre dans la formule φ si elle était remplacée par une quelconque variable syntaxique ayant une occurence dans le terme t, et où la notation $\varphi(x := t)$ signifie que toutes les occurences libres de la variable syntaxique x sont remplacées par le terme t dans la formule φ.

Définition 2.1.5. Soit $\mathcal{S}$ est une structure syntaxique comprenant au moins le connecteur $\to$ et le quantificateur universel $\forall$. La *pseudo-liberté de l'antécédent* est le schéma d'axiomes

$$\forall x(\varphi \to \psi) \to (\varphi \to \forall x\psi)$$

où φ, ψ sont des formules de $\mathcal{S}$ et x une variable syntaxique de $\mathcal{S}$ qui ne possède pas d'occurrence libre dans la formule φ.

2.1.2 Règles d'inférence classiques

Dans les définitions 2.1.6 et 2.1.7, les lettres grecques φ, ψ représentent des formules arbitraires d'une structure syntaxique comprenant au moins les connecteurs $\neg$ et $\to$, ainsi que le quantificateur universel $\forall$.

Définition 2.1.6. Le *modus ponens* est la règle d'inférence qui consiste à déduire le théorème ψ à partir des deux théorèmes $(\varphi \to \psi)$ et φ.

Définition 2.1.7. La *règle de généralisation* est la règle d'inférence qui consiste à déduire le théorème $(\forall x\varphi)$ à partir du théorème φ.

2.1.3 Théories classiques

Définition 2.1.8. Une *théorie classique* est une théorie $\mathcal{T} = (\mathcal{S}, A, I)$ pour laquelle :
- la structure syntaxique $\mathcal{S} = (V, R, R_f, R_c, C, Q)$ est telle que $C = \{\neg, \rightarrow\}$ et $Q = \{\forall\}$,
- les axiomes de A sont au moins ceux compris dans l'affirmation du conséquent, l'autodistributivité de l'implication, la contraposition converse, la particularité ou la pseudo-liberté de l'antécédent.
- les règles d'inférence de I sont exactement le modus ponens et la règle de généralisation.
Les autres axiomes de $\mathcal{T}$ sont appelés les *axiomes purs de* $\mathcal{T}$.

Il ne faut pas penser trop vite qu'imposer les connecteurs et certains schémas d'axiomes à une théorie soit très restrictif. En effet, *primo*, vu la proposition 1.3.21, les connecteurs $\neg$ et $\rightarrow$ sont sémantiquement suffisants pour définir n'importe quels connecteurs. Les théories classiques ne se veraient donc pas enrichies si d'autres connecteurs leur étaient ajoutés car il suffirait de rajouter des axiomes jouant uniquement le rôle de définition pour ces nouveaux connecteurs (par exemple, les deux schémas d'axiomes $(\varphi \vee \psi) \rightarrow (\neg\varphi \rightarrow \psi)$ et $(\neg\varphi \rightarrow \psi) \rightarrow (\varphi \vee \psi)$ définissent sémantiquement le connecteur $\vee$ à partir des seuls connecteurs $\neg$ et $\rightarrow$, et ne changent pas la valeur de la théorie). *Secundo*, les axiomes imposés ont en fait un rôle purement logique et correspondent aux règles de la déduction naturelle du mathématicien. D'ailleurs, la proposition 2.1.9 en témoigne bien.

Par contre, nous avons un avis personnel assez pessimiste sur la restriction consistant à utiliser uniquement le quantificateur universel, même si le quantificateur existentiel peut facilement être redéfini à partir de celui-ci et de la négation. Ceci est en rapport avec la remarque 1.3.24 et il est plus facile de comprendre notre avis (qu'il soit partagé ou pas) dans le contexte de cette remarque-là. Nous pensons qu'il est possible de rendre la logique classique plus riche et plus puissante avec des quantificateurs supplémentaires.

Proposition 2.1.9. *Si $\mathcal{T} = (\mathcal{S}, A, I)$ est une théorie classique, alors :*
- tout axiome non pur de $\mathcal{T}$ est valide dans toute structure mathématique sur $\mathcal{S}$,
- les règles d'inférence de $\mathcal{T}$ n'engendrent que des formules valides dans tout modèle de $\mathcal{T}$ quand elles ne sont appliquées qu'à des théorèmes.

Démonstration. C'est très facile pour l'affirmation du conséquent, d'autodistributivité de l'implication et la contraposition converse car aucun quantificateur n'y apparaît : il suffit de faire une table de vérité, c'est-à-dire d'envisager les deux interprétations possibles (0 ou 1) de chaque formule apparaissant dans le schéma d'axiomes dont il est question. Cela fait 4 ou 8 cas selon

le schéma d'axiomes considérés, et chaque interprétation des variables de $\mathcal{S}$ dans chaque structure mathématique sur $\mathcal{S}$ correspond à un de ces cas-là. Tout marche bien.

Pour la particularité, si une interprétation τ des variables de la structure syntaxique $\mathcal{S}$ dans une structure mathématique $\mathcal{M}$ sur $\mathcal{S}$ ne satisfait pas la formule $\forall x\varphi \to \varphi(x := t)$, cela signifie que la formule $\forall x\varphi$ est satisfaite par τ dans $\mathcal{M}$ et que la formule $\varphi(x := t)$ n'est pas satisfaite par τ dans $\mathcal{M}$. Mais alors, cela signifie d'une part que la formule φ est satisfaite dans $\mathcal{M}$ par toute interprétation des variables de $\mathcal{S}$ ne différant de τ que par la valeur attribuée à la variable syntaxique x, et d'autre part (c'est ici qu'intervient l'hypothèse propre à notre schéma d'axiomes, sur les variables du terme t) que la formule φ est insatisfaite par τ dans $\mathcal{M}$ pour celle de ces interprétations qui prend la valeur t_τ en x, ce qui est impossible !

Pour la pseudo-liberté de l'antécédent, si une interprétation τ des variables de $\mathcal{S}$ dans une structure mathématique $\mathcal{M}$ sur $\mathcal{S}$ ne satisfait pas la formule $\forall x(\varphi \to \psi) \to (\varphi \to \forall x\psi)$, cela signifie que la formule $\forall x(\varphi \to \psi)$ est satisfaite par τ dans $\mathcal{M}$ et que la formule $(\varphi \to \forall x\psi)$ n'est pas satisfaite par τ dans $\mathcal{M}$. Mais ceci revient à satisfaire la formule $(\varphi \to \psi)$ dans $\mathcal{M}$ quelle que soit l'interprétation des variables de $\mathcal{S}$ ne différant de τ que par la valeur attribuée à la variable syntaxique x, alors que la formule φ devrait être satisfaite dans $\mathcal{M}$ par chacune de ces interprétations-là (en effet, la variable syntaxique x ne possède pas d'occurence libre dans la formule φ) et que la formule ψ devrait être non satisfaite dans $\mathcal{M}$ pour au moins une de ces interprétations-là, ce qui est impossible !

Pour le modus ponens, il suffit de faire une récurrence sur la longueur d'une preuve dans laquelle la formule ψ est déduite par modus ponens à partir des deux formules φ et $(\varphi \to \psi)$. Par hypothèse de récurrence (acceptable vu que, par définition, tous les axiomes sont valides dans tout modèle de la théorie $\mathcal{T}$), nous pouvons supposer que les théorèmes φ et $(\varphi \to \psi)$ sont valides dans tout modèle de $\mathcal{T}$. Il est alors évident que la formule ψ ne peut être que valide dans tout modèle de $\mathcal{T}$.

Pour la règle de généralisation, si une formule φ est valide dans tout modèle de $\mathcal{T}$, alors elle est satisfaite pour toute interprétation des variables de $\mathcal{S}$ dans tout modèle de $\mathcal{T}$, mais alors par définition la formule $\forall x\varphi$ est également satisfaite pour toute interprétation des variables de $\mathcal{S}$ dans tout modèle de $\mathcal{T}$, et donc cette dernière est valide dans tout modèle de $\mathcal{T}$. □

2.1.4 Complétude

Le théorème 2.1.10, que nous donnons sans démonstration, est le célèbre théorème de complétude de Gödel, valable pour toute théorie classique du premier ordre. Il prouve que chaque théorie classique est adéquate pour étudier syntaxiquement tous ses modèles de façon correcte et complète. Une démonstration de ce théorème se trouve dans le livre [23].

Théorème 2.1.10. *Si $\mathcal{T} = (\mathcal{S}, A, I)$ est une théorie classique, alors une formule arbitraire de $\mathcal{S}$ est un théorème de $\mathcal{T}$ si et seulement si elle est valide dans tout modèle de $\mathcal{T}$.*

2.2 Théories relatives à $\mathbb{N}$

2.2.1 Théorie Z

Dans cette sous-section, nous énumérons rapidement les axiomes de la *théorie **Z***. C'est une théorie des ensembles et elle sort du cadre des théories du premier ordre : chaque variable de cette théorie est un ensemble et si a et b sont deux ensembles, la relation $a \in b$ signie que a est un élément de b. Il est nécessaire de se placer dans une théorie de ce genre pour définir l'ensemble $\mathbb{N}$ des entiers naturels de façon rigoureuse, c'est-à-dire sans s'exposer davantage à un paradoxe mathématique que la théorie **Z** elle-même ne s'y expose. La théorie **ZFC** (Zermelo-Fraenkel-Skolem (axiome du choix)) est donnée dans le livre [23]. Elle est une extension[1] de la théorie **Z** (Zermelo).

Définition 2.2.1. L'*axiome d'extensionnalité*

$$\forall a \forall b (\forall x (x \in a \leftrightarrow x \in b) \rightarrow a = b)$$

signifie que si deux ensembles a et b ont les mêmes éléments, alors ils sont égaux.

Définition 2.2.2. L'*axiome de la paire*

$$\forall a \forall b \exists c \forall x (x \in c \leftrightarrow (x = a \vee x = b))$$

signifie que si a et b sont deux ensembles, alors le couple $c = \{a, b\}$ est aussi un ensemble.

Définition 2.2.3. L'*axiome de la réunion*

$$\forall a \exists b \forall c (c \in b \leftrightarrow \exists d (d \in a \wedge c \in d))$$

signifie que si a est un ensemble, alors l'union $b = \cup a$ de a, formé en regroupant tous les éléments de tous les éléments de a, est aussi un ensemble.

[1] Elle comporte simplement davantage d'axiomes, mais nous n'en avons pas besoin ici

Définition 2.2.4. L'*axiome de l'ensemble des parties*

$$\forall a \exists b \forall x (x \in b \leftrightarrow \forall y (y \in x \rightarrow y \in a))$$

signifie que si a est un ensemble, alors $b = \wp(a)$ est aussi un ensemble. L'ensemble $\wp(a)$ est appelé *ensemble des parties de* a.

Définition 2.2.5. L'*axiome de l'ensemble vide*

$$\exists a \forall b \neg (b \in a)$$

signifie qu'il existe un ensemble a sans élément. Nous notons $\emptyset$ cet ensemble qui est forcément unique vu l'ensemble d'extentionnalité.

Définition 2.2.6. L'*axiome de l'infini*

$$\exists a (\emptyset \in a \wedge \forall x (x \in a \rightarrow x \cup \{x\} \in a))$$

signifie qu'il existe un ensemble a (forcément infini) auquel appartiennent l'ensemble vide $\emptyset$ et tous les ensembles de la forme $x \cup \{x\}$ pour $x \in a$.

Définition 2.2.7. Le *schéma d'axiomes de compréhension*

$$\forall x_1 \cdots \forall x_n \forall a \exists b \forall x_0 (x_0 \in b \leftrightarrow x_0 \in a \wedge \varphi(x_0, x_1, \ldots x_n))$$

signifie que si a est un ensemble et $\varphi[x_0, x_1, \ldots, x_n]$ est une formule de la théorie **Z**, alors pour tout $(x_1, \ldots, x_n)$, $b = \{x_0 \in a : (x_0, x_1, \ldots, x_n) \text{ satisfait } \varphi\}$ est un ensemble.

2.2.2 Définition de $\mathbb{N}$

Les structures de Dedekind-Peano sont abordées dans le livre [23], mais de façon non formelle, l'introduction des théories du second ordre (telles que **Z** ou **ZFC**) venant seulement par la suite.

Définition 2.2.8. Une *structure de Dedekind-Peano* est la donnée d'un triplet (E, e, f) pour lequel E est un ensemble, f une fonction injective de E dans E et e un élément de l'ensemble $E \setminus \{f(x) : x \in E\}$ tels que l'unique sous-ensemble F de E vérifiant les relations $e \in F$ et $\{f(x) : x \in F\} \subseteq F$ est E.

Proposition 2.2.9. *Il existe au moins une structure de Dedekind-Peano.*

Démonstration. Plaçons-nous dans le cadre de la théorie **Z**. Choisissons e égal à l'ensemble vide $\emptyset$ dont l'existence est assurée par l'axiome de l'ensemble vide. Notons $\varphi[x]$ la formule $e \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x)$. D'après l'axiome de l'infini, il existe au moins un ensemble I vérifiant la formule φ. L'intersection E de tous les ensembles vérifiant la formule φ est donc un

ensemble : elle peut en effet être construite grâce à l'axiome de compréhension appliqué à l'ensemble I et à la formule $\forall x(\varphi(x) \to b \in x)$ dont b est la seule variable libre. Comme e est un élément de chaque ensemble satisfaisant la formule φ, e est un élément de leur intersection E. Considérons la fonction $f : E \to E,\ x \mapsto x \cup \{x\}$. Comme un ensemble de la forme $f(x) = x \cup \{x\}$ n'est jamais vide, e appartient bien à l'ensemble $E \setminus \{f(x) : x \in E\}$. Si F est une partie de E vérifiant les relations $e \in F$ et $\{f(x) : x \in F\} \subseteq F$, alors F est égal à E (sinon F serait un ensemble strictement inclus dans E et vérifiant la formule φ, ce qui est impossible). L'injectivité de la fonction f sur E découle directement du fait que les éléments de E sont tous des ensembles finis possédant deux à deux un nombre d'éléments différents, et que donc l'égalité $x \cup \{x\} = y \cup \{y\}$ implique l'égalité $x = y$. Nous venons de construire une structure de Dedekind-Peano (E, e, f). □

Définition 2.2.10. Deux structures (E_1, e_1, f_1) et (E_2, e_2, f_2) de Dedekind-Peano sont *isomorphes* s'il existe une bijection f de E_1 dans E_2 pour laquelle les fonctions $f \circ f_1$ et $f_2 \circ f$ sont identiques.

Proposition 2.2.11. *Toutes les structures de Dedekind-Peano sont isomorphes.*

Démonstration. Considérons deux structures de Dedekind-Peano (E_1, e_1, f_1) et (E_2, e_2, f_2). Définissons la fonction f sur $\{e_1\} \cup \{f_1(x) : x \in E_1\}$ par

$$f(e_1) = e_2 \wedge \forall x \forall y[x \in E_1 \wedge y \in E_2 \wedge f(x) = y \to f(f_1(x)) = f_2(y)].$$

Ceci est licite car f_1 est une injection de E_1 dans $E_1 \setminus \{e_1\}$. De plus, f est injectif car f_2 est une injection de E_2 dans $E_2 \setminus \{e_2\}$. Ensuite, le fait que la fonction f est définie partout sur E_1 découle du fait qu'elle est définie sur un sous-ensemble F_1 de E_1 pour lequel $e_1 \in F_1$ et $\{f_1(x) : x \in F_1\} \subseteq F_1$ (or, le seul sous-ensemble de E_1 de ce type est E_1 lui-même). Finalement, la surjectivité de f est prouvée grâce au fait que l'ensemble $\{f(x) : x \in E_1\}$ est un sous-ensemble F_2 de E_2 pour lequel $e_2 \in F_2$ et $\{f_2(y) : y \in F_2\} \subseteq F_2$ (or, le seul sous-ensemble de E_2 de ce type est E_2 lui-même). Tout ceci prouve que (E_1, e_1, f_1) et (E_2, e_2, f_2) sont isomorphes. □

Nous représentons l'unique structure de Dedekind-Peano (à isomorphisme près) par le triplet $(\mathbb{N}, 0, s)$ et nous notons $0 = \emptyset$, $1 = s(0) = 0 \cup \{0\}$, $2 = s(1) = 1 \cup \{1\}$, $3 = s(2) = 2 \cup \{2\}$, $4 = s(3) = 3 \cup \{3\}$, et caetera, les éléments de $\mathbb{N}$. La fonction s est appelée *fonction successeur*.

L'*addition* de $\mathbb{N}$ est l'unique fonction $f : \mathbb{N}^2 \to \mathbb{N}$ vérifiant les deux égalités $f(m, 0) = 0$ et $f(m, s(n)) = s(f(m, n))$ quels que soient $m, n \in \mathbb{N}$. Il est clair que cette définition est licite et qu'elle définit f de manière univoque, comme une fonction de $\mathbb{N}^2$ dans $\mathbb{N}$, et même comme la fonction qui correspond à ce que nous considérons depuis toujours comme l'addition. Nous

notons f sous la forme $+$ et $f(m,n)$ sous la forme $(m+n)$, quels que soient $m,n \in \mathbb{N}$.

La *multiplication* de $\mathbb{N}$ est l'unique fonction $g : \mathbb{N}^2 \to \mathbb{N}$ vérifiant les deux égalités $g(m,0) = 0$ et $g(m,s(n)) = g(m,n) + m$ quels que soient $m,n \in \mathbb{N}$. Il est clair que cette définition est licite et qu'elle définit g de manière univoque, comme une fonction de $\mathbb{N}^2$ dans $\mathbb{N}$, et même comme la fonction qui correspond à ce que nous considérons depuis toujours comme la multiplication. Nous notons g sous la forme $\cdot$ et $g(m,n)$ sous la forme $(m \cdot n)$ ou même sous la forme (mn), quels que soient $m,n \in \mathbb{N}$.

2.3 Arithmétiques de Presburger et de Peano

Dans cette section, nous donnons deux exemples particuliers de théorie classique acceptant un modèle basé sur l'ensemble $\mathbb{N}$. La seconde est une extension de la première et elles nous servent toutes les deux dans la suite de cette thèse. Pour la première, le lecteur désireux d'en savoir davantage peut consulter l'article [47], tandis que pour la seconde, il peut se référer au livre [23]. Précisons, sans rentrer dans les détails, que l'arithmétique de Presburger admet l'élimination des quantificateurs.

2.3.1 Arithmétique de Presburger

Dans la définition 2.3.1, il ne faut pas confondre la relation syntaxique $=$, les fonctions syntaxiques $s, +$ et la constante syntaxique 0 avec les symboles correspondant dans $\mathbb{N}$.

Définition 2.3.1. L'*arithmétique de Presburger* est la théorie classique sur la struture syntaxique

$$\mathcal{S} = (V, \{=\}, \{s, +\}, \{0\}, \{\neg, \to\}, \{\forall\})$$

pour laquelle la relation syntaxique $=$ est binaire et les fonctions syntaxiques s et $+$ sont respectivement unaire et binaire, et dont les axiomes purs sont

donnés par la liste (cinq axiomes et un schéma d'axiomes) :

$$
\begin{array}{ll}
A1. & \forall a \neg (s(a) = 0) \\
A2. & \forall a \exists b (\neg a = 0 \to s(b) = a) \\
A3. & \forall a \forall b (s(a) = s(b) \to a = b) \\
A4. & \forall a (a + 0 = a) \\
A5. & \forall a \forall b (a + s(b) = s(a + b)) \\
S1. & \forall a_1 \ldots \forall a_n \\
 & [\varphi (0, a_1, \ldots, a_n) \\
 & \wedge \\
 & \forall a (\varphi (a, a_1, \ldots, a_n) \to \varphi (s(a), a_1, \ldots, a_n)) \\
 & \to \\
 & \forall a \varphi (a, a_1, \ldots, a_n)] .
\end{array}
$$

Il est clair que l'arithmétique de Presburger admet la structure mathématique $(\mathbb{N}, \{=\}, \{s, +\}, \{0\})$ comme modèle. Les axiomes $A1, A2, A3$ et le schéma d'axiome $S1$, qui correspond au principe de récurrence, décrivent syntaxiquement une fonction qui n'est pas plus exigente que la fonction successeur. Les axiomes $A4$ et $A5$ décrivent syntaxiquement la façon d'obtenir l'addition à partir de la fonction successeur.

Insistons sur le fait que le schéma d'axiome $S1$ est beaucoup plus faible que le fait suivant : l'unique sous-ensemble F de $\mathbb{N}$ vérifiant les deux relations $\emptyset \in F$ et $\{s(m) : m \in \mathbb{N}\} \subseteq F$ est $\mathbb{N}$. En effet, il y a un nombre infini non dénombrable de parties de $\mathbb{N}$ alors qu'il n'y a qu'un nombre infini dénombrable de formules de $\mathcal{S}$.

2.3.2 Arithmétique de Peano

Dans la définition 2.3.2, nous étendons la théorie de l'arithmétique de Presburger en lui rajoutant la multiplication et deux axiomes en rapport avec celle-ci. Seuls les axiomes $A6$ et $A7$ n'étaient pas encore présents dans l'arithmétique de Presburger.

Définition 2.3.2. L'*arithmétique de Peano* est la théorie classique sur la struture syntaxique

$$\mathcal{S} = (V, \{=\}, \{s, +, \cdot\}, \{0\}, \{\neg, \to\}, \{\forall\})$$

pour laquelle la relation syntaxique $=$ est binaire et les fonctions syntaxiques $s, +, \cdot$ sont respectivement unaire, binaire et binaire, et dont les axiomes purs

sont donnés par la liste (sept axiomes et un schéma d'axiomes) :

$$
\begin{array}{ll}
A1. & \forall a \neg (s(a) = 0) \\
A2. & \forall a \exists b (\neg a = 0 \rightarrow s(b) = a) \\
A3. & \forall a \forall b (s(a) = s(b) \rightarrow a = b) \\
A4. & \forall a (a + 0 = a) \\
A5. & \forall a \forall b (a + s(b) = s(a + b)) \\
A6. & \forall a (a \cdot 0 = 0) \\
A7. & \forall a \forall b (a \cdot s(b) = (a \cdot b) + a) \\
S1. & \forall a_1 \ldots \forall a_n \\
 & [\varphi (0, a_1, \ldots, a_n) \\
 & \wedge \\
 & \forall a (\varphi (a, a_1, \ldots, a_n) \rightarrow \varphi (s(a), a_1, \ldots, a_n)) \\
 & \rightarrow \\
 & \forall a \varphi (a, a_1, \ldots, a_n)] .
\end{array}
$$

Il est évident que l'arithmétique de Peano admet la structure mathématique $(\mathbb{N}, \{=\}, \{s, +, \cdot\}, \{0\})$ comme modèle. Les deux axiomes supplémentaires par rapport à l'arithmétique de Presburger, $A6$ et $A7$, décrivent syntaxiquement la façon d'obtenir la multiplication à partir de la fonction successeur et de l'addition.

2.4 Indécidabilité

Nous savons déjà qu'en logique classique une théorie $\mathcal{T} = (\mathcal{S}, A, I)$ étudie syntaxiquement toutes les structures mathématiques sur $\mathcal{S}$ pour lesquelles tous ses axiomes sont valides, c'est-à-dire qu'elle étudie tous ses modèles. Posons-nous à présent la question suivante : étant donné un modèle $\mathcal{M}$ de la théorie $\mathcal{T}$, existe-t-il nécessairement une théorie acceptant $\mathcal{M}$ comme modèle et n'acceptant aucun modèle dans lequel une de ses formules valides dans $\mathcal{M}$ serait non valide ? Kurt Gödel a apporté une réponse définitivement négative à cette question dans son premier théorème d'incomplétude. Dans cette section, nous en donnons une version légèrement améliorée : le théorème de Gödel-Rosser.

2.4.1 Indécidabilité

Définition 2.4.1. Soit $\mathcal{T} = (\mathcal{S}, A, I)$ une théorie classique et φ une formule de la structure syntaxique $\mathcal{S}$. La formule φ est dite *indécidable* dans $\mathcal{T}$ si $\mathcal{T}$ admet au moins un modèle dans lequel la formule φ est valide et au moins un modèle dans lequel la formule φ est non valide.

Il est clair que si φ est une formule indécidable dans une théorie $\mathcal{T}$, alors ni φ ni $\neg\varphi$ n'est un théorème de $\mathcal{T}$.

Définition 2.4.2. Soit $\mathcal{T} = (\mathcal{S}, A, I)$ une théorie classique. La théorie $\mathcal{T}$ est dite *décidable* si aucune formule de $\mathcal{S}$ n'est indécidable dans $\mathcal{T}$. La théorie $\mathcal{T}$ est dite *indécidable* si il existe une formule de $\mathcal{S}$ qui est indécidable dans $\mathcal{T}$.

Remarquons en passant que la décidabilité et l'indécidabilité dont il est question ici sont des notions logiques, c'est-à-dire relevant des systèmes formels de déduction. Il existe aussi une telle notion mais relevant des algorithmes (en acceptant ce mot au sens intuitif du terme). En fait, dès qu'une théorie classique est récursivement axiomatisable et décidable d'un point de vue logique, elle est nécessairement décidable aussi d'un point de vue algorithmique. Avec les théories non classiques, il faudrait faire attention non seulement aux axiomes mais également aux règles d'inférences (ce qui est plus délicat).

2.4.2 Théorème de Gödel-Rosser

Voici enfin le fameux premier théorème d'incomplétude de Gödel-Rosser (2.4.3). Il est extrêmement limitateur : il est valable même (surtout !) en dehors du cadre des théories du premier ordre. Nous le donnons sans démonstration. Le lecteur intéressé peut consulter [27] pour la version originel de Gödel (le second théorème d'incomplétude s'y trouve aussi) et [52] pour la version renforcée de Rosser.

Théorème 2.4.3. *Dans toute théorie récursivement axiomatisable, cohérente et "capable de formaliser l'arithmétique", il est possible de construire un énoncé arithmétique qui ne peut être ni prouvé ni réfuté dans cette théorie.*

Corollaire 2.4.4. *Toute théorie récursivement axiomatisable, cohérente et "capable de formaliser l'arithmétique" est indécidable.*

Corollaire 2.4.5. *L'arithmétique de Peano est une théorie indécidable.*

Remarque 2.4.6. Par facilité, nous parlons parfois de langage et parfois de structure pour désigner des expressions telles que

$$\langle \mathbb{N}, + \rangle,$$

$$\langle \mathbb{N}, +, \mathrm{V_p} \rangle,$$

$$\langle \mathbb{N}, +, \cdot \rangle,$$

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle, \ldots$$

En fait, de telles expressions désignent des structures mathématiques. La troisième (par exemple), $\langle \mathbb{N}, +, \cdot \rangle$, désigne précisément la structure mathématique

$$\mathcal{M} = (\mathbb{N}, \{=\}, \{+, \cdot\}, \emptyset)$$

sur la structure syntaxique

$$\mathcal{S} = (V, \{=\}, \{+, \cdot\}, \emptyset, \{\neg, \rightarrow\}, \{\forall\}).$$

Dans nos développements, la relation binaire d'égalité est volontairement omise dans une écriture de la forme $\langle \mathbb{N}, +, \cdot \rangle$ mais elle fait toujours parti de la structure mathématique considérée.

Lorsque nous disons qu'une formule $\phi(a_1, \ldots, a_n)$ du premier ordre dans le langage $\langle \mathbb{N}, +, \cdot \rangle$ est satisfaite par le n-uplet $(a_1, \ldots, a_n) \in \mathbb{N}^n$, nous voulons dire que $(a_1, \ldots, a_n)$ est un élément de $\mathbb{N}^n$ et que $\phi[x_1, \ldots, x_n]$ est une formule de $\mathcal{S}$ (dont les variables syntaxiques sont $x_1, \ldots, x_n$) qui est satisfaite dans $\mathcal{M}$ par une interprétation arbitraire τ des variables de $\mathcal{S}$ dans $\mathcal{M}$ pour laquelle $\tau(x_1) = a_1, \ldots, \tau(x_n) = a_n$. Nous insistons fortement sur le fait que cette satisfaction ne dépend pas de la restriction de τ à $(V \setminus \{x_1, \ldots, x_n\})$. Nous utilisons parfois des autres connecteurs que ceux prévus par $\mathcal{M}$. Cela n'est qu'un raccourci d'écriture autorisé par la proposition 1.3.21. La même remarque vaut pour l'utilisation du quantificateur existentiel.

2.5 Corps et Anneau

2.5.1 Corps fini

Pour l'ensemble de cette sous-section, nous renvoyons le lecteur désireux d'en apprendre davantage à l'ouvrage encyclopédique [38].

Nous donnons la définition d'un groupe pour nous mettre d'accord sur le choix de la définition retenue, mais les propriétés usuelles des groupes sont sensées connues.

Définition 2.5.1. Un *groupe* est la donnée d'un triplet

$$\mathbb{G} = (G, \circ, e)$$

pour lequel G est un ensemble, $\circ$ est une fonction binaire sur G et e est un élément de G vérifiant les trois propriétés suivantes :
$\forall x, y, z \in G, (x \circ y) \circ z = x \circ (y \circ z)$
$\forall x \in G, e \circ x = x = x \circ e$,
$\forall x \in G, \exists y \in G : x \circ y = e = y \circ x$ (cet élément y est appelé *inverse de* x).
Le groupe $\mathbb{G}$ est dit *commutatif* s'il satisfait en plus la propriété suivante :
$\forall x, y \in G, x \circ y = y \circ x$.
L'élément e est appelé *élément neutre* du groupe.

Il est évident que dans un groupe, il existe un seul élément neutre et que chaque élément du groupe possède un seul inverse.

Définition 2.5.2. Un *corps* est la donnée d'un quintuplet

$$\mathbb{K} = (K, +, \times, 0, 1)$$

pour lequel K est un ensemble, $+, \times$ sont des fonctions binaires sur K et $0, 1$ sont des éléments de K vérifiant les quatre propriétés suivantes :
$(K, +, 0)$ est un groupe commutatif, appelé *groupe additif*,
$(K \setminus \{0\}, \times, 1)$ est un groupe, appelé *groupe multiplicatif*,
$\forall x, y, z \in K, x \times (y + z) = x \times y + x \times z$,
$\forall x, y, z \in K, (x + y) \times z = x \times z + y \times z$.
Le corps $\mathbb{K}$ est dit *commutatif* lorsque le groupe multiplicatif $(K \setminus \{0\}, \cdot, 1)$ est commutatif.

Nous utilisons souvent la notation $\cdot$ pour désigner la fonction $\times$ et $(x \cdot y)$ (voire même xy) pour désigner $(x \times y)$. De plus, nous nous contentons de désigner par K toute la structure $\mathbb{K} = (K, +, \times, 0, 1)$.

Nous nous intéressons aux corps finis, c'est-à-dire à ceux dont le cardinal de l'ensemble K est fini. Il est évident que dans un corps les termes de la suite

$$1\ ,\ 1+1\ ,\ 1+1+1\ ,\ 1+1+1+1\ ,\ \ldots$$

sont deux à deux différents jusqu'à ce que l'un d'entre eux soit égal au neutre additif. En effet, si deux d'entre eux a et b sont égaux, avec b qui comporte plus de symboles 1 que a n'en comporte, alors leur différence est 0 (le neutre additif), et celle-ci s'écrit avec un nombre de symboles 1 strictement inférieur au nombre de symboles 1 utilisés pour écrire b. Dans un corps fini, cette suite doit donc obligatoirement posséder un élément égal à 0. Ceci étant, la définition 2.5.3 est licite.

Définition 2.5.3. La *caractéristique* d'un corps fini est le plus petit entier strictement positif n tel que $\underbrace{1 + \cdots + 1}_{n \text{ termes}} = 0$.

Proposition 2.5.4. *La caractéristique d'un corps fini est un nombre premier.*

Démonstration. Il est facile de vérifier (au moyen des lois de distributivité) que le sous-groupe additif engendré par 1 est stable pour la multiplication. Muni de celle-ci, il est donc un anneau et est même isomorphe à l'anneau $\mathbb{Z}/n\mathbb{Z}$ où le nombre entier strictement positif n est la caractéristique du coprs. Or, il est immédiat que cet anneau est un corps si et seulement si n est un nombre premier. □

Théorème 2.5.5. *Soit p un nombre premier. Tout corps fini K de caractéristique p possède un nombre d'éléments qui est égal à une puissance entière strictement positive du nombre p.*

Démonstration. Le sous-corps engendré par 1 étant isomorphe au corps à p éléments, $\mathbb{Z}/p\mathbb{Z}$, et K étant évidemment un espace vectoriel de dimension finie sur ce sous-corps, si q est la dimension de cet espace vectoriel, alors le nombre d'éléments de K est p^q. □

Le théorème 2.5.7 est très connu depuis 1905 et porte généralement le nom de théorème de Weddenburn. Joseph Weddenburn en a fourni plusieurs démonstrations, toutefois sa première preuve comportait une faille et c'est en réalité Leonard Dickson qui a fourni la première preuve complète de ce théorème. La démonstration que nous en donnons date de 1930 et est due à Ernst Witt. Mentionnons qu'il existe plusieurs autres preuves touchant chacune à un domaine particulier des mathématiques, dont notamment une preuve due à Theodore Kaczynski et utilisant la notion de quaternions généralisés, notion proche du premier exemple connu de corps non commutatif. Bien qu'elle soit très élégante en elle-même, nous n'avons pas choisi cette preuve ici car elle s'appuie sur des théorèmes de la théorie des groupes dont les démonstrations ne sont pas simples à obtenir.

Pour tout $n \in \mathbb{N} \setminus \{0\}$, notons U_n le groupe $\{x \in \mathbb{C} : x^n = 1\}$ des racines complexes n-ième de l'unité et V_n l'ensemble des éléments d'ordre n de U_n.

Définition 2.5.6. Le *n-ième polynôme cyclotomique* est le polynôme ϕ_n défini par

$$\phi_n(x) = \prod_{\alpha \in V_n} (x - \alpha).$$

Théorème 2.5.7. *Tout corps fini est commutatif.*

Démonstration. Soit K un corps fini. Soit $C = \{x \in K : \forall y \in K, xy = yx\}$. Il est facile de vérifier que C est un sous-corps commutatif de K. Le corps K est donc un espace vectoriel de dimension finie sur C. Soit n la dimension de cet espace vectoriel. Notre problème revient à prouver que $n = 1$. Procédons par l'absurde. Supposons donc que $n > 1$. Soit q le nombre d'éléments de C. Le nombre d'éléments de K est donc q^n.

Pour tout $x \in (K \setminus C)$, soit $C_x = \{y \in K : xy = yx\}$. Il est facile de vérifier que C_x est un sous-corps de K. Comme $C \subseteq C_x$, il est clair que C est donc un sous-corps commutatif de C_x et donc que C_x est aussi un espace vectoriel sur le corps C. Notons n_x la dimension de cet espace vectoriel. Le corps C_x possède q^{n_x} éléments. Le groupe multiplicatif du corps C_x est évidemment un sous-groupe du groupe multiplicatif du corps K. Donc, par le théorème de Lagrange, $(q^{n_x} - 1)$ divise $(q^n - 1)$. Or, par la loi du reste, la division du polynôme $(x^n - 1)$ par le polynôme $(x^{n_x} - 1)$ est $(x^r - 1)$ où r est le reste de la division euclidienne de n par n_x. Il est donc nécessaire que n_x divise n.

Il est clair que $(C \setminus \{0\})$ et $(C_x \setminus \{0\})$ sont respectivement le centre et le centralisateur de l'élément x du groupe multiplicatif $(K \setminus \{0\})$. L'équation de classe (supposée connue) s'écrit alors

$$\#(K \setminus \{0\}) = \#(C \setminus \{0\}) + \sum_{x \in \Omega} \#\left((K \setminus \{0\})/(C_x \setminus \{0\})\right),$$

où Ω est un ensemble comprenant un représentant de chaque classe de conjugaison des éléments non centraux du groupe multiplicatif $(K \setminus \{0\})$. Par le théorème de Lagrange, il vient donc

$$q^n - 1 = q - 1 + \sum_{x \in \Omega} \frac{q^n - 1}{q^{n_x} - 1}. \tag{2.1}$$

Par ailleurs, il vient aussi :

$$x^n - 1 = \prod_{\alpha \in U_n} (x - \alpha) = \prod_{d|n} \prod_{\alpha \in V_d} (x - \alpha) = \prod_{d|n} \phi_d(x).$$

Vu l'égalité $x^n - 1 = \prod_{d|n} \phi_d(x)$, une récurrence sur n prouve immédiatement que les polynômes cyclotomiques sont des polynômes à coefficients entiers dont le terme indépendant vaut 1 ou -1.

Pour tout diviseur propre m du nombre n, il vient :

$$\begin{aligned} q^n - 1 &= \prod_{d|n} \phi_d(q) \\ &= \phi_n(q) \prod_{\substack{m<d \\ d<n \\ d|n}} \phi_d(q) \prod_{d|m} \phi_d(q) \\ &= \phi_n(q) \prod_{\substack{m<d \\ d<n \\ d|n}} \phi_d(q)(q^m - 1). \end{aligned}$$

De ceci, nous déduisons que pour tout diviseur propre m de n, le nombre $\frac{q^n-1}{q^m-1}$ est entier et est divisible par le nombre $\phi_n(q)$. Mais alors, à cause de l'égalité (2.1), le nombre $\phi_n(q)$ divise nécessairement le nombre $(q-1)$.

Considérons un nombre z tel que $z \in V_n$. Puisque $n \neq 1$, nous avons $\mathfrak{Re}(z) < 1$ et il vient donc :

$$\begin{aligned} |q - z|^2 &= (q - \mathfrak{Re}(z))^2 + (-\mathfrak{Im}(z))^2 \\ &= q^2 - 2q\mathfrak{Re}(z) + (\mathfrak{Re}(z))^2 + (\mathfrak{Im}(z))^2 \\ &= q^2 - 2q\mathfrak{Re}(z) + 1 \\ &> q^2 - 2q + 1 \\ &= (q-1)^2. \end{aligned}$$

Ceci signifie donc que

$$\begin{aligned} |\phi_n(q)| &= \left| \prod_{\alpha \in V_n} (q - \alpha) \right| \\ &= \prod_{\alpha \in V_n} |q - \alpha| \\ &\geq |q - z| \\ &> q - 1, \end{aligned}$$

ce qui contredit le fait que le nombre $\phi_n(q)$ divise le nombre $(q-1)$. La supposition que $n \neq 1$ est donc absurde. □

Proposition 2.5.8. *Le groupe multiplicatif d'un corps fini est cyclique.*

Démonstration. Considérons un corps fini K de p^q éléments, où p est un nombre premier et q un nombre entier strictement positif. Pour chaque élément non nul x du corps, notons a_x le plus petit entier strictement positif tel que $x^{a_x} = 1$. Le nombre a_x existe, pour la même raison que la caractéristique existe (sauf qu'ici, c'est dans le groupe multiplicatif que les choses se passent, alors qu'il s'agissait du groupe additif pour la caractéristique). Comme le corps est fini, cela a un sens de considérer le plus petit commun multiple a de tous les a_x (pour x variant dans $K \setminus \{0\}$). Il est clair que le polynôme $x^a - 1$ s'annule pour chaque élément x de $K \setminus \{0\}$. Ce polynôme est donc de degré au moins $p^q - 1$, et par conséquent $a \geq p^q - 1$. De plus, le nombre a_x est l'ordre du sous-groupe multiplicatif engendré par x et il divise donc le nombre d'éléments du groupe multiplicatif, c'est-à-dire $p^q - 1$. Mais alors $p^q - 1$ est un multiple commun des a_x, donc aussi de leur plus plus petit commun multiple a, et donc $a \leq p^q - 1$. Au total, $a = p^q - 1$.

Pour conclure, prouvons que le groupe multiplicatif possède un élément d'ordre a. Soient p_i un nombre premier divisant a et n_i le plus grand entier strictement positif tel que $p_i^{n_i}$ divise a (si aucun nombre premier ne divise a, il est facile de prouver que $p = 2$ et que le corps K est isomorphe à $(\mathbb{Z}/2\mathbb{Z})$). Si aucun des nombres a_x n'était divisible par le nombre $p_i^{n_i}$, alors il serait impossible que leur plus petit commun multiple, le nombre a, soit divisible par $p_i^{n_i}$. Il est donc clair qu'il existe $x_i \in K \setminus \{0\}$ et $k_i \in \mathbb{N} \setminus \{0\}$ vérifiant $a_{x_i} = k_i p_i^{n_i}$. Mais alors, en posant $y_i = x_i^{k_i}$, nous obtenons $a_{y_i} = p_i^{n_i}$. Soit $y = \prod_i y_i$ (pour i servant à décrire tous les nombres premiers p_i divisant a). Le nombre a_y est alors le plus petit commun multiple des nombres $p_i^{n_i}$, et donc $a_y = a$. L'élément y est donc un générateur du groupe multiplicatif et ce dernier est donc cyclique. □

Dans la suite de ces notes, nous notons généralement un corps fini arbitraire sous la forme $\mathbb{F}$.

2.5.2 Anneau de polynômes sur un corps fini

Dans la suite ce ces notes, nous notons $\mathbb{F}[X]$ l'ensemble

$$\{0 \in \mathbb{F}\} \cup \{a_n X^n + \cdots + a_1 X + a_0 : n \in \mathbb{N},\ a_0, a_1, \ldots a_n \in \mathbb{F},\ a_n \neq 0\}$$

des polynômes sur le corps $\mathbb{F}$, où X est le monôme sur $\mathbb{F}$ qui est du premier degré et dont le coefficient est le neutre multiplicatif du corps $\mathbb{F}$. Le *degré* d'un polynôme $A \in \mathbb{F}[X]$ est noté $\deg(A)$. Avec les notations de l'ensemble ci-dessus, si $A \neq 0$, alors $\deg(A) = n$. De plus, $\deg(0) = -\infty$. Pour tout $n \in (\mathbb{N} \cup \{-\infty\})$, nous désignons par $\mathbb{F}[X]_{>n}$ l'ensemble des polynômes de $\mathbb{F}[X]$ dont le degré est strictement supérieur à n. De même, nous désignons par $\mathbb{F}[X]_{<n}$ l'ensemble des polynômes de $\mathbb{F}[X]$ dont le degré est strictement inférieur à n. Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, nous notons $P^{\mathbb{N}}$ l'ensemble $\{P^n : n \in \mathbb{N}\}$ des puissances du polynôme P.

Définition 2.5.9. La relation $\prec$ est la relation binaire sur $\mathbb{F}[X]$ telle que $A \prec B$ si et seulement si $\deg(A) < \deg(B)$.

La définition 2.5.10 introduit les relations $\preceq$, $\succ$, $\succeq$ et $\approx$ qui sont en fait des relations de comparaison du degré de deux polynômes.

Définition 2.5.10. Les relations binaires $\preceq$, $\succ$, $\succeq$ et $\approx$ sont successivement définies sur l'ensemble $\mathbb{F}[X]$ par :

$$\begin{aligned}
A \preceq B &\Leftrightarrow A = 0 \ \vee\ A \prec B \cdot X,\\
A \succ B &\Leftrightarrow \neg(A \preceq B),\\
A \succeq B &\Leftrightarrow \neg(A \prec B),\\
A \approx B &\Leftrightarrow A \preceq B \ \wedge\ A \succeq B,
\end{aligned}$$

où $B \cdot X$ représente la multiplication du polynôme B par le monôme X.

Proposition 2.5.11. *Pour tout $P \in \mathbb{F}[X]_{>0}$, les relations $\prec$ et $\succ$ sont des relations d'ordre total strict sur l'ensemble $P^{\mathbb{N}}$. Pour tout $P \in \mathbb{F}[X]_{>0}$, les relations $\preceq$ et $\succeq$ sont des relations d'ordre total non strict sur l'ensemble $P^{\mathbb{N}}$.*

Démonstration. Cela résulte du fait que l'ensemble $P^{\mathbb{N}}$ ne possède pas deux polynômes de même degré lorsque $\deg(P) \geq 1$. □

Deuxième partie

Ensembles définissables et ensembles reconnaissables

Dans cette partie, sauf mention explicite du contraire, nous considérons que n est toujours un nombre entier strictement positif lorqu'il est présent dans une expression de la forme $\mathbb{N}^n$ ou $(\mathbb{F}[X])^n$.

Tout au long de cette partie, nous travaillons en parallèle dans le cadre de $\mathbb{N}$ et dans le cadre de $\mathbb{F}[X]$. Insistons à nouveau sur le fait qu'il y a de fortes analogies entre ces deux cadres pour beaucoup de notions et que le lecteur habitué à celles-ci dans $\mathbb{N}$ peut franchement ne s'intéresser qu'au cadre de $\mathbb{F}[X]$. D'ailleurs, sauf mention explicite du contraire, cette introduction de deuxième partie se consacre seulement à $\mathbb{F}[X]$.

Dans le chapitre 3, nous définissons une fonction, $\mathrm{V_P}$, basée sur un polynôme $P \in \mathbb{F}[X]_{>0}$. Celle-ci joue un rôle essentiel dans la suite de cette thèse. Dans la seconde section de ce chapitre, nous montrons que cette fonction permet de construire une autre fonction qui détermine si un polynôme possède ou pas un coefficient donné à une puissance donnée de son développement en base P. C'est l'une des clefs qui conduisent à une caractérisation logique (au chapitre 5) du caractère reconnaissable d'un ensemble de polynômes dans la base P.

Dans le chapitre 4, nous définissons les automates finis déterministes et les ensembles reconnaissables dans une base P de degré au moins 1. Des exemples sont donnés et nous démontrons que la relation d'égalité, l'addition, la multiplication par une constante, la relation d'ordre $\prec$, la fonction $\mathrm{V_P}$ et d'autres relations utiles sont P-reconnaissables.

Dans le chapitre 5, nous fournissons une caractérisation logique des ensembles P-reconnaissables. C'est une adaptation au cadre de $\mathbb{F}[X]$ du théorème de Büchi-Bruyère (voir [11]). Rappelons que ceci est l'une de nos contributions personnelles et qu'il nous a fallu déterminer la structure adéquate permettant une telle caractérisation.

Le chapitre 6 est réservé aux ensembles reconnaissables simultanément dans toutes les bases de degré au moins 1. Aux deux types d'ensembles déjà connus (dans $\mathbb{N}$, il n'y a qu'un seul type de tels ensembles), nous ajoutons un troisième que nous avons découvert. Nous montrons bien entendu que ceux-ci ne sont pas des combinaisons booléennes des deux autres types d'ensembles déjà connus. Nous conjecturons que tous les ensembles reconnaissables sont des combinaisons booléennes d'ensembles pris dans ces trois catégories élémentaires. Nous développons aussi l'aspet logique pour voir quelle structure pourrait décrire les ensembles reconnaissables. Quelques propriétés supplémentaires sont données.

Le chapitre 7 est consacré au théorème de Cobham. Nous étudions d'abord

le caractère syndétique d'un ensemble de nombres naturels et nous montrons qu'une partie infinie de $\mathbb{N}$ qui est p-reconnaissable et q-reconnaissable est syndétique (pour p et q multiplicativement indépendants). Nous conseillons au lecteur de lire cette démonstration qui est une contribution personnelle (pas pour le résultat en lui-même, qui était déjà connu, mais plutôt pour sa preuve qui est élégante et peut venir à point dans une preuve classique du théorème de Cobham). Nous définissons la notion équivalente dans $\mathbb{F}[X]$ et nous expliquons pourquoi notre preuve ne s'adapte pas à ce contexte. Dans la deuxième section, nous abordons la notion de noyau et de P-noyau d'une partie de $\mathbb{F}[X]$. Nous caractérisons les ensembles reconnaissables en base P comme étant ceux dont le P-noyau est fini et nous conjecturons que ceux qui sont reconnaissables dans toutes les bases sont ceux dont le noyau est fini. La troisième section est consacrée au caractère P-automatique et la quatrième à la fonction de complexité d'une suite sur un alphabet Σ indicée dans $\mathbb{F}[X]$ (c'est-à-dire d'une fonction de $\mathbb{F}[X]$ dans Σ). Finalement, dans la cinquième section nous démontrons le théorème de Cobham dans $\mathbb{N}$ et nous expliquons pourquoi nous ne parvenons pas à le démontrer dans $\mathbb{F}[X]$ pour le moment.

Chapitre 3

Ensemble définissable

3.1 Ensemble reconnaissable dans une base

3.1.1 Cas de $\mathbb{N}$

Pour tout entier p strictement supérieur à 1, nous notons $p^{\mathbb{N}}$ l'ensemble $\{p^n : n \in \mathbb{N}\}$ des puissances du nombre p. Pour tout entier p strictement supérieur à 1 et pour toute partie finie et non vide $\mathcal{N}$ de $p^{\mathbb{N}}$, nous désignons respectivement par $\max\mathcal{N}$ et $\min\mathcal{N}$ le plus grand et le plus petit élément de de $\mathcal{N}$.

Si p est un nombre entier strictement supérieur à 1 et si $a \in \mathbb{N}$ est non nul, alors l'ensemble

$$\left\{b \in \ p^{\mathbb{N}} : a \equiv 0 \pmod{b}\right\}$$

est une partie finie et non vide de $p^{\mathbb{N}}$. La définition 3.1.1 a donc un sens. La fonction $\mathrm{V_p}$ dont il y est question associe en fait à chaque nombre non nul la plus grande puissance de p qui le divise.

Définition 3.1.1. Pour tout nombre entier p strictement supérieur à 1, la *fonction* $\mathrm{V_p}$ est définie par

$$\begin{aligned} \mathrm{V_p} \quad : \quad & \mathbb{N} \to p^{\mathbb{N}}, \\ & a \mapsto \max\left\{b \in p^{\mathbb{N}} : a \equiv 0 \pmod{b}\right\} \text{ si } a \neq 0, \\ & 0 \mapsto 1. \end{aligned}$$

Définition 3.1.2. Pour tout nombre entier p strictement supérieur à 1, une *partie p-définissable* de $\mathbb{N}^n$ est une partie $\mathcal{N}$ de $\mathbb{N}^n$ pour laquelle il existe une formule $\phi(a_1, \ldots, a_n)$ du premier ordre dans le langage[1]

$$\langle \mathbb{N}, +, \mathrm{V_p} \rangle,$$

[1] Voir la remarque 2.4.6

qui est satisfaite si et seulement si le n-uplet $(a_1, \ldots, a_n)$ appartient à $\mathcal{N}$.

Définition 3.1.3. Pour tout entier p strictement supérieur à 1, une *relation n-aire p-définissable* est une relation d'arité n sur $\mathbb{N}$ qui est une partie p-définissable de $\mathbb{N}^n$.

Remarquons que comme toute fonction de $\mathbb{N}^m$ dans $\mathbb{N}^n$ est en fait une relation d'arité $(m+n)$ sur $\mathbb{N}$, nous venons également de définir la notion de *fonction p-définissable*, quels que soient $m, n \in \mathbb{N} \setminus \{0\}$.

Précisons également que nous disons volontiers que nous *p-définissons* un ensemble, une relation ou une fonction lorsque nous définissons cet ensemble, cette relation ou cette fonction dans le langage $\langle \mathbb{N}, +, \mathrm{V_p} \rangle$. Il faudra bien entendu veiller à ce que chaque p-définition soit licite.

Par exemple, si $n = 3$ et $p = 11$, alors l'ensemble

$$\{(a, b) \in \mathbb{N}^2 : a \equiv b \pmod 2 \text{ et } a \text{ est une puissance de } 11\}$$

est 11-définissable par la formule

$$\exists m \, (a = b + m + m \vee b = a + m + m) \wedge V_{11}(a) = a$$

du premier ordre dans le langage

$$\langle \mathbb{N}, +, \mathrm{V_p} \rangle.$$

3.1.2 Cas de $\mathbb{F}[X]$

Pour tout $P \in \mathbb{F}[X]$ de degré au moins 1 et pour toute partie finie et non vide $\mathcal{F}$ de $P^{\mathbb{N}}$, nous désignons respectivement par $\max \mathcal{F}$ et par $\min \mathcal{F}$ le polynôme de $\mathcal{F}$ de plus haut degré et le polynôme de $\mathcal{F}$ de plus petit degré.

Remarquons que si $P \in \mathbb{F}[X]_{>0}$ et si $A \in \mathbb{F}[X] \setminus \{0\}$, alors l'ensemble

$$\Big\{ B \in P^{\mathbb{N}} : A \equiv 0 \pmod B \Big\}$$

est une partie finie et non vide de $P^{\mathbb{N}}$. La définition suivante a donc un sens. La fonction $\mathrm{V_P}$ dont il question associe en fait à chaque polynôme non nul la plus grande puissance de P qui le divise.

Définition 3.1.4. Pour tout $P \in \mathbb{F}[X]_{>0}$, la *fonction* $\mathrm{V_P}$ est définie par

$$\begin{array}{rcl} \mathrm{V_P} & : & \mathbb{F}[X] \to P^{\mathbb{N}}, \\ & & A \mapsto \max \Big\{ B \in \ P^{\mathbb{N}} : A \equiv 0 \pmod B \Big\} \text{ si } A \neq 0, \\ & & 0 \mapsto 1. \end{array}$$

La définition 3.1.5 fait intervenir une nouvelle structure qui est assez analogue à la structure $\langle \mathbb{N}, +, \mathrm{V_p} \rangle$, mais qui est adaptée à l'anneau $\mathbb{F}[X]$:

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle.$$

Il est important de remarquer que, *a priori*, nous ne pouvons nous passer ni de la relation d'ordre $\prec$ ni de la multiplication $\cdot C$ par certains polynômes C fixés (nous pourrions toutefois nous contenter des multiplications par un généralteur du groupe multiplicatif $(\mathbb{F} \setminus \{0\})$ et par le monôme X) dans les développements que nous faisons par la suite. Cela est dû à l'absence de report lorsque des additions sont effectuées dans $\mathbb{F}[X]$. Dans $\mathbb{N}$, la raison pour laquelle nous pouvons nous passer de la relation d'ordre $<$ et des multiplications $\cdot c$ par des constantes c est que celles-ci sont définissables à partir de l'addition uniquement comme le prouvent les formules suivantes :

$$a = 0 \Leftrightarrow a + a = a,$$

$$a = 1 \Leftrightarrow V_p(0) = a,$$

$$a < b \Leftrightarrow \exists m(a + m + 1 = b),$$

$$a \cdot c = b \Leftrightarrow \underbrace{a + a + \ldots + a}_{c \text{ termes}} = b.$$

Définition 3.1.5. Pour tout $P \in \mathbb{F}[X]_{>0}$, une *partie P-définissable* de $(\mathbb{F}[X])^n$ est une partie $\mathcal{F}$ de $(\mathbb{F}[X])^n$ pour laquelle il existe une formule $\phi(A_1, \ldots, A_n)$ du premier ordre dans le langage[2]

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle,$$

qui est satisfaite si et seulement si le n-uplet $(A_1, \ldots, A_n)$ appartient à $\mathcal{F}$.

Définition 3.1.6. Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, une *relation n-aire P-définissable* est une relation qui est d'arité n sur $\mathbb{F}[X]$ et qui est une partie P-définissable de $(\mathbb{F}[X])^n$.

Remarquons que comme toute fonction de $(\mathbb{F}[X])^m$ dans $(\mathbb{F}[X])^n$ est en fait une relation d'arité $(m + n)$ sur $\mathbb{F}[X]$, nous venons également de définir la notion de *fonction P-définissable*, quels que soient $m, n \in \mathbb{N} \setminus \{0\}$.

Précisons également que nous disons que nous *P-définissons* un ensemble, une relation ou une fonction lorsque nous définissons cet ensemble, cette relation ou cette fonction dans le langage $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle$. Il faut bien entendu veiller à ce que chaque P-définition soit licite.

[2]Voir la remarque 2.4.6

Par exemple, si $n = 2$, $\mathbb{F} = \mathbb{Z}/4\mathbb{Z}$ et $P = X^3$, alors l'ensemble

$$\{(A, B) \in (\mathbb{Z}_4[X])^2 : A \equiv B + X \pmod{X^2} \text{ et } A \text{ est une puissance de } X^3\}$$

est X^3-définissable par la formule

$$\exists M \left(X^2 \cdot M = \underbrace{A + A + A}_{-A} + B + X \right) \wedge V_{X^3}(A) = A$$

du premier ordre dans le langage

$$\langle \mathbb{Z}/\mathbb{Z}4[X], +, \prec, (\cdot C : C \in \mathbb{Z}_4[X]), V_{X^3} \rangle.$$

Proposition 3.1.7. *Les relations binaires $\preceq$, $\succ$, $\succeq$, $\approx$ sont P-définissables sur $\mathbb{F}[X]$.*

Démonstration. C'est évident puisqu'elles ont en fait été P-définies en 2.5.10. □

3.2 Développement

3.2.1 Cas de $\mathbb{N}$

Pour chaque nombre entier p strictement supérieur à 1, nous notons Σ_p l'ensemble $\{0, 1, \ldots, p-1\}$.

Définition 3.2.1. Soit p un entier strictement supérieur à 1. Le *développement* p-aire d'un nombre entier naturel q est l'unique écriture de ce nombre sous la forme d'une combinaison linéaire $\Sigma_{k=0}^{n} a_k p^k$ de puissances de p à coefficients a_k dans l'ensemble Σ_p, l'éventuel coefficient de plus haut poids a_n étant non nul (le développement p-aire du nombre 0 est la somme sans terme).

Définition 3.2.2. Pour tout entier p strictement supérieur à 1 et pour tout $j \in \Sigma_p$, la relation binaire $X_{p,j}(a, b)$ sur $\mathbb{N}$ est p-définie par la formule :

$$\mathrm{V_p}(a) = a \wedge \exists u \exists v((b = u + a \cdot j + v \wedge u < a) \wedge (a < \mathrm{V_p}(v) \vee v = 0)).$$

Proposition 3.2.3. *Pour tout $a \in p^{\mathbb{N}}$ et tous $b, p \in \mathbb{N}$ tels que $p > 1$, il existe un et un seul $j \in \Sigma_p$ pour lequel la formule $X_{p,j}(a, b)$ est vraie.*

Démonstration. C'est évident : le j dont il est question n'est autre que l'élément de Σ_p qui s'identifie au coefficient de la puissance a dans le développement p-aire du nombre b. □

3.2.2 Cas de $\mathbb{F}[X]$

Pour chaque polynôme P de degré au moins 1, nous notons Σ_P l'ensemble de polynômes $\{Q \in \mathbb{F}[X] : Q \prec P\}$. Un polynôme est donné par une suite de coefficients et ne doit pas être confondu avec la notion de fonction polynomiale. Par exemple, si le corps $\mathbb{F}$ est $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ et si $P = X^4$, alors les polynômes X et X^3 sont deux éléments différents de Σ_{X^4} bien qu'ils aient les mêmes valeurs numériques en chaque point du corps $\{0, 1\}$. Le cardinal de l'ensemble Σ_P est en fait égal à $(\#\mathbb{F})^{\deg(P)}$.

Définition 3.2.4. Soit P un polynôme de degré au moins 1. Le *développement* P-aire d'un polynôme $Q \in \mathbb{F}[X]$ est l'unique écriture de ce polynôme sous la forme d'une combinaison linéaire $\Sigma_{k=0}^{n} A_k P^k$ de puissances de P à coefficients A_k dans l'ensemble Σ_P, l'éventuel coefficient de plus haut poids A_n étant non nul (le développement P-aire du polynôme 0 est la somme sans terme).

Définition 3.2.5. Pour tout $P \in \mathbb{F}[X]_{>0}$ et pour tout $J \in \Sigma_P$, la relation binaire $X_{P,J}(A, B)$ sur $\mathbb{F}[X]$ est P-définie par la formule :

$$\mathrm{V_P}\,(A) = A \wedge \exists U \exists V((B = U + A \cdot J + V \wedge U \prec A) \wedge (A \prec \mathrm{V_P}\,(V) \vee V = 0)).$$

Proposition 3.2.6. *Pour tout $A \in P^{\mathbb{N}}$ et tous $B, P \in \mathbb{F}[X]$ tels que $\deg(P) \geq 1$, il existe un et un seul $J \in \Sigma_P$ pour lequel la formule $X_{P,J}(A, B)$ est vraie.*

Démonstration. C'est évident : le J dont il est question n'est autre que l'élément de Σ_P qui s'identifie au coefficient de la puissance A dans le développement P-aire du polynôme B. □

Chapitre 4

Automate et ensemble reconnaissable

Dans la section 1, nous commençons par définir les automates finis (pas tout à fait au sens général car cela n'est pas nécessaire dans nos développements) et les automates finis déterministes. Nous montrons que les langages acceptés par les automates finis sont ceux acceptés par les automates finis déterministes. Le lecteur intéressé par les automates finis peut consulter le livre [53] de Sakarovitch. Nous conseillons aussi les lectures [24], [**?**] et [39].

Dans la section 2, nous définissons les ensembles reconnaissables dans une base et leurs représentations dans cette base.

Dans la section 3, nous donnons quelques exemples amusants d'ensembles reconnaissables dans une base.

Dans la section 4, nous nous préparons à prouver le théorème du chapitre 5, qui fait le lien entre les caractères logique et reconnaissable, en montrant que les relations et les fonctions de la structure

$$\langle \mathbb{F}[X], + \prec, \mathrm{V_P} \rangle$$

sont P-reconnaissables.

4.1 Automate fini (déterministe)

Définition 4.1.1. Un *alphabet* est un ensemble fini et non vide. Chaque élément d'un alphabet est appelé *lettre*.

Définition 4.1.2. Soit Σ un alphabet. Un *mot* sur Σ est une suite finie

$$a_1 \cdots a_n$$

de lettres $a_1, \ldots, a_n \in \Sigma$. L'ensemble des mots sur Σ est noté Σ^*.

Nous notons parfois le mot $a_1 \cdots a_n$ sous la forme a^n lorsque tous les a_i sont égaux à a. Lorsque cela est clair, nous nous réservons le droit de considérer le mot $a_1 \cdots a_n$ comme un uplet $(a_1, \ldots, a_n) \in \Sigma^n$.

Définition 4.1.3. Soit Σ un alphabet. Un *langage* sur Σ est une partie de Σ^*.

Nous utilisons parfois des raccourcis du genre a^* pour désigner le langage $\{a\}^*$.

Définition 4.1.4. La *longueur* d'un mot m sur un alphabet Σ est le nombre de lettres dont il est formé et est notée $|m|$. Le seul mot de longueur nulle sur un alphabet Σ est appelé le *mot vide* et est noté ε.

Définition 4.1.5. Si $m_1 = a_1 \cdots a_j$ et $m_2 = b_1 \cdots b_k$ sont deux mots sur un alphabet Σ, alors la *concaténation* de ces deux mots (pris dans cet ordre) est le mot $a_1 \cdots a_j b_1 \cdots b_k$ sur Σ et nous le notons $m_1 \cdot m_2$ ou encore $m_1 m_2$.

Il est clair que $m \cdot \varepsilon = m = \varepsilon \cdot m$ pour tout mot m sur l'alphabet Σ.

Définition 4.1.6. Un *automate fini* est la donnée d'un quintuplet

$$(Q, q_0, F, \Sigma, \Delta)$$

pour lequel :
Q est un ensemble fini dont chaque élément est appelé *état*,
q_0 est un des éléments de Q et est appelé *état initial*,
F est une partie de Q et chacun de ses éléments est appelé *état final*,
Σ est un alphabet,
Δ est une relation unaire de $Q \times \Sigma \times Q$ et est appelée *relation de transition*.

Définition 4.1.7. Un *automate fini déterministe* est un automate fini

$$(Q, q_0, F, \Sigma, \Delta)$$

dont la relation de transition Δ est le graphe d'une fonction partielle δ de $Q \times \Sigma$ dans Q. La fonction δ est appelée *fonction de transition*.

Lorsque nous considérons un automate fini déterministe $(Q, q_0, F, \Sigma, \delta)$, nous considérons le plus souvent que δ est sa fonction de transition et non pas le graphe de celle-ci. C'est toujours clairement précisé par le contexte.

Un automate fini $(Q, q_0, F, \Sigma, \Delta)$ peut facilement se représenter par un graphe orienté dont les noeuds correspondent aux états de Q et dont les arcs possèdent un label et représentent la relation Δ. Plus précisément, il existe un arc de label $\sigma \in \Sigma$ partant de l'état $q_1 \in Q$ et aboutissant à l'état $q_2 \in Q$ si et seulement si $(q_1, \sigma, q_2) \in \Delta$. Dans le cas particulier d'un automate fini déterministe $(Q, q_0, F, \Sigma, \delta)$, cette dernière condition peut se noter

$\delta(q_1, \sigma) = q_2$ puisque δ est une fonction de $Q \times \Sigma$ dans Q.

Sur la figure 4.1, nous représentons un automate fini déterministe de trois états par son graphe. L'alphabet de cet automate est $\Sigma = \{a, b\}$. L'état initial q_0 est mis en évidence par une flèche entrante ne provenant d'aucun état et les états finals q_0 et q_1 sont chacun mis en évidence par une flèche sortante n'aboutissant à aucun état. Cet automate accepte en fait le mot vide et les mots commençant par la lettre a et ne comportant pas une seconde lettre a, c'est-à-dire les mots du langage $\{\varepsilon\} \cup \{ab^n : n \in \mathbb{N}\} = \{\varepsilon\} \cup ab^*$, avec les notations précédemment autorisées.

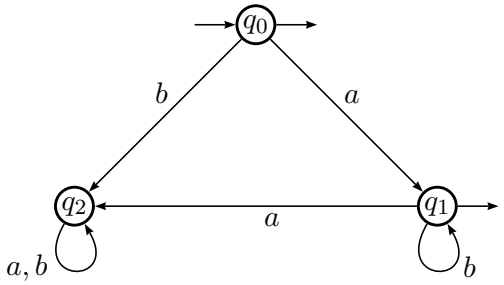

FIG. 4.1 – Exemple d'automate.

Définition 4.1.8. Soit $\mathcal{A} = (Q, q_0, F, \Sigma, \Delta)$ un automate fini. Un mot

$$m = a_1 \cdots a_n$$

de longueur $n > 0$ sur Σ est *accepté* par $\mathcal{A}$ s'il existe un n-uplet d'états $(q_1, \ldots, q_n) \in Q^n$ pour lequel $q_n \in F$ et $(q_{i-1}, a_i, q_i) \in \Delta$ quel que soit $i \in \{1, \ldots, n\}$. Le mot vide ε est *accepté* par $\mathcal{A}$ si l'état initial q_0 est un état final.

Définition 4.1.9. Soient Σ un alphabet et L un langage sur Σ. Un automate fini $(Q, q_0, F, \Sigma, \Delta)$ *accepte* le langage L si L est exactement l'ensemble de tous les mots sur Σ acceptés par cet automate.

Définition 4.1.10. Soit Σ un alphabet et L un langage sur Σ. Le langage L est *régulier* s'il existe un automate fini déterministe $(Q, q_0, F, \Sigma, \delta)$ qui accepte L.

Dans un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma, \delta)$, pour tout état q et tout mot $m = a_1 \cdots a_n$ de longueur $n > 0$ sur Σ, il ne peut exister plus d'un seul n-uplet d'états $(q_1, q_2, \ldots, q_n) \in Q^n$ pour lequel

$$\delta(q, a_1) = q_1, \delta(q_1, a_2) = q_2, \ldots, \delta(q_{n-1}, a_n) = q_n.$$

Remarquons aussi que, quitte à rajouter un *puits*, (un puits est un état non final qu'aucun arc ne quitte pour aboutir à un autre état), ce qui ne change pas le langage accepté par l'automate, nous pouvons considérer que la fonction de transition δ d'un automate fini déterministe $(Q, q_0, F, \Sigma, \delta)$ est partout définie sur l'ensemble $Q \times \Sigma$. Avec ces notations et cette considération, il est alors naturel d'étendre la fonction de transition δ au moyen de l'égalité $\delta(q, m) = q_n$. De plus, nous posons $\delta(q, \varepsilon) = q$. Ainsi, chaque fonction de transition de $Q \times \Sigma$ dans Q peut être vue comme une fonction partielle de $Q \times \Sigma^*$ dans Q.

Le théorème 4.1.11, initialement dû à M. O. Rabin et D. Scott (voir [48]), est fondamental en théorie des automates car il prouve que les automates finis déterministes suffisent à décrire tous les langages acceptés par des automates finis. Notre cadre est d'ailleurs légèrement restreint par rapport au leur.

Théorème 4.1.11. *Soit Σ un alphabet et L un langage sur Σ. Le langage L est régulier si et seulement si il existe un automate fini $(Q, q_0, F, \Sigma, \Delta)$ qui accepte L.*

Démonstration. La condition est évidemment nécessaire, puisque un automate fini déterministe est un automate fini.

Prouvons que la condition est suffisante. Il existe un automate fini qui accepte le langage L. Soit $\mathcal{A} = (Q, q_0, F, \Sigma, \Delta)$ cet automate. Considérons alors l'automate fini $\mathcal{B} = \big(\wp(Q), \{q_0\}, \overline{F}, \Sigma, \Gamma\big)$ dont :
- l'ensemble des états est l'ensemble des parties de Q,
- l'état initial est le singleton $\{q_0\}$,
- l'ensemble $\overline{F}$ des états finals est l'ensemble des parties de Q qui contiennent au moins un état final de $\mathcal{A}$,
- l'alphabet est l'alphabet Σ de $\mathcal{A}$,
- la relation de transition Γ est définie la relation unaire sur $\wp(Q) \times \Sigma \times \wp(Q)$ définie par l'équivalence

$$(Q_1, a, Q_2) \in \Gamma \Leftrightarrow Q_2 = \{q_2 \in Q : (\exists q_1 \in Q_1 : (q_1, a, q_2) \in \Delta)\}.$$

Vu sa définition, il est totalement évident que Γ est le graphe d'une fonction γ de $\wp(Q) \times \Sigma$ dans $\wp(Q)$. L'automate fini $\mathcal{B}$ est donc déterministe.

Soit m un mot accepté par $\mathcal{A}$. Il existe nécessairement un état final $q \in F$ pour lequel la relation $(q_0, m, q) \in \Delta$ est satisfaite. Donc l'ensemble E des états de Q pour lesquels la relation $(q_0, m, q) \in \Delta$ est satisfaite est un état final de $\mathcal{B}$. Or, par définition de Γ et γ, nous avons justement l'égalité $\gamma(\{q_0\}, m) = E$, ce qui prouve que le mot m est accepté par $\mathcal{B}$.

Soit m un mot accepté par $\mathcal{B}$. L'état $\gamma(\{q_0\}, m)$ est alors un état final de $\mathcal{B}$, ce qui prouve qu'il existe un état final q de $\mathcal{A}$ pour lequel la relation

$(q_0, m, q) \in \Delta$ est satisfaite. Mais alors m est accepté par $\mathcal{A}$.

Nous avons donc prouvé que $\mathcal{B}$ est un automate fini déterministe qui accepte le même langage que l'automate fini $\mathcal{A}$, ce qui revient à prouver la suffisance de la condition. □

Définition 4.1.12. Soient Σ et Π deux alphabets. Une fonction f de Σ^* dans Π^* est un *morphisme* si et seulement si pour tous mots $m_1, m_2 \in \Sigma^*$ $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$. Un morphisme $f : \Sigma^* \to \Pi^*$ est dit de *longueur* n si $|f(a)| = n$ pour tout $a \in \Sigma$. Un morphisme $f : \Sigma^* \to \Sigma^*$ de longueur $n \geq 1$ est dit *prolongeable sur* $a \in \Sigma$ si $f(a)$ est un mot commençant par la lettre $a \in \Sigma$.

Proposition 4.1.13. *Soient Σ et Π deux alphabets. Soient f un morphisme de Σ^* dans Π^*, g un morphisme de Π^* dans Σ^* et L un langage régulier sur Σ. Les langages $f(L)$ et $g^{-1}(L)$ sont réguliers.*

Démonstration. Il existe un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma, \delta)$ qui accepte le langage L. En remplaçant le label de chaque arc de cet automate par son image par f, nous obtenons un automate fini déterministe $(Q, q_0, F, \Pi, \delta')$ qui accepte le langage $f(L)$. Ce dernier est donc régulier. De même, en remplaçant le label $a \in \Sigma$ de chaque arc de l'automate $\mathcal{A}$ par tous les labels dont l'image par g donne a, nous obtenons alors un automate fini $(Q, q_0, F, \Sigma, \Gamma)$ (non nécessairement déterministe) qui accepte le langage $g^{-1}(L)$. Ce dernier est régulier par le théorème 4.1.11. □

Définition 4.1.14. Soit $(Q, q_0, F, \Sigma, \delta)$ un automate fini déterministe. Un état $q \in Q$ est *accessible* si il existe un mot $m \in \Sigma^*$ tel que $\delta(q_0, m) = q$. L'état q est dit *accessible par le mot* m.

4.2 Ensemble reconnaissable dans une base

Dans cette section, nous définissons le caractère reconnaissable (par automate fini déterministe) d'une partie de $\mathbb{N}^n$ dans une base $p \in \mathbb{N} \setminus \{0, 1\}$ et son analogue dans le cadre des polynômes $\mathbb{F}[X]^n$. Insistons sur le fait que la première de ces deux notions est bien connue et que sa structure se transpose aisément à la seconde. Voici quelques références pour le lecteur intéressé d'en apprendre davantage : [24], [18] et [11]. Pour le cadre des polynômes, nous renvoyons à celle-ci : [49].

4.2.1 Cas de $\mathbb{N}^n$

Définition 4.2.1. Soit p un entier strictement supérieur à 1. La fonction ρ_p est définie de la façon suivante :

$$\rho_p : \mathbb{N} \to (\Sigma_p)^*,\ m \mapsto \begin{cases} a_K \cdots a_0 \text{ si } m \neq 0 \\ \varepsilon \text{ si } m = 0 \end{cases}$$

où $\Sigma_{k=0}^{K} a_k p^k$ est le développement p-aire de m. Le mot $\rho_p(m)$ est appelé la *p-représentation* du nombre m ou encore sa *représentation en base p*.

La fonction ρ_p s'étend naturellement sur $\mathbb{N}^n$ de la façon suivante. Pour tout $(m_1, \ldots, m_n) \in \mathbb{N}^n \setminus \{(0, \ldots, 0)\}$ et tout entier p strictement supérieur à 1, si

$$\begin{cases} \rho_p(m_1) = a_{k_1}^{(1)} \cdots a_0^{(1)} \\ \vdots \\ \rho_p(m_n) = a_{k_n}^{(n)} \cdots a_0^{(n)} \end{cases}$$

et si

$$\max\{k_1, \ldots, k_n\} = K,$$

alors

$$\rho_p\left(m_1, \ldots, m_n\right) = \left(a_K^{(1)}, \ldots, a_K^{(n)}\right) \cdots \left(a_0^{(1)}, \ldots, a_0^{(n)}\right)$$

où $a_j^{(i)} = 0 \in \Sigma_p$ pour tout (i, j) tel que $i \in \{1, \ldots, n\}$ et $j > k_i$, et où $k_i = -1$ pour tout $i \in \{1, \ldots, n\}$ tel que $m_i = 0$. De plus, nous posons $\rho_p(0, \ldots, 0) = \varepsilon$.

Pour tout nombre entier p strictement supérieur à 1 et tout nombre entier n strictement positif, nous notons Σ_p^n l'alphabet $\{0, 1, \ldots, p-1\}^n$.

Définition 4.2.2. Pour tout entier p strictement supérieur à 1, une *partie p-reconnaissable* de $\mathbb{N}^n$ est une partie $\mathcal{N}$ de $\mathbb{N}^n$ pour laquelle il existe un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_p^n, \delta)$ qui accepte le langage $\rho_p(\mathcal{N})$.

Une relation d'arité n sur $\mathbb{N}$ est une *relation p-reconnaisable* si elle est une partie p-reconnaissable de $\mathbb{N}^n$. Une fonction de $\mathbb{N}^m$ dans $\mathbb{N}^n$ est une *fonction p-reconnaissable* si son graphe est une relation p-reconnaissable.

4.2.2 Cas de $(\mathbb{F}[X])^n$

Définition 4.2.3. Soit P un polynôme de $\mathbb{F}[X]_{>0}$. La fonction ρ_P est définie de la façon suivante :

$$\rho_P : \mathbb{F}[X] \to (\Sigma_P)^*,\ Q \mapsto \begin{cases} A_K \cdots A_0 \text{ si } Q \neq 0 \\ \varepsilon \text{ si } Q = 0 \end{cases}$$

où $\Sigma_{k=0}^{K} A_k P^k$ est le développement P-aire de Q. Le mot $\rho_P(Q)$ est appelé la *P-représentation* du polynôme Q ou encore sa *représentation en base P*.

La fonction ρ_P s'étend naturellement sur $(\mathbb{F}[X])^n$ de la façon suivante. Pour tout $(Q_1, \ldots, Q_n) \in (\mathbb{F}[X])^n \setminus \{(0, \ldots, 0)\}$ et tout $P \in \mathbb{F}[X]_{>0}$, si

$$\begin{cases} \rho_P(Q_1) = A_{k_1}^{(1)} \cdots A_0^{(1)} \\ \vdots \\ \rho_P(Q_n) = A_{k_n}^{(n)} \cdots A_0^{(n)} \end{cases}$$

et si

$$\max\{k_1, \ldots, k_n\} = K,$$

alors

$$\rho_P(Q_1, \ldots, Q_n) = \left(A_K^{(1)}, \ldots, A_K^{(n)}\right) \cdots \left(A_0^{(1)}, \ldots, A_0^{(n)}\right)$$

où $A_j^{(i)} = 0 \in \Sigma_P$ pour tout (i, j) tel que $i \in \{1, \ldots, n\}$ et $j > k_i$, et où $k_i = -1$ pour tout $i \in \{1, \ldots, n\}$ tel que $Q_i = 0$. De plus, nous posons $\rho_P(0, \ldots, 0) = \varepsilon$.

Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$ et tout nombre entier n strictement positif, nous notons Σ_P^n l'alphabet $(\Sigma_P)^n$.

Définition 4.2.4. Pour tout $P \in \mathbb{F}[X]_{>0}$, une *partie P-reconnaissable* de $(\mathbb{F}[X])^n$ est une partie $\mathcal{P}$ de $(\mathbb{F}[X])^n$ pour laquelle il existe un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_P^n, \delta)$ qui accepte le langage $\rho_P(\mathcal{P})$.

Une relation d'arité n sur $\mathbb{F}[X]$ est une *relation P-reconnaisable* si elle est une partie P-reconnaissable de $(\mathbb{F}[X])^n$. Une fonction de $(\mathbb{F}[X])^m$ dans $(\mathbb{F}[X])^n$ est une *fonction P-reconnaissable* si son graphe est une relation P-reconnaissable.

4.3 Premiers exemples et contre-exemples

Les exemples et contre-exemples de cette section ne mettent pas en évidence de différences significatives entre les deux structures étudiées (nombres entiers naturels et polynômes sur un corps fini). Des différences existent néanmoins, elles apparaissent dans la section 6.1.

4.3.1 Cas de $\mathbb{N}$

Proposition 4.3.1. *Pour tout entier p strictement supérieur à 1, l'ensemble $\mathbb{N}$ est p-reconnaissable.*

Démonstration. C'est évident. □

Proposition 4.3.2. *Pour tout entier p strictement supérieur à 1, l'ensemble $\{p^n : n \in \mathbb{N}\}$ est p-reconnaissable.*

Démonstration. C'est évident puisque le langage $\{\rho_p(p^n) : n \in \mathbb{N}\}$ n'est autre que le langage régulier 10^*. □

Définition 4.3.3. Deux nombres $p, q \in \mathbb{N} \setminus \{0, 1\}$ sont *multiplicativement dépendants* si il existe deux nombres $a, b \in \mathbb{N} \setminus \{0\}$ tels que $p^a = q^b$. Ils sont *multiplicativement indépendants* si il n'existe pas deux nombres $a, b \in \mathbb{N} \setminus \{0\}$ tels que $p^a = q^b$.

Proposition 4.3.4. *Pour tous nombres $p, q \in \mathbb{N} \setminus \{0, 1\}$ multiplicativement indépendants, l'ensemble $\{q^n : n \in \mathbb{N}\}$ n'est pas p-reconnaissable.*

Démonstration. Notons $\mathcal{Q}$ l'ensemble $\{q^n : n \in \mathbb{N}\}$. Faisons une démonstration par l'absurde. Suposons que l'ensemble $\mathcal{Q}$ est p-reconnaissable, nous pouvons, au moyen de n'importe quel chemin fermé non trivial de n'importe quel automate fini déterministe acceptant le langage infini $\rho_p(\mathcal{Q})$, exhiber une partie de $\rho_p(\mathcal{Q})$ de la forme uv^*w où $u, v, w \in \Sigma_p^*$ et $v \neq \varepsilon$. Cela étant, l'ensemble $\mathcal{Q}$ contient un sous-ensemble de nombres $\{q_n : n \in \mathbb{N}\}$ pour lequel $\rho_p(q_n) = uv^nw$ quel que soit $n \in \mathbb{N}$. Il existe alors deux nombres $a, b \in \mathbb{N}$ et un nombre $c \in \mathbb{N} \setminus \{0\}$ tels que $q_{n+1} = p^c(q_n - a) + b$ quel que soit le nombre $n \in \mathbb{N}$. Mais dans ce cas, il vient

$$\lim_{n\to\infty} \frac{q_{n+1}}{q_n} = \lim_{n\to\infty} \left(p^c + \frac{b - ap^c}{q_n} \right) = p^c.$$

Donc, vu que la suite $\left(\frac{q_{n+1}}{q_n}\right)_{n\in\mathbb{N}}$ est une suite d'entiers qui converge vers p^c, il existe $n \in \mathbb{N}$ tel que $\frac{q_{n+1}}{q_n} = p^c$ et donc p^c est une puissance de q, ce qui est impossible par hypothèse. La supposition est donc absurde. □

Nous venons d'avoir un premier exemple d'ensemble de nombres entiers naturels qui est q-reconnaissable sans être p-reconnaissable, pour deux nombres arbitraires $p, q \in \mathbb{N}$ strictement supérieurs à 1 et multiplicativement indépendants.

4.3.2 Cas de $\mathbb{F}[X]$

Proposition 4.3.5. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, l'ensemble $\mathbb{F}[X]$ est P-reconnaissable.*

Démonstration. C'est évident. □

Proposition 4.3.6. *Pour tout $P \in \mathbb{F}[X]_{>0}$, l'ensemble $\{P^n : n \in \mathbb{N}\}$ est P-reconnaissable.*

Démonstration. C'est évident puisque le langage $\{\rho_P(P^n) : n \in \mathbb{N}\}$ n'est autre que le langage régulier 10^*. □

Bien que la proposition 4.3.8 ne soit qu'un cas particulier de la proposition 4.3.10, nous en donnons une démonstration pour deux raisons. La première est que nous trouvons celle-ci assez élégante et originale pour être illustrée. La seconde est qu'elle met parfaitement en évidence les avantages de l'addition dans un ensemble de polynômes sur un corps fini. En effet, sans aller jusqu'à prétendre qu'une preuve similaire n'existe pas dans l'ensemble des entiers, nous pouvons facilement nous rendre compte qu'elle y serait délicate à cause de la remarque 4.3.7.

Remarque 4.3.7. L'addition se fait degré par degré dans l'ensemble $\mathbb{F}[X]$ et donc elle s'y effectue lettre par lettre sans retenue dans toute base polynomiale $P \in \mathbb{F}[X]_{>0}$, contrairement à ce qui se passe dans $\mathbb{N}$ en base $p \in \mathbb{N} \setminus \{0,1\}$.

Proposition 4.3.8. *Pour tout $P \in \mathbb{F}[X]_{>0}$, l'ensemble $\{(1+P)^n : n \in \mathbb{N}\}$ n'est pas P-reconnaissable.*

Démonstration. Soit p la caractéristique du corps fini $\mathbb{F}$. L'ensemble dont il est question dans l'énoncé peut s'écrire sous la forme

$$\mathcal{P} = \left\{ \left(\sum_{i=0}^{n} \left(C_n^i \pmod p \right) P^i \right) : n \in \mathbb{N} \right\}$$

Considérons le triangle de Pascal modulo p :

$$(T_{n,i})_{\{(n,i)\in\mathbb{N}^2 : n\geq i\}} = \left(C_n^i \pmod p \right)_{\{(n,i)\in\mathbb{N}^2 : n\geq i\}}.$$

Comme p est un nombre premier, le nombre $T_{p,i}$ est nul quel que soit le nombre $i \in \mathbb{N}$ vérifiant $0 < i < p$. Dans le triangle de Pascal modulo p, la ligne d'indice p est donc de la forme

$$(1, \underbrace{0, 0, \ldots, 0, 0}_{(p-1)}, 1).$$

Une récurrence directe sur k prouve alors l'égalité

$$T_{kp,r} = \begin{cases} T_{k,\frac{r}{p}} \text{ si } r \text{ est un multiple de } p \\ 0 \text{ si } r \text{ n'est pas un multiple de } p \end{cases},$$

quels que soient les nombres $k, r \in \mathbb{N}$ tels que $kp \geq r$. Or, comme p est un nombre premier, le nombre $T_{r,s}$ est non nul quels que soient les nombres $r, s \in \mathbb{N}$ vérifiant $0 \leq s \leq r < p$. Il est alors immédiat qu'aucune des $(p-1)$ lignes qui suivent directement une ligne ayant comme indice un nombre multiple de p n'est de la forme $(1,0,0,0,\ldots,0,0,0,1)$, ce qui revient à dire qu'aucune ligne ayant comme indice un nombre non multiple de p n'est de la forme $(1,0,0,0,\ldots,0,0,0,1)$. Ceci étant, comme $T_{kp^j,p^j} = T_{k,1}$ quels que soient les nombres $k, j \in \mathbb{N}$, seules les lignes du triangle de Pascal modulo p qui ont comme indice un nombre de la forme p^j avec $j \in \mathbb{N}$ peuvent être de la forme de $(1,0,0,0,\ldots,0,0,0,1)$. Il est par ailleurs évident que toutes celles-ci sont de cette forme.

Donc, l'intersection des langages $\rho_P(\mathcal{P})$ et 10^*1 n'est autre que le langage $\left\{10^{p^k-1}1 : k \in \mathbb{N}\right\}$. Comme le langage 10^*1 est régulier, supposer que le langage $\rho_P(\mathcal{P})$ est régulier reviendrait donc à contredire le caractère non régulier du langage $\left\{10^{p^k-1}1 : k \in \mathbb{N}\right\}$. □

Le lecteur désireux d'en savoir davantage sur les propriétés du triangle de Pascal modulo $p \in \mathbb{N}$ peut consulter les articles [1] et [9].

La preuve de la proposition 4.3.10 est une adaptation de la proposition 4.3.4, son analogue pour les nombres entiers.

Définition 4.3.9. Deux polynômes $P, Q \in \mathbb{F}[X]_{>0}$ sont *multiplicativement dépendants* si il existe deux nombres $a, b \in \mathbb{N} \setminus \{0\}$ tels que $P^a = Q^b$. Ils sont *multiplicativement indépendants* si il n'existe pas deux nombres $a, b \in \mathbb{N} \setminus \{0\}$ tels que $P^a = Q^b$.

Proposition 4.3.10. *Pour tous $P, Q \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants, l'ensemble $\{Q^n : n \in \mathbb{N}\}$ n'est pas P-reconnaissable.*

Démonstration. Notons $\mathcal{Q}$ l'ensemble $\{Q^n : n \in \mathbb{N}\}$. Faisons une démonstration par l'absurde. Suposons que l'ensemble $\mathcal{Q}$ est P-reconnaissable, nous pouvons, au moyen de n'importe quel chemin fermé non trivial de n'importe quel automate fini déterministe acceptant le langage infini $\rho_P(\mathcal{Q})$, exhiber une partie de $\rho_P(\mathcal{Q})$ de la forme UV^*W où $U, V, W \in \Sigma_P^*$ et $V \neq \varepsilon$. Cela étant, l'ensemble $\mathcal{Q}$ contient un sous-ensemble de polynômes $\{Q_n : n \in \mathbb{N}\}$ pour lequel $\rho_P(Q_n) = UV^nW$ quel que soit $n \in \mathbb{N}$. Il existe alors deux polynômes $A, B \in \mathbb{F}[X]$ et un nombre $c \in \mathbb{N} \setminus \{0\}$ tels que $Q_{n+1} = P^c(Q_n - A) + B$ quel que soit le nombre $n \in \mathbb{N}$. Mais dans ce cas, dès que n est assez grand pour vérifier l'inégalité $\deg(Q^n) > \deg(P^cA + B)$, le polynôme $P^cA + B$ est le reste de la divisition du polynôme Q_{n+1} par le polynôme Q_n, c'est-à-dire 0. Cela siginifie que P^c est une puissance de Q, ce qui est impossible par hypothèse. La supposition est donc absurde. □

Nous venons d'avoir un exemple d'ensemble de polynômes sur un corps fini qui est Q-reconnaissable sans être P-reconnaissable, pour deux polynômes arbitriares $P, Q \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants.

4.4 Relations reconnaissables dans une base

Dans cette section, nous montrons que certaines relations et fonctions élémentaires sont p-reconnaissables pour un nombre entier naturel p strictement supérieur à 1 ou P-reconnaissables pour un polynômes P de degré au moins 1 sur un corps fini. Toutes ces fonctions jouent un rôle essentiel dans la suite de cette thèse. Citons à nouveau [11], pour le cadre des entiers naturels.

4.4.1 Cas de $\mathbb{N}$

Proposition 4.4.1. *Pour tout nombre entier p strictement supérieur à 1, l'égalité est une relation binaire p-reconnaissable sur $\mathbb{N}$.*

Démonstration. Il est évident que deux entiers naturels sont égaux si et seulement si ils ont la même représentation en base p. Construire un automate fini déterministe qui accepte le langage $\{\rho_p(a,b) : a,b \in \mathbb{N} \text{ et } a = b\}$ est donc facile, comme l'illustre la figure 4.2. □

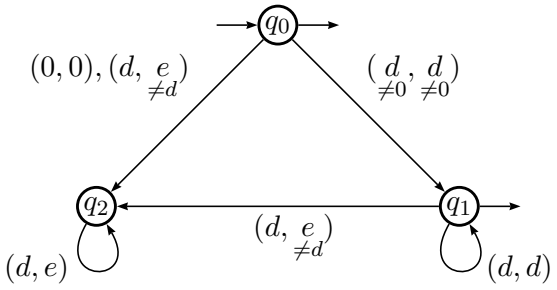

FIG. 4.2 – Égalité.

Proposition 4.4.2. *Pour tout nombre entier p strictement supérieur à 1, l'addition est une relation ternaire p-reconnaissable sur $\mathbb{N}$.*

Démonstration. Lorsque nous désirons additionner deux entiers en passant par leur représentation en base p, nous sommes parfois obligés d'effectuer des retenues. Toutefois, si ces retenues existent, elles ne peuvent valoir que 1. Il est alors aisé de construire un automate fini déterministe qui accepte le langage $\{\rho_p(a,b,c) : a,b,c \in \mathbb{N} \text{ et } a+b=c\}$, comme l'illustre la figure 4.3 où les arcs non représentés ne servent à rien (ils vont vers un puits qui n'est pas représenté). □

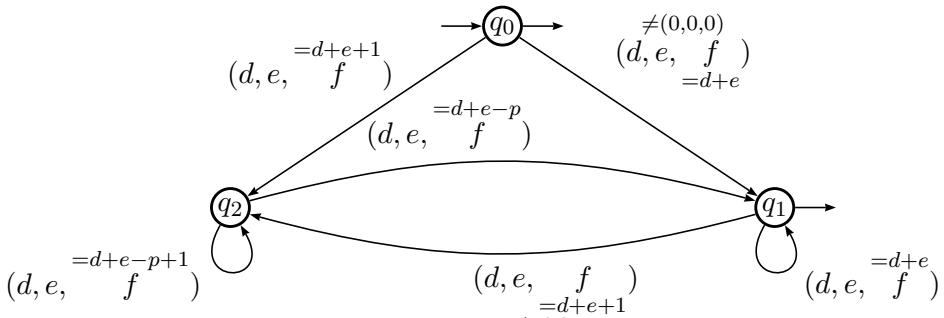

FIG. 4.3 – Addition.

La proposition 4.4.3 montre que la multiplication par une constante est une opération binaire p-reconnaissable dans n'importe quelle base entière p strictement supérieure à 1.

Proposition 4.4.3. *Pour tout nombre entier p strictement supérieur à 1 et tout nombre $c \in \mathbb{N}$, la relation $\sim_c$ binaire sur $\mathbb{N}$, définie par l'équivalence $a \sim_c b \Leftrightarrow ac = b$, est p-reconnaissable sur $\mathbb{N}$.*

Démonstration. Commençons par décrire un automate fini déterministe, ensuite nous prouverons que cet automate accepte le langage

$$\{\rho_p(a,b) : a, b \in \mathbb{N} \text{ et } ac = b\}.$$

Si $c = 0$, le problème est évident. Considérons donc que c est non nul. L'état initial est final. Ainsi le mot vide, qui représente le couple $(0,0) \in \mathbb{N} \times \mathbb{N}$, est accepté par l'automate. L'automate contient $(c+1)$ autres états notés $r_0, r_1, r_2, \ldots, r_{c-1}, r_c$ et dont seul l'état r_0 est final. L'état r_c est un puits. Si les nombres i, j appartiennent à l'ensemble $\{0, 1, 2, \ldots, c-1\}$, alors les arcs allant de l'état r_i à l'état r_j sont ceux dont le label est un couple $(d, e) \in \Sigma_p^2$ pour lequel l'égalité $dc + j = e + ip$ est satisfaite. Les éventuels autres arcs issus des états $r_0, r_1, \ldots, r_{c-1}$ ont leurs extrémités qui aboutissent dans le puits r_c. Finalement, chaque arc issu de l'état initial a la même extrémité que l'arc de même label issu de l'état r_0, à l'exception de l'arc de label $(0,0)$ dont l'extrémité arrive dans le puits r_c. Il est immédiat de vérifier que cet automate fini est bien déterministe.

Vérifions à présent que cet automate accepte le bon langage. D'abord, un mot $(d, e) \in \Sigma_p^2$ de longueur 1 est accepté par cet automate si et seulement si l'arc de label (d, e) issu de l'état initial mène à l'état final r_0, c'est-à-dire si et seulement si $dc = e$ et $(d, e) \neq (0, 0)$, ce qui est conforme à nos attentes. Ensuite, un mot

$$((d_m, e_m), (d_{m-1}, e_{m-1}), \ldots, (d_0, e_0)) \in \left(\Sigma_p^2\right)^*$$

de longueur au moins 2 est accepté par l'automate si et seulement si il existe $a_1, a_2, \ldots, a_m \in \{0, 1 \ldots, c-1\}$ vérifiant le système

$$\begin{cases} d_m c + a_1 = e_m \\ d_{m-1} c + a_2 = e_{m-1} + a_1 p \\ d_{m-2} c + a_3 = e_{m-2} + a_2 p \\ \vdots \\ d_2 c + a_{m-1} = e_2 + a_{m-2} p \\ d_1 c + a_m = e_1 + a_{m-1} p \\ d_0 c = e_0 + a_m p \end{cases}$$

et que (d_m, e_m) diffère de $(0,0)$. Or, ce système est équivalent à celui-ci :

$$\begin{cases} d_m p^m c + a_1 p^m = e_m p^m \\ d_{m-1} p^{m-1} c + a_2 p^{m-1} = e_{m-1} p^{m-1} + a_1 p^m \\ d_{m-2} p^{m-2} c + a_3 p^{m-2} = e_{m-2} p^{m-2} + a_2 p^{m-1} \\ \vdots \\ d_2 p^2 c + a_{m-1} p^2 = e_2 p^2 + a_{m-2} p^3 \\ d_1 pc + a_m p = e_1 p + a_{m-1} p^2 \\ d_0 c = e_0 + a_m p \end{cases}.$$

En sommant membre à membre ces égalités, en simplifiant les termes semblables et en mettant en évidence la constante c, nous trouvons l'égalité

$$\left(\sum_{k=0}^{m} d_k p^k \right) c = \sum_{k=0}^{m} e_k p^k,$$

ce qui prouve que l'automate n'accepte que des mots du langage

$$\{\rho_p(a,b) : a, b \in \mathbb{N} \text{ et } ac = b\}.$$

De plus, si l'égalité

$$\left(\sum_{k=0}^{m} d_k p^k \right) c = \sum_{k=0}^{m} e_k p^k$$

est satisfaite, alors l'existence de $a_1, a_2, \ldots, a_m \in \{0, 1 \ldots, c-1\}$ satisfaisant au (second) système ci-dessus se déduit aisément de proche en proche en commençant par le nombre a_m. En effet, l'égalité ci-dessus implique la congruence $d_0 c \equiv e_0 \pmod{p}$. Le nombre a_m est alors simplement le quotient de la division euclidienne de $(d_0 c)$ par p et est naturellement strictement inférieur à c puisque d_0 est strictement inférieur à p. Il suffit de procéder ensuite modulo p^2 pour prouver l'existence de $a_{m-1} \in \{0, 1, 2, \ldots, c-1\}$, puis modulo p^3 pour prouver l'existence de $a_{m-2} \in \{0, 1, 2, \ldots, c-1\}$, et caetera. Notons bien que, pour chaque valeur de $k \in \{2, 3, 4, \ldots, m\}$, nous utilisons l'inégalité $a_k < c$ pour déduire l'inégalité $a_{k-1} p \leq (p-1)c + a_k < pc$ et donc l'inégalité $a_{k-1} < c$. Tout ceci prouve que l'automate accepte tous les mots du langage $\{\rho_p(a,b) : a, b \in \mathbb{N} \text{ et } ac = b\}$. □

Proposition 4.4.4. *Pour tout nombre entier p strictement supérieur à 1, la fonction Vp est p-reconnaissable.*

Démonstration. Construisons un automate fini déterministe qui accepte le langage $\{\rho_p(a,b) : a, b \in \mathbb{N} \text{ et } \mathrm{V_p}(a) = b\}$. Il suffit de remarquer qu'un couple $(a,b) \in \mathbb{N} \times \mathbb{N}$ est accepté si et seulement si :
$(a,b) = (0,1)$
OU

la représentation de b en base p est une lettre $1 \in \Sigma_p$ suivie d'un certain nombre de lettres $0 \in \Sigma_p$ et la représentation de a en base p se termine par exactement le même nombre de lettres $0 \in \Sigma_p$.

La figure 4.4 représente l'automate recherché. Décrivons-la. Le premier état est l'état initial (noté q_0) et est non final. Le deuxième état, noté q_1, est final et sert uniquement à accueillir la représentation du couple $(0,1) \in (\mathbb{N})^2$, c'est-à-dire qu'il reçoit l'arc de label $(0,1) \in (\Sigma_p)^2$ partant de l'état initial. Il est clair qu'aucun chemin partant de ce deuxième état ne peut aboutir à un état final. Le troisième et le quatrième état sont notés respectivement q_2 et q_3. Le cinquième état, noté q_4, n'est pas représenté sur la figure 4.4 et est un puits. Tous les arcs issus du second état ainsi que tous les arcs dont le label est de la forme $(c,d) \in (\Sigma_p)^2$ avec $d \notin \{0,1\}$ aboutissent directement dans le puits q_4. L'état q_2 n'est pas final et l'état q_3 est final. Les arcs de label $(0,0) \in (\Sigma_p)^2$, $(c,0) \in (\Sigma_p)^2$ avec $c \neq 0$, $(c,1) \in (\Sigma_p)^2$ issus de l'état inial q_0 pointent respectivement vers le puits q_4, vers l'état non final q_2 et vers l'état final q_3. À l'exception des arcs de label $(0,0) \in (\Sigma_p)^2$ et $(0,1) \in (\Sigma_p)^2$, chaque arc issu de l'état q_2 a la même extrémité que l'arc de même label issu de l'état initial q_0. Les arcs de label $(0,0)$ et $(0,1)$ issus de l'état q_2 pointent respectivement vers l'état non final q_2 et vers l'état final q_3. Finalement, l'arc de label $(0,0) \in (\Sigma_p)^2$ issu de l'état final q_5 est une boucle, tandis que tous les autres arcs issus de cet état aboutissent dans le puits q_4.

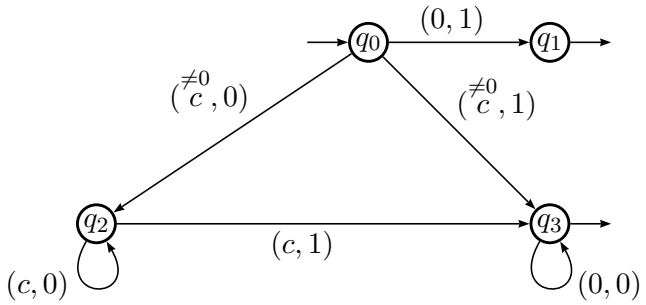

FIG. 4.4 – Fonction $\mathrm{V_p}$.

□

La proposition 4.4.5 est très utile. Par exemple, si p est un entier strictement supérieur à 1, elle permet de ne pas se tracasser pour savoir si l'addition d'une constante $k \in \mathbb{N}$ est une fonction p-reconnaissable de $\mathbb{N}$ dans $\mathbb{N}$. La réponse est automatiquement affirmative, en vertu de la proposition 4.4.5, puisque nous savons déjà, grâce au théorème 4.4.2, que l'addition est une relation ternaire p-reconnaissable sur $\mathbb{N}$.

Proposition 4.4.5. *Pour tout nombre entier p strictement supérieur à 1, tout nombre $n \in \mathbb{N} \setminus \{0\}$ et toute relation $\mathcal{R}$ $(n+1)$-aire p-reconnaissable sur $\mathbb{N}$, la relation $\mathcal{S}$ d'arité n sur $\mathbb{N}$ définie en fixant une des composantes de la relation $\mathcal{R}$ est p-reconnaissable.*

Démonstration. Soit $\mathcal{R}$ une relation qui est $(n+1)$-aire et p-reconnaissable sur $\mathbb{N}$ et soit $\mathcal{S}$ la relation d'arité n sur $\mathbb{N}$ déduite de $\mathcal{R}$ en fixant au nombre $j \in \Sigma_p$ la i-ème composante de $\mathcal{R}$ pour un certain i appartenant à l'ensemble $\{1, \ldots, n+1\}$. Considérons un automate fini déterministe qui prouve que la relation $\mathcal{R}$ est p-reconnaissable, puis retirons lui les arcs dont la composante i du label n'est pas j et effaçons la composante i dans les labels des arcs restant. Nous obtenons ainsi un automate fini (non nécessairement déterministe) qui accepte un langage contenant éventuellement des mots commençant par la lettre $(0, \ldots, 0) \in \Sigma_p^n$, c'est-à-dire des écritures non normalisées de certains n-uplets de nombres. Nous devons modifier cet automate pour qu'il accepte les vraies représentations de ces n-uplets de nombres tout en en refusant les écritures non normalisées. Pour cela, nous supprimons l'arc de label $(0, \ldots, 0) \in \Sigma_p^n$ qui est issu de l'état initial afin de supprimer toutes les écritures non normalisées. L'ennui est que nous perdons alors certains n-uplets de nombres dont ceux qui n'étaient représentés que par des écritures non normalisées. Pour éviter ce souci, nous repérons d'abord les états auxquels mène un mot appartenant à $\{(0, \ldots, 0)\}^*$. Ensuite, nous repérons tous les arcs de label différent de $(0, \ldots, 0) \in \Sigma_p^n$ qui sont issus d'un tel état. Chacun de ces arcs est qualifié de *spécial*. Nous ajoutons alors un tout nouvel état à l'automate. Cet état devient le nouvel état initial et l'ancien état initial perd son statut d'état initial. Aucun arc ne mène au nouvel état initial. Nous rajoutons deux types d'arcs sortants à ce dernier. *Primo*, pour chaque arc de label différent de $(0, \ldots, 0) \in \Sigma_j^n$ issu de l'ancien état initial et arrivant dans un certain état q, il y aura un arc de même label partant de notre nouvel état initial et arriverant dans l'état q (y compris si $q = q_0$). *Secundo*, pour chaque arc *spécial* aboutissant dans un certain état q, il y aura un arc de même label partant de notre nouvel état initial et aboutissant dans l'état q. Nous obtenons ainsi un automate fini qui, en vertu du théorème 4.1.11, prouve que la relation $\mathcal{S}$ est p-reconnaissable. □

4.4.2 Cas de $\mathbb{F}[X]$

La preuve de la proposition 4.4.6 est tout à fait analogue à celle de la proposition 4.4.1. Ce n'est même pas lié à l'analogie entre les ensembles $\mathbb{N}$ et $\mathbb{F}[X]$. C'est simplement dû à la simplicité de la relation d'égalité.

Proposition 4.4.6. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, l'égalité est une relation binaire P-reconnaissable sur $\mathbb{F}[X]$.*

Démonstration. Il est évident que deux polynômes sont égaux si et seulement si ils ont la même représentation en base P. Construire un automate fini

déterministe qui accepte le langage $\{\rho_P(A,B) : A, B \in \mathbb{F}[X] \text{ et } A = B\}$ est donc assez facile, ainsi que l'illustre la figure 4.5. □

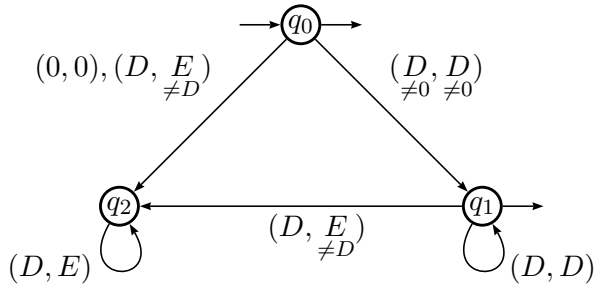

FIG. 4.5 – Égalité.

La preuve de la proposition 4.4.7 est même encore plus simple que celle de la proposition 4.4.2. C'est lié à la remarque 4.3.7. D'ailleurs, nous avons besoin d'un état de moins pour construire un automate fini déterministe répondant au problème (mais nous représentons ici un puits qui n'est pas représenté dans le cadre de $\mathbb{N}$).

Proposition 4.4.7. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, l'addition est une relation ternaire P-reconnaissable sur $\mathbb{F}[X]$.*

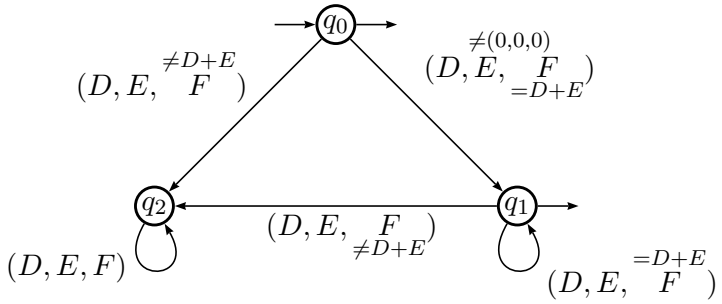

FIG. 4.6 – Addition.

Démonstration. Comme l'addition de deux polynômes s'effectue degré par degré sans retenue, elle peut s'observer facilement dans son écriture en base P ou, de façon équivalente, lettre par lettre dans sa représensation en base P. Il est aisé de construire un automate fini déterministe qui accepte le langage

$$\{\rho_P(A,B,C) : A, B, C \in \mathbb{F}[X] \text{ et } A + B = C\},$$

comme l'illustre la figure 4.6. □

La proposition 4.4.8 exprime que la multiplication par un polynôme fixé C est une relation binaire P-reconnaissable. La preuve est identique à celle de la proposition 4.4.3.

Proposition 4.4.8. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$ et tout polynôme $C \in \mathbb{F}[X]$, la relation $\sim_C$ binaire sur $\mathbb{F}[X]$, définie par $A \sim_C B \Leftrightarrow A \cdot C = B$, est P-reconnaissable.*

Démonstration. Décrivons un automate fini déterministe qui accepte le langage

$$\{\rho_P(A, B) : A, B \in \mathbb{F}[X] \text{ et } A \cdot C = B\}.$$

La vérification du fait que cet automate accepte le bon langage est proche de celle de de la preuve de la proposition 4.4.3 mais est néanmoins détaillée par la suite. Si $C = 0$, le problème est évident. Considérons donc que le polynôme C est non nul. L'état initial est final. Ainsi le mot vide, qui représente le couple $(0, 0) \in \mathbb{F}[X] \times \mathbb{F}[X]$, est accepté par l'automate. Les autres états de l'automate sont les éléments de l'ensemble $\{r_Q : Q \in \mathbb{F}[X]_{<\deg(C)}\}$ et un puits noté r_C. L'état r_0 est final, mais les autres ne le sont pas (sauf l'état initial). Si les polynômes I, J appartiennent à l'ensemble $\mathbb{F}[X]_{<\deg(C)}$, alors les arcs allant de l'état r_I à l'état r_J sont ceux dont le label est un couple $(D, E) \in \Sigma_P^2$ pour lequel l'égalité $D \cdot C + J = E + I \cdot P$ est satisfaite. Les éventuels autres arcs issus des états non initiaux ont leurs extrémités qui aboutissent dans le puits r_C. Finalement, chaque arc issu de l'état initial a la même extrémité que l'arc de même label issu de l'état r_0, à l'exception de l'arc de label $(0, 0) \in \Sigma_P^2$ dont l'extrémité arrive dans le puits r_C. Il est immédiat de vérifier que cet automate fini est bien déterministe.

Vérifions à présent que cet automate accepte le bon langage. Tout d'abord, un mot $(D, E) \in \Sigma_P^2$ de longueur 1 est accepté par cet automate si et seulement si l'arc de label (D, E) issu de l'état initial mène à l'état final r_0, c'est-à-dire si et seulement si $D \cdot C = E$ et $(D, E) \neq (0, 0)$, ce qui est conforme à nos attentes. Ensuite, un mot

$$((D_m, E_m), (D_{m-1}, E_{m-1}), \ldots, (D_0, E_0)) \in \left(\Sigma_P^2\right)^*$$

de longueur au moins 2 est accepté par l'automate si et seulement si il existe $A_1, A_2, \ldots, A_m \in \mathbb{F}[X]_{<\deg(C)}$ vérifiant le système

$$\begin{cases} D_m \cdot C + A_1 = E_m \\ D_{m-1} \cdot C + A_2 = E_{m-1} + A_1 \cdot P \\ D_{m-2} \cdot C + A_3 = E_{m-2} + A_2 \cdot P \\ \vdots \\ D_2 \cdot C + A_{m-1} = E_2 + A_{m-2} \cdot P \\ D_1 \cdot C + A_m = E_1 + A_{m-1} \cdot P \\ D_0 \cdot C = E_0 + A_m \cdot P \end{cases}$$

et que (D_m, E_m) diffère de $(0,0)$. Or, ce système est équivalent à celui-ci :

$$\begin{cases} D_m \cdot P^m \cdot C + A_1 \cdot P^m = E_m \cdot P^m \\ D_{m-1} \cdot P^{m-1} \cdot C + A_2 \cdot P^{m-1} = E_{m-1} \cdot P^{m-1} + A_1 \cdot P^m \\ D_{m-2} \cdot P^{m-2} \cdot C + A_3 \cdot P^{m-2} = E_{m-2} \cdot P^{m-2} + A_2 \cdot P^{m-1} \\ \vdots \\ D_2 \cdot P^2 \cdot C + A_{m-1} \cdot P^2 = E_2 \cdot P^2 + A_{m-2} \cdot P^3 \\ D_1 \cdot P \cdot C + A_m \cdot P = E_1 \cdot P + A_{m-1} \cdot P^2 \\ D_0 \cdot C = E_0 + A_m \cdot P \end{cases}.$$

En sommant membre à membre ces égalités, en simplifiant les termes semblables et en mettant en évidence le polynôme fixé C, nous trouvons l'égalité

$$\left(\sum_{k=0}^{m} D_k \cdot P^k \right) \cdot C = \sum_{k=0}^{m} E_k \cdot P^k,$$

ce qui prouve que l'automate n'accepte que des mots du langage

$$\{\rho_P(A,B) : A, B \in \mathbb{F}[X] \text{ et } A \cdot C = B\}.$$

De plus, si l'égalité

$$\left(\sum_{k=0}^{m} D_k \cdot P^k \right) \cdot C = \sum_{k=0}^{m} E_k \cdot P^k$$

est satisfaite, alors l'existence de $A_1, A_2, \ldots, A_m \in \mathbb{F}[X]_{<deg(C)}$ satisfaisant au (second) système ci-dessus se déduit aisément de proche en proche en commençant par le nombre A_m. En effet, l'égalité ci-dessus implique la congruence $D_0 \cdot C \equiv E_0 \pmod{P}$. Le nombre A_m est alors simplement le quotient de la division polynomiale de $(D_0 \cdot C)$ par P et est naturellement de degré strictement inférieur au degré du polynôme C puisque le polynôme D_0 est de degré strictement inférieur au degré du polynôme P. Il suffit de procéder ensuite modulo P^2 pour prouver l'existence de $A_{m-1} \in \mathbb{F}[X]_{<\deg(C)}$, puis modulo P^3 pour prouver l'existence de $A_{m-2} \in \mathbb{F}[X]_{<\deg(C)}$, et caetera. Notons bien que, pour chaque valeur de $k \in \{2,3,4,\ldots,m\}$, nous utilisons l'inégalité $A_k \prec C$ pour déduire l'inégalité $A_{k-1} \prec C$. Tout ceci prouve que l'automate accepte tous les mots du langage $\{\rho_P(A,B) : A, B \in \mathbb{F}[X] \text{ et } A \cdot C = B\}$. □

Proposition 4.4.9. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, la relation $\prec$ est P-reconnaissable.*

Démonstration. Il est assez facile de construire un automate fini déterministe qui accepte le langage $\{\rho_P(A,B) : A, B \in \mathbb{F}[X] \text{ et } A \prec B\}$. Il suffit de considérer un automate de trois états dans lequel l'acception d'un mot se décide au premier arc emprunté. Le premier état est l'état initial (noté q_0) et

n'est pas final. Le deuxième état, noté q_1, est le seul état final et ne possède que des boucles. Le troisième état, noté q_2, est un puits. Les arcs partant du premier état et ayant un label dont la première composante (celle relative à A) est de degré strictement inférieur à la seconde (celle relative à B) aboutissent au deuxième état, alors que les autres aboutissent au troisième état. Voir figure 4.7. □

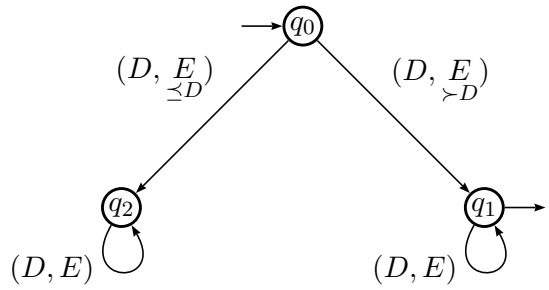

FIG. 4.7 – Relation $\prec$.

La preuve de la proposition 4.4.10 est exactement la même que celle de la proposition 4.4.4. Nous nous contentons donc d'y donner l'automate fini déterministe qui prouve que la fonction VP est P-reconnaissable.

Proposition 4.4.10. *Pour tout polynôme $P \in \mathbb{F}[X]_{>0}$, la fonction $\mathrm{V_P}$ est P-reconnaissable.*

Démonstration. La figure 4.8 représente un automate fini déterministe qui répond au problème. Tous les arcs non représentés vont directement vers un puits non représenté. □

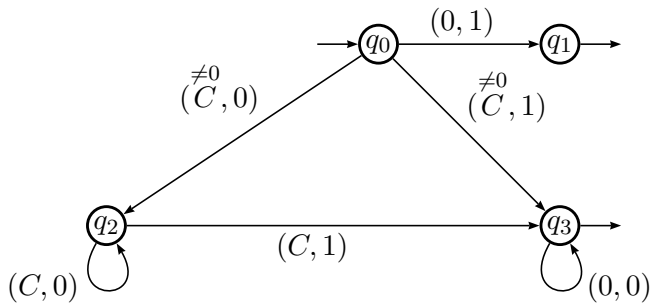

FIG. 4.8 – Fonction $\mathrm{V_P}$.

La proposition 4.4.11 et sa preuve sont similaires à la proposition 4.4.5. Cette proposition est utile dans la preuve du théorème de Büchi-Bruyère

(le théorème 5.2.1) pour ne pas se tracasser à faire la distinction entre les constantes et les variables.

Proposition 4.4.11. *Pour tout $P \in \mathbb{F}[X]_{>0}$, tout nombre $n \in \mathbb{N} \setminus \{0\}$ et toute relation $\mathcal{R}$ $(n+1)$-aire P-reconnaissable sur $\mathbb{F}[X]$, la relation $\mathcal{S}$ d'arité n sur $\mathbb{F}[X]$ définie en fixant une des composantes de la relation $\mathcal{R}$ est P-reconnaissable.*

Démonstration. Soit $\mathcal{R}$ une relation qui est $(n+1)$-aire et P-reconnaissable sur $\mathbb{F}[X]$ et soit $\mathcal{S}$ la relation d'arité n sur $\mathbb{F}[X]$ déduite de $\mathcal{R}$ en fixant à $J \in \Sigma_P$ la i-ème composante de $\mathcal{R}$ pour un certain i appartenant à l'ensemble $\{1, \ldots, n+1\}$. Considérons un automate fini déterministe qui prouve que la relation $\mathcal{R}$ est P-reconnaissable, puis retirons lui les arcs dont la composante i du label n'est pas J et effaçons la composante i dans les labels des arcs restant. Nous obtenons ainsi un automate fini (non nécessairement déterministe) qui accepte un langage contenant éventuellement des mots commençant par la lettre $(0, \ldots, 0) \in \Sigma_P^n$, c'est-à-dire des écritures non normalisées de certains n-uplets de polynômes. Nous devons modifier cet automate pour qu'il accepte les vraies représentations de ces n-uplets de polynômes tout en en refusant les écritures non normalisées. Pour cela, nous supprimons l'arc de label $(0, \ldots, 0) \in \Sigma_P^n$ qui est issu de l'état initial afin de supprimer toutes les écritures non normalisées. L'ennui est que nous perdons alors certains n-uplets de polynômes dont ceux qui n'étaient représentés que par des écritures non normalisées. Pour éviter ce souci, nous repérons d'abord les états auxquels mène un mot appartenant à $\{(0, \ldots, 0)\}^*$. Ensuite, nous repérons tous les arcs de label différent de $(0, \ldots, 0) \in \Sigma_P^n$ qui sont issus d'un tel état. Chacun de ces arcs est qualifié de *spécial*. Nous ajoutons alors un tout nouvel état à l'automate. Cet état devient le nouvel état initial et l'ancien état initial perd son statut d'état initial. Aucun arc ne mène au nouvel état initial. Nous rajoutons deux types d'arcs sortants à ce dernier. *Primo*, pour chaque arc de label différent de $(0, \ldots, 0) \in \Sigma_P^n$ issu de l'ancien état initial et arrivant dans un certain état q, il y aura un arc de même label partant de notre nouvel état initial et arriverant dans l'état q (y compris si $q = q_0$). *Secundo*, pour chaque arc *spécial* aboutissant dans un certain état q, il y aura un arc de même label partant de notre nouvel état initial et aboutissant dans l'état q. Nous obtenons ainsi un automate fini qui, en vertu du théorème 4.1.11, prouve que la relation $\mathcal{S}$ est P-reconnaissable. □

Chapitre 5

Théorème de Büchi-Bruyère

5.1 Énoncé dans $\mathbb{N}$

Le théorème 5.1.1 identifie les ensembles p-reconnaissables de nombres entiers naturels aux ensembles p-définissables de nombres entiers naturels, quel que soit le nombre entier naturel p strictement supérieur à 1. Il est donc très utile car il permet de simplifier considérablement certaines preuves en adoptant au cas par cas l'aspet qui convient le mieux au contexte local. De plus, il prouve la décidabilité algorithmique et donc l'existence d'un moyen automatique de déterminer la validité des formules closes ou la satisfaction des formules de la structure $\langle \mathbb{N}, +, \mathrm{V_p} \rangle$, bien que cette structure soit plus riche que l'arithmétique de Presburger. Le lecteur peut consulter [11], [14], [59].

Théorème 5.1.1. *Pour tout nombre entier p strictement supérieur à 1, une partie de $\mathbb{N}^n$ est p-reconnaissable si et seulement si elle est p-définissable.*

Démonstration. La preuve de ce théorème se trouve dans les travaux [11] et [59] et est proche de la preuve du théorème 5.2.1 présentée ci-dessous. □

5.2 Énoncé et preuve dans $\mathbb{F}[X]$

En identifiant les ensembles P-reconnaissables de polynômes sur un corps fini aux ensembles P-définissables de polynômes sur ce même corps fini, quel que soit le polynôme P de degré au moins 1, le théorème 5.2.1 prouve que la structure

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle$$

est une bonne structure pour étudier dans le langage de la logique des problèmes basés sur des automates finis déterministes dont l'alphabet est Σ_P, et montre qu'en particulier la fonction $\mathrm{V_P}$ a de l'intérêt dans ce cadre-là. De plus, l'analogie avec ce qui se passe dans $\mathbb{N}$ est un encouragement à croire

en l'existence d'un analogue du théorème de Cobham dans le cadre des polynômes sur un corps fini.

Théorème 5.2.1. *Pour tout polynôme $P \in \mathbb{F}[x]_{>0}$, une partie de $(\mathbb{F}[X])^n$ est P-reconnaissable si et seulement si elle est P-définissable.*

Démonstration. En premier lieu, considérons une partie $\mathcal{P}$ de $(\mathbb{F}[X])^n$ qui est P-définissable et prouvons qu'elle est P-reconnaissable. Nous disposons d'une formule qui est satisfaite pour un élément de $(\mathbb{F}[X])^n$ si et seulement si cet élément appartient à $\mathcal{P}$. Quitte à remplacer cette formule par une autre formule équivalente, nous pouvons supposer que celle-ci ne possède pas d'autres connecteurs que des négations $\neg$ et des conjonctions $\wedge$, et pas d'autres quantificateurs que des quantificateurs existentiels $\exists$.

Chaque terme peut être facilement écrit sous l'une des quatre formes

$$\sum_{i=1}^{n} A_i \cdot C_i, \quad (n \in \mathbb{N} \setminus \{0\}),$$

$$C_0 + \sum_{i=1}^{n} A_i \cdot C_i, \quad (n \in \mathbb{N}),$$

$$\mathrm{V_P}\left(\sum_{i=1}^{n} A_i \cdot C_i\right), \quad (n \in \mathbb{N} \setminus \{0\}),$$

$$\mathrm{V_P}\left(C_0 + \sum_{i=1}^{n} A_i \cdot C_i\right), \quad (n \in \mathbb{N}),$$

où $C_0, C_1, \ldots, C_n \in \mathbb{F}[X]$ sont fixés et où $A_1, \ldots, A_n$ sont des variables de $\mathbb{F}[X]$. Chaque formule atomique est de l'une des deux formes $A = B$, $A \prec B$ où A, B sont des termes. Quitte à remplacer une formule atomique par une formule équivalente faisant apparaître de nouvelles variables liées à de nouveaux quantificateurs existentiels, ainsi que de nouvelles conjonctions, nous pouvons supposer que chaque formule atomique est de l'une des cinq formes $A = B$, $A + B = C$, $A \cdot K = B$, $A \prec B$, $\mathrm{V_P}(A) = B$ où $A, B, C \in \mathbb{F}[X]$ sont des variables ou sont fixés et où $K \in \mathbb{F}[X]$ est fixé.

Tout ceci étant, prouvons le caractère P-reconnaissable de $\mathcal{P}$ par induction sur la somme du nombre de quantificateurs et du nombre de connecteurs de la formule utilisée pour P-définir $\mathcal{P}$.

Commençons d'abord par règler le cas des formules atomiques, autrement dit des formules $A = B$, $A + B = C$, $A \cdot K = B$, $A \prec B$, $\mathrm{V_P}(A) = B$ où $A, B, C \in \mathbb{F}[X]$ sont des variables ou sont fixés et où $K \in \mathbb{F}[X]$ est fixé. Si

A, B ou C sont fixés, nous nous ramenons au cas où A, B et C sont des variables grâce à la proposition 4.4.11. Si A, B et C sont des variables, alors le caractère P-reconnaissable de $\mathcal{P}$ découle directement de la proposition 4.4.6, 4.4.7, 4.4.8, 4.4.9 ou 4.4.10 respectivement selon que la formule qui P-définit $\mathcal{P}$ est de la forme $A = B$, $A + B = C$, $A \cdot K = B$, $A \prec B$ ou $\mathrm{V_P}(A) = B$.

Supposons à présent que la proposition est vraie pour toute formule dont la somme du nombre de connecteurs et du nombre de quantificateurs vaut au plus k (k est un entier naturel fixé) et considérons une formule $\phi(A_1, \ldots, A_n)$ qui P-définit $\mathcal{P}$ et dont la somme du nombre de connecteurs et du nombre de quantificateurs est égale à $(k+1)$. Cette formule peut en fait s'écrire sous l'une des trois formes suivantes :

$$\neg\theta(A_1, \ldots, A_n),$$

$$\theta_1(A_1, \ldots, A_n) \wedge \theta_2(A_1, \ldots, A_n),$$

$$\exists A_0(\theta(A_0, A_1, \ldots, A_n))$$

où $\theta, \theta_1, \theta_2$ sont des formules.

Supposons que $\phi(A_1, \ldots, A_n)$ est équivalent à $\neg\theta(A_1, \ldots, A_n)$. Comme la somme du nombre de connecteurs et du nombre de quantificateurs de la formule $\theta(A_1, \ldots, A_n)$ est k, l'ensemble des n-uplets de polynômes qui la satisfont est P-reconnaissable par hypothèse d'induction, ce qui signifie qu'il existe un automate fini déterministe qui accepte l'ensemble des P-représentations des n-uplets de polynômes satisfaisant la formule θ. En inversant les caractères final et non final des états de cet automate, nous obtenons un nouvel automate fini déterministe qui, si il n'acceptait pas les mots commençant par $(0, \ldots, 0) \in \Sigma_P$, prouverait que l'ensemble des n-uplets de polynômes qui satisfont la formule $\phi(A_1, \ldots, A_n)$ est P-reconnaissable. Il nous suffit alors de le modifier de la façon suivante : nous rajoutons un nouvel état qui devient le nouvel état initial et qui se comporte comme l'ancien état initial pour les destinations de chacun de ses arcs sortant, à l'exception de l'arc $(0, \ldots, 0) \in \Sigma_P$ qui est envoyé vers un puits. Le nouvel automate ainsi obtenu prouve que l'ensemble $\mathcal{P}$ est P-reconnaissable.

Si $\phi(A_1, \ldots, A_n)$ est équivalent à $\theta_1(A_1, \ldots, A_n) \wedge \theta_2(A_1, \ldots, A_n)$. Comme la somme du nombre de connecteurs et du nombre de quantificateurs de la formule $\theta_1(A_1, \ldots, A_n)$ est inférieure ou égale à k, l'ensemble des n-uplets de polynômes qui la satisfont est P-reconnaissable par hypothèse d'induction. Il existe donc un automate fini déterministe $\mathcal{A}_1 = (Q_1, (q_0)_1, F_1, \Sigma_P^n, \delta_1)$ qui accepte l'ensemble des P-représentations des n-uplets de polynômes satisfaisant la formule θ_1. De même, il existe un automate fini déterministe $\mathcal{A}_2 = (Q_2, (q_0)_2, F_2, \Sigma_P^n, \delta_2)$ qui accepte l'ensemble des P-représentations des

n-uplets de polynômes satisfaisant la formule θ_2. Construisons l'automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_P^n, \delta)$ de la façon suivante : $Q = Q_1 \times Q_2$, $q_0 = ((q_0)_1, (q_0)_2)$, $F = F_1 \times F_2$, $\delta((q_1, q_2), A) = (\delta_1(q_1, A), \delta_2(q_2, A)$ pour tous $q_1 \in Q_1$, $q_2 \in Q_2$, $A \in \Sigma_P^n$. L'automate $\mathcal{A}$ accepte évidemment l'intersection des langages acceptés par les automates $\mathcal{A}_1$ et $\mathcal{A}_2$. Donc l'automate $\mathcal{A}$ prouve que l'ensemble des n-uplets de polynômes qui satisfont la formule $\phi(A_1, \ldots, A_n)$ est P-reconnaissable, c'est-à-dire que $\mathcal{P}$ est P-reconnaissable.

Supposons que $\phi(A_1, \ldots, A_n)$ est équivalent à $\exists A_0(\theta(A_0, A_1, \ldots, A_n))$. Comme la somme du nombre de connecteurs et du nombre de quantificateurs de la formule $\theta(A_0, A_1, \ldots, A_n)$ est égale à k, l'ensemble des $(n+1)$-uplets de polynômes qui la satisfont est P-reconnaissable par hypothèse d'induction. Il existe donc un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_P^{n+1}, \delta)$ qui accepte l'ensemble des P-représentations de n-uplets de polynômes satisfaisant la formule θ. Nous allons construire une quasi-copie (non nécessairement déterministe) $\mathcal{B} = (Q, q_0, F, \Sigma_P^n, \delta')$ de l'automate $\mathcal{A}$ de la manière suivante : l'ensemble Q des états, l'état initial q_0 et l'ensemble F des états finals ne varient pas mais l'alphabet passe de Σ_P^{n+1} pour $\mathcal{A}$ à Σ_P^n pour $\mathcal{B}$ et un point $(q, (A_0, A_1, \ldots, A_n), q')$ du graphe de la fonction de transition δ de $\mathcal{A}$ devient le point $(q, (A_1, \ldots, A_n), q')$ du graphe de la relation de transition δ' de $\mathcal{B}$, c'est-à-dire que un arc de $\mathcal{A}$ de label $(A_0, A_1, \ldots, A_n) \in \Sigma_P^{n+1}$ devient un arc de $\mathcal{B}$ de label $(A_1, \ldots, A_n) \in \Sigma_P^n$ de même origine et de même extrémité. Remarquons qu'il se peut que l'automate $\mathcal{B}$ accepte des mots commençant par au moins une lettre $(0, \ldots, 0) \in \Sigma_P^n$, c'est-à-dire des écritures non normalisées de certains n-uplets de polynômes. Nous résolvons ce problème en procédant comme dans la preuve de la proposition 4.4.11. Nous disposons alors d'un automate fini déterministe prouvant que l'ensemble des n-uplets de polynômes qui satisfont la formule $\phi(A_1, \ldots, A_n)$ est P-reconnaissable, c'est-à-dire prouvant que $\mathcal{P}$ est P-reconnaissable.

En second lieu, prouvons que toute partie P-reconnaissable de $(\mathbb{F}[X])^n$ est également P-définissable. Considérons donc une partie $\mathcal{P}$ de $(\mathbb{F}[X])^n$ telle que le langage $\rho_P(\mathcal{P})$ est régulier. Soit $\mathcal{A} = (Q, q_0, F, \Sigma_P^n, \delta)$ un automate fini déterministe qui accepte le langage $\rho_P(\mathcal{P})$. Notons ℓ le nombre d'états de cet automate. Codons les ℓ états de cet automate avec les ℓ-uples suivants :

$$(1, 0, \ldots, 0)\ ,\ (0, 1, \ldots, 0)\ ,\ \ldots\ ,\ (0, 0, \ldots, 1) \in (\Sigma_P)^\ell.$$

Pour tout état $q \in Q$ et pour tout $j \in \{1, 2, \ldots, \ell\}$, nous notons q_j la lettre de Σ_P qui code la j-ième composante de l'état q (il est clair que $q_j \in \{0, 1\} \subseteq \Sigma_P$).

Quels que soient l'entier naturel non nul m et le m-uplet de polynômes

$(R_1, \ldots, R_m) \in (\mathbb{F}[X])^m$ différent de $(0, \ldots, 0)$, nous notons

$$((R_1(k), \ldots, R_m(k)), \ldots, (R_1(1), \ldots, R_m(1)), (R_1(0), \ldots, R_m(0))) \in (\Sigma_P^m)^*$$

la P-représentation du m-uplet $(R_1, \ldots, R_m)$. Bien entendu, k dépend du m-uplet considéré. De plus, $(R_1(k), \ldots, R_m(k)) \neq (0, \ldots, 0)$.

Excepté pour le cas trivial où $(A_1, \ldots, A_n) = (0, \ldots, 0)$, il est évident qu'un n-uplet de polynômes $(A_1, \ldots, A_n) \in (\mathbb{F}[X])^n$ appartient à $\mathcal{P}$ si et seulement si il existe un ℓ-uple de polynômes $(B_1, \ldots, B_\ell) \in (\mathbb{F}[X])^\ell$ et un entier $k \in \mathbb{N}$ tels que les quatre conditions suivantes sont réalisées :
1. $\deg(P^k) \leq \max\{\deg(A_1), \ldots, \deg(A_n)\} < \deg(P^{k+1})$,
2. $(B_1(k+1), \ldots, B_l(k+1))$ code l'état initial q_0,
3. quel que soit le nombre $j \in \{0, 1, \ldots, k\}$, si $(B_1(j+1), \ldots, B_\ell(j+1))$ code l'état q alors $(B_1(j), \ldots, B_\ell(j))$ code l'état $\delta(q, (A_1(j), \ldots, A_n(j)))$,
4. l'état codé par $(B_1(0), \ldots, B_\ell(0))$ est final.

Pour conclure, il ne reste donc plus qu'à écrire une formule $\phi(A_1, \ldots, A_n)$ du premier ordre dans le langage

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle$$

qui est satisfaite pour un n-uplet $(A_1, \ldots, A_n)$ si et seulement si celui-ci satisfait ce qui est exprimé au paragraphe précédent. Voici une forme que peut prendre la formule $\phi(A_1, \ldots, A_n)$:

$$\exists K \exists B_1 \cdots \exists B_\ell$$

$$\left[\mathrm{V_P}(K) = K \quad \wedge \quad \bigvee_{i=1}^{n} K \preceq A_i \quad \wedge \quad \bigwedge_{i=1}^{n} A_i \prec P \cdot K \right.$$

$$\wedge$$

$$\bigwedge_{j=1}^{\ell} X_{P,(q_0)_j}(K \cdot P, B_j)$$

$$\wedge$$

$$\forall U$$

$$[U \preceq K$$

$$\rightarrow$$

$$\bigwedge_{\{((V_1,\ldots,V_n),q,q') \in \Sigma_P^n \times Q^2 \,:\, \delta(q,(V_1,\ldots,V_n)) = q'\}}$$

$$\left(\bigwedge_{i=1}^{n} X_{P,V_i}(U, A_i) \ \wedge \ \bigwedge_{j=1}^{\ell} X_{P,q_j}(U \cdot P, B_j) \rightarrow \bigwedge_{j=1}^{\ell} X_{P,(q')_j}(U, B_j) \right)$$

$$\wedge$$

$$\bigvee_{q\in F}\bigwedge_{j=1}^{\ell} X_{P,q_j}(1,B_j)]\Bigg] .$$

Le cas trivial où $(A_1,\ldots,A_n)=(0,\ldots,0)$ peut facilement être pris en compte par une modification minime dans la formule. □

Chapitre 6

Ensemble définissable, reconnaissable

Dans ce chapitre, nous cherchons quelles sont les parties de $\mathbb{N}$ (resp. $\mathbb{F}[X]$) qui sont p-reconnaissables (resp. P-reconnaissables) par un automate fini déterministe d'alphabet Σ_p (resp. Σ_P) indépendamment du nombre entier naturel p strictement supérieur à 1 (resp. du polynôme $P \in \mathbb{F}[X]$ de degré au moins 1). Nous mettons en évidence l'unique type d'ensembles qui le sont dans le cadre des entiers naturels (il s'agit des progressions arithmétiques, ainsi que leurs unions finies) et trois types d'ensembles qui le sont, dont deux étaient déjà connus depuis l'article [49] et dont le troisième a été découvert par nous, dans le cadre des polynômes sur un corps fini (il s'agit des progressions arithmétiques, des progressions arithmétiques basées sur le degré et des ensembles débutant par un même préfixe en base X, ainsi que leurs combinaisons booléennes). Il est plus complexe de cerner ces ensembles dans $\mathbb{F}[X]$ que dans $\mathbb{N}$. Dans $\mathbb{N}$, nous faisons le lien avec le théorème de Cobham qui est démontré dans le chapitre suivant et qui clôt le problème. Dans $\mathbb{F}[X]$, nous faisons une conjecture analogue. Le point de vue de la logique est également abordé dans une seconde section, avant de passer à une brève troisième section concernant la stabilité par combinaison linéaire, puis de terminer par une quatrième section dans laquelle nous considérons des bases dépendantes.

6.1 Ensembles reconnaissables de type 1,2,3 et combinaisons booléennes

6.1.1 Cas de $\mathbb{N}$

Définition 6.1.1. Une *partie reconnaissable* de $\mathbb{N}$ est une partie de $\mathbb{N}$ qui est p-reconnaissable pour tout nombre entier p strictement supérieur à 1.

Les ensembles considérés dans la proposition 6.1.2 sont en fait les progressions arithmétiques de $\mathbb{N}$.

Proposition 6.1.2. *Pour tous $a, b \in \mathbb{N}$, l'ensemble suivant est reconnaissable :*

$$\{ac + b : c \in \mathbb{N}\}.$$

Démonstration. Quel que soit le nombre entier p strictement supérieur à 1, l'ensemble $\{ac + b : c \in \mathbb{N}\} = \{n \in \mathbb{N} : (\exists c \in \mathbb{N} : n = ac + b)\}$ est p-dénississable par la formule

$$\exists c(n = \underbrace{c + c + \cdots c}_{a \text{ termes}} + b)$$

du premier ordre de la structure $\langle \mathbb{N}, +, \mathrm{V_p} \rangle$. Par le théorème 5.1.1, cet ensemble est donc p-reconnaissable quel que soit le nombre entier p strictement supérieur à 1, et il est donc reconnaissable par définition. □

Pour un lecteur familiarisé avec les automates finis déterministes, la proposition 6.1.3 est évidente, même sans faire référence au théorème 5.1.1 de Büchi-Bruyère et sans utiliser d'autres notions que les automates. Nous donnons cependant une preuve qui fait intervenir deux fois ce théorème car la stabilité de la p-définissabilité par combinaison booléenne nous paraît encore plus évidente que celle du caractère p-reconnaissable.

Proposition 6.1.3. *Toute combinaison booléenne d'ensembles reconnaissables est un ensemble reconnaissable.*

Démonstration. Tout ensemble reconnaissable est p-reconnaissable pour tout $p \in \mathbb{N} \setminus \{0, 1\}$, et donc p-définissable pour tout $p \in \mathbb{N} \setminus \{0, 1\}$. Toute combinaison booléenne d'ensembles reconnaissables est donc p-définissable pour tout $p \in \mathbb{N} \setminus \{0, 1\}$, donc p-reconnaissable pour tout $p \in \mathbb{N} \setminus \{0, 1\}$, donc reconnaissable. □

Corollaire 6.1.4. *Toute union finie de progressions arithmétiques est un ensemble reconnaissable.*

Démonstration. En vertu de la proposition 6.1.2, c'est un cas particulier de la proposition 6.1.3. □

La proposition 6.1.5 est la combinaison du corollaire 6.1.4 et de sa réciproque. Nous ne nous en servons pas avant d'avoir démontrer le théorème 7.5.1 de Cobham car nous n'en fournissons pas de preuve ne découlant pas de ce théorème.

Proposition 6.1.5. *Un ensemble est reconnaissable si et seulement si il est une union finie de progressions arithmétiques.*

Démonstration. Cela découle directement du théorème 7.5.1 de Cobham. □

6.1.2 Cas de $\mathbb{F}[X]$

Définition 6.1.6. Une *partie reconnaissable* de $\mathbb{F}[X]$ est une partie de $\mathbb{F}[X]$ qui est P-reconnaissable pour tout polynôme $P \in \mathbb{F}[X]_{>0}$.

Dans la proposition 6.1.7, les ensembles considérés sont l'analogue dans le cadre de l'anneau $\mathbb{F}[X]$ des progressions arithmétiques de $\mathbb{N}$. Ces ensembles sont considérés comme les *ensembles reconnaissables de type 1*.

Proposition 6.1.7. *Pour tous $A, B \in \mathbb{F}[X]$, l'ensemble suivant est reconnaissable :*

$$\{A \cdot C + B : C \in \mathbb{F}[X]\}.$$

Démonstration. Pour tout polynôme $P \in \mathbb{F}[X]$ de degré au moins 1, l'ensemble $\{A \cdot C + B : C \in \mathbb{F}[X]\} = \{Q \in \mathbb{F}[X] : (\exists C \in \mathbb{F}[X] : Q = A \cdot C + B)\}$ est P-dénississable par la formule

$$\exists C(Q = A \cdot C + B)$$

du premier ordre de la structure $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P} \rangle$. Par le théorème 5.2.1, cet ensemble est donc P-reconnaissable quel que soit le polynôme $P \in \mathbb{F}[X]_{>0}$, et il est donc reconnaissable par définition. □

Dans la proposition 6.1.7, il suffit évidemment de considérer tous les couples $(A, B) \in (\mathbb{F}[X])^2$ tels que $B \prec A$ pour disposer de tous les ensembles infinis reconnaissables de type 1. De plus, si $B \prec A$ et $1 \leq \deg(A)$, l'ensemble considéré est l'ensemble des polynômes dont la représentation en base A se termine par la lettre $\rho_A(B)$. Encore mieux : dans les mêmes conditions, si A est en plus de la forme P^n avec $P \in \mathbb{F}[X]_{>0}$ et $n \in \mathbb{N} \setminus \{0\}$, alors l'ensemble considéré est l'ensemble des polynômes dont la représentation en base P se termine par le suffixe $0^m \rho_P(B)$ où $m \in \mathbb{N}$ est tel que $0^m \rho_P(B) \in \Sigma_P^n$. Ceci est à comparer aux ensembles reconnaissables de type 3 introduits à la page 69 et utilisés dans la proposition 6.1.9.

Dans la proposition 6.1.8, l'idée de progression arithmétique porte sur le degré des polynômes. Ces ensembles sont considérés comme les *ensembles reconnaissables de type 2*.

Proposition 6.1.8. *Pour tout $a \in \mathbb{N}$ et pour tout $b \in \mathbb{N} \setminus \{0\}$, l'ensemble suivant est reconnaissable :*

$$\{C \in \mathbb{F}[X] : \deg(C) \equiv a \pmod{b}\}.$$

Démonstration. Montrons que l'ensemble $\{C \in \mathbb{F}[X] : \deg(C) \equiv a \pmod{b}\}$ est P-reconnaissable quel que soit le polynôme $P \in \mathbb{F}[X]_{>0}$. Pour cela décrivons un automate fini déterministe $(Q, q_0, F, \Sigma_P, \delta)$ qui accepte le langage $\{\rho_P(C) : C \in \mathbb{F}[X] \text{ et } \deg(C) \equiv a \pmod{b}\}$. L'état initial q_0 est évidemment non final puisque le polynôme 0 est, par convention, de degré $-\infty$. Il

y a b autres états dans l'automate, notés $r_0, r_1, \ldots, r_{b-1}$, en plus d'un puits noté q_b. Le puits reçoit l'arc de label $0 \in \Sigma_P$ issu de l'état initial. Pour tout $i \in \{0, 1, \ldots, b-1\}$, l'état r_i reçoit tous les arcs de label $D \in \Sigma_P$ issus de l'état initial pour lesquels D représente un polynôme dont le degré est congru à i modulo b, ainsi que tous les arcs issus de l'état r_j pour $j \in \{0, 1, \ldots, b-1\}$ vérifiant la congruence $j + p \equiv i \pmod{b}$. Le seul état final est l'état r_i pour lequel $i \equiv a \pmod{b}$. □

Remarquons que l'analogue dans $\mathbb{N}$ des ensembles reconnaissables de type 2 n'existe pas. Cette différence est due au fait que les nombres d'éléments des ensembles Σ_P et Σ_Q sont multiplicativement dépendants quels que soient les polynômes $P, Q \in \mathbb{F}[X]_{>0}$ (ce sont en effet des puissances de $\#\mathbb{F}$), alors que les nombres d'éléments des ensembles Σ_p et Σ_q sont multiplicativement indépendants si p et q le sont. Dans $\mathbb{N}$, deux nombres peuvent donc avoir simultanément des p-représentations de longueurs identiques et des q-représentations dont les longueurs diffèrent d'une unité. Dans $\mathbb{F}[X]$, ce genre de chose ne se produit pas et c'est pour cela que les ensembles reconnaissables de type 2 y sont légion.

Dans la proposition 6.1.9, nous considérons les ensembles de polynômes de même préfixe dans la base canonique X. Ces ensembles sont considérés comme les *ensembles reconnaissables de type 3*. Dans la description de la proposition 6.1.9, la base X semble jouer un rôle particulier. Il est important de se rendre compte que n'importe quelle autre base polynomiale de degré au moins 1 aurait pu convenir pour décrire ces ensembles, quitte à devoir utiliser des unions finies et des recoupements par des ensembles reconnaissables de type 2. En fait, le polynôme X rend uniquement la description plus facile. La découverte de ce troisième type d'ensembles reconnaissables est due à notre contribution personnelle. Bien entendu, pour parler de nouveauté, il faut vérifier que les ensembles reconnaissables de type 3 ne sont pas des combinaisons booléennes d'ensembles reconnaissables de type 1 et 2.

Proposition 6.1.9. *Pour tout polynôme non nul $C \in \mathbb{F}[X]$, l'ensemble suivant est reconnaissable :*

$$\{X^n \cdot C + R : n \in \mathbb{N},\ R \in \mathbb{F}[X]_{<n}\}.$$

Démonstration. Soient $P \in \mathbb{F}[X]$ un polynôme de degré $p \in \mathbb{N} \setminus \{0\}$ et $C \in \mathbb{F}[X]$ un polynôme de degré $c \in \mathbb{N}$. Pour tout entier n fixé dans $\mathbb{N}$, les polynômes de l'ensemble $\{X^n \cdot C + R : R \in \mathbb{F}[X]_{<n}\}$ ont tous le même degré $(n + c)$ et le même préfixe $\rho_X(C)$ de longueur $(c + 1)$ en base X. De plus, tous les polynômes de degré $(n + c)$ et ayant le préfixe $\rho_X(C)$ en base X sont dans cet ensemble. Cette propriété n'est pas dépendante de la base choisie. Si nous exprimons les polynômes de cet ensemble en base P, ils vont évidemment tous avoir le même "début". Néanmoins ce "début" commun

n'est pas nécessairement un préfixe à proprement parler car il se peut qu'il se termine au milieu d'une lettre de Σ_P (cela arrive lorsque p n'est pas à la fois un diviseur de $(c+1)$ et de n).

Lorsque nous disposons de la P-représentation $A_m \cdots A_0$ d'un polynôme Q de degré q pour laquelle $\deg(A_m) = \alpha$, nous pouvons former une suite dont le premier élément est le coefficient (en base X) du terme de plus haut degré du polynôme $A_m \in \Sigma_P$, dont les α éléments suivants (éventuellement aucun) sont les α coefficients (en base X) des autres termes du polynôme A_m (pris par ordre décroissant de degrés), puis continuer cette suite avec les p coefficients (en base X) des termes du polynôme A_{m-1} (pris par ordre décroissant de degrés et en commençant éventuellement par 0), et continuer la procédure avec les autres A_k (par ordre décroissant d'indices k). La suite obtenue est de longueur $(q+1)$. Si $q \geq c$, nous parlons du *pseudo-P-préfixe de longueur* $(c+1)$ du polynôme Q pour désigner la sous-suite formée des $(c+1)$ premiers éléments de cette suite. Ainsi, pour tout entier n fixé dans $\mathbb{N}$, les polynômes de l'ensemble

$$\{X^n \cdot C + R : R \in \mathbb{F}[X]_{<n}\}$$

ont tous le même degré $(n+c)$ et le même pseudo-P-préfixe de longueur $(c+1)$. De plus, tous les polynômes qui sont de degré $(n+c)$ et qui possèdent le pseudo-P-préfixe en question sont dans cet ensemble.

Les polynômes de la suite $(X^{mp} \cdot C)_{m\in\mathbb{N}}$ n'ont pas nécessairement tous le même pseudo-P-préfixe de longueur $(c+1)$. Néanmoins, celui-ci ne pouvant prendre qu'un nombre fini de valeurs différentes (au maximum $(\#\mathbb{F})^{c+1}$), il existe nécessairement $a, b \in \mathbb{N}$ tels que $a < b$ et que les deux polynômes $X^{ap} \cdot C$ et $X^{bp} \cdot C$ possèdent le même pseudo-P-préfixe de longueur $(c+1)$. Comme ces polynômes ont de plus des degrés de même congruence modulo p, il est clair qu'après avoir été multipliés par X leurs pseudo-P-préfixes de longueur $(c+1)$ restent égaux. En effet, à chaque fois que le passage d'une puissance de P à la suivante a lieu dans un de ces deux produits, il a également lieu au même endroit dans l'autre. De plus, le report et la correction sont indépendants de la puissance considérée. En continuant ainsi, nous prouvons que la suite des pseudo-P-préfixes de longueur $(c+1)$ des polynômes $(X^m \cdot C)_{m\in\mathbb{N}}$ est ultimement périodique et que le nombre $(b-a)p$ est un multiple de la période de cette suite.

Cette périodicité étant acquise, il est facile de construire un automate fini déterministe qui prouve que l'ensemble

$$\{X^n \cdot C + R : n \in \mathbb{N},\ R \in \mathbb{F}[X]_{<n}\}$$

est P-reconnaissable. Il suffit de commencer l'automate sous la forme d'un arbre complet avec l'état initial comme racine (nous ajoutons un nouvel état

après chaque arc) jusqu'au moment où nous disposons de mots plus longs que le mot $\rho_P(C)$. Ensuite, en chaque feuille de cet arbre, nous construisons un cycle de longueur $(b-a)$ (qui correspond à la période) et nous choisissons bien les états finaux et les états non finaux sur le graphe obtenu. □

Remarquons que l'analogue dans $\mathbb{N}$ des ensembles reconnaissables de type 3 n'existe pas non plus. Par exemple, l'ensemble des nombres dont l'écriture en base 3 commence par le chiffre 1 n'est pas reconnaissable en base 2. En effet, cet ensemble étant 3-reconnaissable, infini et non syndétique (en anticipant sur la définition 7.1.1), il ne peut pas être 2-reconnaissable (en anticipant sur la proposition 7.1.7).

Le lemme 6.1.10 et la proposition 6.1.11 ont pour but de prouver que les ensembles reconnaissables de type 3 constituent bien une nouvelle catégorie d'ensembles reconnaissables indépendantes des deux premières catégories et de leurs combinaisons booléennes.

Lemme 6.1.10. *Pour toute combinaison booléenne $\mathcal{B}$ d'ensembles reconnaissables de type 1 et 2, il existe des polynômes $R_1, R_2, \ldots, R_m, D \in \mathbb{F}[X]$ et des entiers*

$$a_1, a_2, \ldots, a_m, b \in \mathbb{N}$$

tels que l'ensemble $\mathcal{B}$ est égal, à un nombre fini d'éléments près, à l'ensemble

$$\bigcup_{i=1}^{m} \{A \in \mathbb{F}[X] : \deg(A) \equiv a_i \pmod{b} \ \wedge \ A \equiv R_i \pmod{D}\}.$$

Démonstration. Soit $\mathcal{B}$ une combinaison booléenne d'ensembles reconnaissables de type 1 et 2. Une combinaison booléenne d'ensembles peut évidemment se réécrire comme une union finie d'intersections finies de ces ensembles et de leurs complémentaires. Or, le complémentaire d'un ensemble reconnaissable infini de type 1 ou 2 est évidemment une union finie d'ensembles reconnaissables infinis de type 1 et 2. Donc, à un nombre fini d'éléments près, $\mathcal{B}$ est égal à une union finie d'intersections finies d'unions finies d'ensembles reconnaissables infinis de type 1 et 2, et donc, grâce à une loi de distributivité, à une union finie d'intersections finies $\mathcal{I}_i$ ($i \in \{1, 2, \ldots, n\}$) d'ensembles reconnaissables infinis de type 1 et 2. Pour être dans l'intersection $\mathcal{I}_i$, un polynôme doit en fait vérifier certaines congruences modulo certains polynômes non nuls et son degré doit également vérifier certaines congruences modulo certains nombres non nuls. En considérant un commun multiple $D_i \in \mathbb{F}[X]$ de ces polynômes (non nuls) et un commun multiple $n_i \in \mathbb{N}$ de ces nombres (non nuls), nous pouvons réécrire l'intersection $\mathcal{I}_i$ sous la forme d'une union finie de la forme

$$\bigcup_{j=1}^{m_i} \{A \in \mathbb{F}[X] : \deg(A) \equiv c_{j,i} \pmod{d_i} \ \wedge \ A \equiv S_{j,i} \pmod{D_i}\}$$

où $c_{1,i}, \ldots, c_{m_i,i} \in \mathbb{N}$ et $S_{1,i}, \ldots, S_{m_i,i} \in \mathbb{F}[X]$. En considérant une fois encore un commun multiple des d_i et un commun multiple des D_i, nous constatons qu'il existe des polynômes $R_1, R_2, \ldots, R_m, D \in \mathbb{F}[X]$ et des entiers $a_1, a_2, \ldots, a_m, b \in \mathbb{N}$ pour lesquels l'ensemble $\mathcal{B}$ est égal, à un nombre fini d'éléments près, à l'ensemble

$$\bigcup_{i=1}^{m} \{A \in \mathbb{F}[X] : \deg(A) \equiv a_i \pmod{b} \ \wedge \ A \equiv R_i \pmod{D}\}.$$

□

Proposition 6.1.11. *À l'exception près de $(\mathbb{Z}/2\mathbb{Z})[X] \setminus \{0\}$ (si le corps considéré est $\mathbb{Z}/2\mathbb{Z}$), aucun ensemble reconnaissable de type 3 n'est une combinaison booléenne d'ensembles reconnaissables de type 1 et 2.*

Démonstration. Soit $\mathcal{E} = \{X^n \cdot C + R : n \in \mathbb{N}, \ R \in \mathbb{F}[X]_{<n}\}$ un ensemble reconnaissable de type 3, avec $C \in \mathbb{F}[X] \setminus \{0, 1\}$. Il est clair que l'ensemble $\mathcal{E}$ n'est pas égal à un nombre fini d'éléments près à l'ensemble $\mathbb{F}[X]$ (nous aurions l'égalité à un ensemble fini près uniquement si $C = 1$ et si le corps considéré est $\mathbb{Z}/2\mathbb{Z}$). Faisons une démonstration par l'absurde : supposons que $\mathcal{E}$ est une combinaison booléenne d'ensembles reconnaissables de type 1 et 2. Par le lemme 6.1.10 dont nous reprenons ici les notations, nous savons que l'ensemble $\mathcal{E}$ est égal à un nombre fini d'éléments près à un ensemble de la forme

$$\bigcup_{i=1}^{m} \{A \in \mathbb{F}[X] : \deg(A) \equiv a_i \pmod{b} \ \wedge \ A \equiv R_i \pmod{D}\}.$$

Donc il existe nécessairement un polynôme $R \in \mathbb{F}[X]$ de degré strictement inférieur à celui de D et un nombre $c \in \mathbb{N}$ strictement inférieur à b tels que l'ensemble $\mathcal{E}$ ne possède pas plus d'un nombre fini de polynômes à la fois congrus à R modulo D et de degrés congrus à c modulo b. Or, ceci est une contradiction évidente avec la forme de l'ensemble $\mathcal{E}$! □

La preuve de la proposition 6.1.12 est identique à celle de la proposition 6.1.3. Encore une fois, la proposition peut être prouvée par automate fini déterministe (stabilité des langages réguliers par union finie, par intersection finie et par complémentaire).

Proposition 6.1.12. *Toute combinaison booléenne d'ensembles reconnaissables est un ensemble reconnaissable.*

Démonstration. Tout ensemble reconnaissable est P-reconnaissable pour tout $P \in \mathbb{F}[X]_{>0}$, et donc P-définissable pour tout $P \in \mathbb{F}[X]_{>0}$. Toute combinaison booléenne d'ensembles reconnaissables est donc P-définissable pour tout $P \in \mathbb{F}[X]_{>0}$, donc P-reconnaissable pour tout $P \in \mathbb{F}[X]_{>0}$, donc reconnaissable.

□

Corollaire 6.1.13. *Toute combinaison booléenne d'ensembles reconnaissables de type 1,2,3 est un ensemble reconnaissable.*

Démonstration. C'est un cas particulier de la proposition 6.1.12. □

La conjecture 6.1.14 est la combinaison du corollaire 6.1.13 et de sa réciproque, si cette dernière est vraie.

Conjecture 6.1.14. *Un ensemble est reconnaissable si et seulement si il est une combinaison booléenne d'ensembles reconnaissables de type 1,2,3.*

Notons bien que nous ne nous permettons pas de remplacer les mots "combinaison booléenne" par les mots "union finie", contrairement à ce qui est possible dans $\mathbb{N}$. La raison est qu'il y a ici plusieurs types d'ensembles reconnaissables et que l'intersection de deux ensembles reconnaissables de types différents ne peut pas nécessairement être remplacée par une union finie d'ensembles reconnaissables de type 1,2,3. L'intersection des ensembles $\{Q \in \mathbb{F}[X] : Q \equiv 0 \pmod{X}\}$ et $\{Q \in \mathbb{F}[X] : \deg(Q) \equiv 0 \pmod{2}\}$ est un ensemble reconnaissable infini mais n'est pas une union finie d'ensembles reconnaissables de type 1,2,3 puisqu'elle ne contient aucun ensemble reconnaissable infini de l'un des trois types.

6.2 Point de vue de la logique

6.2.1 Cas de $\mathbb{N}$

Proposition 6.2.1. *Pour tout nombre entier p strictement supérieur à 1, les ensembles reconnaissables sont p-définissables.*

Démonstration. C'est évident par le théorème 5.1.1 de Büchi-Bruyère. □

En anticipant sur le théorème 7.5.1 de Cobham et en l'interprétant dans le cadre de la logique au moyen du théorème de Büchi-Bruyère, nous constatons que si p et q sont deux nombres multiplicativement indépendants, alors les ensembles définissables dans les deux structures $\langle \mathbb{N}, +, \mathrm{V_p} \rangle$ et $\langle \mathbb{N}, +, \mathrm{V_q} \rangle$ le sont en fait dans la structure élémentaire $\langle \mathbb{N}, + \rangle$.

Nous prouvons la proposition 6.2.2 sans anticiper sur le théorème de Cobham.

Proposition 6.2.2. *Toute union finie de progressions arithmétiques est définissable par une formule du premier ordre dans la structure $\langle \mathbb{N}, + \rangle$.*

Démonstration. En logique du premier ordre, lorsque des ensembles sont définissables dans une structure, il en va de même de toute union d'un nombre fini de ces ensembles. Il suffit donc de fournir une preuve pour les progressions arithmétiques. Or, cela est évident vu la preuve de la proposition 6.1.2. □

La proposition 6.2.3 est un peu moins forte que le théorème de Cobham. Elle est en fait la traduction dans le langage de la logique de la proposition 6.1.5. Nous ne nous en servons pas avant d'avoir démontrer le théorème 7.5.1 de Cobham car nous n'en fournissons pas de preuve ne découlant pas de ce théorème.

Proposition 6.2.3. *Un ensemble est reconnaissable si et seulement si il est définissable dans la structure* $\langle \mathbb{N}, + \rangle$.

Démonstration. Cela découle directement du théorème 7.5.1 de Cobham et de la proposition 6.2.2. □

6.2.2 Cas de $\mathbb{F}[X]$

Proposition 6.2.4. *Pour tout polynôme* $P \in \mathbb{F}[X]_{>0}$*, les ensembles reconnaissables sont* P*-définissables.*

Démonstration. C'est évident par le théorème 5.2.1 de Büchi-Bruyère. □

Il n'est peut-être pas vrai que nous n'aurons besoin d'aucune nouvelle relation pour décrire les ensembles reconnaissables dans la structure

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]) \rangle.$$

À ce jour, nous n'avons pas trouvé de moyen de définir n'importe quel ensemble reconnaissable de type 2 ou 3 dans cette dernière structure. Ceci motive les définitions 6.2.5 et 6.2.6. Remarquons en plus que nous avons dû rajouter le polynôme 1 au langage (comme constante). En effet, sans la fonction $\mathrm{V_P}$, nous ne pouvons plus définir le polynôme 1 par la formule

$$A = 1 \Leftrightarrow \mathrm{V_P}(0) = A,$$

après avoir défini le polynôme 0 par la formule

$$A = 0 \Leftrightarrow \forall B (A \prec B \vee A = B).$$

Or, il faut pouvoir distinguer le polynôme 1 des autres polynômes de degré 0, si le corps $\mathbb{F}$ n'est pas $\mathbb{Z}/2\mathbb{Z}$.

Définition 6.2.5. Pour tout $k \in \mathbb{N} \setminus \{0\}$, la relation Deg_k est la relation unaire sur $\mathbb{F}[X]$ qui est définie par :
$\mathrm{Deg}_k(A)$ est satisfait si et seulement si $\deg(A)$ est un un nombre entier naturel qui est multiple de k.

Définition 6.2.6. Pour tout $C \in \mathbb{F}[X] \setminus \{0\}$, la relation Deb_C est la relation unaire sur $\mathbb{F}[X]$ qui est définie par :
$\mathrm{Deb}_C(A)$ est satisfait si et seulement si le mot $\rho_X(A)$ débute par le préfixe $\rho_X(C)$.

Nous voulons utiliser les deux relations définies ci-dessus pour complèter la structure $\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X])\rangle$ et en faire une nouvelle structure nous permettant de définir tous les ensembles reconnaissables et aucun autre. Il va donc de soi qu'il faut que ces deux nouvelles relations soient P-définissables pour tout $P \in \mathbb{F}[X]$ de degré supérieur à 1. Nous désirons aussi qu'elles soient P-reconnaissables pour les mêmes polynômes P, mais c'est évidemment équivalent.

Proposition 6.2.7. *Soit $P \in \mathbb{F}[X]_{>0}$. Pour tout $k \in \mathbb{N} \setminus \{0\}$, la relation Deg_k est P-reconnaissable et P-définissable. Pour tout $C \in \mathbb{F}[X] \setminus \{0\}$, la relation Deb_C est P-reconnaissable et P-définissable.*

Démonstration. Soient $P \in \mathbb{F}[X]_{>0}$, $k \in \mathbb{N} \setminus \{0\}$ et $C \in \mathbb{F}[X] \setminus \{0\}$. Grâce au théorème de Büchi-Bruyère, il suffit de prouver le caractère P-reconnaissable des relations Deg_k et Deb_C. Or, d'après la proposition 6.1.8, la relation Deg_k décrit un ensemble reconnaissable de type 2 et, en vertu de la proposition 6.1.9, la relation Deb_C décrit un ensemble reconnaissable de type 3. □

Théorème 6.2.8. *Toute combinaison booléenne d'ensembles reconnaissables de type 1,2,3 est définissable par une formule du premier ordre dans la structure*

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]),$$
$$(\mathrm{Deg}_k : k \in \mathbb{N} \setminus \{0,1\}), (\mathrm{Deb}_C : C \in \mathbb{F}[X] \setminus \{0\})\rangle.$$

Démonstration. En logique du premier ordre, si des ensembles sont définissables dans une structure, il en va de même de n'importe quelle combinaison booléenne de ces ensembles. Il suffit donc de fournir une preuve pour les ensembles reconnaissables de type 1,2,3.

Pour tous $A, B \in \mathbb{F}[X]$, l'ensemble

$$\{A \cdot C + B : C \in \mathbb{F}[X]\}$$

peut être défini par la formule du premier ordre ci-dessous, de variable libre D :

$$\exists C\ (A \cdot C + B = D).$$

Pour tout $a \in \mathbb{N}$ et pour tout $k \in \mathbb{N} \setminus \{0\}$, l'ensemble

$$\{C \in \mathbb{F}[X] : \deg(C) \equiv a \pmod{k}\}$$

peut être défini par la formule du premier ordre ci-desous, de variable libre C :

$$\exists A\ \left(\mathrm{Deg}_k(A)\ \wedge\ C \approx A \cdot X^a\right).$$

Pour tout polynôme non nul $C \in \mathbb{F}[X]$, l'ensemble

$$\{X^n \cdot C + R : n \in \mathbb{N},\ R \in \mathbb{F}[X]_{<n}\}$$

peut tout simplement être défini par la formule $\mathrm{Deb}_C(A)$, de variable libre A. □

Pour le théorème 6.2.8 et la conjecture 6.2.9, nous pouvons aussi nous demander si nous pouvons nous passer des fonctions $(\mathrm{Deb}_C : C \in \mathbb{F}[X] \setminus \{0\})$ et $(\mathrm{Deg}_k : k \in \mathbb{N} \setminus \{0,1\})$, c'est-à-dire si celles-ci sont définissables dans la structure

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]) \rangle.$$

Notre avis est plutôt négatif, mais nous ne disposons pas de preuve jusqu'à ce jour.

Conjecture 6.2.9. *Un ensemble est reconnaissable si et seulement si il est définissable dans la structure*

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]),$$
$$(\mathrm{Deg}_k : k \in \mathbb{N} \setminus \{0,1\}), (\mathrm{Deb}_C : C \in \mathbb{F}[X] \setminus \{0\}) \rangle.$$

6.3 Stabilité

6.3.1 Cas de $\mathbb{N}$

Proposition 6.3.1. *Soit p un entier strictement supérieur à 1. Soient $a_1, \ldots, a_k$ des entiers naturels et $\mathcal{N}_1, \ldots, \mathcal{N}_k$ des parties p-reconnaissables de $\mathbb{N}$. L'ensemble*

$$a_1\mathcal{N}_1 + \cdots a_k\mathcal{N}_k = \{a_1n_1 + \cdots + a_kn_k : n_1 \in \mathcal{N}_1, \ldots, n_k \in \mathcal{N}_k\}$$

est p-reconnaissable.

Démonstration. Cela découle directement du fait qu'un nombre entier naturel n appartient à l'ensemble $a_1\mathcal{N}_1 + \cdots + a_k\mathcal{N}_k$ si et seulement si il satisfait la formule

$$\exists n_1 \in \mathcal{N}_1 \cdots \exists n_k \in \mathcal{N}_k (n = a_1n_1 + \cdots + a_kn_k)$$

dans laquelle les relations d'appartenance sont des relations p-définissables par hypothèse. En effet, cette formule p-définit donc cet ensemble et ce dernier est donc p-reconnaissable en vertu du théorème de Büchi-Bruyère. □

6.3.2 Cas de $\mathbb{F}[X]$

Proposition 6.3.2. *Soit $P \in \mathbb{F}[X]$ un polynôme de degré au moins 1. Soient $A_1, \ldots, A_k \in \mathbb{F}[X]$ des polynômes et $\mathcal{P}_1, \ldots, \mathcal{P}_k$ des sous-ensembles P-reconnaissables de $\mathbb{F}[X]$. L'ensemble*

$$A_1 \cdot \mathcal{P}_1 + \cdots + A_k \cdot \mathcal{P}_k = \{P_1 \cdot A_1 + \cdots + P_k \cdot + A_k : P_1 \in \mathcal{P}_1, \ldots, P_k \in \mathcal{P}_k\}$$

est P-reconnaissable.

Démonstration. Cela découle directement du fait qu'un polynôme $Q \in \mathbb{F}[X]$ appartient à l'ensemble $A_1 \cdot \mathcal{P}_1 + \cdots + A_k \cdot \mathcal{P}_k$ si et seulement si il satisfait la formule

$$\exists P_1 \in \mathcal{P}_1 \cdots \exists P_k \in \mathcal{P}_k (Q = P_1 \cdot A_k + \cdots + P_k \cdot A_k)$$

dans laquelle les relations d'appartenance sont des relations P-définissables par hypothèse. En effet, cette formule P-définit donc cet ensemble et ce dernier est donc P-reconnaissable en vertu du théorème de Büchi-Bruyère. □

6.4 Bases dépendantes

6.4.1 Cas de $\mathbb{N}$

Proposition 6.4.1. *Soient $p \in \mathbb{N} \setminus \{0,1\}$ et $m \in \mathbb{N} \setminus \{0\}$. Une partie de $\mathbb{N}^n$ est p-définissable si et seulement si elle est p^m-définissable.*

Démonstration. Il suffit de prouver que la fonction V_p est p^m-définissable, puis que la fonction V_{p^m} est p-définissable.

Primo, $V_{p^m}(a) = b$ est vrai si et seulement si le couple $(a,b) \in \mathbb{N}^2$ satisfait la formule

$$\exists c \left[V_p(c) = c \wedge c \leq b < cp \wedge X_{p,1}(1,c) \wedge \bigwedge_{k=1}^{m-1} X_{p,0}(p^k, c) \right.$$
$$\left. \wedge \forall d \left(dp^m \leq c \rightarrow \bigwedge_{j \in \Sigma_p} \left(X_{p,j}(d,c) \leftrightarrow X_{p,j}\left(dp^m, c\right)\right)\right)\right]$$
$$\wedge \bigvee_{k=0}^{m-1} V_p(a) = bp^k.$$

Secundo, $V_p(a) = b$ est vrai si et seulement si le couple $(a,b) \in \mathbb{N}^2$ satisfait la formule

$$\bigvee_{k=0}^{m-1} \left(V_{p^m}(a)p^k = b \wedge \ V_{p^m}(ap^{m-k-1}) \neq V_{p^m}(ap^{m-k}) \right).$$

□

Proposition 6.4.2. *Soient $p \in \mathbb{N} \setminus \{0,1\}$ et $m \in \mathbb{N} \setminus \{0\}$. Une partie de $\mathbb{N}^n$ est p-reconnaissable si et seulement si elle est p^m-reconnaissable.*

Démonstration. Cela découle directement de la proposition 6.4.1 et du théorème de Büchi-Bruyère. □

6.4.2 Cas de $\mathbb{F}[X]$

Proposition 6.4.3. *Soient $P \in \mathbb{F}[X]_{>0}$ et $m \in \mathbb{N} \setminus \{0\}$. Une partie de $(\mathbb{F}[X])^n$ est P-définissable si et seulement si elle est P^m-définissable.*

Démonstration. Il suffit de prouver que la fonction V_P est P^m-définissable, puis que la fonction V_{P^m} est P-définissable.

Primo, $V_{P^m}(A) = B$ est vrai si et seulement si le couple $(A, B) \in (\mathbb{F}[X])^2$ satisfait la formule

$$\exists C \left[C \approx B \wedge X_{P,1}(1, C) \wedge \bigwedge_{k=1}^{m-1} X_{P,0}(P^k, C) \right.$$

$$\left. \wedge \forall D \left(D \cdot P^m \preceq C \rightarrow \bigwedge_{J \in \Sigma_P} \left(X_{P,J}(D, C) \leftrightarrow X_{P,J}\left(D \cdot P^m, C\right)\right)\right)\right]$$

$$\wedge \bigvee_{k=0}^{m-1} V_P(A) = B \cdot P^k.$$

Secundo, $V_P(A) = B$ est vrai si et seulement si le couple $(A, B) \in (\mathbb{F}[X])^2$ satisfait la formule

$$\bigvee_{k=0}^{m-1} \left(V_{P^m}(A) \cdot P^k = B \wedge \ V_{P^m}(A \cdot P^{m-k-1}) \neq V_{P^m}(A \cdot P^{m-k}) \right).$$

□

Proposition 6.4.4. *Soient $P \in \mathbb{F}[X]_{>0}$ et $m \in \mathbb{N} \setminus \{0\}$. Une partie de $(\mathbb{F}[X])^n$ est P-reconnaissable si et seulement si elle est P^m-reconnaissable.*

Démonstration. Cela découle directement de la proposition 6.4.3 et du théorème de Büchi-Bruyère. □

Chapitre 7

Théorème de Cobham

Le théorème de Cobham stipule que si un ensemble de nombres entiers naturels est simultanément p-reconnaissable et q-reconnaissable dans deux bases p et q multiplicativement indépendantes, alors cet ensemble est nécessairement une union finie de progressions arithmétiques.

Dans ce chapitre, nous donnons une preuve de ce théorème et nous mettons clairement en évidence les difficultés liées à une adaptation directe de cette preuve au cadre de $\mathbb{F}[X]$.

7.1 Ensembles syndétiques

La preuve originelle [18], due à Cobham, est assez compliquée. D'autres preuves, plus simples, sont apparues par la suite ([3] et [45]). Le plus souvent ces preuves simplifiées commencent par démontrer qu'un ensemble infini de nombres entiers naturels simultanément p-reconnaissable et q-reconnaissable dans deux bases p et q multiplicativement indépendantes est nécessairement syndétique. Mais dans la littérature, les démonstrations de cette première étape comportent un trou présent sous la forme d'un lemme erroné ! Insistons sur le fait que la preuve originelle de Cobham est complète car elle n'est pas concernée par ce lemme. Michel Rigo a remarqué cette erreur et nous avons trouvé une nouvelle démonstration contournant le lemme tabou. Celle-ci est publiée dans l'article [50] (le lemme erroné et un contre-exemple s'y trouvent aussi). Nous l'exposons naturellement dans cette section. Dans cette preuve, nous exploitons l'indépendance multiplicative de p et de q afin de prouver, par un argument de densité, que pour un automate fini déterministe acceptant le langage $\rho_q(\mathcal{N})$ ($\mathcal{N}$ est un ensemble p-reconnaissable, q-reconnaissable et infini), il existe une constante $c \in \mathbb{N}$ pour laquelle il est possible d'arriver à un état final en suivant un chemin de longueur exactement c à partir de n'importe quel état accessible par un mot non vide, ce qui permet immédiatement de conclure.

Définition 7.1.1. Soit $\mathcal{N}$ une partie infinie de $\mathbb{N}$. L'ensemble $\mathcal{N}$ est *syndétique* si il existe une constante $c > 0$ telle que, pour tout $n \in \mathcal{N}$, il existe $m \in \mathcal{N}$ vérifiant les inégatilités $n < m < n + c$.

Lemme 7.1.2. *Soit $(Q, q_0, F, \Sigma, \delta)$ un automate fini déterministe. Pour tout état $q \in Q$, la fonction caractéristique $\chi_{\{|w|:w\in\Sigma^* \text{ et } \delta(q,w)\in F\}}$ est ultimement périodique.*

Démonstration. Pour tout $q \in Q$, définissons la fonction f_q de $\mathbb{N}$ dans $\wp(Q)$ par $f_q(n) = \{\delta(q, w) : w \in \Sigma^* \text{ et } |w| = n\}$. Cette fonction étant à valeurs dans l'ensemble fini $\wp(Q)$, il existe deux entiers naturels distincts a_q et b_q tels que $f_q(a_q) = f_q(b_q)$. Mais alors, pour tout $n \in \mathbb{N}$, il vient :

$$f_q(a_q + n) = \bigcup_{p\in f_q(a_q)} f_p(n) = \bigcup_{p\in f_q(b_q)} f_p(n) = f_q(b_q + n),$$

ce qui prouve que la fonction f_q est ultimement périodique. Comme

$$\chi_{\{|w|:w\in\Sigma^* \text{ et } \delta(q,w)\in F\}} = \chi_{\{n\in\mathbb{N}:f_q(n)\cap F\neq\emptyset\}},$$

nous pouvons conclure que l'ensemble $\chi_{\{|w|:w\in\Sigma^* \text{ et } \delta(q,w)\in F\}}$ est également ultimement périodique. □

Le lemme 7.1.2 est bien connu en théorie des automates finis déterministes. Comme il concerne les longueurs des mots d'un langage régulier sur un alphabet quelconque, il est valable aussi bien pour l'alphabet Σ_p, où p est un nombre entier strictement supérieur à 1, que pour l'alphabet Σ_P, où P est un polynôme de degré au moins 1 sur un corps fini.

Lemme 7.1.3. *Soient p un entier naturel strictement supérieur à 1 et $\mathcal{N}$ une partie infinie p-reconnaissable de $\mathbb{N}$. Il existe trois entiers naturels non nuls m, a, b tels que, pour tout $k \in \mathbb{N}$, l'ensemble $\mathcal{N} \cap [mp^{a+bk}, (m+1)p^{a+bk}[$ est non vide.*

Démonstration. Comme l'ensemble $\mathcal{N}$ est p-reconnaissable, il existe un automate fini déterministe de la forme $(Q, q_0, F, \Sigma_p, \delta)$ qui accepte le langage $\rho_p(\mathcal{N})$. Comme $\mathcal{N}$ est infini, nous pouvons choisir un nombre entier naturel non nul m tel que $\rho_p(m)$ est le préfixe d'une infinité de mots de $\rho_p(\mathcal{N})$. Posons $q = \delta(q_0, \rho_p(m))$. Grâce au lemme 7.1.2, nous savons que la fonction caractéristique $\chi_{\{|w|:w\in(\Sigma_p)^* \text{ et } \delta(q,w)\in F\}}$ est ultimement périodique. Notons a' le nombre à partir duquel cette fonction devient périodique et b sa période. L'intervalle $[mp^{a'}, (m + 1)p^{a'}[$ contient tous les nombres entiers naturels dont la représentation en base p commence par $\rho_p(m)$ et est de longueur $|\rho_p(m)| + a'$. Comme l'ensemble $\rho_p(\mathcal{N})$ contient une infinité de mots commençant par $\rho_p(m)$, il en contient nécessairement un dont la longueur ℓ est strictement supérieure à $|\rho_p(m)| + a'$. Posons $a = \ell - |\rho_p(m)|$. L'intervalle $[mp^a, (m+1)p^a[$ contient un élément de $\mathcal{N}$. Par ultime périodicité, il en va de même de tous les intervalles de la forme $[mp^{a+bk}, (m + 1)p^{a+bk}[$ avec $k \in \mathbb{N}$, ce qui suffit. □

Le lemme 7.1.3 et sa preuve s'adapte aisément au cadre des polynômes sur un corps fini. Dans le cadre des polynômes, si $P \in \mathbb{F}[X]_{>0}$, $M \in \mathbb{F}[X]$ et $a \in \mathbb{N}$, l'intervalle $[MP^a, (M+1)P^a[$ est simplement l'ensemble des polynômes dont la représentation en base P est un mot de longueur $(|\rho_P(M)| + a)$ commençant par le préfixe $\rho_P(M)$.

Lemme 7.1.4. *Soient p un entier naturel strictement supérieur à 1 et $\mathcal{N}$ une partie infinie p-reconnaissable de $\mathbb{N}$. Soit $(Q, q_0, F, \Sigma_p, \delta)$ un automate fini déterministe acceptant le langage $\rho_p(\mathcal{N})$. Si il existe un état $q \in Q$ accessible par un mot non vide et tel que $\{|w| : w \in (\Sigma_p)^*$ et $\delta(q, w) \in F\}$ n'est pas cofini dans $\mathbb{N}$, alors il existe trois entiers naturels non nuls m, a, b tels que, pour tout $k \in \mathbb{N}$, l'ensemble $\mathcal{N} \cap [mp^{a+bk}, (m+1)p^{a+bk}[$ est vide.*

Démonstration. Comme q est accessible par un mot non vide, il existe un entier naturel non nul m tel que $q = \delta(q_0, \rho_p(m))$. Par le lemme 7.1.2, la fonction $\chi_{\{|w|:w\in(\Sigma_p)^* \text{ et } \delta(q,w)\in F\}}$ est ultimement périodique. Notons a' le nombre à partir duquel cette fonction devient périodique et b sa période. L'intervalle $[mp^{a'}, (m+1)p^{a'}[$ ne contient que les nombres entiers naturels dont la représentation en base p commence par $\rho_p(m)$ et est de longueur $|\rho_p(m)| + a'$. Comme l'ensemble $\{|w| : w \in (\Sigma_p)^*$ et $\delta(q, w) \in F\}$ n'est pas cofini dans $\mathbb{N}$, il existe un nombre entier naturel ℓ strictement supérieur à $|\rho_p(m)| + a'$ pour lequel l'ensemble $\rho_p(\mathcal{N})$ ne possède aucun mot de longueur ℓ commençant par $\rho_p(\mathcal{N})$. Posons $a = \ell - |\rho_p(m)|$. Il est clair que l'intervalle $[mp^a, (m+1)p^a[$ est disjoint de $\mathcal{N}$. Par ultime périodicité, il en va de même de tous les intervalles de la forme $[mp^{a+bk}, (m+1)p^{a+bk}[$ avec $k \in \mathbb{N}$, ce qui suffit. □

L'adaptation du lemme 7.1.4 au cadre des polynômes sur un corps fini est immédiate et nécessite simplement la même remarque que pour le lemme 7.1.3.

Lemme 7.1.5. *Soient p, q deux nombres entiers naturels multiplicativement indépendants et strictement supérieurs à 1. Soient m, a, b, n, c, d six nombres entiers naturels non nuls tels que $n < m$. Il existe deux nombres entiers naturels k, l tels que l'intervalle $[mp^{a+bk}, (m+1)p^{a+bk}[$ est inclus dans l'intervalle $[nq^{c+dl}, (n+1)q^{c+dl}[$.*

Démonstration. Il suffit de prouver qu'il existe des entiers naturels k et l vérifiant le système

$$\begin{cases} nq^{c+dl} \leq mp^{a+bk} \\ (m+1)p^{a+bk} \leq (n+1)q^{c+dl} \end{cases},$$

c'est-à-dire tels que

$$\frac{n}{m}\frac{q^c}{p^a} \leq \frac{(p^b)^k}{(q^d)^l} \leq \frac{n+1}{m+1}\frac{q^c}{p^a}.$$

Or, ceci est possible car l'ensemble $\left\{\frac{(p^b)^k}{(q^d)^l} : k, l \in \mathbb{N}\right\}$ est dense dans $[0, +\infty[$ et le nombre $\frac{n}{m}$ est strictement inférieur au nombre $\frac{n+1}{m+1}$. □

Adapter directement le lemme 7.1.5 aux cadres des polynômes sur un corps fini est impossible. Nous le prouvons dans les deux petits paragraphes de discussion qui suivent directement la démonstration du lemme 7.1.6.

Lemme 7.1.6. *Soient p, q deux nombres entiers naturels multiplicativement indépendants et strictement supérieurs à 1. Soit $\mathcal{N}$ une partie infinie p-reconnaissable et q-reconnaissable de $\mathbb{N}$. Soit $(Q, q_0, F, \Sigma_q, \delta)$ un automate fini déterministe acceptant le langage $\rho_q(\mathcal{N})$. Pour tout état $r \in Q$ accessible par un mot non vide, l'ensemble $\{|w| : w \in (\Sigma_q)^* \text{ et } \delta(r, w) \in F\}$ est cofini dans $\mathbb{N}$.*

Démonstration. Démontrons cela par l'absurde. Supposons qu'il existe $r \in Q$ accessible par un mot non vide et tel que $\{|w| : w \in (\Sigma_q)^* \text{ et } \delta(r, w) \in F\}$ est non cofini dans $\mathbb{N}$. Par le lemme 7.1.4, il existe des entiers naturels non nuls n, c, d tels que, pour tout $l \in \mathbb{N}$, l'ensemble $\mathcal{N} \cap [nq^{c+dl}, (n+1)q^{c+dl}[$ est vide. Par le lemme 7.1.3, il existe des entiers naturels non nuls m, a, b tels que, pour tout $k \in \mathbb{N}$, l'ensemble $\mathcal{N} \cap [mp^{a+bk}, (m+1)p^{a+bk}[$ est non vide. De plus, m peut être choisi arbitrairement grand et en particulier tel que $n < m$. Or, par le lemme 7.1.5, il existe deux nombres entiers naturels k et l tels que l'intervalle $[mp^{a+bk}, (m+1)p^{a+bk}[$ est inclus dans l'intervalle $[nq^{c+dl}, (n+1)q^{c+dl}[$, ce qui est une contradiction avec ce qui précède. □

Le lemme 7.1.6 ne peut pas s'adapter directement au cadre d'un ensemble de polynômes sur un corps fini. En effet, les ensembles reconnaissables de type 2 de $\mathbb{F}[X]$ sont des ensembles infinis reconnaissables dans toutes les bases $P \in \mathbb{F}[X]_{>0}$, mais pourtant (en reprenant les notations du lemme 7.1.6) certains ensembles

$$\{|w| : w \in (\Sigma_Q)^* \text{ et } \delta(r, w) \in F\}$$

qui leur correspondent ne sont pas nécessairement cofinis. Un contre-exemple est donné par l'ensemble des polynômes de degré pair, sur n'importe quel corps fini, en base $Q = X$.

Remarquons que, exception éventuelle faite de l'utilisation du lemme 7.1.5, toute la preuve du lemme 7.1.6 s'adapte directement au cadre des polynômes sur un corps fini. Nous déduisons donc que le lemme 7.1.5 ne peut pas s'adapter directement à ce cadre.

Proposition 7.1.7. *Soient p et q deux entiers naturels multiplicativement indépendants et strictement supérieurs à 1. Si $\mathcal{N}$ une partie infinie de $\mathbb{N}$ qui est p-reconnaissable et q-reconnaissable, alors $\mathcal{N}$ est syndétique.*

Démonstration. Considérons un automate fini déterministe $(Q, q_0, F, \Sigma_q, \delta)$ acceptant le langage $\rho_q(\mathcal{N})$. Pour tout entier naturel non nul n, posons $q_n = \delta(q_0, \rho_q(n))$. Comme q_n est accessible par le mot non vide $\rho_q(n)$, nous déduisons du lemme 7.1.6 que l'ensemble $\{|w| : w \in (\Sigma_q)^* \text{ et } \delta(q_n, w) \in F\}$ est cofini dans $\mathbb{N}$. Donc, pour tout entier naturel non nul n, il existe un entier naturel non nul c_n tel que, pour tout $k \geq c_n$, le nombre k appartient à l'ensemble $\{|w| : w \in (\Sigma_q)^* \text{ et } \delta(q_n, w) \in F\}$. Nous pouvons évidement choisir les c_n de façon à ce que l'égalité $q_m = q_n$ implique l'égalité $c_m = c_n$. Comme le nombre d'éléments de Q est fini, le nombre $c = \sup\{c_n : n \in \mathbb{N} \setminus \{0\}\}$ existe dans $\mathbb{N}$. Donc, pour tout entier naturel non nul n, il existe $w_n \in (\Sigma_q)^*$ tel que $|w_n| = c$ et que $\delta(q_n, w_n) \in F$. Pour tout entier naturel non nul n, soit x_n le nombre entier naturel tel que $\rho_q(x_n) = w_n$. Comme $|w_n| = c$, le nombre x_n vérifie l'inégalité $x_n < q^c$. De plus, le nombre $(nq^c + x_n)$ appartient évidemment à $\mathcal{N}$. Or, comme

$$\begin{aligned}&((n+1)q^c + x_{n+1})) - (nq^c + x_n))\\ &= q^c + x_{n+1} - x_n \in [1, 2q^c - 1],\end{aligned}$$

nous déduisons que $\mathcal{N}$ est syndétique. □

Définition 7.1.8. Soit $\mathcal{P}$ une partie infinie de $\mathbb{F}[X]$. L'ensemble $\mathcal{P}$ est *syndétique* si les termes de la suite

$$s_n = \frac{\#\{Q \in \mathcal{P} : deg(Q) = n\}}{(\#\mathbb{F})^n}$$

ne prennent qu'un nombre fini de valeurs différentes et sont tels que chacun des ensembles $E_n = \{m \in \mathbb{N} : s_m = s_n\}$ est une partie finie ou syndétique de $\mathbb{N}$.

Dans l'état actuel de nos connaissances, rien ne prouve que toute partie reconnaissable de $\mathbb{F}[X]$ est syndétique au sens de la définition 7.1.8. Toutefois, il nous semble raisonnable de le penser puisque les ensembles reconnaissables de type 1,2,3 de $\mathbb{F}[X]$ sont syndétiques et que les combinaisons booléennes des ensembles syndétiques sont syndétiques. De plus, l'ensemble $P^{\mathbb{N}}$ n'est pas une partie syndétique de $\mathbb{F}[X]$ (la sous-suite formée des termes non nuls de la suite s_n est une progression géométrique de raison $(\#\mathbb{F})^{-\deg(P)}$) à l'instar de $p^{\mathbb{N}}$ qui n'est pas une partie syndétique de $\mathbb{N}$.

7.2 Noyau

Le lecteur désireux d'en savoir plus sur les notions abordées dans cette section (noyau, p-noyau) et la suivante (suite p-automatique) peut consulter l'ouvrage [3], ainsi que les articles [19], [34], [21] et [22].

7.2.1 Cas de $\mathbb{N}$

Définition 7.2.1. Soit $\mathcal{N}$ une partie de $\mathbb{N}$. La relation binaire $\sim_{\mathcal{N}}$ sur $\mathbb{N}$ est satisfaite par un couple $(m, n) \in \mathbb{N}^2$ si et seulement si celui-ci satisfait la formule

$$\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ (am + b \in \mathcal{N} \Leftrightarrow an + b \in \mathcal{N}).$$

Proposition 7.2.2. *Soit $\mathcal{N}$ une partie de $\mathbb{N}$. La relation $\sim_{\mathcal{N}}$ est une relation d'équivalence sur $\mathbb{N}$.*

Démonstration. Il est évident que cette relation est réflexive, symétrique et transitive. □

Comme la relation $\sim_{\mathcal{N}}$ est une relation d'équivalence sur $\mathbb{N}$, nous pouvons considérer le quotient de $\mathbb{N}$ par cette relation. Ce dernier est appelé *noyau* de $\mathcal{N}$.

Proposition 7.2.3. *Soit $\mathcal{N}$ une partie de $\mathbb{N}$. Le quotient $(\mathbb{N}/\sim_{\mathcal{N}})$ est un ensemble fini si et seulement si l'ensemble $\mathcal{N}$ est une union finie de progressions arithmétiques.*

Démonstration. En premier lieu, supposons que le quotient $(\mathbb{N}/\sim_{\mathcal{N}})$ est un ensemble fini. Alors, au moins une classe d'équivalence de la relation $\sim$ possède au moins deux éléments distincts. Soient $m, n \in \mathbb{N}$ deux éléments d'une même classe d'équivalence de la relation $\sim_{\mathcal{N}}$ pour lesquels $(n - m)$ est un nombre entier strictement positif que nous notons t. Il est clair que pour chaque valeur de $b \in \mathbb{N}$, les nombres $(m + b)$ et $(n + b) = (m + b + t)$ sont tous les deux dans l'ensemble $\mathcal{N}$ ou n'y sont aucun des deux. Cela signifie que la fonction caractéristique de l'ensemble $\mathcal{N}$ est ultimement périodique (sa période est un diviseur du nombre t et commence au plus tard avec le nombre m) et donc que $\mathcal{N}$ est une union finie de progressions arithmétiques.

En second lieu, supposons que $\mathcal{N}$ est une union finie de progressions arithmétiques. Sa fonction caractéristique est alors ultimement périodique. Soit t sa période et c le nombre à partir duquel celle-ci débute. Quels que soient $a, b, m \in \mathbb{N}$ tels $m \geq c$, le nombre $(a(m + t) + b) = (am + b + at)$ appartient à $\mathcal{N}$ si et seulement si le nombre $am + b$ appartient à $\mathcal{N}$. Cela signifie que pour tout $m \in \mathbb{N}$ tel que $m \geq c$, $(m \sim_{\mathcal{N}} m + t)$. Il ne peut donc pas y avoir plus de $(c + t)$ éléments dans le quotient $(\mathbb{N}/\sim_{\mathcal{N}})$, et celui-ci est donc un ensemble fini. □

Définition 7.2.4. Soient $\mathcal{N}$ une partie de $\mathbb{N}$ et p un nombre entier strictement supérieur à 1. La relation binaire $\sim^p_{\mathcal{N}}$ sur $\mathbb{N}$ est satisfaite par un couple $(m, n) \in \mathbb{N}^2$ si et seulement si celui-ci satisfait la formule

$$\forall a \in p^{\mathbb{N}}\ \forall b \in \{0, 1, \ldots, a - 1\}\ (am + b \in \mathcal{N} \Leftrightarrow an + b \in \mathcal{N}).$$

Proposition 7.2.5. *Soient $\mathcal{N}$ une partie de $\mathbb{N}$ et p un nombre entier strictement supérieur à 1. La relation $\sim^p_{\mathcal{N}}$ est une relation d'équivalence sur $\mathbb{N}$.*

Démonstration. Il est évident que cette relation est réflexive, symétrique et transitive. □

Le quotient $(\mathbb{N}/\sim^p_{\mathcal{N}})$ est appelé *p-noyau* de $\mathcal{N}$.

Proposition 7.2.6. *Soient $\mathcal{N}$ une partie de $\mathbb{N}$ et p un nombre entier strictement supérieur à 1. Le quotient $(\mathbb{N}/\sim^p_{\mathcal{N}})$ est un ensemble fini si et seulement si l'ensemble $\mathcal{N}$ est p-reconnaissable.*

Démonstration. Si $\mathcal{N}$ est p-reconnaissable, alors il existe un automate fini déterministe $(Q, q_0, F, \Sigma_p, \delta)$ qui accepte le langage $\rho_p(\mathcal{N})$. Si deux nombres $m, n \in \mathbb{N}$ sont tels que $\delta(q_0, \rho_p(m)) = \delta(q_0, \rho_p(n))$, alors il vient :

$$\begin{aligned} & \delta(q_0, \rho_p(p^k m + b)) \\ = \ & \delta(\delta(q_0, \rho_p(m)), 0^{k-|\rho_p(b)|}\rho_p(b)) \\ = \ & \delta(\delta(q_0, \rho_p(n)), 0^{k-|\rho_p(b)|}\rho_p(b)) \\ = \ & \delta(q_0, \rho_p(p^k n + b)) \end{aligned}$$

quels que soient $k \in \mathbb{N}$ et $b \in \{0, 1, \ldots, p^k - 1\}$, ce qui implique que l'état $\delta(q_0, \rho_p(p^k m + b))$ est final si et seulement si l'état $\delta(q_0, \rho_p(p^k n + b))$ l'est aussi (quels que soient $k \in \mathbb{N}$ et $b \in \{0, 1, \ldots, p^k - 1\}$), et donc que $m \sim^p_{\mathcal{N}} n$. Comme le nombre d'états de l'automate est fini, il est alors clair que le quotient $(\mathbb{N}/\sim^p_{\mathcal{N}})$ est un ensemble fini.

Inversement, si le quotient $(\mathbb{N}/\sim^p_{\mathcal{N}})$ est un ensemble fini, alors prouvons que nous pouvons construire un automate fini déterministe acceptant le langage $\rho_p(\mathcal{N})$ et pour lequel chaque état correspond à un élément de ce quotient. L'alphabet est évidemment Σ_p. Si $m \in \mathbb{N}$ et $n \in \mathbb{N}$ sont deux représentants d'un même élément de ce quotient, comme $m \sim^p_{\mathcal{N}} n$, les nombres $(p^{k+j}m + (p^j b + c))$ et $(p^{k+j}n + (p^j b + c))$ sont tous les deux dans $\mathcal{N}$ ou n'y sont aucun des deux, quels que soient $k, j \in \mathbb{N}$, $b \in \{0, 1, \ldots, p^k - 1\}$ et $c \in \{0, 1, 2, \ldots, p^j - 1\}$. Mais, comme ces nombres s'écrivent aussi sous les formes $(p^j(p^k m + b) + c)$ et $(p^j(p^k n + b) + c)$, cela signifie alors évidemment que $(p^k m + b \sim^p_{\mathcal{N}} p^k n + b)$ quels que soient $k \in \mathbb{N}$ et $b \in \{0, 1, \ldots, p^k - 1\}$. Ce dernier point assure l'existence d'une fonction de transition respectant la correspondance entre une classe d'équivalence et un état, l'état initial est l'état auquel correspond la classe d'équivalence du nombre 0 et, comme la relation $m \sim^p_{/n} n$ implique que les nombres $(m = 1 \cdot m + 0)$ et $(n = 1 \cdot n + 0)$ sont tous les deux dans $\mathcal{N}$ ou n'y sont aucun des deux, il est possible de choisir les états finals de façon à ce que le langage accepté par l'automate soit $\rho_p(\mathcal{N})$. □

7.2.2 Cas de $\mathbb{F}[X]$

Nous essayons ici de transposer les mêmes idées que dans le cadre des entiers naturels, mais nous sommes obligés de limiter le degré de B dans la définition 7.2.7, notamment pour éviter un éventuel conflit indésirable entre le coefficient de plus haut degré de AM et celui de B. Nous reviendrons sur ce point dans la preuve de la proposition 7.2.9.

Définition 7.2.7. Soit $\mathcal{P}$ une partie de $\mathbb{F}[X]$. La relation binaire $\sim_{\mathcal{P}}$ sur $\mathbb{F}[X]$ est satisfaite par un couple $(M, N) \in (\mathbb{F}[X])^2$ si et seulement si celui-ci satisfait la formule

$$\forall A \in \mathbb{F}[X]\ \forall B \in \mathbb{F}[X]_{<\deg(A)}\ (AM + B \in \mathcal{P} \Leftrightarrow AN + B \in \mathcal{P}).$$

Proposition 7.2.8. *Soit $\mathcal{P}$ une partie de $\mathbb{F}[X]$. La relation $\sim_{\mathcal{P}}$ est une relation d'équivalence sur $\mathbb{F}[X]$.*

Démonstration. Il est évident que cette relation est réflexive, symétrique et transitive. □

Le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est appelé *noyau* de $\mathcal{P}$.

Proposition 7.2.9. *Soit $\mathcal{P}$ une partie de $\mathbb{F}[X]$. Le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est un ensemble fini si l'ensemble $\mathcal{P}$ est une combinaison booléenne d'ensembles reconnaissables de type 1,2,3.*

Démonstration. Remarquons d'abord que si les polynômes $M, N \in \mathbb{F}[X]$ sont tels que $M \equiv N \pmod{D}$ pour un certain polynôme $D \in \mathbb{F}[X] \setminus \{0\}$, alors $AM + B \equiv AN + B \pmod{D}$ quels que soient les polynômes $A, B \in \mathbb{F}[X]$ tels que $B \prec A$. Il résulte de ceci que, si $\mathcal{P}$ est un ensemble infini reconnaissable de type 1, alors l'ensemble $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est fini (le caractère fini de l'ensemble $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ ne dépend pas de $\mathcal{P}$ à un nombre fini d'éléments près). Cela est évidemment vrai aussi si $\mathcal{P}$ est un ensemble fini.

Remarquons[1] ensuite que si les polynômes $M, N \in \mathbb{F}[X]$ sont tels que $\deg(M) \equiv \deg(N) \pmod{d}$ pour un certain nombre $d \in \mathbb{N} \setminus \{0\}$, alors $\deg(AM + B) \equiv \deg(AN + B) \pmod{d}$ quels que soient les polynômes $A, B \in \mathbb{F}[X]$ tels que $B \prec A$. Il résulte de ceci que, si $\mathcal{P}$ est un ensemble reconnaissable de type 2, alors l'ensemble $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est fini.

Remarquons également que si les polynômes $M, N \in \mathbb{F}[X]$ sont tels que $\rho_X(M)$ et $\rho_X(N)$ commencent par le même préfixe $\rho_X(C)$ pour un certain polynôme $C \in \mathbb{F}[X] \setminus \{0\}$, alors $\rho_X(AM + B)$ et $\rho_X(AN + B)$ commencent aussi par le même préfixe de même longueur que $\rho_X(C)$ quels que soient les

[1] Si dans la définition 7.2.7 nous n'avions pas limité le degré du polynôme B, alors ce paragraphe et le suivant seraient faux.

polynômes $A, B \in \mathbb{F}[X]$ tels que $B \prec A$. Il résulte de ceci que, si $\mathcal{P}$ est un ensemble reconnaissable de type 3, alors l'ensemble $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est fini.

Remarquons finalement que si $\mathcal{P}_1$ et $\mathcal{P}_2$ sont des parties de $\mathbb{F}[X]$ telles que les ensembles $(\mathbb{F}[X]/\sim_{\mathcal{P}_1})$ et $(\mathbb{F}[X]/\sim_{\mathcal{P}_2})$ sont finis, alors les ensembles $(\mathbb{F}[X]/\sim_{(\mathcal{P}_1\cup\mathcal{P}_2)})$, $(\mathbb{F}[X]/\sim_{(\mathcal{P}_1\cap\mathcal{P}_2)})$ et $(\mathbb{F}[X]/\sim_{(\mathbb{F}[X]\setminus\mathcal{P}_1)})$ sont finis aussi. En effet, pour l'union par exemple, si $M, N \in \mathbb{F}[X]$ sont tels que $(M \sim_{\mathcal{P}_1} N)$ et $(M \sim_{\mathcal{P}_2} N)$, alors les équivalences suivantes sont satisfaites pour tous polynômes $A, B \in \mathbb{F}[X]$ tels que $B \prec A$, ce qui prouve que $(M \sim_{(\mathcal{P}_1\cup\mathcal{P}_2)} N)$: $(AM + B \in \mathcal{P}_1 \cup \mathcal{P}_2)$ si et seulement si $(AM + B \in \mathcal{P}_1 \vee AM + B \in \mathcal{P}_2)$ si et seulement si $(AN + B \in \mathcal{P}_1 \vee AN + B \in \mathcal{P}_2)$ si et seulement si $(AN + B \in \mathcal{P}_1 \cup \mathcal{P}_2)$.

De tout ceci, il résulte que, pour tout ensemble $\mathcal{P}$ qui est une combinaison booléenne d'ensembles reconnaissables de type 1,2,3, le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est un ensemble fini. □

Conjecture 7.2.10. *Soit $\mathcal{P}$ une partie de $\mathbb{F}[X]$. Le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est un ensemble fini si et seulement si l'ensemble $\mathcal{P}$ est une combinaison booléenne d'ensembles reconnaissables de type 1,2,3.*

La proposition 7.2.11 est plutôt encourageante.

Proposition 7.2.11. *Soit $P \in \mathbb{F}[X]_{>0}$. Le quotient $(\mathbb{F}[X]/\sim_{P^{\mathbb{N}}})$ est un ensemble infini.*

Démonstration. Quels que soient $m, n \in \mathbb{N}$ tels que $m < n$, le polynôme $AP^m + B$ appartient à $P^{\mathbb{N}}$ et et le polynôme $AP^n + B$ n'y appartient pas, si $A = P^n - 1$ et $B = P^m \prec A$. Cela signifie que le quotient $(\mathbb{F}[X]/\sim_{P^{\mathbb{N}}})$ possède un nombre infini d'éléments. □

Le reste de cette sous-section est proche de son analogue dans le cadre des entiers naturels. C'est dû au fait que la restriction sur le degré de B dans la définition 7.2.12 a son analogue dans la définition 7.2.4.

Définition 7.2.12. Soient $\mathcal{P}$ une partie de $\mathbb{F}[X]$ et $P \in \mathbb{F}[X]_{>0}$. La relation binaire $\sim^P_{\mathcal{P}}$ sur $\mathbb{F}[X]$ est satisfaite par un couple $(M, N) \in (\mathbb{F}[X])^2$ si et seulement si celui-ci satisfait la formule

$$\forall A \in P^{\mathbb{N}}\ \forall B \in \mathbb{F}[X]_{<\deg(A)}\ (AM + B \in \mathcal{P} \Leftrightarrow AN + B \in \mathcal{P}).$$

Proposition 7.2.13. *Soient $\mathcal{P}$ une partie de $\mathbb{F}[X]$ et $P \in \mathbb{F}[X]_{>0}$. La relation $\sim^P_{\mathcal{P}}$ est une relation d'équivalence sur $\mathbb{F}[X]$.*

Démonstration. Il est évident que cette relation est réflexive, symétrique et transitive. □

Le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}}^{P})$ est appelé *P-noyau* de $\mathcal{P}$.

Proposition 7.2.14. *Soient $\mathcal{P}$ une partie de $\mathbb{F}[X]$ et $P \in \mathbb{F}[X]_{>0}$. Le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}}^{P})$ est un ensemble fini si et seulement si l'ensemble $\mathcal{P}$ est P-reconnaissable.*

Démonstration. Si $\mathcal{P}$ est P-reconnaissable, alors il existe un automate fini déterministe $(Q, q_0, F, \Sigma_P, \delta)$ qui accepte le langage $\rho_P(\mathcal{P})$. Si deux polynômes $M, N \in \mathbb{F}[X]$ sont tels que $\delta(q_0, \rho_P(M)) = \delta(q_0, \rho_P(N))$, alors il vient :

$$\begin{aligned} & \delta(q_0, \rho_P(P^k M + B)) \\ = \ & \delta(\delta(q_0, \rho_P(M)), 0^{k-|\rho_P(B)|}\rho_P(B)) \\ = \ & \delta(\delta(q_0, \rho_P(N)), 0^{k-|\rho_P(B)|}\rho_P(B)) \\ = \ & \delta(q_0, \rho_P(P^k N + B)) \end{aligned}$$

quels que soient $k \in \mathbb{N}$ et $B \in \mathbb{F}[X]_{<k\deg(P)}$, ce qui implique que, quels que soient $k \in \mathbb{N}$ et $B \in \mathbb{F}[X]_{<k\deg(P)}$, l'état $\delta(q_0, \rho_P(P^k M + B))$ est final si et seulement si l'état $\delta(q_0, \rho_P(P^k N + B))$ l'est aussi, et donc que $M \sim_{\mathcal{P}}^{P} N$. Comme le nombre d'états de l'automate est fini, il est alors clair que le quotient $(\mathbb{N}/\sim_{\mathcal{P}}^{P})$ est un ensemble fini.

Inversement, si le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}}^{P})$ est un ensemble fini, alors prouvons que nous pouvons construire un automate fini déterministe acceptant le langage $\rho_P(\mathcal{P})$ et pour lequel chaque état correspond à un élément de ce quotient. L'alphabet est évidemment Σ_P. Si $M \in \mathbb{F}[X]$ et $N \in \mathbb{F}[X]$ sont deux représentants d'un même élément de ce quotient, comme $M \sim_{\mathcal{P}}^{P} N$, les nombres $(P^{k+j}M + (P^j B + C))$ et $(P^{k+j}N + (P^j B + C))$ sont tous les deux dans $\mathcal{P}$ ou n'y sont aucun des deux, quels que soient $k, j \in \mathbb{N}$, $B \in \mathbb{F}[X]_{<k\deg(P)}$ et $C \in \mathbb{F}[X]_{<j\deg(P)}$. Mais alors comme ces nombres s'écrivent aussi sous la forme $(P^j(P^k M + B) + C)$ et $(P^j(P^k N + B) + C)$, cela signifie que $(P^k M + B \sim_{\mathcal{P}}^{P} P^k N + B)$ quels que soient $k \in \mathbb{N}$ et $B \in \mathbb{F}[X]_{<k\deg(P)}$. Ce dernier point assure l'existence d'une fonction de transition respectant la correspondance entre une classe d'équivalence et un état, l'état initial est l'état auquel correspond la classe d'équivalence du polynôme 0 et, comme la relation $M \sim_{/p}^{P} N$ implique que les polynômes $(M = 1 \cdot M + 0)$ et $(N = 1 \cdot N + 0)$ sont tous les deux dans $\mathcal{P}$ ou n'y sont aucun des deux, il est possible de choisir les états finals de façon à ce que le langage accepté par l'automate soit $\rho_P(\mathcal{P})$. □

7.3 Suite automatique

Le lecteur qui désire approfondir ses connaissances sur les notions de cette section (suite p-automatique) et de la précédente (noyau, p-noyau) peut consulter le livre [3] et les articles [19], [21], [22], [34].

7.3.1 Cas de $\mathbb{N}$

Définition 7.3.1. Un *automate fini déterministe avec sortie* est la donnée d'un sextuplet $(Q, q_0, \Sigma, \delta, \Pi, \pi)$ pour lequel :
Q est un ensemble fini dont chaque élément est appelé *état*,
q_0 est un des éléments de Q et est appelé *état initial*,
Σ est un alphabet,
δ est une fonction de $Q \times \Sigma$ dans Q et est appelée *fonction de transition*,
Π est un alphabet et est appelé *alphabet de sortie*,
π est une fonction totale de Q dans Π et est appelée *fonction de sortie*.

Les automates finis déterministes avec sortie sont une généralisation des automates finis déterministes. Dans un automate fini déterministe, il n'y a que deux possibilités pour les états : ceux qui sont finals et ceux qui ne le sont pas. Dans un automate fini déterministe avec sortie, il y en a $\#\Pi$. La fonction de transition s'étend naturellement sur $Q \times \Sigma^*$ comme dans le cadre des automates finis déterministes.

Définition 7.3.2. Soient p un nombre entier strictement supérieur à 1 et $(x_n)_{n\in\mathbb{N}}$ une suite infinie construite sur un alphabet Π. La suite $(x_n)_{n\in\mathbb{N}}$ est *p-automatique* si et seulement si il existe un morphisme f de Σ^* dans Σ^* de longueur p prolongeable sur un élément $a \in \Sigma$ et un morphisme g de Σ^* dans Π^* de longueur 1 pour lesquels $(x_n)_{n\in\mathbb{N}} = g(f^\omega(a))$.

Remarque 7.3.3. La notation f^ω signifie que le morphisme f est appliqué de façon illimitée. Cette répétition génère une suite de mot $f(a)$, $f(f(a))$, $f(f(f(a)))$, ... dont les longueurs sont strictement croissantes (une progression géométrique de raison $p > 1$). Comme f est un morphisme prolongeable sur a, chaque mot de cette suite est le préfixe du mot suivant. La limite de cette suite est notée $f^\omega(a)$ et est, par définition, l'unique suite infinie ayant chacun des mots de la suite $f(a), f(f(a)), f(f(f(a))), \ldots$ comme préfixe. Le morphisme g, de longueur 1, est étendu naturellement sur l'ensemble des mots infinis.

Théorème 7.3.4. *Soient p un nombre entier strictement supérieur à 1 et $(x_n)_{n\in\mathbb{N}}$ une suite infinie construite sur un alphabet Π. Il existe un automate fini déterministe avec sortie $\mathcal{A} = (Q, q_0, \Sigma_p, \delta, \Pi, \pi)$ tel que, pour tout $n \in \mathbb{N}$,*

$$x_n = \pi(\delta(q_0, \rho_p(n))),$$

si et seulement si la suite $(x_n)_{n\in\mathbb{N}}$ est p-automatique.

Corollaire 7.3.5. *Soit p un nombre entier strictement supérieur à 1. Une partie $\mathcal{N}$ de $\mathbb{N}$ est p-reconnaissable si et seulement si son mot caractéristique $\chi(\mathcal{N})$ est p-automatique.*

Démonstration. C'est une conséquence directe du théorème 7.3.4. □

7.3.2 Cas de $\mathbb{F}[X]$

Définition 7.3.6. Soient Σ et Π deux alphabets finis et P un polynôme de degré au moins 1 de $\mathbb{F}[X]$. Une suite infinie $(x_A)_{A\in\mathbb{F}[X]}$ construite sur Π est dite *P-automatique* si il existe une fonction f de $\mathbb{F}[X]$ dans Σ telle que, pour tout $Q \in \mathbb{F}[X]$ et tout $R \in \Sigma_P$, $f(P\cdot Q + R)$ ne dépend que du couple $(f(Q), R)$ et une fonction g de Σ dans Π pour lesquelles

$$\forall A \in \mathbb{F}[X] : x_A = g(f(A)).$$

Théorème 7.3.7. *Soient P un polynôme de degré au moins 1 de $\mathbb{F}[X]$ et $(x_A)_{A\in\mathbb{F}[X]}$ une suite infinie construite sur un alphabet Π. Il existe un automate fini déterministe avec sortie $\mathcal{A} = (Q, q_0, \Sigma_P, \delta, \Pi, \pi)$ tel que, pour tout $A \in \mathbb{F}[X]$,*

$$x_A = \pi(\delta(q_0, \rho_P(A))),$$

si et seulement si la suite $(x_A)_{A\in\mathbb{F}[X]}$ est P-automatique.

Démonstration. Si la suite infinie $(x_A)_{A\in\mathbb{F}[X]}$ est P-automatique, alors elle est décrite par deux fonctions f et g (au sens de la définition 7.3.6). Construisons un automate fini déterministe avec sortie. L'ensemble des états de l'automate est Σ. L'état initial est $f(0) \in \Sigma$. L'alphabet est Σ_P. La fonction de transition δ est définie pour tout $M \in \Sigma$ et tout $N \in \Sigma_P$ par $\delta(M, N) = f(L\cdot P + N) \in \Sigma$ où $L \in \mathbb{F}[X]$ est tel que $f(L) = M$, ce qui est licite car $f(L\cdot P + N)$ ne dépend que de $f(L)$ et N. L'alphabet de sortie est Π. La fonction de sortie π est g. Comme g est π, il suffit de démontrer que pour tout $A \in \mathbb{F}[X]$, $f(A) = \delta(f(0), \rho_P(A))$. Procédons par récurrence.

Pour $A = 0$, il vient : $\delta(f(0), \rho_P(0)) = \delta(f(0), \varepsilon) = f(0)$.

Pour $A \in (\mathbb{F}[X]\setminus\{0\})$, soient B le quotient et C le reste de la division de A par P. Grâce à l'hypothèse de récurrence $\delta(f(0), \rho_P(B)) = f(B)$, il vient :

$$\delta(f(0), \rho_P(A)) = \delta(f(0), \rho_P(B)C) = \delta(\delta(f(0), \rho_P(B)), C)$$
$$= \delta(f(B), C) = f(B\cdot P + C) = f(A).$$

Réciproquement, supposons qu'il existe un alphabet avec sortie

$$\mathcal{A} = (Q, q_0, \Sigma_P, \delta, \Pi, \pi)$$

pour lequel $x_A = \pi(\delta(q_0, \rho_P(A)))$ quel que soit $A \in \mathbb{F}[X]$. Définissons les fonctions f et g par $g = \pi$ et $f : \mathbb{F}[X] \to Q,\ A \mapsto \delta(q_0, \rho_P(A))$. Nous avons

$$(x_A)_{A\in\mathbb{F}[X]} = (g(f(A)))_{A\in\mathbb{F}[X]}.$$

De plus, pour tout $N \in \Sigma_P$ et tout $L \in \mathbb{F}[X]$, il vient

$$f(L\cdot P + N) = \delta(q_0, \rho_P(L\cdot P + N)) = \delta(\delta(q_0, \rho_P(L)), N) = \delta(f(L), N),$$

ce qui signifie que $f(L\cdot P + N)$ ne dépend que du couple $(f(L), N)$.

□

Corollaire 7.3.8. *Soit P un polynôme de degré au moins 1 de $\mathbb{F}[X]$. Une partie $\mathcal{P}$ de $\mathbb{F}[X]$ est P-reconnaissable si et seulement si son mot caractéristique $\chi(\mathcal{P})$ est P-automatique.*

Démonstration. C'est une conséquence directe du théorème 7.3.7. □

7.4 Fonction de complexité

7.4.1 Cas de $\mathbb{N}$

Définition 7.4.1. Soit Σ un alphabet. Un *mot infini* sur Σ est une suite infinie

$$a_0 a_1 a_2 \cdots$$

de lettres $a_0, a_1, a_2, \ldots$ de Σ.

Définition 7.4.2. Soit $\omega = a_0 a_1 a_2 \cdots$ un mot infini sur un alphabet Σ. Un *facteur* de ω est un mot m sur Σ pour lequel il existe des entiers $k, n \in \mathbb{N}$ tels que $m = a_k \cdots a_{k+n-1}$. Un *facteur récurrent* de ω est un facteur m de ω pour lequel il existe une infinité de valeurs de $k \in \mathbb{N}$ telles que $m = a_k \cdots a_{k+n-1}$ pour un certain $n \in \mathbb{N}$.

Si ω est un mot infini sur un alphabet Σ, le mot vide ε est le seul facteur de longueur nulle de ω et il est récurrent. Si le mot ω est ultimement périodique, alors il existe une constante $c \in \mathbb{N}$ telle que, pour tout $n \in \mathbb{N}$, le nombre de facteurs de longueur n du mot ω est borné par c. La réciproque de ce résultat est donnée dans le théorème 7.4.4 et est due à M. Morse et G. A. Hedlund.

Définition 7.4.3. Soit ω un mot infini sur un alphabet Σ. La *fonction de complexité* de ω est notée p_ω et est définie par

$$p_\omega : \mathbb{N} \to \mathbb{N},\ n \mapsto \#\{m \in \Sigma^* : m \text{ facteur de } \omega, |m| = n\}.$$

La fonction de complexité p_ω d'un mot infini ω sur un alphabet Σ associe à n le nombre $p_\omega(n)$ de facteurs de longueur n de ω. Elle est donc croissante sur $\mathbb{N}$.

Le théorème suivant est dû à Morse et à Hedlund. Pour sa preuve et des compléments sur cette section, nous conseillons les références suivantes : [30], [31] et [39].

Théorème 7.4.4. *Soit ω un mot infini sur un alphabet Σ. Soit Π l'ensemble des lettres apparaissant dans le mot infini ω. Les propositions suivantes sont équivalentes :*
(1) ω est ultimement périodique,
(2) p_ω n'est pas strictement croissant sur $\mathbb{N}$,
(3) il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $p_\omega(n) < n - 1 + \#\Pi$,
(4) p_ω est borné par une constante.

Corollaire 7.4.5. *Soit ω un mot infini sur un alphabet Σ. Le mot infini ω est ultimement périodique si et seulement si il existe un nombre entier $n \in \mathbb{N}$ tel que le nombre de facteurs récurrents de longueur n de ω est inférieur ou égal à n*

Démonstration. Comme il n'existe qu'un nombre fini de facteurs de longueur n de ω, il existe une lettre du mot infini ω au delà de laquelle aucun facteur non récurrent de longueur n n'apparaît dans ω. En tronquant le début du mot infini ω, nous obtenons donc un mot infini qui est nécessairement ultimement périodique, vu le théorème 7.4.4. Le mot infini ω est donc également ultimement périodique. □

Remarquons qu'une partie $\mathcal{N}$ de $\mathbb{N}$ est une union finie de progressions arithmétiques si et seulement si le mot infini $w = a_0a_1a_2\cdots$ défini par

$$\forall i \in \mathbb{N},\ \begin{cases} a_i = 0 \text{ si } i \notin \mathcal{N} \\ a_i = 1 \text{ si } i \in \mathcal{N} \end{cases}$$

est ultimement périodique. La fonction de complexité est donc un outil pratique pour déterminer si une partie de $\mathbb{N}$ est reconnaissable.

7.4.2 Cas de $\mathbb{F}[X]$

Dans $\mathbb{N}$, un mot infini ω sur un alphabet Σ représente une fonction totale de $\mathbb{N}$ dans Σ. Dans l'ensemble $\mathbb{F}[X]$, il semble judicieux de représenter un mot infini sur Σ par une fonction totale de $\mathbb{F}[X]$ dans Σ. Mais alors, comment définir l'équivalent, dans la structure non linéaire qu'est $\mathbb{F}[X]$, de la notion de facteur du cadre de $\mathbb{N}$? Nous optons pour des uplets dont l'indice varie dans certaines parties de $\mathbb{F}[X]$.

Définition 7.4.6. Soit Σ un alphabet. Un *mot $\mathbb{F}[X]$-infini* sur Σ est une fonction de $\mathbb{F}[X]$ dans Σ, c'est-à-dire un uplet infini de la forme

$$(a_Q)_{Q\in\mathbb{F}[X]}$$

où $a_Q \in \Sigma$ pour tout $Q \in \mathbb{F}[X]$.

Définition 7.4.7. Soit $\omega = (a_Q)_{Q\in\mathbb{F}[X]}$ un mot $\mathbb{F}[X]$-infini sur un alphabet Σ. Une *pyramide* de ω est un uplet m de la forme

$$(a_Q)_{Q\in\{A\cdot P+B\ :\ A,B\in\mathbb{F}[X],\ \deg(B)<\deg(A)<n\}}$$

pour lequel $n \in \mathbb{N}$ et $P \in \mathbb{F}[X]$. Le nombre n est appelé *hauteur* de la pyramide et est aussi noté sous la forme $|m|$.

Définition 7.4.8. Soit ω un mot $\mathbb{F}[X]$-infini sur un alphabet Σ. La *fonction de complexité* de ω est notée P_ω et est définie par

$$P_\omega : \mathbb{N} \to \mathbb{N},\ n \mapsto \#\{m\ :\ m \text{ pyramide de } \omega,\ |m| = n\}.$$

La conjecture 7.4.9 est à comparer à la conjecture 7.2.10 : une réponse affirmative à la conjecture 7.4.9 impliquerait une réponse affirmative à la conjecture 7.2.10.

Conjecture 7.4.9. *Soit $\mathcal{P}$ une partie de $\mathbb{F}[X]$ et ω le mot $\mathbb{F}[X]$-infini sur l'alphabet $\{0,1\}$, défini par*

$$\forall i \in \mathbb{F}[X],\ \begin{cases} a_i = 0 \text{ si } i \notin \mathcal{P} \\ a_i = 1 \text{ si } i \in \mathcal{P} \end{cases}.$$

Les propositions suivantes sont équivalentes :
(1) $\mathcal{P}$ est une combinaison booléenne d'ensembles de type 1,2,3,
(2) le quotient $(\mathbb{F}[X]/\sim_{\mathcal{P}})$ est un ensemble fini,
(3) P_ω n'est pas strictement croissant sur $\mathbb{N}$,
(4) P_ω est borné par une constante.

L'astuce principale du théorème 7.4.4 est la propriété

$$\forall \omega[p_\omega(n) = p_\omega(n+1) \Rightarrow p_\omega(n+1) = p_\omega(n+2)].$$

Mais dans $\mathbb{F}[X]$, il n'est peut-être pas vrai que

$$\forall \omega[P_\omega(n) = P_\omega(n+1) \Rightarrow P_\omega(n+1) = P_\omega(n+2)].$$

7.5 Preuve dans $\mathbb{N}$

Le théorème 7.5.1 est le fameux théorème de Cobham. La preuve que nous allons suivre est basée sur celle de Dominique Perrin [45], sauf pour toute la partie concernant le caractère syndétique, partie pour laquelle nous utilisons nos propres développements. De nombreuses autres preuves et généralisations existent dans la littérature. Citons, par exemple, [11], [21], [10] et [12].

Théorème 7.5.1. *Soient p et q deux entiers naturels multiplicativement indépendants et strictement supérieurs à 1. Si $\mathcal{N}$ une partie p-reconnaissable et q-reconnaissable de $\mathbb{N}$, alors $\mathcal{N}$ est une union finie de progressions arithmétiques.*

Démonstration. Si $\mathcal{N}$ est un ensemble fini, alors $\mathcal{N}$ est une union finie de progressions arithmétiques de raison nulle et le problème est résolu. Nous pouvons à présent nous restreindre à un ensemble $\mathcal{N}$ qui est infini.

L'ensemble $\mathcal{N}$ est p-reconnaissable. Il existe donc un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_p, \delta)$ acceptant le langage $\rho_p(\mathcal{N})$. Si deux états $q_1, q_2 \in Q$ de l'automate fini déterministe sont tels que les deux ensembles $\{m \in (\Sigma_p)^* : \delta(q_1, m) \in F\}$ et $\{m \in (\Sigma_p)^* : \delta(q_2, m) \in F\}$ sont égaux, alors

nous pouvons évidemment fusionner ces deux états en un seul état q (les arcs entrant dans q sont tous ceux qui rentraient dans q_1 ou dans q_2 (labels et origines inchangés) et les arcs sortant de q sont tous ceux qui sortaient de q_1 ou de q_2 (labels et extrémités inchangés)) sans changer le langage accepté par l'automate (q est final si q_1 (et donc q_2) l'était, q est initial si q_1 ou q_2 l'était). Cette fusion rend l'automate non déterministe si et seulement si il existait $a \in \Sigma_p$ tel que les états $\delta(q_1, a)$ et $\delta(q_2, a)$ étaient différents. Mais dans ce cas, il est possible de récommencer l'opération de fusion avec les états $\delta(q_1, a)$ et $\delta(q_2, a)$. Comme l'automate est fini, le processus fini par s'arrêter et l'automate qui en résulte est un automate fini déterministe (quitte à supprimer certains arcs doublons, c'est-à-dire ceux de même origine, de même extrémité et de même label) qui accepte le même langage qu'au début. Nous disons que le nouvel automate fini déterministe est *réduit*. Quitte à le remplacer par un automate réduit, considérons que l'automate $\mathcal{A}$ est réduit.

Prouvons à présent que le langage $A_q = \{m \in (\Sigma_p)^* : \delta(q_0, m) = q\}$ est une combinaison boolénne d'ensembles $E_w = \{m \in (\Sigma_p)^* : mw \in \rho_p(\mathcal{N})\}$ où $w \in (\Sigma_p)^*$. Comme l'automate $\mathcal{A}$ est réduit, pour tout état r différent de q, il existe $m_r \in (\Sigma_p)^*$ tel que $\delta(q, m_r) \neq \delta(r, m_r)$. Pour tout $m \in (\Sigma_p)^*$, il vient alors :

$$\begin{aligned}
m \in A_q &\Leftrightarrow \delta(q_0, m) = q \\
&\Leftrightarrow (\forall r \in Q \setminus \{q\})[\delta(\delta(q_0, m), m_r) \in F \leftrightarrow \delta(q, m_r) \in F] \\
&\Leftrightarrow (\forall r \in Q \setminus \{q\})[\delta(q_0, mm_r) \in F \leftrightarrow \delta(q, m_r) \in F] \\
&\Leftrightarrow (\forall r \in Q \setminus \{q\})[mm_r \in \rho_p(\mathcal{N}) \leftrightarrow \delta(q, m_r) \in F] \\
&\Leftrightarrow (\forall r \in Q \setminus \{q\})[m \in E_{m_r} \leftrightarrow \delta(q, m_r) \in F] \\
&\Leftrightarrow m \in \left(\bigcap_{\{r:\delta(q,m_r)\in F\}} E_{m_r} \right) \cap \left(\bigcap_{\{r:\delta(q,m_r)\notin F\}} ((\Sigma_p)^* \setminus E_{m_r}) \right).
\end{aligned}$$

Considérons la relation $\sim_{\mathcal{A}}$ binaire sur $(\Sigma_p)^*$ et définie par $m_1 \sim_{\mathcal{A}} m_2$ si et seulement si $\delta(q_0, m_1) = \delta(q_0, m_2)$. Il s'agit bien évidemment d'une relation d'équivalence et, en vertu du paragraphe précédent, chacune de ses classes d'équivalence est une combinaison boolénne d'ensembles de la forme $E_w = \{m \in (\Sigma_p)^* : mw \in \rho_p(\mathcal{N})\}$ où $w \in (\Sigma_p)^*$. Considérons la relation $\approx_{\mathcal{A}}$ binaire sur $\mathbb{N}$ définie par $m \approx_{\mathcal{A}} n$ si et seulement si $\rho_p(m) \sim_{\mathcal{A}} \rho_p(n)$. Chaque classe d'équivalence de $\approx_{\mathcal{A}}$ est évidemment un ensemble p-reconnaissable de nombres entiers naturels.

Montrons que chaque classe d'équivalence de $\approx_{\mathcal{A}}$ est aussi un ensemble q-reconnaissable de nombres entiers naturels. En vertu de ce qui précède, du théorème 5.1.1 de Büchi-Bruyère et de la stabilité par combinaison booléenne des ensembles q-définissables, il suffit de démontrer que tous les ensembles $\mathcal{N}_1$ de nombres entiers naturels pour lesquels il existe un mot $w \in (\Sigma_p)^*$

tel que $\rho_p(\mathcal{N}_1) = \{m \in (\Sigma_p)^* : mw \in \rho_p(\mathcal{N})\}$ sont q-définissables. C'est le cas car l'ensemble $\mathcal{N}$ est q-reconnaissable par hypothèse et un nombre entier naturel n appartient à l'ensemble $\mathcal{N}_1$ si et seulement si

$$\exists \ell(\ell \in \mathcal{N} \wedge \ell = \underbrace{n + \cdots + n}_{p^{|w|} \text{ termes}} + t)$$

où t est l'entier naturel tel que $\rho_p(t) = w$.

Vu tout ce qui précède, il est clair que nous pouvons considérer un automate fini déterministe $\mathcal{B} = (Q', q'_0, F', \Sigma_q, \lambda)$ qui accepte le langage $\rho_q(\mathcal{N})$ et qui est tel que, pour tous $m_1, m_2 \in (\Sigma_q)^*$, l'égalité $\lambda(q'_0, m_1) = \lambda(q'_0, m_2)$ implique que m_1 et m_2 sont les images par ρ_q de deux nombres dans une même classe d'équivalence de $\approx_{\mathcal{A}}$. Il suffit en effet de considérer l'automate produit des automates finis déterministes qui acceptent les représentations en base q des différentes classes d'équivalence de la relation $\approx_{\mathcal{A}}$. Nous définissons la relation $\sim_{\mathcal{B}}$ binaire sur $(\Sigma_q)^*$ par $m_1 \sim_{\mathcal{B}} m_2$ si et seulement si $\lambda(q'_0, m_1) = \lambda(q'_0, m_2)$, ainsi que la relation $\approx_{\mathcal{B}}$ binaire sur $\mathbb{N}$ par $m \approx_{\mathcal{B}} n$ si et seulement $\rho_q(m) \sim_{\mathcal{B}} \rho_q(n)$. Ce sont des relations d'équivalence et la relation $\approx_{\mathcal{B}}$ est un raffinement de la relation $\approx_{\mathcal{A}}$. De plus, pour tous mots $m_1, m_2, m_3 \in (\Sigma_q)^*$, nous avons : $m_1 \sim_{\mathcal{B}} m_2 \Rightarrow m_1 m_3 \sim_{\mathcal{B}} m_2 m_3$.

Soit v le mot infini $v = v_0 v_1 v_2 v_3 \ldots$ où $v_n = n^{\approx_{\mathcal{A}}}$ pour tout $n \in \mathbb{N}$. Comme $\mathcal{N}$ est une union finie de classes d'équivalence de la relation $\approx_{\mathcal{A}}$, il suffit de montrer que v est ultimement périodique pour prouver que l'ensemble $\mathcal{N}$ est une union finie de progressions arithmétiques. Or, en vertu du corollaire 7.4.5, pour prouver que v est ultimement périodique, il nous suffit de prouver qu'il existe un nombre entier naturel m pour lequel v possède au plus m facteurs récurrents de longueur m. Soit $a = a_1 a_2$ un facteur récurrent de longueur 2 de v. L'ensemble $\{n \in \mathbb{N} : v_n v_{n+1} = a_1 a_2\}$ est p-reconnaissable et q-reconnaissable car d'une part un nombre n lui appartient si et seulement si il satisfait la formule $(n \in a_1 \wedge (n+1) \in a_2)$ et que d'autre part la relation d'appartenance à la classe d'équivalence a_1 (idem pour a_2) est p-définissable et q-définissable vu que chacune des classes d'équivalence de la relation $\approx_{\mathcal{A}}$ est p-reconnaissable et q-reconnaissable. Par la proposition 7.1.7, l'ensemble infini $\{n \in \mathbb{N} : v_n v_{n+1} = a_1 a_2\}$ est donc syndétique. Comme il ne peut exister que au plus p^2 facteurs récurrents de longueur 2, il existe même un nombre $d \in \mathbb{N}$ tel que tout facteur de longueur d de v contient une copie de chaque facteur récurrent de longueur 2 de v. Soit u le mot infini $u = u_0 u_1 u_2 u_3 \ldots$ où $u_n = n^{\approx_{\mathcal{B}}}$ pour tout $n \in \mathbb{N}$.

Soit C le nombre de classes d'équivalence de la relation $\approx_{\mathcal{B}}$. Soit ϵ un nombre réel de l'intervalle $]0, \frac{1}{2C+1}[$. Remarquons que ϵ vérifie les inégalités $\epsilon C < \frac{1-\epsilon}{2}$ et $0 < \epsilon < 1$. Il existe des entiers naturels k et ℓ vérifiant les

inégalités $1 < \frac{q^l}{p^k} < 1 + \frac{\epsilon}{d}$. Posons $P = p^k$ et $Q = q^\ell$. Choisissons m égal au plus grand entier inférieur ou égal à $P(1-\epsilon)$.

Nous allons prouver que, pour tout facteur récurrent w de v de longueur m, il existe un entier y, tel que le mot

$$v_{yQ}v_{yQ+1}\cdots v_{(y+1)Q-1}$$

est de la forme swt pour un mot s de longueur inférieure ou égale ϵP. Remarquons que comme w est de longueur au plus P, il apparaît forcément infiniment souvent dans un mot de longueur de la forme

$$v_{xP}v_{xP+1}\cdots v_{(x+2)P-1}.$$

De plus, comme il n'y a qu'un nombre fini de positions dans ces mots, w apparaît même infiniment souvent à la même position dans certains d'entre eux. Remarquons aussi que le mot

$$v_{xP}v_{xP+1}\cdots v_{(x+2)P-1}$$

est entièrement déterminé par le mot v_xv_{x+1}. Alors, v_xv_{x+1}, qui est de longueur 2 et qui est forcément aussi un facteur récurrent de v, doit apparaître dans tout facteur de longueur d de v. Ceci signifie qu'il existe une suite strictement croissante d'entiers $(x_n)_{n\in\mathbb{N}}$ telle que $x_{n+1} \leq x_n + d$ et que

$$v_{xP}v_{xP+1}\cdots v_{(x+2)P-1} = w'ww''.$$

Il est alors possible de montrer[2] qu'il existe $n, y \in \mathbb{N}$ tels que

$$yQ \leq x_nP + |w'| \leq yQ + P\epsilon,$$

et d'en déduire ce qui était annoncé au début de ce paragraphe.

Comme $\approx_{\mathcal{B}}$ est un raffinement de $\approx_{\mathcal{A}}$, le nombre de facteurs distincts de la forme $v_{yQ}v_{yQ+1}\cdots v_{(y+1)Q-1}$ est borné par le nombre de facteurs distincts de la forme $u_{yQ}u_{yQ+1}\cdots u_{(y+1)Q-1}$. Or, le mot $u_{yQ}u_{yQ+1}\cdots u_{(y+1)Q-1}$ est entièrement déterminé par u_y et il n'y a que C classes d'équivalence dans $\approx_{\mathcal{B}}$. Donc, le nombre de facteurs récurrents de la forme $v_{yQ}u_{yQ+1}\cdots v_{(y+1)Q-1}$ est borné par C.

Finalement, comme le mot $v_{yQ}v_{yQ+1}\cdots v_{(y+1)Q-1}$ est de la forme swt pour un mot s de longueur inférieure ou égale ϵP, le nombre de facteurs récurrents w de v de longueur m est au plus égal[3] à $(P\epsilon+1)C$. Donc, les

[2]Le lecteur peut se référer à [45] pour des détails supplémentaires. Ce ne sont que des propriétés arithmétiques élémentaires.

[3]Il ne me semble pas qu'on puisse (directement) se passer du "+1" dans "$(P\epsilon+1)C$".

inégalités $(P\epsilon + 1)C = P\epsilon C + C \leq \frac{P(1-\epsilon)}{2} + C \leq \frac{m+1}{2} + C \leq m$ permettent de conclure, quitte à choisir m arbitrairement grand, ce qui est possible en choisissant P arbitrairement grand une fois ϵ fixé (argument de densité).

□

Ce qui nous empêche, pour le moment, de démontrer le théorème de Cobham dans $\mathbb{F}[X]$ est d'une part, la difficulté de montrer qu'un ensemble infini de polynômes P-reconnaissable et Q-reconnaissable est syndétique dans $\mathbb{F}[X]$ et d'autre part, la difficulté d'obtenir des résultats analogues à ceux de Morse et Hedlund sur la complexité.

Troisième partie

Définissabilité de la multiplication

Dans cette partie, sauf mention explicite du contraire, nous considérons que n est toujours un nombre entier strictement positif lorqu'il est présent dans une expression de la forme $\mathbb{N}^n$ ou $(\mathbb{F}[X])^n$.

Cette partie est la contribution personnelle la plus importante de notre thèse. Nous y prouvons que, si S et T sont deux polynômes non nuls multiplicativement indépendants sur un corps fini, alors la multiplication est une relation ternaire (S,T)-définissable (en anticipant sur la définition 8.1.1). Ce résultat est très important car il montre que si nous disposons de deux fonctions $\mathrm{V_S}$ et $\mathrm{V_T}$ avec des bases S et T indépendantes (en plus de quelques autres relations reconnaissables dans toutes les bases), nous pouvons définir tout ce que nous aurions pu définir en disposant également de la multiplication. En particulier, il est inutile de se demander ce qui se passerait si nous rajoutions une troisième fonction $\mathrm{V_U}$ à notre structure : cela ne l'enrichirait absolument pas.

Un théorème similaire existe pour des nombres entiers naturels et est présenté dans l'article [59] de R. Villemaire. Le présent théorème et la structure générale de la présente preuve en sont inspirés, mais nous avons trouvé deux failles dans celui-ci. Il ne nous a pas été facile de les combler, il nous a fallu modifier substantiellement le développement d'origine pour y parvenir. Nous en avons profité pour faire une preuve qui s'adapte directement aux deux contextes. Nous la présentons dans le cadre des polynômes, mais, telle qu'elle est ici présentée, il est aisé de la transposer aux cadres des entiers.

Dans le premier chapitre de cette partie, nous mettons en évidence une structure (P,Q)-définissable (*confer* la définition 8.1.1) pour certaines puissances $P,Q \in \mathbb{F}[X]_{>0}$ de n'importe quels polynômes $R,S \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants. Nous exposons également brièvement les deux failles que nous avons trouvées dans l'article [59]. Dans le second chapitre, nous exploitons la structure (P,Q)-définie au premier chapitre pour prouver que la multiplication est définissable dans celle-ci. Dans le troisième chapitre, nous prouvons finalement que la multiplication est (R,S)-définissable pour n'importe quels polynômes $R,S \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants. Nous donnons au passage le résultat analogue dans $\mathbb{N}$ et un corollaire concernant l'indécidabilité de certaines structures.

Chapitre 8

Partition de $P^{\mathbb{N}}$

Le but de ce chapitre est de prouver que si deux polynômes $S, T \in \mathbb{F}[X]$ sont non nuls et multiplicativement indépendants, alors il existe nécessairement des puissances $P, Q \in \mathbb{F}[X]$ de ces polynômes pour lesquelles nous pouvons (P, Q)-définir (en anticipant sur la définition 8.1.1) une fonction strictement croissante F de $P^{\mathbb{N}}$ dans lui même et une partition finie $(E_i)_{i\in\{1,\ldots,c\}}$ de $P^{\mathbb{N}}$ qui vérifient la propriété suivante :

$$\forall i \in \{1, \ldots, c\}\ \forall A, B \in E_i$$
$$\left[A \prec B \Rightarrow \exists C \in \left(P^{\mathbb{N}} \setminus F\left(P^{\mathbb{N}}\right)\right) : F(A) \prec C \prec F(B)\right].$$

Ceci est une étape intermédiaire vers la preuve complète de la possibilité de (S, T)-définir la multiplication de polynômes, si $S, T \in \mathbb{F}[X]$ sont des polynômes non nuls multiplicativement indépendants. L'idée de cette étape intermédiaire est inspirée de l'article [59], de R. Villemaire, qui prouve le même résultat mais dans le cas de la structure $\langle \mathbb{N}, +, \mathrm{V_p}, \mathrm{V_q} \rangle$ où $p, q \in \mathbb{N} \setminus \{0, 1\}$ sont multiplicativement indépendants. Toutefois cette preuve-là comporte deux failles, et il a été nécessaire d'adapter substantiellement le développement d'origine pour les combler.

Ce chapitre débute par une section avec quelques définitions. Ensuite, il se poursuit avec deux sections dans lequelles un analogue du théorème ciblé est prouvé dans des cas particuliers. Dans une quatrième section, le cas général de ce théorème est déduit des deux cas particuliers. Finalement, le chapitre s'achève dans une cinquième section mettant en évidence deux failles dans la preuve d'origine (celle de l'article [59]) du théorème dans le cadre des entiers naturels.

8.1 Définitions de base

Définition 8.1.1. Pour tout $n \in \mathbb{N} \setminus \{0\}$ et pour tous $P, Q \in \mathbb{F}[X]$ de degré au moins 1, une *partie* (P, Q)*-définissable* de $(\mathbb{F}[X])^n$ est une partie $\mathcal{F}$ de

$(\mathbb{F}[X])^n$ pour laquelle il existe une formule $\phi(A_1, \ldots, A_n)$ du premier ordre dans le langage

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P}, \mathrm{V_Q} \rangle,$$

qui est satisfaite si et seulement si le n-uplet $(A_1, \ldots, A_n)$ appartient à $\mathcal{F}$.

De même que dans le cadre de la P-définissabilité, nous parlons de *relations* et de *fonctions* (P,Q)-*définissables* et nous n'hésitons pas à dire que nous (P,Q)-*définissons* un ensemble, une relation ou une fonction. Il faut bien entendu veiller à ce que chaque (P,Q)-définition soit licite.

Sur l'anneau $\mathbb{F}[X]$, deux polynômes non nuls possèdent plusieurs plus petits communs multiples (sauf si le corps $\mathbb{F}$ est $\mathbb{Z}/2\mathbb{Z}$). En fait, ils en possèdent un et un seul de coefficient principal k pour chaque élément $k \in \mathbb{F} \setminus \{0\}$. Ceci motive la définition suivante.

Définition 8.1.2. Si $k \in \mathbb{F} \setminus \{0\}$, alors la fonction ppcm_k est définie par

$$\mathrm{ppcm}_k : \mathbb{F}[X] \times \mathbb{F}[X] \to \mathbb{F}[X],$$

$$(A, B) \mapsto C \text{ si } A \neq 0 \text{ et } B \neq 0,$$

$$(A, B) \mapsto 0 \text{ si } A = 0 \text{ ou } B = 0$$

où C est le polynôme de coefficient principal k parmi les plus petits communs multiples de A et B.

8.2 Premier cas particulier

Dans la preuve clef de ce chapitre, c'est-à-dire celle du théorème 8.4.1, nous décomposons deux polynômes S et T en facteurs irréductibles et, en faisant intervenir des puissances P et Q de ces deux polynômes (ce qui est autorisé parce que un polynôme de degré au moins 1 est multiplicativement dépendant avec n'importe laquelle de ses puissances entières strictement positives), nous nous ramenons rapidement à l'étude de deux cas particuliers selon les formes relatives des deux décompositions en question. La présente section traite de l'un des deux cas, celui où il est possible de choisir des puissances P et Q correspondant à leurs homologues décrits dans le lemme 8.2.1 et dans la proposition 8.2.2. La section suivante traite du second cas, celui où un tel choix est impossible.

Lemme 8.2.1. *Si $k \in \mathbb{F} \setminus \{0\}$ et si $P, Q \in \mathbb{F}[X]$ sont des polynômes multiplicativement indépendants qui peuvent s'écrire sous la forme $P = P_0 R$ et $Q = Q_0 R$ où $P_0, Q_0, R \in \mathbb{F}[X]$ sont trois polynômes deux à deux premiers entre eux et tels que $P_0 \succeq Q_0$, alors la restriction au domaine $P^{\mathbb{N}} \times Q^{\mathbb{N}}$ de la fonction ppcm_k est (P,Q)-définissable.*

Démonstration. Tout d'abord, remarquons que comme P, Q sont non nuls et multiplicativement indépendants, il est nécessaire que $P, Q \succ 1$. Les fonctions $\mathrm{V_P}$ et $\mathrm{V_Q}$ ont donc leur sens habituel.

Le graphe $\{(A, B, C) : A \in P^{\mathbb{N}}, B \in Q^{\mathbb{N}} \text{ et } \mathrm{ppcm}_k(A, B) = C\}$ de cette fonction peut être (P, Q)-défini au moyen de la formule suivante :

$$\begin{aligned}
&[A = 0 \vee B = 0 \to C = 0] \\
&\wedge \\
&[A \neq 0 \ \wedge \ B \neq 0 \to C \neq 0 \\
&\wedge \ \mathrm{V_P}(A) = \mathrm{V_P}(C) = A \ \wedge \ \mathrm{V_Q}(B) = \mathrm{V_Q}(C) = B \\
&\wedge \forall T (\mathrm{V_P}(T) = A \ \wedge \ \mathrm{V_Q}(T) = B \to T \succeq C) \ \wedge \ \mathrm{Deb}_K(C)],
\end{aligned}$$

où le $K \in \mathbb{F}[X]$ de Deb_K est en fait le polynôme de degré 0 correspondant naturellement au scalaire k.
Cette formule tient d'abord compte du cas trivial dans lequel un au moins des deux polynômes A et B s'annulent, puis elle s'attaque à tous les autres cas. Raisonnons dans le cas où A, B, C sont non nuls. La formule implique que A et B sont respectivement des puissances de P et de Q. Pour comprendre son sens, considérons donc que $A = P^m \in P^{\mathbb{N}}$ et $B = Q^\ell \in Q^{\mathbb{N}}$. Avec les conditions de l'énoncé, il est alors clair que $W = P_0^m Q_0^\ell R^{\max\{m,\ell\}}$ est un plus petit commun multiple de A et B. Il est évident que $\mathrm{V_P}(W) = A$, que $\mathrm{V_Q}(W) = B$, et qu'aucun polynôme de degré strictement inférieur à W ne peut être à la fois tel que $\mathrm{V_P}(W) = A$ et $\mathrm{V_Q}(W) = B$. Donc W est égal à C à un scalaire multiplicatif non nul près, ce qui signifie que C est bien un plus petit commun multiple des nombres A et B. Comme de plus la formule n'est satisfaite que si $\mathrm{Deb}_K(C)$ l'est aussi, elle définit bien la fonction voulue. □

Proposition 8.2.2. *Si $P, Q \in \mathbb{F}[X]$ sont des polynômes multiplicativement indépendants qui peuvent s'écrire sous la forme $P = P_0 R$ et $Q = Q_0 R$ où $P_0, Q_0, R \in \mathbb{F}[X]$ sont trois polynômes deux à deux premiers entre eux et tels que $P_0 \succeq Q_0$, alors il existe une constante $c \in \mathbb{N} \setminus \{0\}$ et une fontion $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ strictement croissante pour la relation d'ordre $\prec$ qui vérifie l'inégalité*

$$P^{c+1} \cdot F\left(P^k\right) \preceq F\left(P^{k+c}\right)$$

quel que soit $k \in \mathbb{N}$ et qui est (P, Q)-définissable.

Démonstration. Avant toute chose, remarquons que P et Q sont de degré au moins 1. Ceci évite des incohérences (lorsque nous considèrons le minimum d'une partie de $P^{\mathbb{N}}$ ou de $Q^{\mathbb{N}}$, par exemple).

Prouvons d'abord que la fonction

$$G : P^{\mathbb{N}} \to Q^{\mathbb{N}}, A \mapsto \min\left\{Q^k : k \in \mathbb{N} \ \wedge \ Q^k \succ A\right\}$$

est (P,Q)-définissable. Pour cela, il nous suffit de (P,Q)-définir le graphe $\{(A,B) : G(A) = B\}$, ce qui est possible au moyen de la formule suivante :

$$\mathrm{V_P}(A) = A \wedge \mathrm{V_Q}(B) = B \wedge B \succ A \wedge \forall C\,(\mathrm{V_Q}(C) = C \wedge C \succ A \rightarrow C \succeq B)\,.$$

Prouvons ensuite que la fonction

$$H : \mathbb{F}[X] \rightarrow P^{\mathbb{N}}, A \mapsto \min\left\{P^k : k \in \mathbb{N} \ \wedge \ P^k \succ A\right\},$$

est (P,Q)-définissable. Pour cela, il nous suffit de (P,Q)-définir le graphe $\{(A,B) : H(A) = B\}$, ce qui est possible au moyen de la formule suivante :

$$\mathrm{V_P}(B) = B \ \wedge \ B \succ A \ \wedge \ \forall C\,(\mathrm{V_P}(C) = C \ \wedge \ C \succ A \rightarrow C \succeq B)\,.$$

Il est à présent clair que la fonction

$$F : P^{\mathbb{N}} \rightarrow P^{\mathbb{N}}, A \mapsto F(A) = H(\mathrm{ppcm}_1(A, G(A)))$$

est (P,Q)-définissable. Il ne reste plus qu'à prouver que cette fonction possède bien les caractéristiques énoncées. Comme $Q \succ 1$, pour tout $k \in \mathbb{N}$, nous pouvons désigner par $v(k)$ le plus petit entier tel que $P^k \prec Q^{v(k)}$. Puisque nous avons $P = P_0 R \succeq Q_0 R = Q$, il est évident que pour tout $k \in \mathbb{N},\ v(k) + 1 \leq v(k+1)$.

Prouvons maintenant que la fonction F est strictement croissante pour l'ordre $\prec$ sur $P^{\mathbb{N}}$. Cela revient à prouver l'inégalité $F\left(P^k\right) \prec F\left(P^{k+1}\right)$ pour tout $k \in \mathbb{N}$. Or, pour tout $k \in \mathbb{N}$, il vient :

$$\begin{aligned}
F\left(P^{k+1}\right) &= H\left(\mathrm{ppcm}_1\left(P^{k+1}, Q^{v(k+1)}\right)\right) \\
&\approx H\left(P_0^{k+1} Q_0^{v(k+1)} R^{\max\{k+1, v(k+1)\}}\right) \\
&\succeq H\left(P_0^{k+1} Q_0^{v(k)+1} R^{v(k)+1}\right) \\
&\succeq H\left(P P_0^k Q_0^{v(k)} R^{v(k)}\right) \\
&= P \cdot H\left(P_0^k P_0^{v(k)} R^{v(k)}\right) \\
&\succ H\left(P_0^k Q_0^{v(k)} R^{v(k)}\right) \\
&= H\left(P_0^k Q_0^{v(k)} R^{\max\{k, v(k)\}}\right) \\
&\approx H\left(\mathrm{ppcm}_1\left(P^k, Q^{v(k)}\right)\right) \\
&= F\left(P^k\right).
\end{aligned}$$

Remarquons ensuite que pour tous $k, c \in \mathbb{N}$, il vient :

$$\begin{aligned}
& F\left(P^k\right) \cdot P^{c+1} \preceq F\left(P^{k+c}\right) \\
\Leftrightarrow\ & H\left(\mathrm{ppcm}_1\left(P^k, G\left(P^k\right)\right)\right) \cdot P^{c+1} \preceq H\left(\mathrm{ppcm}_1\left(P^{k+c}, G\left(P^{k+c}\right)\right)\right) \\
\Leftarrow\ & P^{c+2} \cdot \mathrm{ppcm}_1\left(P^k, G\left(P^k\right)\right) \preceq \mathrm{ppcm}_1\left(P^{k+c}, G\left(P^{k+c}\right)\right) \\
\Leftrightarrow\ & P_0^{c+2} R^{c+2}\left(P_0^k Q_0^{v(k)} R^{\max\{k,v(k)\}}\right) \preceq P_0^{k+c} Q_0^{v(k+c)} R^{\max\{(k+c),v(k+c)\}} \\
\Leftrightarrow\ & P_0^2 Q_0^{v(k)} R^{v(k)+c+2} \preceq Q_0^{v(k+c)} R^{v(k+c)} \\
\Leftarrow\ & P_0^2 Q_0^{v(k)} R^{v(k)+c+2} \preceq Q_0^{v(k)+c} R^{v(k)+c} \\
\Leftrightarrow\ & P_0^2 R^2 \preceq Q_0^c \\
\Leftrightarrow\ & 2(\deg(P_0) + \deg(R)) \leq c \deg(Q_0).
\end{aligned}$$

Or, si $\deg(Q_0) > 0$, la dernière inégalité est vraie dès que $c \geq \frac{2(\deg(P_0)+\deg(R))}{\deg(Q_0)}$. Finalement, si $\deg(Q_0) = 0$, alors $\deg(P_0) \succ \deg(Q_0)$ (sinon P et Q seraient égaux à une constante scalaire multiplicative près et seraient donc multiplicativement dépendants) et $\deg(R) = \deg(RQ_0) = \deg(Q)$, si bien qu'il reste juste à prouver que l'inégalité

$$P_0^2 Q^{v(k)+c+2} \preceq Q^{v(k+c)}$$

est vraie pour tout $k \in \mathbb{N}$ dès que c est assez grand. Il vient bien sûr

$$\begin{aligned}
& P_0^2 Q^{v(k)+c+2} \preceq Q^{v(k+c)} \\
\Leftrightarrow\ & 2\deg(P_0) + (v(k) + c + 2)\deg(Q) \leq v(k+c)\deg(Q) \\
\Leftrightarrow\ & 2\deg(P_0) \leq (v(k+c) - v(k) - c - 2)\deg(Q).
\end{aligned}$$

Par définition, $P^{k+c} \prec Q^{v(k+c)}$ et $Q^{v(k)-1} \preceq P^k$ pour tous $k, c \in \mathbb{N}$. Donc nous obtenons l'inégalité $(k+c)\deg(P) < v(k+c)\deg(Q)$ et l'inégalité $(v(k)-1)\deg(Q) \leq k\deg(P)$ pour tous $k, c \in \mathbb{N}$. Pour tous $k, c \in \mathbb{N}$, il vient donc

$$[(k+c)\deg(P)] - [k\deg(P)] < [v(k+c)\deg(Q)] - [(v(k)-1)\deg(Q)],$$

puis

$$c[\deg(P) - \deg(Q)] - 3\deg(Q) < (v(k+c) - v(k) - c - 2)\deg(Q).$$

Pour conclure, il ne reste plus qu'à prouver l'existence d'une valeur de c assez grande pour satisfaire l'inégalité $2\deg(P_0) \leq c(\deg(P) - \deg(Q)) - 3\deg(Q)$, ce qui est évident puisque $\deg(P) - \deg(Q) > 0$. □

8.3 Second cas particulier

Dans la preuve clef de ce chapitre, c'est-à-dire celle du théorème 8.4.1, nous décomposons deux polynômes en facteurs irréductibles et nous nous ramenons rapidement à l'étude de deux cas particuliers selon les formes relatives des deux décompositions en question. Cette section-ci traite de l'un de ces deux cas, plus exactement de celui qui n'a pas été traité dans la section précédente.

Proposition 8.3.1. *Si $P, Q \in \mathbb{F}[X]$ sont des polynômes dont les décompositions en facteurs irréductibles sont*

$$P = \prod_{i=1}^{m} P_i^{\gamma_i} \prod_{i=1}^{\ell} R_i^{\alpha_i}$$

et

$$Q = \prod_{i=1}^{n} Q_i^{\delta_i} \prod_{i=1}^{\ell} R_i^{\beta_i}$$

où les P_i ($i \in \{1, \dots, m\}$), Q_i ($i \in \{1, \dots, n\}$), R_i($i \in \{1, \dots \ell\}$) sont deux à deux premiers entre eux et où

$$m, n, \ell \in \mathbb{N},\ \ell \geq 2,\ 1 = \frac{\alpha_1}{\beta_1} \leq \cdots \leq \frac{\alpha_i}{\beta_i} \cdots \leq \frac{\alpha_\ell}{\beta_\ell} = \theta \text{ et } 1 < \theta,$$

alors la fontion F définie par

$$F : P^{\mathbb{N}} \to P^{\mathbb{N}},\ P^k \mapsto P^{\lceil \theta k \rceil}$$

est strictement croissante pour la relation $\prec$ et il existe une constante entière $c \in \mathbb{N} \setminus \{0\}$ vérifiant l'inégalité

$$P^{c+1} \cdot F\left(P^k\right) \preceq F\left(P^{k+c}\right)$$

quel que soit $k \in \mathbb{N}$.

Démonstration. En effet, pour tous $c, k \in \mathbb{N}$, il vient :

$$F\left(P^{k+c}\right) = P^{\lceil \theta(k+c) \rceil} \succeq P^{\lceil \theta k + \lfloor \theta c \rfloor \rceil} = P^{\lceil \theta k \rceil + \lfloor \theta c \rfloor} = F\left(P^k\right) \cdot P^{\lfloor \theta c \rfloor}.$$

D'abord, pour $c = 1$, nous avons $F\left(P^{k+1}\right) \succeq F\left(P^k\right) \cdot P^{\lfloor \theta \rfloor} \succ F\left(P^k\right)$ quel que soit $k \in \mathbb{N}$, ce qui prouve que la fonction F est strictement croissante pour la relation d'ordre $\prec$.

Ensuite, dès que $c \geq \frac{1}{\theta - 1}$, nous obtenons $\theta c \geq 1 + c$ et donc $\lfloor \theta c \rfloor \geq \lfloor 1 + c \rfloor$. Donc il existe $c \in \mathbb{N}$ tel que, pour tout $k \in \mathbb{N}$:

$$P^{c+1} \cdot F\left(P^k\right) \preceq F\left(P^{k+c}\right).$$

□

Proposition 8.3.2. *Si $P, Q \in \mathbb{F}[X]$ sont des polynômes qui satisfont la même condition que dans l'énoncé de la proposition 8.3.1, alors la fontion F définie, comme dans la proposition 8.3.1, par*

$$F : P^{\mathbb{N}} \to P^{\mathbb{N}},\ P^k \mapsto P^{\lceil \theta k \rceil}$$

est (P, Q)-définissable.

Démonstration. Prouvons d'abord que la fonction

$$G : P^{\mathbb{N}} \to Q^{\mathbb{N}},\ P^k \mapsto Q^{\lceil \theta k \rceil}$$

est (P, Q)-définissable. Pour cela, il nous suffit de (P, Q)-définir le graphe $\{(A, B) : G(A) = B\}$, ce qui se fait au moyen de la conjonction des trois formules suivantes :

$$\mathrm{V_P}(A) = A \wedge \mathrm{V_Q}(B) = B,$$

$$\forall T \left(\mathrm{V_P} \left(T \prod_{i=1}^{\ell} R_i \right) \succeq A \wedge \mathrm{V_Q}(T) \succeq B \to \mathrm{V_P}(T) \succeq A \right),$$

$$\forall C [\mathrm{V_Q}(C) = C$$

$$\wedge \forall T \left(\mathrm{V_P} \left(T \prod_{i=1}^{\ell} R_i \right) \succeq A \wedge \mathrm{V_Q}(T) \succeq C \to \mathrm{V_P}(T) \succeq A \right)$$

$$\to C \succeq B].$$

En effet, la première formule signifie que A et B sont respectivement des puissances de P et de Q. Pour comprendre le sens de la deuxième formule, considérons donc que $A = P^k \in P^{\mathbb{N}}$ et $B = Q^r \in Q^{\mathbb{N}}$ où $k, r \in \mathbb{N}$. Chaque polynôme $T \in \mathbb{F}[X] \setminus \{0\}$ peut s'écrire sous la forme

$$T = T_0 \prod_{i=1}^{m} P_i^{\gamma'_i} \prod_{i=1}^{n} Q_i^{\delta'_i} \prod_{i=1}^{\ell} R_i^{\epsilon_i}$$

où T_0 est un polynôme premier avec chacun des facteurs P_i, Q_i, R_i et où chaque exposant $\gamma'_i, \delta'_i, \epsilon_i$ est un entier positif ou nul. Il vient :

$$\begin{aligned}
\mathrm{V_P}(T) &= \mathrm{V_P} \left(T_0 \prod_{i=1}^{m} P_i^{\gamma'_i} \prod_{i=1}^{n} Q_i^{\delta'_i} \prod_{i=1}^{\ell} R_i^{\epsilon_i} \right) \\
&= \mathrm{V_P} \left(\prod_{i=1}^{m} P_i^{\gamma'_i} \prod_{i=1}^{\ell} R_i^{\epsilon_i} \right) \\
&= \mathrm{V_P} \left(\prod_{i=1}^{m} (P_i^{\gamma_i})^{\frac{\gamma'_i}{\gamma_i}} \prod_{i=1}^{\ell} (R_i^{\alpha_i})^{\frac{\epsilon_i}{\alpha_i}} \right) \\
&= \mathrm{V_P} \left(\prod_{i=1}^{m} (P_i^{\gamma_i})^{\left\lfloor \frac{\gamma'_i}{\gamma_i} \right\rfloor} \prod_{i=1}^{\ell} (R_i^{\alpha_i})^{\left\lfloor \frac{\epsilon_i}{\alpha_i} \right\rfloor} \right) \\
&= P^{\min\left\{ \left\lfloor \frac{\gamma'_i}{\gamma_i} \right\rfloor, \left\lfloor \frac{\epsilon_j}{\alpha_j} \right\rfloor \,:\, i \in \{1,\ldots,m\},\ j \in \{1,\ldots,\ell\} \right\}}.
\end{aligned}$$

De manière analogue, nous obtenons les deux égalités suivantes :

$$\begin{aligned} \mathrm{V_Q}(T) &= Q^{\min\left\{\left\lfloor\frac{\delta'_i}{\delta_i}\right\rfloor,\left\lfloor\frac{\epsilon_j}{\beta_j}\right\rfloor\ :\ i\in\{1,\ldots,n\},\ j\in\{1,\ldots,\ell\}\right\}}, \\ \mathrm{V_P}\left(T\prod_{i=1}^{\ell}R_i\right) &= P^{\min\left\{\left\lfloor\frac{\gamma'_i}{\gamma_i}\right\rfloor,\left\lfloor\frac{1+\epsilon_j}{\alpha_j}\right\rfloor\ :\ i\in\{1,\ldots,m\},\ j\in\{1,\ldots,\ell\}\right\}}. \end{aligned}$$

Donc, l'implication

$$\mathrm{V_P}\left(T\prod_{i=1}^{\ell}R_i\right)\succeq A\wedge\mathrm{V_Q}(T)\succeq B\rightarrow\mathrm{V_P}(T)\succeq A$$

est équivalente à l'implication

$$\begin{aligned} &\min\left\{\left\lfloor\frac{\gamma'_i}{\gamma_i}\right\rfloor,\left\lfloor\frac{1+\epsilon_j}{\alpha_j}\right\rfloor\ :\ i\in\{1,\ldots,m\},\ j\in\{1,\ldots,\ell\}\right\}\geq k \\ &\wedge \\ &\min\left\{\left\lfloor\frac{\delta'_i}{\delta_i}\right\rfloor,\left\lfloor\frac{\epsilon_j}{\beta_j}\right\rfloor\ :\ i\in\{1,\ldots,n\},\ j\in\{1,\ldots,\ell\}\right\}\geq r \\ \Rightarrow\ &\min\left\{\left\lfloor\frac{\gamma'_i}{\gamma_i}\right\rfloor,\left\lfloor\frac{\epsilon_j}{\alpha_j}\right\rfloor\ :\ i\in\{1,\ldots,m\},\ j\in\{1,\ldots,\ell\}\right\}\geq k. \end{aligned}$$

Or, cette dernière implication est vérifiée pour tous les polynômes T_0 et toutes les valeurs entières naturelles des nombres $\gamma'_1,\ldots,\gamma'_m,\delta'_1,\ldots,\delta'_n,\epsilon_1,\ldots,\epsilon_\ell$ décrivant la variable T si et seulement si l'implication suivante est vérifiée :

$$\begin{aligned} &\min\left\{\left\lfloor\frac{1+\epsilon_j}{\alpha_j}\right\rfloor\ :\ j\in\{1,\ldots,\ell\}\right\}\geq k \\ &\wedge \\ &\min\left\{\left\lfloor\frac{\epsilon_j}{\beta_j}\right\rfloor\ :\ j\in\{1,\ldots,\ell\}\right\}\geq r \\ \Rightarrow\ &\min\left\{\left\lfloor\frac{\epsilon_j}{\alpha_j}\right\rfloor\ :\ j\in\{1,\ldots,\ell\}\right\}\geq k. \end{aligned}$$

Cette dernière implication est équivalente à l'inexistence d'un $j\in\{1,\ldots,\ell\}$ et d'une valeur de $\epsilon_j\in\mathbb{N}$ pour laquelle les inégalités $\frac{1+\epsilon_j}{\alpha_j}\geq k>\frac{\epsilon_j}{\alpha_j}$ et $\frac{\epsilon_j}{\beta_j}\geq r$ sont vraies, et donc telle que $k\alpha_j-1=\epsilon_j\geq r\beta_j$. Ces dernières inégalités sont impossibles pour tous les $j\in\{1,\ldots,\ell\}$ et tous les $\epsilon_j\in\mathbb{N}$ si et seulement si $\frac{r}{k}\geq\frac{\alpha_j}{\beta_j}$ quel que soit $j\in\{1,\ldots,\ell\}$ si et seulement si $\frac{r}{k}\geq\max\left\{\frac{\alpha_j}{\beta_j}:j\in\{1,\ldots,\ell\}\right\}=\theta$, c'est-à-dire si et seulement si B est une puissance de Q supérieure ou égale à $Q^{\theta k}$. Finalement, la troisième formule

$$\forall C[\mathrm{V_Q}(C)=C$$

$$\wedge\, \forall T \left(\mathrm{V_P} \left(T \prod_{i=1}^{\ell} R_i \right) \succeq A \wedge \mathrm{V_Q}\,(T) \succeq C \rightarrow \mathrm{V_P}\,(T) \succeq A \right)$$
$$\rightarrow C \succeq B]$$

sert à garantir que B est de degré inférieur ou égal à celui de toutes les puissances de Q supérieures ou égales à $Q^{\theta k}$, et donc que B est la plus petite d'entre-elles. Ainsi, le couple (A, B) vérifie l'égalité $G(A) = B$ si et seulement si il satisfait la conjonction des trois formules présentées.

Prouvons ensuite que la fonction

$$H : Q^{\mathbb{N}} \rightarrow P^{\mathbb{N}},\ Q^k \mapsto P^k$$

est (P, Q)-définissable. Pour cela, il nous suffit de (P, Q)-définir le graphe $\{(A, B) : H(A) = B\}$, ce que la conjonction des trois formules suivantes fait :

$$\mathrm{V_Q}\,(A) = A \wedge \mathrm{V_P}\,(B) = B,$$
$$\forall T \left(\mathrm{V_Q} \left(T \prod_{i=1}^{\ell} R_i \right) \succeq A \wedge \mathrm{V_P}\,(T) \succeq B \rightarrow \mathrm{V_Q}\,(T) \succeq A \right),$$
$$\forall C[\mathrm{V_P}\,(C) = C$$
$$\wedge\, \forall T \left(\mathrm{V_Q} \left(T \prod_{i=1}^{\ell} R_i \right) \succeq A \wedge \mathrm{V_P}\,(T) \succeq C \rightarrow \mathrm{V_Q}\,(T) \succeq A \right)$$
$$\rightarrow C \succeq B].$$

La preuve est analogue à ce que nous avons fait pour la fonction G. Ici, nous posons $A = Q^k$ et $B = P^r$ et, comme $\max\left\{\frac{\beta_j}{\alpha_j} : j \in \{1, \ldots, \ell\}\right\} = 1$, nous obtenons, par analogie à ce qui a été fait ci-dessus, que B est la plus petite des puissances de P supérieures ou égales à P^k (c'est-à-dire est P^k) si et seulement le couple (A, B) satisfait la formule.

Pour conclure, vérifions que la fonction

$$F : P^{\mathbb{N}} \rightarrow P^{\mathbb{N}},\ P^k \mapsto P^{\lceil \theta k \rceil}$$

est (P, Q)-définissable. Pour cela, il nous suffit de (P, Q)-définir l'ensemble $\{(A, B) : F(A) = B\}$, ce qui est possible au moyen de la formule suivante :

$$\exists C : G(A) = C \ \wedge\ H(C) = B.$$

□

8.4 Cas général

Théorème 8.4.1. *Si $S, T \in \mathbb{F}[X]$ sont des polynômes non nuls et multiplicativement indépendants, alors il existe des polynômes non nuls et multiplicativement indépendants $P, Q \in S^{\mathbb{N}} \cup T^{\mathbb{N}}$, une fonction $F : P^{\mathbb{N}} \mapsto P^{\mathbb{N}}$ strictement croissante et une partition finie $(E_i)_{i\in\{1,\dots,c\}}$ de l'ensemble $P^{\mathbb{N}}$ qui vérifient la propriété*

$$\forall i \in \{1, \dots, c\}\ \forall A, B \in E_i$$

$$\left[A \prec B \Rightarrow \exists C \in \left(P^{\mathbb{N}} \setminus F\left(P^{\mathbb{N}}\right)\right) : F(A) \prec C \prec F(B)\right]$$

et qui sont (P, Q)-définissables.

Démonstration. Soient

$$S = k \prod_{i=1}^{m} S_i^{\gamma_i} \prod_{i=1}^{\ell} R_i^{\alpha_i}$$

et

$$T = k' \prod_{i=1}^{n} T_i^{\delta_i} \prod_{i=1}^{\ell} R_i^{\beta_i}$$

où les S_i $(i \in \{1, \dots, m\})$, T_i $(i \in \{1, \dots, n\})$, $R_i (i \in \{1, \dots \ell\})$ sont deux à deux premiers entre eux et où

$$k, k' \in \mathbb{F} \setminus \{0\}, m, n, \ell \in \mathbb{N},\ 0 < \theta_1 = \frac{\alpha_1}{\beta_1} \leq \cdots \leq \frac{\alpha_i}{\beta_i} \leq \cdots \leq \frac{\alpha_\ell}{\beta_\ell} = \theta_2$$

sont des décompositions en facteurs premiers de S et T.

Si $\ell \geq 2$ et $\theta_1 < \theta_2$, alors nous choisissons

$$P = S^{\beta_1(\#\mathbb{F}-1)}$$

et

$$Q = T^{\alpha_1(\#\mathbb{F}-1)}$$

pour nous placer dans les conditions d'application des propositions 8.3.1 et 8.3.2. En effet, l'odre d'un élément (ici, k ou k') d'un groupe fini (ici, le groupe multiplicatif $\mathbb{F} \setminus \{0\}$) est toujours un diviseur du nombre d'éléments (ici, $\#\mathbb{F} - 1$) de ce groupe.

Si $\ell \in \{0, 1\}$ ou $\theta_1 = \theta_2$, alors nous choisissons

$$P = \left(\max\left\{S^{\beta_1}, T^{\alpha_1}\right\}\right)^{\#\mathbb{F}-1}$$

et

$$Q = \left(\min\left\{S^{\beta_1}, T^{\alpha_1}\right\}\right)^{\#\mathbb{F}-1}$$

pour nous placer dans les conditions d'application de la proposition 8.2.2. Bien entendu, si $S^{\beta_1} \approx T^{\alpha_1}$, nous choisissons n'importe lequel de ces deux polynômes comme maximum et l'autre comme minimum. De plus, si $\ell = 0$, nous posons $\alpha_1 = 1$ et $\beta_1 = 1$ (car α_1 et β_1 n'existent pas si $\ell = 0$).

Dans les deux cas, grâce aux propositions citées, nous prouvons l'existence d'une constante $c \in \mathbb{N} \setminus \{0\}$ et d'une fontion strictement croissante $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ qui est (P, Q)-définissable et qui vérifie l'inégalité

$$P^{c+1} \cdot F\left(P^k\right) \preceq F\left(P^{k+c}\right)$$

quel que soit $k \in \mathbb{N}$.

À présent, il ne nous reste plus qu'à (P, Q)-définir tous les ensembles E_i ($i \in \{1, \ldots, c\}$) en disant qu'un polynôme A appartient à E_i si et seulement si il satisfait la formule suivante :

$$\mathrm{V_P}(A) = A \ \wedge \ \bigwedge_{j=1}^{i-1} \left[F(A) \cdot P^j = F\left(A \cdot P^j\right)\right] \ \wedge \ F(A) \cdot P^i \prec F\left(A \cdot P^i\right).$$

En vertu des propriétés de la fonction F, il est évident que $(E_i)_{i \in \{1,\ldots,c\}}$ est une partion finie de $P^{\mathbb{N}}$ qui répond à la question. □

8.5 Compléments

Les développements de cette section sont basés sur des idées de l'article [59] qui traite le problème analogue dans le cas des nombres entiers naturels. Trois cas sont abordés dans cet article-là mais deux d'entre eux comportent une erreur que nous avons relevée. La démonstration n'était donc pas complète. Bien entendu, cela ne remet nullement en cause l'excellent travail accompli par Roger Villemaire, travail qui reste la ligne directrice des présents développements. La preuve que nous avons exposée aux sections précédentes ne comporte plus que deux cas au lieu de trois et est conçue pour s'adapter facilement au cadre des entiers naturels également.

Nous écrivons les deux sous-sections ci-dessous en nous basant sur les notations, que nous ne détaillons pas, de l'article [59].

8.5.1 Premier complément

Le lemme 3.4 de l'article [59] fait partie d'un cas où on considère des nombres entiers naturels multiplicativement indépendants k et l qui sont tels que chacun des deux possèdent au moins un diviseur premier que l'autre ne possède pas. Dans la preuve de ce lemme-là, on désire définir la restriction

de la multiplication $g : k^{\mathbb{N}} \times l^{\mathbb{N}} \to \mathbb{N}$ dans la structure $\langle \mathbb{N}, +, V_k, V_l \rangle$. Pour cela, on considère que le plus petit entier z tel que $V_k(z) = x$ et $V_l(z) = y$ est le produit de x et de y. Mais ceci est une erreur ! Voici un contre-exemple : $k = 10 = x$ et $l = 6 = y$ donne $z = 30$ au lieu de 60. En fait, z est le plus petit commun multiple de x et de y et n'est leur produit que si x et y sont des nombres premiers entre eux. La preuve du premier cas n'est donc pas générale : elle n'est correcte que pour des nombres k et l qui sont premiers entre eux.

8.5.2 Second complément

Le lemme 3.13 de l'article [59] fait partie d'un cas particulier dans lequel $k = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et $l = p_1^{\beta_1} \cdots p_m^{\beta_m}$ avec des conditions sur les exposants. Dans la preuve du lemme 3.13 de cet article-là, il y a un erreur lorsque m est différent de n : les bornes pour l'indice i disparaissent et la preuve suppose alors que $m = n$. Un contre-exemple est donné par $k = 2^1 \cdot 3^2 \cdot 5^1 = 90$, $l = 2^1 \cdot 3^1 = 6$ et $x = 90 \in k^{\mathbb{N}}$. Il faudrait que $f'(90) = 36$ (voir article [59]) soit le plus petit naturel y vérifiant la condition $\forall u[V_l(u) \geq y \Rightarrow V_k(u) \geq x]$. Pourtant, $y = 36$ ne vérifie même pas cette condition ! La preuve du troisième cas n'est donc pas générale : elle n'est correcte que pour des nombres k et l qui ont les mêmes facteurs premiers.

Chapitre 9

La multiplication est $\mathcal{P}$-définissable

Dans ce chapitre, $\mathcal{P}$ est la donnée d'un triplet

$$(P, (E_i)_{i\in\{1,\dots,c\}}, F)$$

pour lequel P est un polynôme de degré au moins 1 sur le corps fini $\mathbb{F}$, $(E_i)_{i\in\{1,\dots,c\}}$ est une partition finie de $P^{\mathbb{N}}$ et F est une fonction strictement croissante de l'ensemble $P^{\mathbb{N}}$ dans lui-même. La propriété suivante est supposée satisfaite :

$$\forall i \in \{1,\dots,c\}\ \forall A, B \in E_i$$
$$\left[A \prec B \Rightarrow \exists C \in \left(P^{\mathbb{N}} \setminus F\left(P^{\mathbb{N}}\right)\right) : F(A) \prec C \prec F(B)\right].$$

Dans la première section de ce chapitre, nous exposons le concept d'ensembles $\mathcal{P}$-définissables. Dans la seconde section, nous construisons quelques fonctions P-définissables qui servent elles-mêmes à définir la multiplication dans la troisième section de ce chapitre. Il est conseillé au lecteur de prendre le temps de bien assimiler les différentes fonctions définies dans la deuxième section avant d'aborder celle qui suit.

9.1 Définitions de base

Définition 9.1.1. Pour tout $n \in \mathbb{N} \setminus \{0\}$, une *partie $\mathcal{P}$-définissable* de $(\mathbb{F}[X])^n$ est une partie $\mathcal{F}$ de $(\mathbb{F}[X])^n$ pour laquelle il existe une formule $\phi(A_1,\dots,A_n)$ du premier ordre dans le langage

$$\left\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P}, F, (E_i)_{i\in\{1,\dots,c\}} \right\rangle,$$

qui est satisfaite si et seulement si le n-uplet $(A_1,\dots,A_n)$ appartient à $\mathcal{F}$.

De même que dans le cadre de la P-définissabilité, ainsi que dans celui de la (P,Q)-définissabilité, nous parlons volontiers de *relations* et de *fonctions $\mathcal{P}$-définissables* et nous n'hésitons pas à dire que nous *$\mathcal{P}$-définissons* un ensemble, une relation ou une fonction. Il faut bien entendu veiller à ce que chaque $\mathcal{P}$-définition soit licite.

9.2 Quelques fonctions $\mathcal{P}$-définissables utiles

Définition 9.2.1. Pour tout $i \in \{1,\dots,c\}$, la fonction K_i est définie par

$$K_i : P^{\mathbb{N}} \times E_i \to P^{\mathbb{N}},\ (A,B) \mapsto F^{(m_{A,B})}(S(F(B)))$$

où $S(F(B))$ est le polynôme de plus petit degré parmi ceux qui sont à la fois de degré strictement supérieur à $F(B)$ et dans l'ensemble infini $P^{\mathbb{N}} \setminus F\left(P^{\mathbb{N}}\right)$ et où $m_{A,B}$ est le plus petit nombre entier strictement positif pour lequel l'inégalité $A \preceq F^{(m_{A,B})}(S(F(B)))$ est satisfaite.

La définition 9.2.1 est licite puisque d'une part il est évident que $S(F(B))$ existe toujours, et d'autre part, comme la fonction F est strictement croissante pour $\prec$, le nombre $m_{A,B}$ existe également.

Proposition 9.2.2. *Quel que soit $i \in \{1,\dots,c\}$, la fonction K_i est $\mathcal{P}$-définissable et telle que pour tout $A \in P^{\mathbb{N}}$, la fonction*

$$K_{i,A} : E_i \to P^{\mathbb{N}},\ B \mapsto K_i(A,B)$$

est injective et minorée par A pour $\prec$.

Démonstration. Notons d'abord que S est une fonction $\mathcal{P}$-définissable de l'ensemble $P^{\mathbb{N}}$ dans lui-même. En effet, $\{(B,C) \in P^{\mathbb{N}} \times P^{\mathbb{N}} : S(B) = C\}$ est $\mathcal{P}$-définissable de la façon suivante :

$$\begin{aligned}
&\mathrm{V_P}(B) = B \\
\wedge\ &\mathrm{V_P}(C) = C \ \wedge\ B \prec C \ \wedge\ \forall A\,(\mathrm{V_P}(A) = A \to C \neq F(A)) \\
\wedge\ &\forall T \\
&[\mathrm{V_P}(T) = T \ \wedge\ B \prec T \ \wedge\ \forall A\,(\mathrm{V_P}(A) = A \to T \neq F(A)) \to C \preceq T]\,.
\end{aligned}$$

Ensuite, remarquons que par définition, pour tout $A \in P^{\mathbb{N}}$, la fonction

$$B \mapsto K_{i,A}(B) = K_i(A,B)$$

est minorée par A. Montrons qu'elle est aussi injective ; pour tout $B, B' \in E_i$

tels que $K_{i,A}(B) = K_{i,A}(B')$, il vient :

$$\begin{aligned}
& K_{i,A}(B) = K_{i,A}(B') \\
\Rightarrow\ & K_i(A,B) = K_i(A,B) \\
\Rightarrow\ & F^{(m_{A,B})}(S(F(B))) = F^{(m_{A,B'})}(S(F(B'))) \\
\Rightarrow\ & F^{\max\{m_{A,B}-m_{A,B'},0\}}(S(F(B))) = F^{\max\{m_{A,B'}-m_{A,B},0\}}(S(F(B'))) \\
\Rightarrow\ & S(F(B)) = S(F(B')) \\
\Rightarrow\ & F(B) = F(B') \\
\Rightarrow\ & B = B',
\end{aligned}$$

où les deux premières implications sont évidentes, la troisième et la sixième résultent de l'injectivité de la fonction strictement croissante F, la quatrième est une conséquence du fait que les images des fonctions F et S sont disjointes, et la cinquième découle de l'injectivité de la restriction sur $F(E_i)$ de la fonction S.

Il ne reste donc plus qu'à prouver que pour tout $i \in \{1, \ldots, c\}$, la fonction K_i est $\mathcal{P}$-définissable. Sous l'hypothèse que $A \in P^{\mathbb{N}}$ et $B \in E_i$, la formule $\varphi_1(A, B, U)$, définie par

$$\begin{aligned}
& X_{P,1}(S(F(B)), U) \wedge X_{P,1}(F(S(F(B))), U) \\
& \wedge \\
& \forall V(V \prec A \wedge X_{P,1}(V, U) \rightarrow X_{P,1}(F(V), U)),
\end{aligned}$$

est satisfaite par (A, B, U) si et seulement si l'écriture en base P du polynôme U ne possède que des lettres $1 \in \Sigma_P$ à chacune des puissances de P suivantes :

$$S(F(B)), F(S(F(B))), F(F(S(F(B)))), \ldots, F^{(m_{A,B})}(S(F(B))).$$

Sous l'hypothèse que $A \in P^{\mathbb{N}}$ et $B \in E_i$, la formule $\varphi_2(A, B, U)$, définie par

$$\forall W(\varphi_1(A, B, W) \rightarrow U \preceq W),$$

est satisfaite par (A, B, U) si et seulement si la formule $\varphi_1(A, B, W)$ n'est satisfaite par (A, B, W) pour aucun polynôme W de degré strictement inférieur à celui de U. Sous l'hypothèse que $A \in P^{\mathbb{N}}$ et $B \in E_i$, la satisfaction de la formule $(\varphi_1 \wedge \varphi_2)$ par (A, B, U) implique donc que U est de même degré que $F^{(m_{A,B})}(S(F(B)))$. La formule $\varphi_3(C, U)$, définie par

$$X_{P,1}(C, U) \ \wedge \ \forall Y(X_{P,1}(Y, U) \rightarrow Y \preceq C),$$

est satisfaite par (C, U) si et seulement si C est la plus grande puissance de P dont le coefficient est 1 dans le P-développement de U. Donc, en vertu de ce qui précède, la formule

$$\mathrm{V_P}\,(A) = A \wedge B \in E_i \wedge \exists U[\varphi_1(A, B, U) \wedge \varphi_2(A, B, U) \wedge \varphi_3(C, U)]$$

est satisfaite par (A, B, C) si et seulement si $C = F^{(m_{A,B})}(S(F(B)))$, ce qui prouve que la fonction K_i est $\mathcal{P}$-définissable. □

Définition 9.2.3. La fonction K est définie par

$$K : P^{\mathbb{N}} \times (\mathbb{F}[X])^c \to \mathbb{F}[X],\ (U, B_1, \ldots, B_c) \mapsto \sum_{P^j \preceq U} P_j P^j$$

où, pour tout $j \in \mathbb{N}$ tel que $P^j \preceq U$, P_j est l'unique polynôme de Σ_P pour lequel

$$\bigwedge_{i=1}^{c} \left[P^j \in E_i \Rightarrow X_{P,P_j}\left(K_i\left(U, P^j\right), B_i\right)\right].$$

Proposition 9.2.4. *La fonction K est $\mathcal{P}$-définissable.*

Démonstration. Cela revient à prouver que son graphe

$$\{(U, B_1, \ldots, B_c, L) \in P^{\mathbb{N}} \times (\mathbb{F}[X])^{c+1} : K(U, B_1, \ldots, B_c) = L\}$$

est bien $\mathcal{P}$-définissable. Ceci est évident, en regardant la formule suivante :

$$\begin{aligned} & \mathrm{V_P}(U) = U \wedge L \prec U \cdot P \\ \wedge\ & \forall V \\ & \left[\bigwedge_{i=1}^{c}\left(V \in E_i \wedge V \preceq U \to \bigwedge_{J \prec P}\left(X_{P,J}(V, L) \leftrightarrow X_{P,J}(K_i(U, V), B_i)\right)\right)\right]. \end{aligned}$$

□

Définition 9.2.5. La fonction L est définie par

$$L : \mathbb{F}[X] \to P^{\mathbb{N}},\ B \mapsto \max\left(\{1\} \cup \left\{Q \in P^{\mathbb{N}} : Q \preceq B\right\}\right).$$

Proposition 9.2.6. *La fonction L est $\mathcal{P}$-définissable.*

Démonstration. En effet, son graphe $\{B, C) \in \mathbb{F}[X] \times P^{\mathbb{N}} : L(B) = C\}$ est $\mathcal{P}$-définissable par la formule

$$(B = 0\ \wedge\ C = 1)\ \vee\ (\mathrm{V_P}(C) = C\ \wedge\ C \preceq B \prec C \cdot P).$$

□

Définition 9.2.7. La notation $\kappa(T)$ désigne la formule du premier ordre

$$\forall U \forall V \forall W$$

$$\bigwedge_{i=1}^{c}(W \in E_i \wedge X_{P,1}(U, T) \wedge X_{P,1}(V, T) \wedge U \succ V \succeq W \to U \succ K_i(V, W))$$

du langage

$$\left\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P}, F, (E_i)_{i \in \{1,\ldots,c\}} \right\rangle.$$

Expliquons le sens de la formule κ. Soit T un polynôme qui satisfait la formule κ. Si U et V sont deux puissances arbitraires de P pour lesquelles le P-développement de T possède 1 comme coefficient, et si U est de degré strictement supérieur à V, alors U doit être de degré strictement supérieur à celui de n'importe quel polynôme de l'ensemble

$$\bigcup_{i}^{c}\{K_i(V,W) : W \in E_i, W \preceq V\}.$$

Comme ce dernier ensemble est fini, ceci n'empêche pas l'existence de polynômes de degré arbitrairement grand et dont le développement en base P possède un nombre arbitrairement grand de coefficients égaux à $1 \in \Sigma_P$.

9.3 La multiplication est $\mathcal{P}$-définissable.

Pour comprendre la preuve du théorème 9.3.1, il est préférable d'avoir bien en tête les fonctions particulières définies à la section 2 de ce chapitre.

Théorème 9.3.1. *La multiplication de $\mathbb{F}[X]\times\mathbb{F}[X] \to \mathbb{F}[X]$ est une relation ternaire $\mathcal{P}$-définissable.*

Démonstration. Nous détaillons la construction d'une formule $\varphi(A,B,C)$ du premier ordre dans le langage

$$\left\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P}, F, (E_i)_{i\in\{1,\dots,c\}} \right\rangle,$$

qui est satisfaite si et seulement si les polynômes $A,B,C \in \mathbb{F}[X]$ vérifient l'égalité $AB = C$. À une modification élémentaire près, cela revient à construire une formule valable pour $A,B,C \in \mathbb{F}[X]\setminus\{0\}$. Considérons $A = \sum_{m=0}^{M} A_m P^m$ et $B = \sum_{n=0}^{N} B_n P^n$, où $M,N \in \mathbb{N}$ et $A_M, B_N \neq 0$, les décompositions en base P des polynômes A et B.

Pour tout $i \in \{1,\dots,c\}$, il existe (au moins) un polynôme Y_i qui vérifie la relation

$$X_{P,B_n}\left(K_i\left(L(B),P^n\right),Y_i\right)$$

quel que soit $P^n \in E_i$ tel que $n \leq N$. Grâce à la fonction K, cela peut se résumer très simplement de la façon suivante :

$$\exists Y_1 \cdots \exists Y_c \left[K\left(L(B),Y_1,\dots,Y_c\right) = B\right].$$

La seule contrainte que doivent satisfaire les polynômes $Y_1,\dots,Y_c$ est celle de posséder certains coefficients bien précis à certaines puissances bien précises de leurs P-représentations. À chaque coefficient du P-développement de B correspond un coefficient identique (correspondant à une puissance déterminée par un des K_i) du développement P-aire de l'un des Y_i. Nous disons que

les coefficients de la P-représentation du polynôme B sont *codés* dans une partie des coefficients de la P-représentation des polynômes $Y_1, \ldots, Y_c$.
De façon analogue, nous pouvons coder les coefficients (ils sont tous nuls) d'une P-représentation non normalisée du polynôme 0 dans une partie des coefficients de l'écriture en base P des polynômes $Z_1, \ldots, Z_c$:

$$\exists Z_1 \cdots \exists Z_c \; [K\left(L(B), Z_1, \ldots, Z_c\right) = 0].$$

Considérons les deux suites finies de polynômes suivantes et remarquons que nous venons en fait de coder le premier terme de chacune d'elles :

$$\begin{aligned}
&0\\
&A \cdot B_N,\\
&A \cdot B_N \cdot P + A \cdot B_{N-1}\\
&\ldots,\\
&A \cdot B_N \cdot P^k + \cdots + A \cdot B_{N-k},\\
&\ldots,\\
&A \cdot B_N \cdot P^N + \cdots + A \cdot B_0 = A \cdot B
\end{aligned}$$

et

$$\begin{aligned}
&B\\
&B - B_N \cdot P^N\\
&B - B_N \cdot P^N - B_{N-1} \cdot P^{N-1}\\
&\ldots,\\
&B - B_N \cdot P^N - B_{N-1} \cdot P^{N-1} - \cdots - B_{N-k} \cdot P^{N-k}\\
&\ldots,\\
&B - B_N \cdot P^N - B_{N-1} \cdot P^{N-1} - \cdots - B_0 = 0
\end{aligned}$$

Supposons que nous disposons d'un polynôme T vérifiant la relation $\kappa(T)$. Considérons deux polynômes $U, V \in \mathbb{F}[X]$ tels que $P \cdot L(B) \preceq V \prec U$, que $X_{P,1}\left(U, T\right) \wedge X_{P,1}\left(V, T\right)$, et que $\forall W(V \prec W \prec U \rightarrow \neg(X_{P,1}(W, T)))$. Examinons la formule suivante pour un polynôme $J \in \Sigma_P$:

$$\begin{aligned}
X_{P,J}[\; L(K(V, Y_1, \ldots, Y_c)) \quad &, \quad K(V, Y_1, \ldots, Y_c)\;]\\
&\rightarrow\\
K(U, Z_1, \ldots, Z_c) \quad &= \quad K(V, Z_1, \ldots, Z_c) \cdot P + J \cdot A\\
&\wedge\\
K(U, Y_1, \ldots, Y_c) \quad &= \quad K(V, Y_1, \ldots, Y_c) - J \cdot L(K(V, Y_1, \ldots, Y_c)).
\end{aligned}$$

Cette formule signifie que si J est le plus grand coefficient de la décomposition en base P du polynôme $K(V, Y_1, \ldots, Y_c)$, alors les polynômes

$$K(U, Z_1, \ldots, Z_c) \quad \text{et} \quad K(U, Y_1, \ldots, Y_c)$$

sont respectivement égaux aux polynômes

$$K(V, Z_1, \ldots, Z_c) \cdot P + J \cdot A \quad \text{et} \quad K(V, Y_1, \ldots, Y_c) - J \cdot L(K(V, Y_1, \ldots, Y_c).$$

Donc, si $K(V, Z_1, \ldots, Z_c)$ et $K(V, Y_1, \ldots, Y_c)$ sont des termes correspondants des deux suites mises en évidences ci-dessus, alors $K(U, Z_1, \ldots, Z_c)$ et $K(U, Y_1, \ldots, Y_c)$ sont les termes suivants de ces suites. Nous codons en fait les coefficients de certains polynômes de ces suites en fonction des précédents. Les codages se font par l'intermédiaire de certains coefficients des polynômes $Y_1, \ldots, Y_c, Z_1, \ldots Z_c$. Il est très important de remarquer ici que les itérations successsives du codage ne rentrent pas en contradiction les unes avec les autres : en effet, ceci est assuré par le fait que le polynôme T vérifie la relation $\kappa(T)$ et que les fonctions $B \mapsto K_i(A, B)$ sont minorées par A.

En appliquant à la formule précédente une conjonction sur les différentes valeurs possibles de $J \in \Sigma_P$, puis en quantifiant sur tous les polynômes $U, V \in \mathbb{F}[X]$ qui vérifient les conditions ci-dessus, nous pouvons coder de proche en proche les deux suites données précédemment, à condition de travailler avec un polynôme T pour lequel la formule $\kappa(T)$ est vraie et dont la décomposition en base P possède assez de coefficients égaux à $1 \in \Sigma_P$. Mais cette dernière condition est possible.

Pour la suite, nous devons distinguer deux cas complémentaires : B n'est pas un multiple de P ou B est un multiple de P.

Si B n'est pas un multiple de P, alors la seconde des suites décrites ci-dessus ne devient nulle qu'à son dernier terme. Tout revient alors à quantifier sur l'existence d'un polynôme T pour lequel nous avons

$$K(U, Y_1, \ldots, Y_c) = 0 \to K(U, Z_1, \ldots, Z_c) = C.$$

Appelons $\omega(A, B, C)$ la formule que nous venons de construire. Dans le cas où B n'est pas un multiple de P, celle-ci est vraie si et seulement si $AB = C$.

Si B est un multiple de P, alors la seconde des suites ci-dessus devient nulle avant son dernier terme. Nous pouvons nous sortir très facilement de ce problème en utilisant la technique suivante : nous remplaçons B par $B+1$ et C par $C + A$ partout dans la formule $\omega(A, B, C)$. Remarquons que $B + 1$ sera de toute façon non nul dans ce cas et que si $C + A$ est nul, alors la multiplication $AB = C$ ne peut être vraie dans ce cas.

Voici alors une formule valable pour ces deux cas réunis :

$$[\mathrm{V_P}\,(B) = 1 \to \omega(A, B, C)] \vee [\mathrm{V_P}\,(B) \neq 1 \to \omega(A, B{+}1, C{+}A) \wedge C{+}A \neq 0].$$

□

Corollaire 9.3.2. *Pour tout polynôme $Q \in \mathbb{F}[X]_{>0}$, la fonction $\mathrm{V_Q}$ est $\mathcal{P}$-définissable.*

Démonstration. C'est évident, puisqu'il est facile de construire la fonction V_Q au moyen d'une formule du premier ordre du langage $\langle \mathbb{F}[X], +, \cdot, \prec \rangle$ et que la multiplication est elle-même définissable dans le langage

$$\left\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]), \mathrm{V_P}\,, F, (E_i)_{i\in\{1,\ldots,c\}} \right\rangle .$$

□

Chapitre 10

La multiplication est (S, T)-définissable

Ce chapitre est en fait la conclusion des deux chapitres précédents. Nous prouvons que la multiplication est une relation ternaire (S, T)-définissable, à condition de choisir deux polynômes $S, T \in \mathbb{F}[X]_{>0}$ multiplicativement indépendants.

Ce résultat est intéressant car il montre que disposer de deux fonctions $\mathrm{V_S}$ et $\mathrm{V_T}$ avec des bases S et T indépendantes (en plus de quelques autres relations reconnaissables dans toutes les bases) permet de définir tout ce que nous aurions pu définir avec la multiplication, et donc qu'il est inutile de se demander ce qui se passerait si nous rajoutions une troisième fonction $\mathrm{V_U}$ car celle-ci n'enrichierait pas la structure.

De plus, la forte analogie avec ce qui se passe dans le cas classique de $\mathbb{N}$ est plutôt encourageant pour la recherche d'un analogue du théorème de Cobham.

10.1 La multiplication est (S, T)-définissable

Avant de démontrer le théorème clef de cette partie, donnons l'énoncé de son analogue dans $\mathbb{N}$, le théorème 10.1.1. Une preuve de ce dernier se trouve dans l'article [59], mais celle-ci est incomplète. Cependant, les développements faits dans cette partie s'adaptent naturellement au cadre des entiers naturels.

Théorème 10.1.1. *Si $p, q \in \mathbb{N}$ sont des nombres strictement supérieurs à 1 et multiplicativement indépendants, alors la multiplication est définissable dans la structure $\langle \mathbb{N}, +, \mathrm{V_p}, \mathrm{V_q} \rangle$.*

Corollaire 10.1.2. *Si $p, q \in \mathbb{N}$ sont des nombres strictement supérieurs à 1 et multiplicativement indépendants, alors aucune théorie récursivement axiomatisable, cohérente et décidable n'est "capable de formaliser" la structure mathématique $\langle \mathbb{N}, +, \mathrm{V_p}, \mathrm{V_q} \rangle$.*

Démonstration. Cela découle directement du théorème 10.1.1 et du corollaire 2.4.5. □

Ceci nous enseigne qu'il ne faut pas espérer pouvoir inventer une nouvelle sorte d'automates adaptés à cette structure.

Théorème 10.1.3. *Si $S, T \in \mathbb{F}[X]$ sont des polynômes non nuls et multiplicativement indépendants, alors la multiplication est une relation ternaire (S,T)-définissable.*

Démonstration. Comme les polynômes S et T sont non nuls et multiplicativement indépendants, par le théorème 8.4.1, il existe des polynômes non nuls et multiplicativement indépendants $P, Q \in S^{\mathbb{N}} \cup T^{\mathbb{N}}$, une fonction $F : P^{\mathbb{N}} \mapsto P^{\mathbb{N}}$ strictement croissante et une partition finie $(E_i)_{i\in\{1,\ldots,c\}}$ de l'ensemble $P^{\mathbb{N}}$ qui vérifient la propriété

$$\forall i \in \{1, \ldots, c\}\ \forall A, B \in E_i$$

$$\Big[A \prec B \Rightarrow \exists C \in \Big(P^{\mathbb{N}} \setminus F\Big(P^{\mathbb{N}}\Big)\Big) : F(A) \prec C \prec F(B)\Big]$$

et qui sont (P,Q)-définissables.

Or, en vertu du théorème 9.3.1, la multiplication est $\mathcal{P}$-définissable (nous associons ici $\mathcal{P}$ aux objets P, $(E_i)_{i\in\{1,\ldots,c\}}$ et F, comme dans le chapitre précédent).

Ceci implique évidemment que la multiplication est (P,Q)-définissable, puisqu'elle est définissable dans une structure dont toutes les relations sont (P,Q)-définissables.

Or, grâce à la proposition 6.4.3, nous savons que l'une des deux fonctions $\mathrm{V_P}$ et $\mathrm{V_Q}$ est S-définissable et que l'autre est T-définissable, et par conséquent la multiplication est (S,T)-définissable. □

Quatrième partie

Perspectives

Nous présentons ci-dessous quelques questions intéressantes dans la continuité de cette thèse. Nous les classons en sept catégories.

Cobham

Existe-t-il un théorème de Cobham dans $\mathbb{F}[X]$? Existe-t-il d'autres ensembles reconnaissables que les combinaisons booléennes d'ensembles reconnaissables de type 1,2,3 ? Peut-on s'inspirer des techniques du papier [10] pour démontrer le théorème de Cobham ?

Le cadre de la logique s'est avéré suffisant pour adapter les théories de l'article [59]. Il semble naturel de tenter une approche du théorème de Cobham dans celui-ci. Dans ce cas, la notion de partie syndétique de $\mathbb{F}[X]$ pourrait jouer un rôle important.

Décision

Étant donné un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_P, \delta)$ acceptant une partie $\mathcal{P}$ de $\mathbb{F}[X]$, est-il possible de décider si $\mathcal{P}$ est une partie reconnaissable (resp. reconnaissable de type 1, reconnaissable de type 2, reconnaissable de type 3) de $\mathbb{F}[X]$?

Il est peu probable de répondre à ces questions en l'absence de théorème de Cobham. Nous pouvons également poser ces questions sous l'hypothèse qu'il existe un théorème de Coham. Nous renvoyons le lecteur intéressé aux références suivantes : [15], [34], [2], [37], [43], [29].

Étant donné un automate fini déterministe $\mathcal{A} = (Q, q_0, F, \Sigma_P, \delta)$ acceptant une partie reconnaissable $\mathcal{P}$ de $\mathbb{F}[X]$, est-il possible de décider si $\mathcal{P}$ est une partie reconnaissable de type 1 (resp. de type 2, de type 3) ?

Numérations en base non entière

Existe-t-il des β-numérations dans $\mathbb{F}[X]$, c'est-à-dire des bases non entières analogues à la β-numération dans $\mathbb{N}$? Si oui, quelles sont leurs propriétés intéressantes ?

Le lecteur peut trouver des informations utiles dans l'article [55] qui concerne les corps finis.

Caractère P-automatique

Que peut apporter le caractère P-automatique ? Est-il possible de définir une concaténation de pyramides de $\mathbb{F}[X]$ donnant lieu à une nouvelle notion de morphisme de l'ensemble $\Sigma^{\mathbb{F}[X]}$ dans lui-même et à des propriétés intéressantes telles que le tag système ?

Nous renvoyons le lecteur intéressé aux références suivantes : [21], [22], [3].

Complexité

Est-il possible de démontrer la conjecture 7.4.9 ?

Élimination des quantificateurs

Les trois structures

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]) \rangle,$$

$$\langle \mathbb{F}[X], +, \prec, 1, (\cdot C : C \in \mathbb{F}[X]), (\mathrm{Deg}_k : k \in \mathbb{N} \setminus \{0,1\}) \rangle,$$

$$\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), (\mathrm{Deg}_k : k \in \mathbb{N} \setminus \{0,1\}), (\mathrm{Deb}_C : C \in \mathbb{F}[X] \setminus \{0\}) \rangle$$

admettent-elles une élimination des quantificateurs, à l'instar de la structure $\langle \mathbb{N}, + \rangle$?

Les deux premières correspondent-elles respectivement aux unions finies d'ensembles de type 1 et aux combinaisons booléennes d'ensembles de type 1,2 ?

Pour des références sur l'élimination des quantificateurs, le lecteur peut consulter [47].

Polynômes irréductibles

L'ensemble des polynômes irréductibles de $\mathbb{F}[X]$ est-il non reconnaissable quelle que soit la base $P \in \mathbb{F}[X]_{>0}$ choisie ?

Bibliographie

[1] J.-P. Allouche, V. Berthé, Triangle de Pascal, complexité et automates, *Bull. Belg. Math. Soc. Simon Stevin* **4** (1997), 1–23.

[2] J.-P. Allouche, N. Rampersad, J. Shallit, Periodicity, repetitions, and orbits of an automatic sequence, to appear in *Theoret.Comput. Sci.*

[3] J.-P. Allouche, J. Shallit, Automatic sequences, Theory, applications, generalizations, *Cambridge University Press, Cambridge* (2003).

[4] H. Barendregt, The Lambda-Calculus, volume 103, *Elsevier Science Publishing Company*, Amsterdam (1984).

[5] J. Barwise, An introduction to first-order logic, in : *Handbook of Mathematical Logic*, J. Barwise, Ed., North Holland, Amsterdam (1977) 5-46.

[6] P. T. Bateman, C. G. Jockusch, A. R. Woods, Decidability and undecidability with a predicate for the primes, *J. Symbolic Logic* **58** (1993), 672-687.

[7] A. Bès, An extension of the Cobham-Semënov theorem, *J. Symbolic Logic* **65** (2000), 201–211.

[8] A. Bès, A Survey of Arithmetical Definability, *Bull. Belg. Math. Soc. Simon Stevin* (2001), suppl., 1–54.

[9] A. Bès, On Pascal triangles modulo a prime power, *Ann. Pure Appl. Logic* **89** (1997), 17–35.

[10] A. Bès, Undecidable extensions of Büchi arithmetic and Cobham-Semënov theorem, *J. Symbolic Logic* **62** (1997), 1280–1296.

[11] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, *Bull. Belg. Math. Soc. Simon Stevin* **1** (1994), 191–238.

[12] V. Bruyère, F. Point, On the Cobham-Semenov theorem, *Theory Comput. Syst.* **30** (1997), 197–220.

[13] J. R. Büchi, Finite automata, their algebras and grammars. Towards a theory of formal expressions. Edited and with a preface by Dirk Siefkes. *Springer-Verlag, New York,* 1989.

[14] J. R. Büchi, Weak second-order arithmetic and finite automata, *Z. Math. Logik Grundlag. Math* **6** (1960), 66-92.

[15] E. Charlier, M. Rigo, A decision problem for ultimately periodic sets in non-standard numeration systems, *Mathematical Foundations of Computer Science* 2008 (Torun), Lecture Notes in Comput. Sci **5162**, pp. 241–252, Springer-Verlag (2008).

[16] G. Christol, Ensembles presque périodiques k-reconnaissables, *Theoret. Comput. Sci* **9** (1979), 141-145.

[17] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, Suites algébriques, automatiques et substitutions, *Bull. Soc. Math. France* **108** (1980), 401–419.

[18] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory* **3** (1969), 186–192.

[19] A. Cobham, Uniform tag sequences, *Math. Systems Theory* **6** (1972), 164–192.

[20] M. Drmota, G. Gutenbrunner, The joint distribution of Q-additive functions on polynomials over finite fields, *J. Théor. Nombres Bordeaux* **17** (2005), 125–150.

[21] F. Durand, A theorem of Cobham for non-primitive substitutions, *Acta Arith.* **104** (2002), 225–241.

[22] F. Durand, M. Rigo, Syndeticity and independent substitutions, *Adv. in Appl. Math.* **42** (2009), 1–22.

[23] H.-D. Ebbinghaus, J. Flum, W. Thomas, Mathematical Logic (Second Edition), *Springer Undergraduate Texts in Mathematics* (1996).

[24] S. Eilenberg, *Automata, Languages, and Machines*, Vol. A. Pure and Applied Mathematics, Academic Press, New York **58** (1974).

[25] H. E. Enderton, An introduction to mathematical logic, *Academic Press* (1972).

[26] C. Frougny, Representations of numbers and finite automata, *Math. Systems Theory* **25** (1992), 37–60.

[27] K. Gödel : Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatshefte für Mathematik und Physik* **38** (1931), 173–198.

[28] G. Hansel, À propos d'un théorème de Cobham, In D. Perrin Ed., *Actes de la fête des mots*, 55–59, Greco de programmation, CNRS, Rouen, (1982).

[29] T. Harju, M. Linna, On the periodicity of morphisms on free monoids, *RAIRO Inform. Théor. Appl.* **20** (1986), 47–54.

[30] G. A. Hedlund, M. Morse, Symbolic dynamics, *Amer. J. Math.* **60** (1938), 815–866.

[31] G. A. Hedlund, M. Morse, Symbolic dynamics II. Sturmian trajectoris, *Amer. J. Math.* **62** (1940), 1–42.

[32] B. R. Hodgson, Décidabilité par automate fini. *Ann. Sci. Math. Québec* **7** (1983), 39–57.

[33] M. Hollander, Greedy numeration systems and regularity, *Theory Comput. Syst.* **31** (1998), 111–133.

[34] J. Honkala, A decision method for the recognizability of sets defined by number systems, *RAIRO Inform. Théor. Appl.* **20** (1986), 395–403.

[35] J. Honkala, Bases and ambiguity of number systems. *Theoret. Comput. Sci.* **31** (1984), 61–71.

[36] P. Lecomte, M. Rigo, Numeration systems on a regular language, *Theory Comput. Syst.* **34** (2001), 27–44.

[37] J. Leroux, Apolynomial Time Presburger Criterion and Synthesis for Number Decision Diagrams, 20th IEEE Symposium on Logic in Computer Science (LiCS 2005), Chicago, IL, USA, IEEEE Computer Society (2005), 147–156.

[38] R. Lidl, H. Niederreiter, Finite Fields, *Encyclopedia of Mathematics and its applications* **20**, *Cambridge University Press, Cambridge*, (2002).

[39] M. Lothaire, Algebraic combinatorics on words, *Encyclopedia of Mathematics and its Applications* **90**, *Cambridge University Press, Cambridge*, (2002).

[40] C. Michaux, F. Point, Les ensembles k-reconnaissables sont définissables dans $\langle \mathbb{N}, +, V_k \rangle$, *C. R. Acad. Sci Paris* **303** (1986) 939–942.

[41] C. Michaux, R. Villemaire, Cobham's theorem seen through Büchi's theorem, *Automata, languages and programming* (Lund, 1993), 325–334, Lecture Notes *in Comput. Sci.*, **700**, Springer, Berlin, (1993).

[42] A. A. Muchnik, The definable criterion for definability in Presburger arithmetic and its applications, *Theoret. Comput. Sci.* **290** (2003), 1433–1444.

[43] J.-J. Pansiot, Decidability of periodicity for infinite words, *RAIRO Inform. Théor. Appl.* **20** (1986), 43–46.

[44] C. H. Papadimitriou, Computational complexity, *Addison-Wesley* (1994).

[45] D. Perrin, Finite Automata, J. Van Leeuwen Ed. *Handbook of Theoret. Comput. Sci.*, vol. B, 1–57, Elsevier-MIT Press, (1990).

[46] T. Pheidas, K. Zahidi, Elimination theory for addition and the Frobenius map in polynomial rings, *J. Symbolic Logic* **69** (2004), 1006–1026.

[47] M. Presburger, Über die Volständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, C. R. *1er congrès des Mathématiques des pays slaves*, Varsovie (1929), 92-101.

[48] M. O. Rabin, D. Scott, Finite automata and their decision problems, *IBM J. of Research and Development* **3** (1959), 114–125.

[49] M. Rigo, Syntactictal and automatic properties of sets of polynomials over finite fields, *Finite Fields Appl.* **14** (2008), 258–276.

[50] M. Rigo, L. Waxweiler, A note on syndeticity, recognizable sets and Cobham's theorem, *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS* **88** (2006), 169–173.

[51] R. M. Robinson, Undecidable rings, *Trans. Amer. Math. Soc.* **70** (1951), 137–159.

[52] J. B. Rosser : Extensions of some theorems of Gödel and Church, *Journal of Symbolic Logic* ***1*** (1936), 87–91.

[53] J. Sakarovitch, Éléments de théorie des automates, *Vuibert* (2003).

[54] J. Shallit, Numeration systems, linear recurrences and regular sets, *Inform. and Comput.* **113** (1994) 331–347.

[55] K. Scheicher, β-expansions in algebraic function fields over finite fields, *Finite Fields Appl.* **13** (2007), 394–410.

[56] K. Scheicher, J. Thuswaldner, Digit systems in polynomial rings over finite fields, *Finite Fields Appl.* **9** (2003), 322–333.

[57] R. Villemaire, $\langle N, +, V_2, V_3\rangle$ est indécidable, in : C.R. *Acad. Sci. Paris Sér I Math* **314** (1992), 775–777.

[58] R. Villemaire, Joining k- and l-recognizable sets of natural numbers, in : *Proc. STACS'92*, Lecture Notes in *Computer Science*, **577** (Springer, Berlin, 1992), 83–94.

[59] R. Villemaire, The theory of $\langle \mathbb{N}, +, V_k, V_l\rangle$ is undecidable, *Theoret. Comput. Sci.* **106** (1992), no. 2, 337–349.

Index

(P,Q)-définissable, 100
K, 115
K_i, 113
L, 115
P-automatique, 90
P-définissable, 37
P-noyau, 88
P-reconnaissable, 46
P-représentation, 45
$P^{\mathbb{N}}$, 31
P_ω, 92
$X_{P,J}(A,B)$, 39
$X_{p,j}(a,b)$, 38
$\mathbb{F}[X]$, 31
$\mathbb{F}[X]_{<n}$, 31
$\mathbb{F}[X]_{>n}$, 31
$\mathbb{N}$, 21
Σ^*, 40
Σ_P^n, 46
Σ_p^n, 45
$\mathrm{V_P}$, 36
$\mathrm{V_p}$, 35
$\approx$, 31
Deb_C , 74
deg, 31
Deg_k , 74
$\exists$, 13
$\forall$, 13
$\imath$, 10
κ, 115
$\langle\ \rangle$, 25
$\leftrightarrow$, 12
$\mathbb{F}$, 30
$\mathcal{P}$-définissable, 112
$\neg$, 10
ppcm_k, 101
$\prec$, 31
$\preceq$, 31
ρ_P, 45
ρ_p, 44
$\rightarrow$, 12
$\sim_{\mathcal{N}}$, 84
$\sim_{\mathcal{N}}^p$, 84
$\sim_{\mathcal{P}}$, 86
$\sim_{\mathcal{P}}^P$, 87
$\succ$, 31
$\succeq$, 31
ε (mot vide), 41
$\vee$, 10
$\wedge$, 10
p-automatique, 89
p-définissable, 35, 36
p-noyau, 85
p-reconnaissable, 45
p-représentation, 45
$p^{\mathbb{N}}$, 35
p_ω, 91

accepté, 42
accessible, 44
addition de $\mathbb{N}$ dans la théorie **Z**, 21
affirmation, 10
affirmation du conséquent, 15
alphabet, 40
alphabet de sortie, 89
arité, 3
arithmétique de Peano, 23
arithmétique de Presburger, 22
autodistributivité de l'implication, 16
automate fini, 41
automate fini déterministe, 41

automate fini déterministe avec sortie, 89
automatique, 89
axiome d'extensionnalité, 19
axiome de l'ensemble des parties, 20
axiome de l'ensemble vide, 20
axiome de l'infini, 20
axiome de la paire, 19
axiome de la réunion, 19
axiome pur, 17

binaire, 3

caractéristique, 27
close, 5
cohérente, 14
complète, 13
complexité, 91, 92
concaténation, 41
conjonction, 10
connecteur, 9
connecteur syntaxique, 3
consistante, 14
constante syntaxique, 3
contradiction, 10
contraposition converse, 16
corps, 27
corps commutatif, 27
correcte, 13

décidable, 25
déductible, 6
degré d'un polynôme, 31
développement P-aire, 39
développement p-aire, 38
directement déductible, 6
disjonction, 10

ensemble (P, Q)-définissable, 100
ensemble $\mathcal{P}$-définissable, 112
ensemble P-reconnaissable, 46
ensemble p-reconnaissable, 45
ensemble reconnaissable de type 1, 68
ensembles reconnaissables de type 2, 68
ensembles reconnaissables de type 3, 69
équivalence, 12
état, 41, 89
état accessible, 44
état final, 41
état initial, 41, 89

facteur, 91
facteur récurrent, 91
fausse, 10
fonction (P, Q)-définissable, 101
fonction $\mathcal{P}$-définissable, 113
fonction P-reconnaissable, 46
fonction p-reconnaissable, 45
fonction de complexité, 91, 92
fonction de sortie, 89
fonction de transition, 41, 89
fonction syntaxique, 3
formule, 4, 5
formule fausse, 10
formule indécidable, 24
formule vraie, 10

graphe orienté d'un automate fini, 41
groupe, 26
groupe additif d'un corps, 27
groupe commutatif, 26
groupe multiplicatif d'un corps, 27

hauteur, 92

implication, 12
indécidable, 24, 25
interprétation, 7, 8
interprétation des variables, 8
isomorphe (Dedekind-Peano), 21

langage, 41, 42
langage accepté, 42
langage régulier, 42
lettre, 40
libre, 4, 5
longueur (morphisme), 44
longueur (mot), 41

modèle, 10
modus ponens, 16
morphisme, 44
mot, 40, 91, 92
mot $\mathbb{F}[X]$-infini, 92
mot accepté, 42
mot infini, 91
mot vide, 41
multiplication de $\mathbb{N}$ dans la théorie **Z**, 22
multiplicativement dépendants, 46, 49
multiplicativement indépendants, 46, 49

négation, 10
non satisfaite, 9
non valide, 10
noyau ($\mathbb{F}[X]$), 86
noyau ($\mathbb{N}$), 84

occurence libre dans un terme, 4
occurence libre dans une formule, 5

particularité, 16
partie (P, Q)-définissable, 100
partie $\mathcal{P}$-définissable, 112
partie P-reconnaissable, 46
partie p-reconnaissable, 45
partie reconnaissable de $\mathbb{F}[X]$, 68
partie reconnaissable de $\mathbb{N}$, 66
polynôme, 31
polynôme cyclotomique, 28
prolongeable, 44
pseudo-liberté de l'antécédent, 16
puits, 43
pyramide, 92

quantificateur, 9
quantificateur existentiel, 13
quantificateur syntaxique, 3
quantificateur universel, 13

reconnaissable, 66, 68
récurrent, 91
récursif, 6
récursivement axiomatisable, 6
règle d'inférence, 6
règle de généralisation, 16
régulier, 42
relation (P, Q)-définissable, 101
relation $\mathcal{P}$-définissable, 113
relation P-reconnaissable, 46
relation p-reconnaissable, 45
relation de transition, 41
relation syntaxique, 3
représentation en base P, 45
représentation en base p, 45

s (successeur), 21
satisfaite, 9
schéma, 7
schéma d'axiomes de compréhension, 20
sémantiquement associatif, 11
sortie, 89
structure de Dedekind-Peano, 20
structure mathématique, 7
structure syntaxique, 3
successeur, 21
suite P-automatique, 90
suite p-automatique, 89
syndétique (dans $\mathbb{F}[X]$), 83
syndétique (dans $\mathbb{N}$), 80

tautologie, 10
terme, 4
ternaire, 3
théorème, 6
théorie, 6
théorie **Z**, 19
théorie classique, 17
théorie décidable, 25
théorie indécidable, 25
transition, 41, 89

unaire, 3

valide, 10
variable syntaxique, 3
vraie, 10