Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Razika NIBOUCHA et Alain SALINIER

Composition d'applications quasi-polynomiales

Tome 29, n[o] 2 (2017), p. 569-601.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_2_569_0>

Journal de Théorie des Nombres de Bordeaux **29** (2017), 569–601

Composition d'applications quasi-polynomiales

par Razika NIBOUCHA et Alain SALINIER

Résumé. L'objet de ce travail est l'étude de la composition des applications quasi-polynomiales de $\mathbb{Z}$ dans $\mathbb{Z}$, et plus particulièrement des applications quasi-affines, définies comme les applications quasi-polynomiales de degré au plus 1. On montre que les applications quasi-affines correspondent aux endomorphismes continus de l'algèbre des suites reconnaissables indexées par $\mathbb{Z}$. On représente les applications quasi-affines par des suites finies d'entiers, et on donne les formules explicites sur ces suites traduisant la composition ou la réversion des fonctions quasi-affines. Enfin, est étudié un problème de coloriage équivalent à la caractérisation de telles suites pour des bijections quasi-affines.

Abstract. *Composition of quasi-polynomial maps.*
The aim of this work is to study compositional properties of quasi-polynomial maps from $\mathbb{Z}$ to $\mathbb{Z}$, and more particularly of quasi-affine maps, namely quasi-polynomial maps of degree at most 1. We show that quasi-affine maps correspond to continuous endomorphisms of the algebra of recognizable bi-infinite sequences. We represent quasi-affine maps by means of finite sequences of integers, and we give explicit formulae on these sequences which translate composition or reversion of quasi-affine maps. Finally, we consider a coloring problem equivalent to the characterization of such sequences for quasi-affine bijections.

Introduction

Les applications quasi-polynomiales sont les applications de $\mathbb{Z}$ dans $\mathbb{C}$ qui sont combinaisons linéaires à coefficients périodiques des fonctions puissances d'exposant entier naturel. Ce type d'applications semble être apparu dans les travaux de Cayley [7], qui a en substance observé que le dénumérant [9, p. 120] d'un entier naturel n par rapport à une suite strictement croissante $\mathbf{a} = (a_1, a_2, \ldots)$ d'entiers naturels non nuls, c'est-à-dire le nombre de solutions en entiers naturels de l'équation $a_1x_1 + a_2x_2 + \cdots = n$, est une fonction quasi-polynomiale de l'entier n. Ehrhart [10] en a mené une étude

Manuscrit reçu le 19 janvier 2016, révisé le 13 septembre 2016, accepté le 17 octobre 2016.
Mathematics Subject Classification. 11B37.
Mots-clefs. Bijections entre entiers rationnels, coloriages, quasi-polynômes, suites récurrentes linéaires.

plus systématique dans le cadre de ses recherches relatives au nombre de points à coordonnées entières dans certains polytopes.

L'objet de ce travail est l'étude des propriétés de ces quasi-polynômes relativement à l'opération de composition des applications. Aucun des travaux qui nous sont connus n'avait envisagé ces propriétés. Bien sûr, pour pouvoir définir cette composition, il convient de se restreindre aux applications quasi-polynomiales à valeurs entières, pour lesquelles nous réservons le nom de quasi-polynômes arithmétiques. (Ehrhart [10, p. 12] les dénommait plus brièvement des polars ou des polynômes arithmétiques). Le fait fondamental dans notre étude est la stabilité de l'ensemble des quasi-polynômes arithmétiques pour la composition (théorème 1.6). Nous nous intéressons aux éléments inversibles du monoïde ainsi défini, c'est-à-dire aux quasi-polynômes arithmétiques qui induisent des bijections de $\mathbb{Z}$ dans $\mathbb{Z}$, en montrant qu'ils sont tous quasi-affines (théorème 1.10), c'est-à-dire combinaisons linéaires à coefficients périodiques des deux fonctions 1 et $\mathrm{Id}_{\mathbb{Z}}$.

Le reste de cet article est consacré aux propriétés de ces fonctions quasi-affines, qui constituent un sous-monoïde QA du monoïde de tous les quasi-polynômes arithmétiques (théorème 2.9). Nous représentons chacune de ces fonctions φ par un triplet $(d, \mathbf{a}, \mathbf{b})$, appelé présentation de φ, où $d \geq 1$ est un entier période des coefficients, et où $\mathbf{a}$ et $\mathbf{b}$ sont deux suites d'entiers, chacune de longueur d, et nous explicitons les règles de calcul sur ces objets qui correspondent à la composition des fonctions, à l'égalité des fonctions et à la réversion d'une fonction bijective. Ceci revient à décrire le monoïde QA comme le quotient d'un monoïde PQA, dont l'ensemble sous-jacent est la réunion disjointe $\coprod_{d\geq 1} \mathbb{Z}^{2d}$, et dont l'opération est celle donnée par les formules de notre proposition 2.10. La relation d'équivalence par laquelle on quotiente le monoïde PQA pour obtenir QA est précisée par l'énoncé de la proposition 2.13.

Cette étude des fonctions quasi-affines de $\mathbb{Z}$ dans $\mathbb{Z}$ est inspirée de la notion d'application purement semi-affine de $\mathbb{N}$ dans $\mathbb{N}$ introduite dans [1], elle-même cas particulier des applications semi-affines de $\mathbb{N}$ dans $\mathbb{N}$ définies dans [3]. En effet, de même que [3] interprétait les applications semi-affines comme endomorphismes continus de l'algèbre des suites indexées par l'ensemble $\mathbb{N}$ récurrentes linéaires sur un corps commutatif de caractéristique nulle, les applications quasi-affines correspondent exactement, d'après notre théorème 3.19, aux endomorphismes continus de l'algèbre des suites indexées par l'ensemble $\mathbb{Z}$ reconnaissables sur une $\mathbb{Q}$-algèbre commutative complètement intégralement close. La possibilité d'une telle description explique l'intérêt particulier qui s'attache au monoïde QA.

On aimerait donc décrire le groupe $\mathrm{QA}^\star$ de ses éléments symétrisables, c'est-à-dire des quasi-polynômes arithmétiques bijectifs. En préalable à cette question, nous cherchons dans la dernière section du présent article à caractériser les suites finies $\mathbf{a} \in \mathbb{Z}^d$ telles qu'il existe une bijection quasi-affine de rapport $\mathbf{a}$, c'est-à-dire représentée par un triplet $(d, \mathbf{a}, \mathbf{b})$ pour un certain $\mathbf{b} \in \mathbb{Z}^d$. Pour ce faire, nous associons à la suite $\mathbf{a}$ le multiensemble d'entiers naturels obtenu en prenant pour multiplicité d'un entier le nombre d'occurrences de cet entier dans la suite des valeurs absolues des termes de $\mathbf{a}$; en effet, l'existence d'une bijection quasi-affine de rapport $\mathbf{a}$ ne dépend que du multiensemble ainsi associé à la suite $\mathbf{a}$ (proposition 5.1). On cherche donc à caractériser les multiensembles associés aux rapports des bijections quasi-affines, dénommés multiensembles idoines. La question de la caractérisation des multiensembles idoines est ramenée par la proposition 5.2 à un certain problème de coloriage qui, à notre connaissance, n'avait pas été abordé jusqu'à présent. On montre ainsi qu'une condition suffisante pour qu'un multiensemble donné soit idoine est que tous les plus grands diviseurs communs de deux éléments distincts du support sont égaux entre eux (proposition 5.3) et on étudie quelques exemples de multiensembles idoines ou non (exemples 5.5 et 5.6).

Les remarques qui suivent pourront éclairer le lecteur sur la terminologie et les méthodes de démonstration utilisées. En premier lieu, notons que l'appellation d'application semi-affine précédemment utilisée [1, 3] a été ici écartée pour être remplacée par celle d'application quasi-affine. Plus que par le fait que sont ici considérées des applications de $\mathbb{Z}$ dans $\mathbb{Z}$, et non de $\mathbb{N}$ dans $\mathbb{N}$, ce changement est motivé par le fait que ces applications sont des cas particuliers de quasi-polynômes. Dans l'étude des quasi-polynômes arithmétiques bijectifs, nous utilisons la notion (analytique) de densité d'une partie de l'ensemble $\mathbb{Z}$. Il aurait été aussi possible d'utiliser cette notion dans l'étude faite dans la section 4 des bijections quasi-affines, la condition 1 de la proposition 4.4 ayant une interprétation directe à l'aide des densités. Cependant, nous avons préféré justifier cette condition par des arguments purement combinatoires, en introduisant une notion appelée empreinte, qui est une application à valeurs dans un groupe, et dont la source est une réunion disjointe de groupes.

Dans la section 3 du présent travail, nous nous conformons, pour alléger l'expression, à l'usage, inauguré dans le contexte des suites indexées par l'ensemble $\mathbb{N}$ par G. Hansel [13], consistant à utiliser le vocable de « reconnaissable » comme synonyme de « récurrente linéaire ». La démonstration de la caractérisation des applications quasi-affines au moyen des endomorphismes continus de l'algèbre des suites reconnaissables est très proche de celle de [3] : c'est pourquoi nous avons omis de reprendre un certain nombre d'arguments en renvoyant pour leur exposé à la littérature existante lorsque cela nous a paru possible. Notons que cette caractérisation peut se comprendre comme une solution, dans un cas particulier, du problème général de la théorie des bigèbres concernant le rapport susceptible d'exister entre les endomorphismes de l'algèbre duale finie et ceux de l'algèbre duale : en effet, Larson et Taft [14] ont observé, tout au moins lorsque l'anneau de base A est un corps, que l'algèbre des suites reconnaissables $r_{\mathbb{Z}}(A)$ dont nous déterminons les endomorphismes continus, s'identifie au dual fini de l'algèbre de Hopf dont l'algèbre sous-jacente est l'algèbre $A[X, X^{-1}]$ des polynômes de Laurent et dont la comultiplication est donnée par $\Delta(X^n) = X^n \otimes X^n$ pour tout $n \in \mathbb{Z}$, alors que l'algèbre $S_{\mathbb{Z}}(A)$ de toutes les suites s'interprète comme son dual tout entier. Ainsi notre résultat revient, pour cette bigèbre particulière, à décrire les endomorphismes continus du dual fini en tant que sous-ensemble des endomorphismes continus du dual.

Notation. Étant donnés deux nombres réels x et y, la notation $[x..y]$ désigne l'intersection $[x, y] \cap \mathbb{Z}$. Même convention pour des intervalles ouverts ou semi-ouverts.

1. Les quasi-polynômes

1.1. La notion de quasi-polynôme. La définition suivante des quasi-polynômes est celle donnée dans l'ouvrage [18] de R. Stanley.

Définition 1.1. Étant donné un entier naturel ℓ, un *quasi-polynôme de degré* ℓ est une fonction $f : \mathbb{Z} \to \mathbb{C}$ telle qu'existent $\ell+1$ fonctions périodiques $a_0, \ldots, a_\ell$ de $\mathbb{Z}$ dans $\mathbb{C}$ satisfaisant l'identité

$$\forall\, m \in \mathbb{Z}, \qquad f(m) = a_0(m) + a_1(m)m + \cdots + a_\ell(m)m^\ell, \tag{1.1}$$

avec $a_\ell \neq 0$. Un entier non nul période de toutes les fonctions a_j pour $j \in [0..\ell]$ est alors appelé une *quasi-période* de f.

On convient que la fonction nulle est l'unique quasi-polynôme de degré $-\infty$. La notation $\deg(f) = \ell$ signifie que le quasi-polynôme f est de degré ℓ.

Pour pouvoir définir la composition de quasi-polynômes, on se restreint au cas particulier de fonctions à valeurs entières. Dans ce cas, E. Ehrhart [10] a employé les vocables de polynôme arithmétique ou de polar. Ceci nous conduit à la définition suivante.

Définition 1.2. Si f est un quasi-polynôme tel que $f(m) \in \mathbb{Z}$ pour tout $m \in \mathbb{Z}$, l'application de $\mathbb{Z}$ dans lui-même induite par f est appelée un *quasi-polynôme arithmétique.*

Lemme 1.3. *Les fonctions périodiques $a_j : \mathbb{Z} \to \mathbb{C}$ figurant dans l'écriture* (1.1) *sont déterminées de façon unique par le quasi-polynôme $f : \mathbb{Z} \to \mathbb{C}$.*

Démonstration. Si la combinaison linéaire $a_0(m)+a_1(m)m+\cdots+a_\ell(m)m^\ell$, où $\ell \in \mathbb{N}$ et où chaque coefficient $a_j(m)$ est périodique de période T, représente la fonction nulle, alors, pour tout entier $r \in [0..T[$, la fonction

$m \mapsto a_0(r) + a_1(r)(r+Tm) + \cdots + a_\ell(r)(r+Tm)^\ell$ est une fonction polynomiale ne prenant que la valeur zéro ; par conséquent, tous ses coefficients $\sum_{k=j}^{\ell} a_k(r)\binom{k}{j} r^{k-j}T^j$, pour $j \in [0..\ell]$, sont nuls, ce qui nécessite que $a_j(r) = 0$ pour tout indice $j \in [0..\ell]$ et pour tout $r \in [0..T[$. Par périodicité, il s'ensuit que les coefficients $a_j(m)$ sont nuls sur $\mathbb{Z}$. □

Lemme 1.4. *Soit $f : \mathbb{Z} \to \mathbb{Z}$ un quasi-polynôme arithmétique de degré ℓ et de quasi-période $T \in \mathbb{Z} \setminus \{0\}$, donné par $\ell+1$ fonctions $a_j, 0 \le j \le \ell$ satisfaisant l'identité* (1.1)*. Alors, pour tout indice $j \in [0..\ell]$, on a*

$$\forall\, m \in \mathbb{Z}, \qquad T^\ell \ell! a_j(m) \in \mathbb{Z}\,.$$

Démonstration. Envisageons d'abord le cas où $T = 1$, c'est-à-dire celui où les fonctions a_j sont constantes. On sait [16] qu'alors $f(m)$ est combinaison $\mathbb{Z}$-linéaire des polynômes $\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!}$, avec $k \in [0..\ell]$. Donc le polynôme $\ell! f(m)$ est à coefficients entiers, ce qui montre le résultat dans ce cas.

Dans le cas général, on se ramène au cas $T = 1$ en définissant, pour tout entier $r \in [0..T[$, un polynôme f_r par

$$\forall\, m \in \mathbb{Z}, \qquad f_r(m) = f(r+mT) = \sum_{j=0}^{\ell} A_j m^j,$$

avec $A_j = T^j \sum_{k=j}^{\ell} \binom{k}{j} a_k(r) r^{k-j}$. Comme f_r est un polynôme de degré ℓ à valeurs entières, on a $\ell! A_j \in \mathbb{Z}$ pour tout indice $j \in [0..\ell]$. En particulier $\ell! A_\ell = T^\ell \ell! a_\ell(r)$ est entier. Supposons qu'il existe un indice $j \in [0..\ell[$ tel que $T^\ell \ell! a_j(r) \notin \mathbb{Z}$. On peut choisir j le plus grand possible satisfaisant cette condition, de sorte que $T^\ell \ell! a_k(r)$ est entier pour tout indice $k \in]j..\ell]$. Alors

$$T^\ell \ell! a_j(r) = T^{\ell-j} \ell! A_j - \sum_{k=j+1}^{\ell} \binom{k}{j} (T^\ell \ell! a_k(r)) r^{k-j}$$

est entier, contrairement à l'hypothèse. □

1.2. Composition de quasi-polynômes arithmétiques.

Lemme 1.5. *Si f est un quasi-polynôme arithmétique non nul de degré ℓ et de quasi-période T, et si g est un quasi-polynôme de degré au plus zéro et de période $P \neq 0$, alors $g \circ f$ est un quasi-polynôme de degré au plus zéro et de période $L = T^{\max(1,\ell)} \ell! P$.*

Démonstration. On remarque que $L = T^{\max(1,\ell)} \ell! P$ est un multiple commun des entiers T et P. Par hypothèse, il existe $\ell+1$ fonctions $a_j : \mathbb{Z} \to \mathbb{C}$, $j = 0 \ldots \ell$ de période T satisfaisant l'identité (1.1). On va vérifier que $g \circ f$ est périodique de période L : il suffit pour cela de montrer que la différence

$f(m+L)-f(m)$ est un multiple de P. Or

$$\ell! T^{\ell}\left(f(m+L)-f(m)\right) = L\sum_{j=1}^{\ell} a_j(m)\ell! T^{\ell}\left(\sum_{k=0}^{j-1}\binom{j}{k}L^{j-k-1}m^k\right).$$

Comme les nombres $a_j(m)\ell! T^{\ell}$ sont entiers pour tout indice $j \in [1..\ell]$ par le lemme 1.4, on voit que les entiers $\ell! T^{\ell}(f(m+L)-f(m))$ sont des multiples de L. Par division par $\ell! T^{\ell}$, on en déduit que $f(m+L)-f(m)$ est divisible par P. $\square$

Théorème 1.6. *Le composé de deux quasi-polynômes arithmétiques est un quasi-polynôme arithmétique. De plus, si ces deux quasi-polynômes arithmétiques sont non nuls, le degré de leur composé est au plus égal au produit de leurs degrés. Si T est une quasi-période du quasi-polynôme arithmétique $f \neq 0$ de degré ℓ, et si P est une quasi-période du quasi-polynôme arithmétique g, alors $L = T^{\max(1,\ell)}\ell! P$ est une quasi-période de $g \circ f$.*

Démonstration. On sait [10] que les quasi-polynômes forment un anneau quand on les munit de l'addition et de la multiplication usuelles ; en particulier, le produit de deux quasi-polynômes admet pour quasi-période tout multiple commun des quasi-périodes des deux facteurs ; de plus, on a évidemment $\deg(f+g) \leq \max(\deg(f), \deg(g))$ et $\deg(fg) \leq \deg(f)+\deg(g)$.

L'anneau des quasi-polynômes est, au vu de la relation (1.1), engendré par les quasi-polynômes de degré au plus zéro (les fonctions périodiques) et la fonction identique de $\mathbb{Z}$. Soit f un quasi-polynôme arithmétique. L'ensemble de tous les quasi-polynômes g tels que $g \circ f$ soit un quasi-polynôme est un sous-anneau de l'anneau des quasi-polynômes, qui comprend les fonctions périodiques d'après le lemme 1.5, et qui comprend évidemment la fonction identique de $\mathbb{Z}$. Par conséquent, cet ensemble est celui de tous les quasi-polynômes. Ainsi nous avons montré que, si g est un quasi-polynôme et f un quasi-polynôme arithmétique, alors le composé $g \circ f$ est un quasi-polynôme. Si g est supposé être de plus un quasi-poynôme arithmétique, on a en outre les inclusions $(g \circ f)(\mathbb{Z}) \subseteq g(\mathbb{Z}) \subseteq \mathbb{Z}$, de sorte que le composé de deux quasi-polynômes arithmétiques est un quasi-polynôme arithmétique.

De plus, si g est non nul, de sorte que son degré d est un entier naturel, il existe $d+1$ fonctions périodiques b_j, avec $j \in [0..d]$, telles que $g(m) = b_0(m) + b_1(m)m + \cdots + b_d(m)m^d$ pour tout $m \in \mathbb{Z}$, et donc

$$\forall\, m \in \mathbb{Z}, \quad (g \circ f)(m) = b_0(f(m)) + b_1(f(m))f(m) + \cdots + b_d(f(m))f(m)^d.$$

Comme les fonctions $b_j \circ f$ sont périodiques de période L d'après le lemme 1.5, et que les quasi-polynômes arithmétiques f^j sont de quasi-période L, on voit que, si $f \neq 0$, le degré de $g \circ f$ est au plus $d\ell$ et que L en est une quasi-période. $\square$

1.3. Les quasi-polynômes bijectifs. On va maintenant préciser quels sont les quasi-polynômes bijectifs. Nous nous appuierons pour cela sur la notion de densité naturelle d'une partie de $\mathbb{Z}$, qui est une variante simple de la notion bien connue de densité naturelle d'une partie de $\mathbb{N}$ [15].

Définition 1.7. Soit A une partie de $\mathbb{Z}$. On dit que la partie A a une *densité* si la suite de terme général

$$\frac{\operatorname{card}(A \cap [-n, +n])}{2n+1} \tag{1.2}$$

admet une limite pour n tendant vers l'infini. Lorsque A a une densité, la *densité* (naturelle) de A, notée $\operatorname{dens}(A)$, est la limite de la suite (1.2).

On a évidemment l'énoncé suivant.

Lemme 1.8. *Si A et B sont deux parties disjointes de $\mathbb{Z}$ ayant toutes deux une densité, alors $A \cup B$ a une densité, et la densité de $A \cup B$ est la somme des densités de A et de B.*

Lemme 1.9. *Soit f un polynôme de degré ℓ tel que $f(\mathbb{Z}) \subset \mathbb{Z}$. Si $\ell \geq 2$, alors la densité naturelle de l'ensemble $f(\mathbb{Z})$ est nulle.*

Démonstration. Il est clair qu'il suffit de montrer que la densité naturelle de l'ensemble $f(\mathbb{N})$ est nulle, et qu'on peut pour cela se restreindre au cas où le coefficient dominant de f, noté $\operatorname{cd}(f)$, est positif. Dans ce cas il existe un nombre réel $\rho > 0$ tel que f est strictement croissante sur $[\rho, +\infty[$. Et, puisque $f(x)$ tend vers l'infini avec x, on voit qu'il existe un entier $N \geq \rho$ tel que $f(N) > f(k)$, pour tout entier naturel $k < \rho$.

L'ensemble des valeurs prises par la suite croissante $(f(N+n))_{n\in\mathbb{N}}$ est alors identique à l'ensemble de tous les éléments de $f(\mathbb{N})$ au moins égaux à $f(N)$. Rangeons tous les éléments de l'ensemble $f(\mathbb{N}) \cap \mathbb{N}^*$ dans une suite strictement croissante $(a_n)_{n\geq 1}$. Il résulte de ce qui précède l'équivalent

$$a_n \sim \operatorname{cd}(f) n^\ell \quad \text{pour } n \to +\infty \ ,$$

d'où, comme $\ell \geq 2$, l'on déduit $\lim_{n\to+\infty} \frac{n}{a_n} = 0$. Par une propriété connue de la densité naturelle des ensembles d'entiers naturels [15], on aboutit au résultat voulu. $\square$

Théorème 1.10. *Un quasi-polynôme arithmétique bijectif est de degré 1.*

Démonstration. Soit f un quasi-polynôme arithmétique bijectif ; il existe un entier naturel $T > 0$ qui est une quasi-période de f.

Pour $r \in [0..T[$, définissons f_r l'application de $\mathbb{Z}$ dans $\mathbb{Z}$ telle que

$$\forall\, m \in \mathbb{Z}, \qquad f_r(m) = f(r + Tm).$$

Alors, f_r est un polynôme de degré $\leq \ell$ qui induit une application injective de $\mathbb{Z}$ dans lui-même. Comme les fonctions constantes ne sont pas injectives, le degré de f_r est nécessairement ≥ 1. On introduit l'ensemble A dont les éléments sont les entiers $r \in [0..T[$ tels que le polynôme f_r est de degré 1. Pour $r \in A$, il existe deux entiers $a_r \neq 0$ et b_r tels que $f_r(m) = a_r m + b_r$, ce qui montre que $f_r(\mathbb{Z})$ a une densité $\frac{1}{|a_r|}$.

On a évidemment

$$\mathbb{Z} = f(\mathbb{Z}) = f\left(\bigcup_{r=0}^{T-1}(r + T\mathbb{Z})\right) = \bigcup_{r=0}^{T-1} f_r(\mathbb{Z}).$$

Comme les $f_r(\mathbb{Z})$ sont deux à deux disjoints et ont chacun une densité, on a par les lemmes 1.8 et 1.9 :

$$1 = \mathrm{dens}(\mathbb{Z}) = \sum_{r=0}^{T-1} \mathrm{dens}(f_r(\mathbb{Z})) = \sum_{r \in A} \frac{1}{|a_r|},$$

Posons $N = \mathrm{ppcm}\{a_r,\ r \in A\}$ et soit l'ensemble $X = \bigcup_{r \in A} f_r(\mathbb{Z})$. On observe que X est réunion de classes modulo N : en effet, soit $x \in X$ et un entier $m \in \mathbb{Z}$, tel que $m = x + Nz$ pour un certain entier z. Par définition de X, il existe $r \in A$ et $y \in \mathbb{Z}$ tels que $x = f_r(y) = a_r y + b_r$, d'où $m = x + Nz = a_r(y + c_r z) + b_r$, où $c_r = N/a_r \in \mathbb{Z}$. Par conséquent $m = f_r(y + c_r z)$ est élément de X. D'autre part, l'ensemble X a, d'après le lemme 1.8, la densité

$$\mathrm{dens}(X) = \sum_{r \in A} \mathrm{dens}(f_r(\mathbb{Z})) = \sum_{r \in A} \frac{1}{|a_r|} = 1,$$

ainsi on a nécessairement $X = \mathbb{Z}$.

Par conséquent, $A = [0..T[$, de sorte que, pour tout $r \in [0..T[$, on a $\deg(f_r) = 1$, ce qui montre que f est de degré 1. □

2. Présentations d'une application quasi-affine

2.1. Applications quasi-affines. On sait que les applications affines $\varphi : \mathbb{Z} \to \mathbb{Z}$ sont les solutions de la récurrence $\varphi(m+1) - 2\varphi(m) + \varphi(m-1) = 0$. Ceci suggère de généraliser la notion d'application affine de la manière suivante.

Définition 2.1. Soit φ une application de $\mathbb{Z}$ dans $\mathbb{Z}$ et $d \geq 1$ un entier naturel. On dit que φ est *quasi-affine de largeur d* si elle satisfait la récurrence

$$\forall\, m \in \mathbb{Z}, \qquad \varphi(m + d) - 2\varphi(m) + \varphi(m - d) = 0\,. \tag{2.1}$$

On note QA_d l'ensemble des applications quasi-affines de largeur d, et on pose

$$\mathrm{QA} = \bigcup_{d \geq 1} \mathrm{QA}_d \,.$$

On appelle *application quasi-affine* tout élément de QA.

Remarque 2.2. Cette définition est l'analogue, pour les applications de $\mathbb{Z}$ dans $\mathbb{Z}$, de celle des applications purement semi-affines donnée par [1].

Proposition 2.3. *Soit φ une application de $\mathbb{Z}$ dans $\mathbb{Z}$ et $d \geq 1$ un entier naturel. Les quatre assertions suivantes sont équivalentes.*

(i) *L'application φ est quasi-affine de largeur d.*

(ii) *Pour tout couple d'entiers $(m, k) \in \mathbb{Z}^2$, on a*

$$\varphi(m + kd) - \varphi(m) = k\left(\varphi(m + d) - \varphi(m)\right). \tag{2.2}$$

(iii) *L'application $\varphi : \mathbb{Z} \to \mathbb{Z}$ est un quasi-polynôme arithmétique de degré au plus un et de quasi-période d.*

(iv) *Si m et n sont deux entiers rationnels tels que $m \equiv n \bmod 2d$ alors on a*

$$\varphi\left(\frac{m+n}{2}\right) = \frac{\varphi(m) + \varphi(n)}{2}\,. \tag{2.3}$$

Démonstration. L'implication (i) ⇒ (ii) résulte d'une simple récurrence sur l'entier naturel $|k|$.

Pour montrer l'implication (ii) ⇒ (iii), étant donné un entier $m \in \mathbb{Z}$, on écrit par division euclidienne $m = dq + r$, où $q \in \mathbb{Z}$ et $r \in [0..d[$. On a alors par hypothèse $\varphi(m) - \varphi(r) = q\left(\varphi(r + d) - \varphi(r)\right)$. Il vient alors :

$$\varphi(m) = \frac{\varphi(r + d) - \varphi(r)}{d} m + \varphi(r) - \frac{r}{d}\left(\varphi(r + d) - \varphi(r)\right)$$

et on conclut en remarquant que les deux fonctions $m \mapsto \frac{\varphi(r+d)-\varphi(r)}{d}$ et $m \mapsto \varphi(r) - \frac{r}{d}(\varphi(r + d) - \varphi(r))$ sont toutes deux de période d.

Pour montrer que (iii) implique (iv), on écrit $n = m + (2k)d$, d'où $\frac{m+n}{2} = m + kd$, on exprime $\varphi(m + (2k)d)$ et $\varphi(m + kd)$ et $\varphi(m)$ à l'aide de l'hypothèse, et on combine les trois équations ainsi obtenues.

Enfin, l'implication (iv) ⇒ (i) résulte de la congruence $m + d \equiv m - d \bmod 2d$. □

Les deux lemmes suivants sont des conséquences immédiates des relations (2.2) et (2.3).

Lemme 2.4. *Soit $d \geq 1$ et $k \geq 1$ deux entiers naturels. Alors* $\mathrm{QA}_d \subset \mathrm{QA}_{kd}$.

Lemme 2.5. *Si l'application $\varphi : \mathbb{Z} \to \mathbb{Z}$ est quasi-affine de largeur d, alors pour tout couple d'entiers $(m, k) \in \mathbb{Z}^2$, on a*

$$\varphi(m + kd) \equiv \varphi(m) \bmod k\,.$$

Notation. Si x est un nombre réel, nous utiliserons le symbole usuel $\lfloor x \rfloor$ pour désigner la partie entière de x, c'est-à-dire le plus grand entier rationnel qui minore x, et le symbole $\{x\} = x - \lfloor x \rfloor$ pour la partie fractionnaire de x.

La proposition suivante précise comment on peut donner sous forme explicite les applications quasi-affines de largeur d donnée.

Proposition 2.6. *Soit $d \geq 1$ un entier naturel, et φ une application de $\mathbb{Z}$ dans $\mathbb{Z}$. Les propriétés suivantes sont équivalentes :*

(1) *Il existe deux suites finies d'entiers rationnels $\mathbf{a} = (a_i)_{0 \leq i < d} \in \mathbb{Z}^d$, $\mathbf{b} = (b_i)_{0 \leq i < d} \in \mathbb{Z}^d$, telles que*

$$\forall\, m \in \mathbb{Z}, \quad \varphi(m) = a_{r(m)} \left\lfloor \frac{m}{d} \right\rfloor + b_{r(m)}, \quad \textit{avec} \;\; r(m) = d \left\{ \frac{m}{d} \right\} \in [0..d[.$$

(2) *L'application φ est quasi-affine de largeur d.*

Démonstration. On montre d'abord l'implication (1) $\Rightarrow$ (2). En utilisant le fait que $x \mapsto \{x\}$ est périodique de période 1, on a $r(m+d) = r(m) = r(m-d)$, donc l'identité

$$\forall\, m \in \mathbb{Z}, \qquad \varphi(m) = a_{r(m)} \left\lfloor \frac{m}{d} \right\rfloor + b_{r(m)}$$

entraîne que $\varphi(m+d) - 2\varphi(m) + \varphi(m-d) = 0$.

Réciproquement, on va montrer l'implication (2) $\Rightarrow$ (1). Pour $r \in [0..d[$, on pose

$$a_r = \varphi(r+d) - \varphi(r) \qquad \text{et} \qquad b_r = \varphi(r)\ .$$

Soit m un entier rationnel. Comme on a $\frac{m}{d} = \lfloor \frac{m}{d} \rfloor + \{\frac{m}{d}\}$, on en déduit $m = d\lfloor \frac{m}{d} \rfloor + r(m)$, d'où en vertu de l'équation (2.2) :

$$\varphi(m) = \varphi\left(r(m) + \left\lfloor \frac{m}{d} \right\rfloor d \right) = \varphi(r(m)) + \left\lfloor \frac{m}{d} \right\rfloor \left(\varphi(r(m)+d) - \varphi(r(m)) \right)\ ,$$

ce qui est bien l'égalité $\varphi(m) = a_{r(m)} \lfloor \frac{m}{d} \rfloor + b_{r(m)}$ qu'on désirait montrer. $\square$

Définition 2.7. Pour toute application quasi-affine φ, le triplet $(d, \mathbf{a}, \mathbf{b})$ constitué de la largeur d et des suites finies $\mathbf{a} = (a_i)_{0 \leq i < d} \in \mathbb{Z}^d$ et $\mathbf{b} = (b_i)_{0 \leq i < d} \in \mathbb{Z}^d$ de la proposition 2.6, est appelé une *présentation* de φ. La suite finie $\mathbf{a} \in \mathbb{Z}^d$ est appelée le *rapport* de la présentation.

Remarque 2.8. Il est important de remarquer qu'il n'y a pas unicité de la présentation d'une application quasi-affine φ fixée, car, ainsi que le fait voir le lemme 2.4, la largeur de φ n'est pas déterminée par l'application elle-même. Par contre, si on se donne une largeur d de φ, alors les deux suites $\mathbf{a}$ et $\mathbf{b}$ de la proposition 2.6 sont uniquement déterminées : en effet, on a toujours $a_r = \varphi(r+d) - \varphi(r)$ et $b_r = \varphi(r)$ quelque soit l'entier $r \in [0..d[$.

2.2. Composition d'applications quasi-affines.

Théorème 2.9. *L'ensemble* QA *de toutes les applications quasi-affines est un sous-monoïde du monoïde des quasi-polynômes arithmétiques pour la composition. Plus précisément, si* $\varphi \in \mathrm{QA}_d$ *et* $\varphi' \in \mathrm{QA}_{d'}$*, alors leur composé* $\varphi \circ \varphi'$ *appartient à* $\mathrm{QA}_{dd'}$*.*

Démonstration. Cas particulier du théorème 1.6. □

La proposition suivante explicite le calcul de la composée de deux applications quasi-affines.

Proposition 2.10. *Soit* φ *et* φ' *deux applications quasi-affine, de présentations respectives* $(d, \mathbf{a}, \mathbf{b})$ *et* $(d', \mathbf{a}', \mathbf{b}')$*. Alors une présentation de l'application quasi-affine* $\varphi'' = \varphi \circ \varphi'$ *est le triplet* $(dd', \mathbf{a}'', \mathbf{b}'')$*, où* $\mathbf{a}'' \in \mathbb{Z}^{dd'}$ *et* $\mathbf{b}'' \in \mathbb{Z}^{dd'}$ *sont les suites, indexées par l'ensemble des entiers naturels plus petits que* dd'*, données par*

$$(2.4) \quad \forall\, k \in [0..dd'[\,,$$

$$a''_k = a_{u(k)} a'_{s(k)} \qquad \textit{et} \qquad b''_k = a_{u(k)} \left\lfloor \frac{a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)}}{d} \right\rfloor + b_{u(k)},$$

avec

$$(2.5) \quad \forall\, k \in [0..dd'[\,,$$

$$s(k) = d' \left\{ \frac{k}{d'} \right\} \qquad \textit{et} \qquad u(k) = d \left\{ \frac{a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)}}{d} \right\}.$$

Démonstration. D'après le théorème 2.9, l'application φ'' est quasi-affine de largeur dd' . La proposition 2.6 montre qu'il existe deux suites $\mathbf{a}'' = (a''_k)_{0 \le k < dd'}$ et $\mathbf{b}'' = (b''_k)_{0 \le k < dd'}$ d'entiers rationnels telles que

$$\forall\, m \in \mathbb{Z}, \quad \varphi''(m) = a''_{k(m)} \left\lfloor \frac{m}{dd'} \right\rfloor + b''_{k(m)}$$

où $k(m) = dd' \left\{ \frac{m}{dd'} \right\}$. Il en résulte que, pour tout $k \in [0..dd'[$, on a

$$a''_k = \varphi''(k + dd') - \varphi''(k) \tag{2.6}$$

et

$$b''_k = \varphi''(k). \tag{2.7}$$

En appliquant la formule (2.2) à l'application quasi-affine φ', de largeur d', on a :

$$\varphi'(k + dd') - \varphi'(k) = d(\varphi'(k + d') - \varphi'(k))\,.$$

Par hypothèse

$$\varphi'(k) = a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)}\,. \tag{2.8}$$

D'autre part, puisque $d'\left\{\frac{k+d'}{d'}\right\} = d'\left\{\frac{k}{d'}\right\} = s(k)$, on a

$$\varphi'(k+d') = a'_{s(k)} \left\lfloor \frac{k+d'}{d'} \right\rfloor + b'_{s(k)}\,.$$

Donc $\varphi'(k+d') - \varphi'(k) = a'_{s(k)}$, d'où :

$$\varphi'(k+dd') = \varphi'(k) + da'_{s(k)}.$$

On utilise alors la formule (2.2) pour l'application quasi-affine φ de largeur d, en posant $m = \varphi'(k)$. On obtient :

$$\begin{aligned}\varphi''(k+dd') - \varphi''(k) &= \varphi\left(\varphi'(k) + da'_{s(k)}\right) - \varphi\left(\varphi'(k)\right)\\ &= a'_{s(k)}\left(\varphi\left(\varphi'(k)+d\right) - \varphi\left(\varphi'(k)\right)\right).\end{aligned}$$

Pour tout $m \in \mathbb{Z}$, on note $r(m) = d\left\{\frac{m}{d}\right\}$. Par hypothèse, on a

$$\varphi\left(\varphi'(k)\right) = a_{r(\varphi'(k))} \left\lfloor \frac{\varphi'(k)}{d} \right\rfloor + b_{r(\varphi'(k))} \tag{2.9}$$

et $\varphi\left(\varphi'(k)+d\right) = a_{r(\varphi'(k)+d)} \left\lfloor \frac{\varphi'(k)+d}{d} \right\rfloor + b_{r(\varphi'(k)+d)}$. Comme $r(\varphi'(k)+d) = r(\varphi'(k))$, et que l'équation (2.8) montre que $r(\varphi'(k)) = u(k)$, on en déduit que

$$\varphi\left(\varphi'(k)+d\right) - \varphi\left(\varphi'(k)\right) = a_{u(k)},$$

ce qui donne, d'après la relation (2.6), l'égalité $a''_k = a_{u(k)}a'_{s(k)}$ qu'on voulait montrer. En outre, la relation (2.9) donne $\varphi''(k) = \varphi\left(\varphi'(k)\right) = a_{u(k)} \left\lfloor \frac{\varphi'(k)}{d} \right\rfloor + b_{u(k)}$. En reportant dans cette dernière relation la valeur de $\varphi'(k)$ donnée par l'équation (2.8), on obtient, compte tenu de (2.7), l'expression voulue de b''_k. □

Remarque 2.11. On pourra comparer notre résultat à l'énoncé donné par [2, Proposition 2.3] pour les applications purement semi-affines de $\mathbb{N}$ dans $\mathbb{N}$, qui est entaché d'une imprécision dans la définition du paramètre r qui y prend la place de notre nombre $u(k)$, et qui est erroné en ce qu'il introduit un nombre d parasite dans l'écriture de b''_k.

Remarque 2.12. Introduisons le magma PQA, dont l'ensemble sous-jacent est $\coprod_{d\geq 1} \mathbb{Z}^{2d} = \cup_{d\geq 1}\{d\} \times \mathbb{Z}^{2d}$, et où la loi de composition est donnée par les applications $\mathbb{Z}^{2d} \times \mathbb{Z}^{2d'} \to \mathbb{Z}^{2dd'}$ données par les formules (2.4) et (2.5). En notant $\mathbb{N}^*$ le monoïde multiplicatif des entiers naturels non nuls, l'application de PQA dans $\mathbb{N}^*$ qui associe l'entier d à tout élément de $\mathbb{Z}^{2d}$ est un morphisme de magmas, et la proposition 2.10 signifie que l'application de PQA dans le monoïde QA des applications quasi-affines qui au couple $(\mathbf{a}, \mathbf{b}) \in \mathbb{Z}^d \times \mathbb{Z}^d = \mathbb{Z}^{2d}$ associe l'application φ définie par la condition (1) de la proposition 2.6 est aussi un morphisme de magmas. Par conséquent, on a un morphisme de PQA dans $\mathbb{N}^* \times \mathrm{QA}$. Ce morphisme est injectif d'après la remarque 2.8 ; en particulier, le magma PQA est un monoïde qui admet QA comme un quotient.

2.3. Changement de présentations. Nous allons maintenant expliciter la relation d'équivalence sur le monoïde PQA par laquelle on quotiente pour obtenir QA, c'est-à-dire caractériser sous quelles conditions deux présentations d'applications quasi-affines de différentes largeurs sont en fait présentations d'une même application.

Proposition 2.13. *On se donne deux entiers naturels $d \geq 1$ et $d' \geq 1$, et des suites finies $\mathbf{a} \in \mathbb{Z}^d, \mathbf{b} \in \mathbb{Z}^d, \mathbf{a}' \in \mathbb{Z}^{d'}, \mathbf{b}' \in \mathbb{Z}^{d'}$. On note q le plus grand commun diviseur des entiers d et d'. Pour que les triplets $(d, \mathbf{a}, \mathbf{b})$ et $(d', \mathbf{a}', \mathbf{b}')$ soient deux présentations d'une même application quasi-affine, il faut et il suffit que, pour tout couple (r, r') d'entiers naturels tel que $r < d, r' < d'$ et $r \equiv r' \bmod q$, on ait les égalités*

$$d' a_r = d a'_{r'} \quad \text{et} \quad d(b_r - b'_{r'}) = a_r (r - r') \,.$$

Démonstration. Vérifions d'abord que cette condition est suffisante. Soit φ l'application quasi-affine de largeur d et de présentation $(d, \mathbf{a}, \mathbf{b})$, et φ' l'application quasi-affine de largeur d' et de présentation $(d', \mathbf{a}', \mathbf{b}')$. On note $r : \mathbb{Z} \to [0..d[$ (resp. $r' : \mathbb{Z} \to [0..d'[$) l'application telle que $r(m) = d \left\{ \frac{m}{d} \right\}$ (resp. $r'(m) = d' \left\{ \frac{m}{d'} \right\}$) pour tout entier $m \in \mathbb{Z}$. Comme d est un diviseur de $m - r(m)$, et que d' est un diviseur de $m - r'(m)$, on voit que $r(m) \equiv r'(m) \bmod q$ pour tout entier $m \in \mathbb{Z}$.

Il s'agit de vérifier qu'on a $\varphi = \varphi'$ sous la condition donnée dans l'énoncé. Or, pour tout entier $m \in \mathbb{Z}$, on a alors :

$$\begin{aligned}
\varphi(m) &= a_{r(m)} \left\lfloor \frac{m}{d} \right\rfloor + b_{r(m)} \\
&= a_{r(m)} \left(\frac{m}{d} - \left\{ \frac{m}{d} \right\} \right) + b'_{r'(m)} + \frac{a_{r(m)}}{d} (r(m) - r'(m)) \,.
\end{aligned}$$

Comme $r(m) = d \left\{ \frac{m}{d} \right\}$, cette expression se simplifie en

$$\varphi(m) = a_{r(m)} \frac{m - r'(m)}{d} + b'_{r'(m)} = a'_{r'(m)} \frac{m - r'(m)}{d'} + b'_{r'(m)} \,,$$

ce qui donne finalement

$$\varphi(m) = a'_{r'(m)} \left\lfloor \frac{m}{d'} \right\rfloor + b'_{r'(m)} = \varphi'(m) \,.$$

Montrons réciproquement que la condition indiquée est nécessaire. On suppose donc que les triplets $(d, \mathbf{a}, \mathbf{b})$ et $(d', \mathbf{a}', \mathbf{b}')$ sont deux présentations d'une même application quasi-affine φ. Alors, d'après la proposition 2.3, on sait que d et d' sont deux quasi-périodes du quasi-polynôme φ. Comme le plus grand commun diviseur q des entiers d et d' est de la forme $q = ud+vd'$, où u et v sont deux entiers, on voit que q est aussi une quasi-période de φ, et donc φ appartient à QA_q. Par la proposition 2.3, il existe donc deux fonctions $c_1 : \mathbb{Z} \to \mathbb{C}$ et $c_0 : \mathbb{Z} \to \mathbb{C}$ de période q telles que $\varphi(m) = c_1(m)m + c_0(m)$ pour tout entier rationnel m. Considérons deux entiers naturels r et r' tels que $r \equiv r' \bmod q$, de sorte que $c_j(r+d) = c_j(r'+d') = c_j(r) = c_j(r')$ pour tout indice $j \in \{0, 1\}$. On a donc

$$\begin{aligned} d' a_r &= d' \left(\varphi(r+d) - \varphi(r)\right) = c_1(r) d d' \\ &= d c_1(r') d' = d \left(\varphi(r'+d') - \varphi(r')\right) = d a'_{r'} \,. \end{aligned}$$

D'autre part :

$$\begin{aligned} d(b_r - b'_{r'}) &= d(\varphi(r) - \varphi(r')) = d c_1(r)(r - r') \\ &= \left(\varphi(r+d) - \varphi(r)\right)(r - r') = a_r (r - r') \,. \end{aligned}$$ □

2.4. Forme réduite d'une application quasi-affine. Soit φ une application quasi-affine ; l'ensemble des entiers $d \geq 1$ tels que φ est de largeur d admet un plus petit élément, que nous appelons la *largeur minimale* de l'application quasi-affine φ.

Définition 2.14. Pour toute application quasi-affine $\varphi : \mathbb{Z} \to \mathbb{Z}$ de largeur minimale $d_0 \geq 1$, la donnée des deux suites $\mathbf{a} = (a_i)_{0 \leq i < d_0}$ et $\mathbf{b} = (b_i)_{0 \leq i < d_0}$ éléments de $\mathbb{Z}^{d_0}$ de la proposition 2.6 est appelée la *forme réduite* de φ.

Puisque $\mathbb{Z}$ est un anneau principal, la proposition 2.3 montre que, si d_0 est la largeur minimale de φ, alors φ est élément de QA_d si et seulement si d est un multiple de d_0.

Proposition 2.15. *Soit $(d, \mathbf{a}, \mathbf{b})$ une présentation de l'application quasi-affine φ. Pour que cette présentation ne soit pas la forme réduite de φ, il faut et il suffit qu'il existe une factorisation de l'entier d en deux facteurs $d = qd'$ telle que $q > 1$ soit un diviseur commun à tous les termes a_r de la suite finie $\mathbf{a}$ et vérifiant de plus :*

$$\forall\, r \in [0..d - d'[, \qquad a_{r+d'} = a_r \quad \text{et} \quad b_{r+d'} = b_r + \frac{a_r}{q} \,.$$

Si cette condition est satisfaite, alors une autre présentation de l'application φ est $(d', \mathbf{a}', \mathbf{b}')$, en posant, pour tout entier naturel r' tel que $r' < d'$,

$$a'_{r'} = \frac{a_{r'}}{q} \quad \text{et} \quad b'_{r'} = b_{r'} \,.$$

Démonstration. Supposons que le triplet $(d, \mathbf{a}, \mathbf{b})$ ne soit pas la présentation réduite de l'application φ, et soit d' la largeur minimale de φ. Ainsi, il existe une autre présentation $(d', \mathbf{a}', \mathbf{b}')$ de φ telle que $d = qd'$, où $q > 1$.

Selon la proposition 2.13 , pour tout couple (r, r') d'entiers naturels tel que $r < d, r' < d'$ et $r \equiv r' \bmod d'$, on a les égalités

$$d' a_r = d a'_{r'} \quad \text{et} \quad d(b_r - b'_{r'}) = a_r(r - r')\,.$$

En particulier, pour tout entier naturel $r < d$, on peut choisir $r' = d'\left\{\frac{r}{d'}\right\}$, de sorte qu'on ait $r \equiv r' \bmod d'$ et $r' < d'$, d'où $a_r = q a'_{r'}$, ce qui montre que q est un diviseur commun à tous les termes a_r de la suite $\mathbf{a}$.

Si maintenant l'entier naturel r satisfait l'inégalité $r < d - d'$, alors $r + d' < d,\ r + d' \equiv r' \bmod d'$, et par conséquent on a aussi

$$a_{r+d'} = q a'_{r'} = a_r\,.$$

D'autre part :

$$d(b_r - b'_{r'}) = a_r(r - r') \quad \text{et} \quad d(b_{r+d'} - b'_{r'}) = a_{r+d'}(r + d' - r')\,.$$

Par différence entre ces deux dernières égalités, et en tenant compte que $d = qd'$ et que $a_r = a_{r+d'}$, on obtient

$$b_{r+d'} = b_r + \frac{a_r}{q}\,.$$

Réciproquement, on suppose l'existence d'une factorisation $d = qd', q > 1$ telle que q divise tous les termes a_r $(0 \le r < d)$, et que soient vérifiées les égalités

$$\forall\, r \in [0..d - d'[, \qquad a_{r+d'} = a_r \quad \text{et} \quad b_{r+d'} = b_r + \frac{a_r}{q}\,.$$

Soit le triplet $(d', \mathbf{a}', \mathbf{b}')$ où on a posé, pour tout entier naturel $r' < d'$, $a'_{r'} = \frac{a_{r'}}{q}$ et $b'_{r'} = b_{r'}$. On se donne deux entiers naturels r et r' tels que $r \equiv r' \bmod d'$. Par hypothèse, ceci entraîne que $a_r = a_{r'}$ et $b_r = b_{r'} + \frac{r-r'}{d'}\frac{a_{r'}}{q}$. On voit donc que

$$d a'_{r'} = d' q a'_{r'} = d' a_{r'} = d' a_r$$

et que

$$d(b_r - b'_{r'}) = d(b_r - b_{r'}) = d\frac{r - r'}{d'}\frac{a_{r'}}{q} = (r - r')a_r\,.$$

Ainsi selon la proposition 2.13, le triplet $(d', \mathbf{a}', \mathbf{b}')$ est une autre présentation de l'application φ. □

Exemple 2.16. Soit la présentation $(6, \mathbf{a}, \mathbf{b})$ avec $\mathbf{a} = (4, 8, 8, 4, 8, 8)$ et $\mathbf{b} = (0, 1, 3, 2, 5, 7)$. En prenant $q = 2$ et $d' = 3$, on a une factorisation de d qui satisfait la condition indiquée. Donc cette présentation n'est pas forme réduite d'une application quasi-affine. La proposition 2.15 montre qu'une présentation de largeur 3 de cette même application est donnée par les triplets $\mathbf{a}' = (2, 4, 4)$ et $\mathbf{b}' = (0, 1, 3)$. Cette deuxième présentation est d'ailleurs de forme réduite puisque le plus grand commun diviseur des éléments du triplet $\mathbf{a}'$ est 2 qui est premier à $d' = 3$.

3. Endomorphismes continus de l'algèbre des suites bi-infinies

Dans cette section, le terme anneau est utilisé pour « anneau commutatif unifère ». On réserve le nom de morphisme d'anneaux pour les morphismes envoyant l'élément unité de la source sur l'élément unité de la cible. Nous commençons par décrire la structure de l'ensemble de toutes les suites indexées par l'ensemble $\mathbb{Z}$ des entiers rationnels.

3.1. L'algèbre des suites bi-infinies. Soit A un anneau. On identifie le produit $A^{\mathbb{Z}}$ à l'ensemble de toutes les applications de $\mathbb{Z}$ dans A : une telle application est appelée une *suite bi-infinie sur* A. On note T_A l'application *décalage* de $A^{\mathbb{Z}}$ dans $A^{\mathbb{Z}}$ telle que

$$\forall\, u \in A^{\mathbb{Z}}, \forall\, m \in \mathbb{Z}\,, \qquad T_A(u)(m) = u(m+1)\,.$$

Notation. On note $S_{\mathbb{Z}}(A)$ l'anneau produit $A^{\mathbb{Z}}$, muni de l'automorphisme T_A.

La loi multiplicative de l'anneau $S_{\mathbb{Z}}(A)$ est donc celle du produit d'anneaux, c'est-à-dire la multiplication terme à terme, analogue au produit de Hadamard des suites [4]. Son élément unité est la suite bi-infinie dont tous les termes sont égaux à l'unité de A. L'anneau $S_{\mathbb{Z}}(A)$ est, en tant qu'anneau produit, muni naturellement des morphismes d'anneaux $\kappa_{m,A} : S_{\mathbb{Z}}(A) \to A$ définis pour tout entier $m \in \mathbb{Z}$ par

$$\forall\, u \in S_{\mathbb{Z}}(A), \qquad \kappa_{m,A}(u) = u(m)\,.$$

La proposition suivante énonce une propriété universelle de l'anneau $S_{\mathbb{Z}}(A)$.

Proposition 3.1. *Soit R un anneau et τ un automorphisme de R. Pour tout morphisme d'anneaux $\psi : R \to A$, il existe un unique morphisme d'anneaux $\Psi : R \to S_{\mathbb{Z}}(A)$ tel que $T_A \circ \Psi = \Psi \circ \tau$ et $\kappa_{0,A} \circ \Psi = \psi$.*

En particulier, en prenant $R = A$ et $\tau = \mathrm{Id}_A$, on obtient l'existence et l'unicité d'un morphisme d'anneaux $\iota_A : A \to S_{\mathbb{Z}}(A)$ tel que $T_A \circ \iota_A = \iota_A$ et $\kappa_{0,A} \circ \iota_A = \mathrm{Id}_A$. Explicitement, on a pour tout $a \in A$ l'égalité $\iota_A(a) = (a)_{m\in\mathbb{Z}}$. Ceci permet de voir $S_{\mathbb{Z}}(A)$ comme une A-algèbre de morphisme structural ι_A.

Nous appellerons $S_{\mathbb{Z}}(A)$ l'*algèbre des suites bi-infinies sur* A. Cette algèbre sera munie de la topologie initiale définie par les applications $\kappa_{m,A} (m \in \mathbb{Z})$ de $S_{\mathbb{Z}}(A)$ dans A, l'anneau A étant supposé muni de la topologie discrète. Notons que cette topologie produit est compatible avec les opérations algébriques de $S_{\mathbb{Z}}(A)$ et fait de $S_{\mathbb{Z}}(A)$ un anneau topologique complet et métrisable [11, Theorem 8.3.9] [17, Théorème VII, 1 ; 1, p. 61]. Par ailleurs, puisque $\kappa_{m,A} \circ T_A = \kappa_{m+1,A}$, il est immédiat de vérifier que l'automorphisme décalage T_A est bicontinu.

3.2. Suites récurrentes linéaires. La notion de suites récurrentes linéaires indexées par $\mathbb{N}$ est connue [12], de manière analogue on va définir les suites récurrentes linéraires indexées par $\mathbb{Z}$. Pour cela, on commence par définir sur le A-module $S_{\mathbb{Z}}(A)$ une structure de $A[x]$-module en faisant agir x comme le décalage T_A.

Définition 3.2. Soit $u \in S_{\mathbb{Z}}(A)$, on appelle *annulateur* de u l'idéal de $A[x]$ dont les éléments sont les polynômes $P \in A[x]$ tels que $P(T_A)(u) = 0$.

Définition 3.3. Une suite bi-infinie u élément de $S_{\mathbb{Z}}(A)$ est dite *récurrente linéaire sur A* ou *reconnaissable sur A*, si son annulateur comprend un polynôme unitaire à coefficients dans A. L'ensemble des suites récurrentes linéaires éléments de $S_{\mathbb{Z}}(A)$ sera noté $r_{\mathbb{Z}}(A)$.

Par un raisonnement analogue au cas classique des suites indexées par $\mathbb{N}$ [5, proposition 5.1, p. 11], on peut caractériser les suites reconnaissables comme les éléments des sous-A-modules de $S_{\mathbb{Z}}(A)$ qui sont de type fini et stables par T_A.

Théorème 3.4 (Schützenberger)**.** *Soit A un anneau commutatif unifère. L'ensemble $r_{\mathbb{Z}}(A)$ des suites bi-infinies reconnaissables sur A est une sous-algèbre de l'algèbre des suites $S_{\mathbb{Z}}(A)$, qui est stable par l'automorphisme décalage T_A.*

Démonstration. Identique à [5, pp. 14–15] qui traite le cas de suites indexées par un monoïde libre sur un alphabet. □

Nous appelons cette sous-algèbre $r_{\mathbb{Z}}(A)$ l'*algèbre des suites bi-infinies reconnaissables sur A*.

Proposition 3.5. *Pour tout anneau A, la sous-algèbre $r_{\mathbb{Z}}(A)$ des suites bi-infinies reconnaissables sur A est dense dans l'algèbre $S_{\mathbb{Z}}(A)$ des suites bi-infinies sur A.*

Démonstration. Soit u élément de $S_{\mathbb{Z}}(A)$. Pour tout voisinage V de u dans $S_{\mathbb{Z}}(A)$, il existe une partie finie non vide F de $\mathbb{Z}$ telle que

$$\forall\, v \in S_{\mathbb{Z}}(A), \qquad (\forall\, m \in F, u(m) = v(m)) \Rightarrow v \in V\ .$$

Soit alors l'entier naturel $T = \max F - \min F + 1 \geq 1$. Il existe une suite périodique $v = (v(m))_{m\in\mathbb{Z}}$ de période T telle que $u(m) = v(m)$ pour tout entier $m \in [\min F, \max F]$, donc en particulier pour tout $m \in F$, de sorte que $v \in V$. Puisque l'annulateur de v contient alors le polynôme unitaire $x^T - 1$, le résultat s'ensuit. □

Remarque 3.6. Cette preuve montre en fait un énoncé plus fort : l'ensemble des suites bi-infinies périodiques est dense dans $S_{\mathbb{Z}}(A)$.

Lorsque l'anneau A est un corps $\mathbb{K}$ algébriquement clos de caractéristique nulle, les éléments de $r_{\mathbb{Z}}(\mathbb{K})$ ont la même description que dans le cas classique des suites indexées par $\mathbb{N}$.

Proposition 3.7. *Soit $\mathbb{K}$ un corps algébriquement clos de caractéristique nulle et u une suite élément de $S_{\mathbb{Z}}(\mathbb{K})$. Les assertions suivantes sont équivalentes :*

(1) *la suite bi-infinie u est récurrente linéaire ;*

(2) *il existe un entier naturel d, d éléments $\alpha_1, \dots, \alpha_d$ non nuls de $\mathbb{K}$, et d polynômes $p_1, \dots, p_d$ à coefficients dans $\mathbb{K}$, tels que*

$$\forall\, m \in \mathbb{Z}, \qquad u(m) = \sum_{i=1}^{d} p_i(m)\alpha_i^m. \tag{3.1}$$

Démonstration. Complètement identique à la démonstration usuelle [12, pp. 3–4]. □

3.3. Constructions préservant la reconnaissabilité.

Lemme 3.8. *Soit u une suite bi-infinie reconnaissable sur un anneau A. Alors, pour tout entier $b \in \mathbb{Z}$, la suite bi-infinie $T_A^b u = (u(m+b))_{m\in\mathbb{Z}}$ est reconnaissable.*

Démonstration. Comme T_A est bijective, les deux suites u et $T_A^b u$ ont le même annulateur. □

Lemme 3.9. *Soit A un anneau intègre et $u \in r_{\mathbb{Z}}(A)$. S'il existe un entier naturel N tel que pour tout $n \geq N, u(n) = 0$, alors $u = 0$.*

Démonstration. Raisonnons par l'absurde ; supposons $u \neq 0$; alors l'ensemble $\{n \in \mathbb{Z}, u(n) \neq 0\}$ est non vide et majoré par N. Donc il existe un plus grand élément n_0 tel que $u(n_0) \neq 0$ et un élément unitaire $X^h + q_1X^{h-1} + \cdots + q_h$ de degré minimal h dans l'annulateur de u. On a $u(n_0 + h) + q_1u(n_0 + h - 1) + \cdots + q_hu(n_0) = 0$, c'est-à-dire $q_hu(n_0) = 0$ par définition de n_0. Or $q_h \neq 0$ par minimalité du degré h. Comme $u(n_0) \neq 0$, on a une contradiction avec l'hypothèse d'intégrité de l'anneau A. □

Lemme 3.10. *Soit $u = (u(m))_{m\in\mathbb{Z}}$ une suite bi-infinie reconnaissable sur un anneau complètement intégralement clos A* [6, p. 16]*. Alors la suite bi-infinie $\widehat{u} = (u(-m))_{m\in\mathbb{Z}}$ est reconnaissable.*

Démonstration. Soit K le corps des fractions de l'anneau intègre A. Un polynôme $P \in K[x]$ de degré $d \in \mathbb{N}$ est élément de l'annulateur de la suite bi-infinie $\widehat{u}$ si et seulement si son polynôme réciproque $x^dP(x^{-1})$ est élément de l'annulateur de u. Si donc $P(x)$ est un polynôme unitaire de $A[x]$ de degré minimal d dans l'annulateur de u, on a $P(0) \neq 0$ par minimalité du degré d, et le polynôme $P(0)^{-1}x^dP(x^{-1})$ est un polynôme unitaire de

$K[x]$ élément de l'annulateur de la suite $\widehat{u}$. Il en résulte que $\widehat{u}$ appartient à l'algèbre $r_{\mathbb{Z}}(K)$.

Soit par ailleurs $Q(x)$ un polynôme unitaire de $K[x]$ vérifiant

$$\forall\, m \in \mathbb{N}, \qquad Q(T_A)(\widehat{u})(m) = 0\ .$$

Comme $\widehat{u}$ est élément de l'algèbre $r_{\mathbb{Z}}(K)$, le lemme 3.9 entraîne alors que $Q(T_A)(\widehat{u}) = 0$. Ainsi un polynôme unitaire $\widehat{P}(x) \in K[x]$ de degré minimal dans l'annulateur de $\widehat{u}$ est aussi un polynôme unitaire de $K[x]$ de degré minimal tel que $\widehat{P}(T_A)(\widehat{u})(m) = 0$ pour tout entier $m \in \mathbb{N}$. On sait par un théorème de Chabert [8] que l'anneau complètement intégralement clos A est un anneau de Fatou au sens de Benzaghou ; comme la suite $\left(\widehat{u}(m)\right)_{m\in\mathbb{N}}$ prend ses valeurs dans A, on en déduit que le polynôme unitaire $\widehat{P}(x)$ est élément de $A[x]$. Comme il est élément de l'annulateur de $\widehat{u}$, on conclut que la suite $\widehat{u}$ est élément de $r_{\mathbb{Z}}(A)$. □

Définition 3.11. Soit un entier naturel $d \geq 1$. On appelle :

- *d-décimation* l'application ϑ_d de $S_{\mathbb{Z}}(A)$ dans $S_{\mathbb{Z}}(A)$ qui à la suite bi-infinie $u = \left(u(m)\right)_{m\in\mathbb{Z}}$ associe la suite bi-infinie $\vartheta_d(u) = \left(u(dm)\right)_{m\in\mathbb{Z}}$;
- *d-emboîtement* l'application E_d de $S_{\mathbb{Z}}(A)^d$ dans $S_{\mathbb{Z}}(A)$, telle que, pour tout d-uplet $\mathbf{u} = (u_j)_{0\leq j<d}$ de suites bi-infinies sur A, on a :

$$\forall\, m \in \mathbb{Z}, \qquad E_d(\mathbf{u})(m) = u_{d\{\frac{m}{d}\}}\left(\left\lfloor \frac{m}{d} \right\rfloor\right).$$

Remarque 3.12. On vérifie immédiatement que $T_A \circ \vartheta_d = \vartheta_d \circ T_A^d$. D'autre part, si $\mathbf{u} = (u_j)_{0\leq j<d}$ est élément de $S_{\mathbb{Z}}(A)^d$, alors il est facile de vérifier que $(T_A \circ E_d)(\mathbf{u}) = E_d(u_1, \ldots, u_{d-1}, T_A u_0)$, d'où résulte aussi que $T_A^d \circ E_d = E_d \circ T_A^{\times d}$, où $T_A^{\times d}$ est l'application de $S_{\mathbb{Z}}(A)^d$ dans lui-même telle que

$$\forall\, \mathbf{u} = (u_j)_{0\leq j<d} \in S_{\mathbb{Z}}(A)^d, \qquad T_A^{\times d}(\mathbf{u}) = (T_A u_j)_{0\leq j<d}\,.$$

Lemme 3.13. *Soit $d \geq 1$ un entier naturel. Si u est une suite bi-infinie reconnaissable sur un anneau A, alors sa d-décimée $\vartheta_d(u)$ est reconnaissable sur A. Si $u_0, \ldots, u_{d-1}$ sont des suites bi-infinies reconnaissables sur A, alors leur d-emboîtement $E_d(u_0, \ldots, u_{d-1})$ est une suite reconnaissable sur A.*

Démonstration. Compte tenu de la remarque 3.12, elle est identique à celle de [3] qui traite le cas des suites indexées par $\mathbb{N}$. □

Proposition 3.14. *Soit φ une application quasi-affine de $\mathbb{Z}$ dans $\mathbb{Z}$, A un anneau complètement intégralement clos, et u une suite bi-infinie reconnaissable sur A. Alors la suite bi-infinie $u \circ \varphi$ est reconnaissable.*

Démonstration. Soit une présentation $(d, \mathbf{a} = (a_r)_{0\le r<d}, \mathbf{b} = (b_r)_{0\le r<d})$ de l'application quasi-affine φ. La suite bi-infinie $u \circ \varphi$ est alors le d-emboîtement des d suites u_r, où $r \in [0..d[$, définies par $u_r(m) = u(a_r m + b_r)$. Par les lemmes 3.8, 3.10 et 3.13, chaque suite u_r est reconnaissable, donc aussi leur emboîtement $u \circ \varphi$. $\square$

3.4. Endomorphismes continus d'algèbres de suites bi-infinies. Si l'anneau A est intègre, les endomorphismes continus de l'algèbre $S_{\mathbb{Z}}(A)$ des suites bi-infinies ont été caractérisés dans [3], où se trouve démontré l'énoncé suivant.

Proposition 3.15. *Soit A un anneau intègre. Le monoïde* $\mathrm{End}^c(S_{\mathbb{Z}}(A))$ *des endomorphismes continus de l'algèbre $S_{\mathbb{Z}}(A)$ est isomorphe à l'opposé du monoïde $\mathbb{Z}^{\mathbb{Z}}$ de toutes les applications de $\mathbb{Z}$* dans $\mathbb{Z}$ *quand on associe à $\varphi \in \mathbb{Z}^{\mathbb{Z}}$ l'endomorphisme $u \mapsto u \circ \varphi$ de $S_{\mathbb{Z}}(A)$.*

On s'intéresse maintenant aux endomorphismes continus de la sous-algèbre $r_{\mathbb{Z}}(A)$ lorsque A est un anneau de caractéristique nulle : dans ce cas, on identifie $\mathbb{Z}$ au sous-anneau de A engendré par l'élément unité de A et on note η_A le plongement de $\mathbb{Z}$ dans A tel que $\eta_A(m) = m$ pour tout m dans $\mathbb{Z}$. Alors la suite η_A est élément de $r_{\mathbb{Z}}(A)$, puisque le polynôme unitaire $(x-1)^2$ appartient à son annulateur.

Proposition 3.16. *Soit A un anneau intègre de caractéristique nulle. L'application $f \longmapsto \varphi$ déterminée par la relation $f(\eta_A) = \eta_A \circ \varphi$ est un antimorphisme injectif du monoïde* $\mathrm{End}^c(r_{\mathbb{Z}}(A))$ *de tous les endomorphismes continus de la A-algèbre $r_{\mathbb{Z}}(A)$ dans le monoïde des applications de $\mathbb{Z}$ dans $\mathbb{Z}$. Son image est précisement l'ensemble des applications $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ vérifiant la condition :*

$$\forall\, u \in r_{\mathbb{Z}}(A), \qquad u \circ \varphi \in r_{\mathbb{Z}}(A)\,. \tag{3.2}$$

Démonstration. Puisque $r_{\mathbb{Z}}(A)$ est dense dans $S_{\mathbb{Z}}(A)$ par la proposition 3.5, tout endomorphisme continu de $r_{\mathbb{Z}}(A)$ se prolonge en un unique endomorphisme continu de $S_{\mathbb{Z}}(A)$ en vertu du théorème de prolongement des applications uniformément continues [17, Théorème XI, 3 ; 1, p. 132]. Par la proposition 3.15, on en déduit que tout endomorphisme continu f de $r_{\mathbb{Z}}(A)$ est de la forme $f = f_\varphi$ où pour toute application $\varphi : \mathbb{Z} \to \mathbb{Z},\ f_\varphi(u) = u \circ \varphi$. Puisque l'image de f est contenue dans $r_{\mathbb{Z}}(A)$, il est patent que l'application φ satisfait la condition (3.2). Il est simple de vérifier que, réciproquement, si φ vérifie la condition (3.2), alors l'application $f_\varphi : S_{\mathbb{Z}}(A) \to S_{\mathbb{Z}}(A)$ induit un endomorphisme continu de l'algèbre $r_{\mathbb{Z}}(A)$. En particulier, on doit avoir $f(\eta_A) = \eta_A \circ \varphi$, ce qui, puisque η_A est injective, détermine une unique application $\varphi : \mathbb{Z} \to \mathbb{Z}$. Enfin, la relation évidente $f_{\varphi_1 \circ \varphi_2} = f_{\varphi_2} \circ f_{\varphi_1}$ entraîne que l'application $f \mapsto \varphi$ est un antimorphisme. $\square$

3.5. Quelques lemmes.

Lemme 3.17. *Pour tout corps commutatif K et pour toute K-algèbre commutative L, on a $r_{\mathbb{Z}}(L) \cap S_{\mathbb{Z}}(K) = r_{\mathbb{Z}}(K)$.*

Démonstration. Identique au cas des suites indexées par $\mathbb{N}$, traité dans [3, Lemme 2.4]. □

Lemme 3.18. *Soit $\mathbb{K}$ une $\mathbb{Q}$-algèbre commutative complètement intégralement close, et φ une application de $\mathbb{Z}$ dans $\mathbb{Z}$. Si pour toute suite $u \in r_{\mathbb{Z}}(\mathbb{K})$, $u \circ \varphi$ est un élément de $r_{\mathbb{Z}}(\mathbb{K})$, alors l'ensemble $\left\{\frac{\varphi(m)}{m}, m \in \mathbb{Z} \setminus \{0\}\right\}$ est une partie bornée de $\mathbb{Q}$.*

Démonstration. Considérons les deux suites géométriques bi-infinies $g_{2,\epsilon} \in r_{\mathbb{Z}}(\mathbb{K})$ telle que $g_{2,\epsilon}(m) = 2^{\epsilon m}$ pour tout entier $m \in \mathbb{Z}$ et pour $\epsilon \in \{-1, 1\}$. Par hypothèse, les suites $g_{2,\epsilon} \circ \varphi$ sont toutes deux reconnaissables sur $\mathbb{K}$, donc reconnaissables sur $\mathbb{Q}$ par le lemme 3.17, donc aussi reconnaissables sur $\mathbb{C}$. Puisque de plus elles sont évidemment non nulles, on voit par la proposition 3.7 que, pour tout $\epsilon \in \{-1, 1\}$, il existe un entier $d_\epsilon > 0$, une suite $(p_{i,\epsilon})_{1 \le i \le d_\epsilon}$ de polynômes à coefficients dans $\mathbb{C}$, et une suite $(\alpha_{i,\epsilon})_{1 \le i \le d_\epsilon}$ d'éléments de $\mathbb{C}$ tels que :

$$\forall\, m \in \mathbb{Z}, \qquad 2^{\epsilon\varphi(m)} = \sum_{i=1}^{d_\epsilon} p_{i,\epsilon}(m)\alpha_{i,\epsilon}^m\,.$$

Posant $c_1 = \max\left(\max_{1 \le i \le d_1} |\alpha_{i,1}|, \max_{1 \le i \le d_{-1}} |\alpha_{i,-1}|\right)$, on en déduit pour tout entier $n \in \mathbb{N}^*$ et pour tout $\epsilon \in \{-1, 1\}$ l'inégalité $2^{\epsilon\varphi(n)} \le c_1^n \sum_{i=1}^{d_\epsilon} |p_{i,\epsilon}(n)|$. En prenant le logarithme en base 2 , on en tire

$$\forall\, n \ge 1, \qquad \epsilon\frac{\varphi(n)}{n} \le \log_2 c_1 + \frac{\log_2(\sum_{i=1}^{d_\epsilon} \mid p_{i,\epsilon}(n) \mid)}{n}\,.$$

Comme les deux suites $\left(\frac{\log_2(\sum_{i=1}^{d_\epsilon} |p_{i,\epsilon}(n)|)}{n}\right)_{n \ge 1}$, où $\epsilon \in \{-1, 1\}$, convergent vers 0 quand n tend vers l'infini, elle sont bornées. On en déduit que les deux suites $\left(\epsilon\frac{\varphi(n)}{n}\right)_{n \ge 1}$, où $\epsilon \in \{-1, +1\}$, sont majorées, c'est-à-dire que l'ensemble des valeurs prises par la suite $(\frac{\varphi(n)}{n})_{n \ge 1}$ est borné.

D'autre part, soit $\widehat{\varphi}$ l'application de $\mathbb{Z}$ dans $\mathbb{Z}$ telle que $\widehat{\varphi}(m) = \varphi(-m)$ pour tout entier $m \in \mathbb{Z}$. Si $u \circ \varphi$ est reconnaissable sur $\mathbb{K}$, il résulte du lemme 3.10 que $u \circ \widehat{\varphi}$ l'est aussi. Donc $\widehat{\varphi}$ satisfait la même hypothèse que φ, et donc l'ensemble des valeurs prises par la suite $\left(\frac{\varphi(-n)}{n}\right)_{n \ge 1}$ est borné, ce qui achève la démonstration. □

3.6. Caractérisation des endomorphismes continus de l'algèbre des suites bi-infinies reconnaissables sur une $\mathbb{Q}$-algèbre. Nous allons déterminer complètement les endomorphismes continus de l'algèbre $r_{\mathbb{Z}}(A)$ dans le cas où $A = \mathbb{K}$ est une $\mathbb{Q}$-algèbre commutative complètement intégralement close en montrant qu'il n'y a pas d'autre endomorphisme continu que les applications $u \mapsto u \circ \varphi$, où $\varphi : \mathbb{Z} \to \mathbb{Z}$ est une application quasi-affine. D'après les propositions 3.14 et 3.16, on sait en effet déjà que ces applications sont des endomorphismes continus de l'algèbre $r_{\mathbb{Z}}(\mathbb{K})$, et tout revient à montrer que toute application $\varphi : \mathbb{Z} \to \mathbb{Z}$ satisfaisant la condition (3.2) est quasi-affine.

Théorème 3.19. *Soit $\mathbb{K}$ une $\mathbb{Q}$-algèbre commutative complètement intégralement close, et f une application de $r_{\mathbb{Z}}(\mathbb{K})$ dans $r_{\mathbb{Z}}(\mathbb{K})$. Les assertions suivantes sont équivalentes :*

(1) *l'application f est un endomorphisme continu de $r_{\mathbb{Z}}(\mathbb{K})$;*
(2) *il existe une application quasi-affine φ de $\mathbb{Z}$ dans $\mathbb{Z}$ telle que, pour tout u dans $r_{\mathbb{Z}}(\mathbb{K})$, on ait $f(u) = u \circ \varphi$.*

Démonstration. Il ne reste à démontrer que l'implication (1) $\Rightarrow$ (2). Soit donc f un endomorphisme continu de l'algèbre $r_{\mathbb{Z}}(\mathbb{K})$. En vertu de la proposition 3.16, il existe une application φ de $\mathbb{Z}$ dans $\mathbb{Z}$ satisfaisant la condition (3.2) telle que, pour tout $u \in r_{\mathbb{Z}}(\mathbb{K})$, on ait $f(u) = u \circ \varphi$. En particulier, pour le plongement d'anneaux $\eta_{\mathbb{K}} : \mathbb{Z} \to \mathbb{K}$, on voit que $f(\eta_{\mathbb{K}}) = \eta_{\mathbb{K}} \circ \varphi = (\varphi(m))_{m\in\mathbb{Z}}$ est une suite bi-infinie reconnaissable sur $\mathbb{K}$. D'après le lemme 3.17, la suite $(\varphi(m))_{m\in\mathbb{Z}}$ d'entiers rationnels, étant reconnaissable sur $\mathbb{K}$, l'est aussi sur $\mathbb{Q}$, et donc sur la clôture algébrique $\mathbb{Q}^{\mathrm{alg}}$ de $\mathbb{Q}$ dans $\mathbb{C}$. À partir de la proposition 3.7, il existe un entier $d \in \mathbb{N}$, une suite $(\alpha_j)_{1\le j\le d}$ de nombres complexes algébriques non nuls, et une suite $(p_j)_{1\le j\le d}$ de polynômes à coefficients algébriques, tels que

$$\forall\, m \in \mathbb{Z}, \qquad \varphi(m) = \sum_{j=1}^{d} p_j(m)\alpha_j^m \,.$$

Sans restreindre la généralité, on peut supposer que $\alpha_i \neq \alpha_j$ pour $i \neq j$.

La suite $(\varphi(n))_{n\in\mathbb{N}}$ est une suite d'entiers rationnels telle que $\left(\frac{\varphi(n)}{n}\right)_{n\ge 1}$ est bornée et s'exprime sous la forme

$$\forall\, n \in \mathbb{N}, \qquad \varphi(n) = \sum_{j=1}^{d} p_j(n)\alpha_j^n \,.$$

La démonstration de [3, pp. 18–19] s'applique sans modification, et montre que tous les nombres α_j sont des racines de l'unité, et que tous les polynômes p_j sont de degré au plus un.

Soit ξ une racine de l'unité dans $\mathbb{Q}^{\text{alg}}$ d'ordre égal au plus petit commun multiple N des ordres des racines α_j, $1 \leq j \leq d$. Pour tout $j \in [1..d]$, il existe un entier naturel k_j tel que $\alpha_j = \xi^{k_j}$. D'autre part, pour tout $j \in [1..d]$, il existe deux nombres algébriques A_j et B_j tels que $p_j(x) = A_j x + B_j$. On a alors, pour tout entier $m \in \mathbb{Z}$:

$$\varphi(m) = \sum_{j=1}^{d} (A_j m + B_j)\xi^{k_j m} .$$

On en déduit que $(x^N - 1)^2$ est un polynôme annulateur de la suite reconnaissable φ. Par conséquent, la suite φ vérifie la récurrence $\varphi(m + 2N) - 2\varphi(m+N)+\varphi(m) = 0$ pour tout entier $m \in \mathbb{Z}$, elle est donc quasi-affine. $\square$

4. Bijections quasi-affines

4.1. Empreinte d'une présentation d'une application quasi-affine. Soit φ une application quasi-affine de présentation $(d, \mathbf{a}, \mathbf{b})$. On note N le plus petit commun multiple de tous les termes non nuls de la suite $\mathbf{a}$ s'il en existe, et $N = 0$ si au contraire tous les termes de la suite $\mathbf{a}$ sont nuls. Pour tout entier naturel r tel que $r < d$, on pose

$$c_r = \begin{cases} \frac{N}{|a_r|} & \text{si} \quad a_r \neq 0 \\ 0 & \text{si} \quad a_r = 0 \end{cases} \tag{4.1}$$

Soit, pour tout entier naturel r tel que $r < d$, l'application $\overline{\varphi}_r$ de $\mathbb{Z}$ dans le quotient $\mathbb{Z}/N\mathbb{Z}$ définie par

$$\forall\, m \in \mathbb{Z}, \qquad \overline{\varphi}_r(m) = \varphi(md + r) + N\mathbb{Z} = a_r m + b_r + N\mathbb{Z} .$$

On remarque que, si m et n sont deux entiers congrus modulo c_r, alors $\overline{\varphi}_r(m) = \overline{\varphi}_r(n)$. Il en résulte qu'il existe une unique application f_r de $\mathbb{Z}/c_r\mathbb{Z}$ dans $\mathbb{Z}/N\mathbb{Z}$ telle que

$$f_r(m + c_r\mathbb{Z}) = \overline{\varphi}_r(m) .$$

Définition 4.1. On appelle *empreinte* de la présentation $(d, \mathbf{a}, \mathbf{b})$ de l'application quasi-affine φ l'application

$$f : \prod_{r=0}^{d-1} \frac{\mathbb{Z}}{c_r\mathbb{Z}} \to \frac{\mathbb{Z}}{N\mathbb{Z}}$$

canoniquement associée à la suite $(f_r)_{0 \leq r < d}$.

Proposition 4.2. *Une application quasi-affine est injective si et seulement si l'empreinte d'une quelconque de ses présentations est injective.*

Démonstration. Soit φ une application quasi-affine, et f l'empreinte d'une des présentations $(d, \mathbf{a}, \mathbf{b})$ de φ. Pour tout entier naturel r tel que $r < d$, on note φ_r l'application de $\mathbb{Z}$ dans $\mathbb{Z}$ définie par $\varphi_r(m) = \varphi(md+r) = a_r m + b_r$ pour tout entier $m \in \mathbb{Z}$. On remarque que l'application φ est injective si et seulement si les images $\varphi_r(\mathbb{Z})$ sont deux à deux disjointes et toutes les applications φ_r sont injectives. De même, l'application f est injective si et seulement si les images $f_r\left(\frac{\mathbb{Z}}{c_r\mathbb{Z}}\right)$ sont deux à deux disjointes et toutes les applications f_r sont injectives.

Supposons que l'application quasi-affine φ est injective. Chacune des applications φ_r est alors injective, donc chaque terme de la suite $\mathbf{a}$ est non nul. Soit un entier naturel $r < d$ et deux entiers m et n tels que $f_r(m+c_r\mathbb{Z}) = f_r(n+c_r\mathbb{Z})$, c'est-à-dire tels que $a_rm+b_r \equiv a_rn+b_r \bmod N$. Puisque $a_r \neq 0$, on peut diviser cette congruence par a_r, ce qui conduit à l'égalité $m + c_r\mathbb{Z} = n + c_r\mathbb{Z}$, de sorte que l'application f_r est injective. Supposons maintenant l'existence de deux entiers naturels $r \neq s$ plus petits que d tels que les images de f_r et de f_s ne soient pas disjointes. Alors il existe deux entiers m et n tels que $f_r(m + c_r\mathbb{Z}) = f_s(n + c_s\mathbb{Z})$, c'est-à-dire tels que $\varphi_r(m) \equiv \varphi_s(n) \bmod N$. Puisque $a_s \neq 0$, ceci entraîne l'existence d'un entier $k \in \mathbb{Z}$ tel que $\varphi_r(m) = \varphi_s(n) + a_sk$. Or $\varphi_s(n) + a_sk = a_sn + b_s + a_sk = \varphi_s(n + k)$, ce qui est exclu puisque l'application φ est injective. Cette contradiction montre que les images des applications f_r sont deux à deux disjointes, ce qui montre que l'empreinte f est injective.

Réciproquement, supposons f injective. On observe d'abord que ceci empêche que tous les termes de la suite $\mathbf{a}$ soient nuls. En effet, si on avait $a_r = 0$ pour tout entier naturel $r < d$, on aurait aussi $c_r = 0$ et $N = 0$, donc l'application f_r serait une application constante et injective de $\mathbb{Z}$ dans $\mathbb{Z}$, ce qui est absurde. Donc l'ensemble $\mathbb{Z}/N\mathbb{Z}$ est fini, et donc la source de l'application injective f doit également être finie, ce qui impose que tous les termes de la suite $\mathbf{a}$ sont non nuls. Donc toutes les applications φ_r sont injectives. D'autre part, s'il existait deux entiers m et n tels que $\varphi_r(m) = \varphi_s(n)$ pour deux indices $r \neq s$, on en déduirait $\overline{\varphi}_r(m) = \overline{\varphi}_s(n)$, ce qui impliquerait que les images $f_r\left(\frac{\mathbb{Z}}{c_r\mathbb{Z}}\right)$ et $f_s\left(\frac{\mathbb{Z}}{c_s\mathbb{Z}}\right)$ ne soient pas disjointes, ce qui est exclu si f est injective. On en conclut que φ est alors injective. $\square$

Proposition 4.3. *Si une application quasi-affine φ est surjective, alors l'empreinte d'une quelconque de ses présentations est surjective. Réciproquement, si l'empreinte d'une de ses présentations $(d, \mathbf{a}, \mathbf{b})$ est surjective, et si aucun des termes de $\mathbf{a}$ n'est nul, alors l'application φ est surjective.*

Démonstration. L'application φ est surjective si et seulement si la réunion des images $\varphi_r(\mathbb{Z})$ pour $r \in [0..d[$ est égale à $\mathbb{Z}$, c'est-à-dire si et seulement si, pour tout entier $n \in \mathbb{Z}$, il existe un entier naturel $r < d$ et un entier $m \in \mathbb{Z}$ tels que $n = a_rm+b_r$. De même l'empreinte f est surjective si et seulement si la réunion des images $f_r\left(\frac{\mathbb{Z}}{c_r\mathbb{Z}}\right)$ pour $r \in [0..d[$ est égale à $\mathbb{Z}/N\mathbb{Z}$, donc si et seulement si, pour tout entier n dans $\mathbb{Z}$, il existe un entier naturel $r < d$ et un entier $m \in \mathbb{Z}$ tels que $n \equiv a_rm + b_r \bmod N$. Il est donc évident que la surjectivité de φ entraîne celle de f. D'autre part, si $a_r \neq 0$, on sait que

N est un multiple de a_r, donc la congruence $n \equiv a_r m + b_r \bmod N$ entraîne que $n = a_r m' + b_r$ pour un entier $m' \in \mathbb{Z}$, ce qui établit que, si tous les termes de la suite $\mathbf{a}$ sont non nuls, alors la surjectivité de f entraîne celle de φ. □

4.2. Caractérisation des bijections quasi-affines.

Proposition 4.4. *Une application quasi-affine de présentation* $(d, \mathbf{a}, \mathbf{b})$ *est bijective si et seulement si les deux conditions suivantes sont satisfaites :*

(1) *on a* $a_r \neq 0$ *pour tout* $r \in [0..d[$ *et* $\sum_{r=0}^{d-1} \frac{1}{|a_r|} = 1$.

(2) *pour tout couple* (r, s) *d'entiers naturels plus petits que* d*, et tel que* $r \neq s$*, le plus grand commun diviseur de* a_r *et* a_s *ne divise pas la différence* $b_s - b_r$.

Démonstration. Soit $(d, \mathbf{a}, \mathbf{b})$ une présentation de l'application quasi-affine φ, d'empreinte f.

Montrons d'abord la nécessité des conditions (1) et (2). On suppose que φ est bijective, il résulte des propositions 4.2 et 4.3 que f est bijective. Comme φ est injective, on voit que tous les entiers a_r sont non nuls. Comme f est bijective, le nombre d'éléments de la source de f est égal à N, de sorte que $N = \sum_{r=0}^{d-1} c_r$, relation équivalente à $\sum_{r=0}^{d-1} \frac{1}{|a_r|} = 1$. Soit (r, s) un couple d'entiers naturels plus petits que d tel que $r \neq s$. Puisque f est injective, les images $f_r\left(\frac{\mathbb{Z}}{c_r\mathbb{Z}}\right)$ et $f_s\left(\frac{\mathbb{Z}}{c_s\mathbb{Z}}\right)$ sont disjointes, ce qui signifie que, pour tout couple (m, n) d'entiers, on a $a_r m + b_r \not\equiv a_s n + b_s \bmod N$. Or on sait que l'ensemble des entiers $a_r m - a_s n$ est précisément l'ensemble des multiples du plus grand commun diviseur de a_r et a_s. Comme N est un multiple commun à a_r et à a_s, on en déduit que $b_s - b_r$ n'est pas divisible par le plus grand commun diviseur de a_r et a_s.

Réciproquement, supposons vérifiées les hypothèses (1) et (2). Montrons d'abord l'injectivité de f. Soit deux entiers naturels r et s plus petits que d, et $m + c_r\mathbb{Z} \in \mathbb{Z}/c_r\mathbb{Z}$ et $n + c_s\mathbb{Z} \in \mathbb{Z}/c_s\mathbb{Z}$ tels que $f(m + c_r\mathbb{Z}) = f(n + c_s\mathbb{Z})$. On a donc

$$a_r m + b_r \equiv a_s n + b_s \bmod N .$$

Si on avait $r \neq s$, cela entraînerait que le plus grand commun diviseur de a_r et a_s diviserait $b_s - b_r$, contrairement à l'hypothèse (2). Donc $s = r$, ce qui conduit par division par a_r à la congruence $m \equiv n \bmod c_r$, c'est-à-dire que $m + c_r\mathbb{Z} = n + c_s\mathbb{Z}$. Ainsi f est injective.

Comme la source et la cible de l'application f ont le même nombre d'éléments par l'hypothèse (1), on voit que f est bijective, ce qui implique que φ est une bijection en vertu des propositions 4.2 et 4.3. □

4.3. Réciproque d'une bijection quasi-affine. Nous allons montrer que la bijection réciproque d'une bijection quasi-affine est aussi quasi-affine et en expliciter une présentation.

Proposition 4.5. *Soit* $(d, \mathbf{a}, \mathbf{b})$ *une présentation d'une bijection quasi-affine* φ*. On considère le plus petit commun multiple* N *des termes de la suite* $\mathbf{a}$*, et, pour tout entier naturel* $r < d$*, on note* $c_r = \frac{N}{|a_r|}$.

Alors la bijection réciproque $\varphi^{\circ(-1)}$ *de* φ *est quasi-affine de présentation* $(N, \mathbf{a}', \mathbf{b}')$ *avec, pour tout entier naturel* $s < N$ *:*

$$a'_s = \frac{dN}{a_{v(s)}} \qquad \textit{et} \qquad b'_s = v(s) + d\,\frac{s - b_{v(s)}}{a_{v(s)}},$$

où $v(s) = d\left\{\frac{\varphi^{\circ(-1)}(s)}{d}\right\}$ *est l'unique entier naturel plus petit que* d *vérifiant la congruence* $s \equiv b_{v(s)} \bmod a_{v(s)}$.

Démonstration. Soit m un entier, $n = \varphi^{\circ(-1)}(m)$, et $v(m) = d\left\{\frac{n}{d}\right\}$. Alors, d'après la proposition 2.3, on a $\varphi\left(n \pm d\frac{N}{a_{v(m)}}\right) = m \pm N$, ce qui est équivalent à $\varphi^{\circ(-1)}(m \pm N) = n \pm d\frac{N}{a_{v(m)}}$. Il en résulte que l'application réciproque $\varphi^{\circ(-1)}$ est quasi-affine de largeur N.

Une présentation de $\varphi^{\circ(-1)}$ est donc $(N, \mathbf{a}', \mathbf{b}')$ où les suites $\mathbf{a}'$ et $\mathbf{b}'$ se calculent au moyen des formules

$$\forall\, s \in [0..N[, \qquad a'_s = \varphi^{\circ(-1)}(s+N) - \varphi^{\circ(-1)}(s) \qquad \text{et} \qquad b'_s = \varphi^{\circ(-1)}(s)\ .$$

Comme on l'a vu, $\varphi^{\circ(-1)}(s + N) = \varphi^{\circ(-1)}(s) + \frac{dN}{a_{v(s)}}$, d'où on déduit $a'_s = \frac{dN}{a_{v(s)}}$.

On a d'autre part $\varphi(\varphi^{\circ(-1)}(s)) = s = a_{v(s)}\left\lfloor\frac{b'_s}{d}\right\rfloor + b_{v(s)}$, avec $\left\{\frac{b'_s}{d}\right\} = \frac{v(s)}{d}$, relations d'où l'on tire la valeur de $b'_s = d\left\lfloor\frac{b'_s}{d}\right\rfloor + d\left\{\frac{b'_s}{d}\right\}$. $\square$

À partir du théorème 2.9 et de la proposition 4.5, nous pouvons énoncer le résultat suivant :

Corollaire 4.6. *L'ensemble* QA^* *des applications quasi-affines bijectives est un groupe non abélien pour la composition.*

5. Caractérisation des rapports des bijections quasi-affines

Le problème que nous allons maintenant étudier est celui de caractériser les suites finies $\mathbf{a} \in \mathbb{Z}^d$ qui interviennent comme les rapports des présentations des bijections quasi-affines de largeur d. La proposition 4.4 nous fournit la condition nécessaire qu'aucun terme de la suite $\mathbf{a}$ ne soit nul et que $\sum_{r=0}^{d-1} \frac{1}{|a_r|} = 1$. Il est immédiat que cette condition n'est pas suffisante : si par exemple deux termes d'une suite $\mathbf{a} \in \mathbb{Z}^d$ sont premiers entre eux, alors quelque soit le choix de la suite $\mathbf{b} \in \mathbb{Z}^d$, la même proposition 4.4 montre que $(d, \mathbf{a}, \mathbf{b})$ ne pourra jamais être présentation d'une bijection quasi-affine.

5.1. Multiensembles. Soit $\mathbf{a}$ une suite élément de $\mathbb{Z}^d$. La première observation concernant la propriété de $\mathbf{a}$, d'être rapport dans une présentation d'une bijection quasi-affine de largeur d, est qu'elle ne dépend en fait que du multiensemble associé à la suite des valeurs absolues des éléments de la suite $\mathbf{a}$. Pour expliciter ce point, nous définissons un *multiensemble* fini (d'entiers naturels) [18, p. 25] comme une application « multiplicité » de $\mathbb{N}$ dans $\mathbb{N}$ nulle en dehors d'une partie finie ; on appelle *support* d'un tel multiensemble l'ensemble, nécessairement fini, des entiers naturels de multiplicité non nulle. À la suite finie $\mathbf{a} \in \mathbb{Z}^d$ nous associons le multiensemble $\alpha \mapsto n_\alpha$ tel que, pour tout $\alpha \in \mathbb{N}$, on a

$$n_\alpha = \operatorname{card}\{r \in [0..d[, |a_r| = \alpha\} \ . \tag{5.1}$$

On remarque que le cardinal $\sum_{\alpha\in\mathbb{N}} n_\alpha$ [18, p. 25] de ce multiensemble $\alpha \mapsto n_\alpha$ n'est autre que l'entier d.

Proposition 5.1. *Soit* $\mathbf{a}$ *et* $\mathbf{a}'$ *deux suites appartenant à* $\mathbb{Z}^d$ *associées à un même multiensemble* $\alpha \mapsto n_\alpha$*. Alors* $\mathbf{a}$ *est le rapport dans une présentation d'une bijection quasi-affine de largeur* d *si et seulement si* $\mathbf{a}'$ *l'est aussi.*

Démonstration. Les conditions caractéristiques de la proposition 4.4 sont clairement stables par toute permutation de l'ensemble $[0..d[$ des indices des suites $\mathbf{a}$ et $\mathbf{b}$. □

Dans le reste de cette section, nous conviendrons pour abréger d'appeler *multiensemble idoine* tout multiensemble $\alpha \mapsto n_\alpha$ d'entiers naturels qui est associé par la formule (5.1) au rapport d'une présentation d'une bijection quasi-affine. Dans la suite, nous étudions le problème suivant : comment déterminer si un multiensemble donné est idoine ?

5.2. Un problème de coloriage. On commence par réduire le problème à la construction d'une certaine application.

Proposition 5.2. *Soit* $n : \alpha \mapsto n_\alpha$ *un multiensemble fini d'entiers naturels de support* F*, avec* $0 \notin F$*, et* N *un multiple commun de tous les entiers appartenant à* F*. Pour que le multiensemble* n *soit idoine, il faut et il suffit qu'il existe une application* $\mathfrak{C} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}^*$ *telle que :*

(i) $\forall\, \alpha \in \mathbb{N}^*, \quad \operatorname{card}(\mathfrak{C}^{-1}(\alpha)) = n_\alpha \frac{N}{\alpha}$;
(ii) $\forall\, \overline{m} \in \mathbb{Z}/N\mathbb{Z}, \quad \mathfrak{C}(\overline{m} + \mathfrak{C}(\overline{m}) + N\mathbb{Z}) = \mathfrak{C}(\overline{m})$.

Démonstration. Si le multiensemble n est idoine, en notant d son cardinal, on sait qu'il existe une bijection quasi-affine φ de présentation $(d, \mathbf{a}, \mathbf{b})$ telle que, pour tout $\alpha \in \mathbb{N}$, l'entier n_α est donné par la formule (5.1). Soit $N_0 = \frac{N}{k}$ le plus petit commun multiple des éléments de F. Par les propositions 4.2 et 4.3, nous savons que l'empreinte f de la présentation $(d, \mathbf{a}, \mathbf{b})$ est une bijection de l'ensemble $\coprod_{r=0}^{d-1} \mathbb{Z}/c_r\mathbb{Z}$ sur $\mathbb{Z}/N_0\mathbb{Z}$, où on a posé $c_r = N_0/|a_r|$ pour tout entier $r \in [0..d[$. Nous considérons l'application ω, définie sur la réunion disjointe $\coprod_{r=0}^{d-1} \mathbb{Z}/c_r\mathbb{Z}$ et à valeurs dans $\mathbb{N}^*$, telle que $\omega(m + c_r\mathbb{Z}) = |a_r|$ pour tout $(m, r) \in \mathbb{Z} \times [0..d[$. Notons également ϖ le morphisme naturel de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{Z}/N_0\mathbb{Z}$. Soit alors l'application $\mathfrak{C} = \omega \circ f^{\circ(-1)} \circ \varpi$. Alors, pour tout entier naturel $\alpha \neq 0$, on a $\mathfrak{C}^{-1}(\alpha) = \varpi^{-1}(f(\omega^{-1}(\alpha)))$, de sorte que le nombre d'éléments de $\mathfrak{C}^{-1}(\alpha)$ est égal au produit de l'entier $k = N/N_0$ par le cardinal de $\omega^{-1}(\alpha) = \coprod_{|a_r|=\alpha} (\mathbb{Z}/c_r\mathbb{Z})$ qui est précisément $n_\alpha c_\alpha = n_\alpha \frac{N_0}{\alpha}$. D'autre part, soit $(\overline{m}, \alpha) \in (\mathbb{Z}/N\mathbb{Z}) \times \mathbb{N}^*$ tel que $\mathfrak{C}(\overline{m}) = \alpha$, c'est-à-dire tel qu'il existe un entier $r \in [0..d[$ vérifiant d'une part $|a_r| = \alpha$, de sorte que α est élément de F, et donc diviseur de N_0, et d'autre part $f^{\circ(-1)}(\varpi(\overline{m})) \in \mathbb{Z}/c_r\mathbb{Z}$. Par définition de l'empreinte f, on a $f\left(f^{\circ(-1)}(\varpi(\overline{m})) + \frac{a_r}{\alpha} + c_r\mathbb{Z}\right) = \varpi(\overline{m}) + \alpha + N_0\mathbb{Z}$, par où l'on voit que $f^{\circ(-1)}(\varpi(\overline{m}) + \alpha + N_0\mathbb{Z})$ est élément de $\omega^{-1}(\alpha)$. On a donc $\mathfrak{C}(\overline{m} + \alpha + N\mathbb{Z}) = \alpha$. L'application $\mathfrak{C} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}^*$ satisfait donc les conditions voulues.

Supposons réciproquement qu'il existe une application $\mathfrak{C} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}^*$ satisfaisant les conditions (i) et (ii). Si on note encore d le cardinal du multiensemble n, il existe une application $r \mapsto a_r$ de l'intervalle $[0..d[$ dans $\mathbb{Z}$ reliée par la formule (5.1) au multiensemble n. La condition (ii) nous montre que, pour tout $\alpha \in \mathbb{N}^*$, la partie $\mathfrak{C}^{-1}(\alpha)$ du groupe $\mathbb{Z}/N\mathbb{Z}$ est réunion d'orbites $\{\overline{m} + \ell\alpha + N\mathbb{Z}, \ell \in \mathbb{Z}\}$ sous l'action par translation du sous-groupe engendré par $\alpha + N\mathbb{Z}$. Soit B_α une partie de $\mathfrak{C}^{-1}(\alpha)$ telle que chacune de ces orbites contient exactement un élément de B_α. Compte tenu de la condition (i), on voit que B_α est de cardinal n_α, de sorte qu'il existe une bijection $r \mapsto b_r + N\mathbb{Z}$ entre l'ensemble des indices $r \in [0..d[$ tels que $|a_r| = \alpha$ et l'ensemble B_α. On définit ainsi un entier rationnel b_r pour tout entier naturel $r < d$. Soit maintenant deux entiers naturels $r \neq s$, avec $r < d$ et $s < d$. Si $|a_r| = |a_s| = \alpha$, on sait que b_r et b_s sont dans deux orbites différentes sous l'action par translation du sous-groupe engendré par $\alpha + N\mathbb{Z}$, et ceci montre que α ne divise pas $b_s - b_r$. Si par contre $|a_r| \neq |a_s|$, alors la fonction $\mathfrak{C}$ est constamment égale à $|a_r|$ (resp. à $|a_s|$) sur l'orbite O_r de b_r (resp. O_s de b_s) sous l'action par translation du sous-groupe engendré par $a_r + N\mathbb{Z}$ (resp. $a_s + N\mathbb{Z}$). Donc $O_r \cap O_s = \varnothing$, ce qui prouve que le plus grand commun diviseur de a_r et a_s ne peut diviser $b_s - b_r$. Dans tous les cas, l'hypothèse $r \neq s$ suffit à obtenir que le plus grand commun diviseur de a_r et a_s ne divise pas $b_s - b_r$. Par ailleurs, comme $\mathbb{Z}/N\mathbb{Z}$ est la réunion disjointe des $\mathfrak{C}^{-1}(\alpha)$ pour α décrivant F, on a

$$\sum_{r=0}^{d-1} \frac{1}{|a_r|} = \sum_{\alpha \in F} \frac{n_\alpha}{\alpha} = \frac{1}{N} \sum_{\alpha \in F} n_\alpha \frac{N}{\alpha} = \frac{\sum_{\alpha \in F} \operatorname{card}(\mathfrak{C}^{-1}(\alpha))}{N} = 1\ .$$

On en conclut que la présentation $(d, \mathbf{a}, \mathbf{b})$ satisfait les conditions (1) et (2) de la proposition 4.4, et est donc la présentation d'une bijection quasi-affine. $\square$

Cette proposition 5.2 nous apprend que, étant donné un multiple commun N des éléments du support d'un multiensemble $n : \alpha \mapsto n_\alpha$, avec $n_0 = 0$, le caractère idoine de n est équivalent à l'existence d'un coloriage des éléments du groupe $\mathbb{Z}/N\mathbb{Z}$, dont l'ensemble des couleurs est en bijection avec le support F de n, de telle sorte que l'ensemble des éléments de $\mathbb{Z}/N\mathbb{Z}$ qui sont de la couleur correspondant à l'élément $\alpha \in F$ a exactement $n_\alpha \frac{N}{\alpha}$ éléments, et est stable par la translation $\overline{m} \mapsto \overline{m} + \alpha + N\mathbb{Z}$; autrement dit, si on fait correspondre les éléments de $\mathbb{Z}/N\mathbb{Z}$ aux sommets d'un polygone régulier à N côtés, on doit obtenir un coloriage des sommets du polygone où l'ensemble des sommets de la couleur correspondant à α est réunion disjointe de n_α polygones réguliers à N/α côtés.

Remarquons d'ailleurs que l'entier N peut être choisi arbitrairement parmi tous les multiples communs des entiers éléments de F. On aurait donc pu imposer dans cet énoncé que N soit exactement le plus petit commun multiple. Cependant, il est souvent plus simple de vérifier l'existence d'un coloriage $\mathfrak{C} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}^*$ pour un multiple commun N qui n'est pas forcément le plus petit.

5.3. Une condition suffisante. Nous allons voir qu'un multiensemble d'entiers naturels non nuls est idoine dès qu'il y a unicité du pgcd de deux quelconques éléments de son support.

Proposition 5.3. *Soit $n : \alpha \mapsto n_\alpha$ un multiensemble fini d'entiers naturels de support F, avec $0 \notin F$ et $\sum_{\alpha \in F} \frac{n_\alpha}{\alpha} = 1$. On suppose qu'il existe un entier naturel D tel que $D = \operatorname{pgcd}(\alpha, \beta)$ pour tout couple (α, β) d'éléments distincts de F. Alors le multiensemble n est idoine.*

Démonstration. Soit N le plus petit commun multiple des éléments de F. Comme l'entier naturel D divise tous les éléments de F, pour tout $\alpha \in F$, il existe un entier naturel k_α tel que $\alpha = k_\alpha D$. Soit $\alpha \neq \beta$ deux éléments de F ; on remarque que, puisque D est le plus grand commun diviseur de α et de β, l'entier k_α est premier à l'entier k_β. En multipliant la relation $\sum_{\alpha \in F} \frac{n_\alpha}{\alpha} = 1$ par l'entier $D \prod_{\beta \in F} k_\beta$, on obtient

$$D \prod_{\beta \in F} k_\beta = \sum_{\alpha \in F} n_\alpha \prod_{\beta \in F \setminus \{\alpha\}} k_\beta \ ;$$

l'entier k_γ divisant évidemment les entiers $D \prod_{\beta \in F} k_\beta$ et $\prod_{\beta \in F \setminus \{\alpha\}} k_\beta$ pour $\alpha \neq \gamma$ doit aussi diviser l'entier $n_\gamma \prod_{\beta \in F \setminus \{\gamma\}} k_\beta$; puisqu'il est premier à tout k_β pour $\beta \neq \gamma$, on en conclut que pour tout $\gamma \in F, n_\gamma$ est multiple de k_γ, ce qui nous permet d'écrire l'entier D comme la somme d'entiers

$$D = \sum_{\alpha \in F} \frac{n_\alpha}{k_\alpha} \ .$$

De cette décomposition additive de l'entier D, on peut tirer l'existence d'une application $\mathfrak{C}' : \mathbb{Z}/D\mathbb{Z} \to F \subset \mathbb{N}^*$ telle que

$$\forall\, \alpha \in F, \qquad \text{card }\ \mathfrak{C}'^{-1}(\alpha) = \frac{n_\alpha}{k_\alpha} = \frac{n_\alpha D}{\alpha}.$$

On définit alors l'application $\mathfrak{C}$ de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{N}^*$ par $\mathfrak{C} = \mathfrak{C}' \circ \varpi$ où ϖ est la projection de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{Z}/D\mathbb{Z}$, de sorte que

$$\forall\, \alpha \in F, \qquad \text{card }\ \mathfrak{C}^{-1}(\alpha) = \frac{N}{D}\frac{n_\alpha D}{\alpha} = n_\alpha \frac{N}{\alpha}\ .$$

Pour tout $\overline{m} \in \mathbb{Z}/N\mathbb{Z}$, l'entier naturel $\mathfrak{C}(\overline{m})$ est un multiple de D, donc $\varpi(\overline{m} + \mathfrak{C}(\overline{m}) + N\mathbb{Z}) = \varpi(\overline{m})$, d'où $\mathfrak{C}(\overline{m} + \mathfrak{C}(\overline{m}) + N\mathbb{Z}) = \mathfrak{C}(\overline{m})$. D'après la proposition 5.2, on en déduit que le multiensemble n est idoine. $\square$

Corollaire 5.4. *Soit $n : \alpha \mapsto n_\alpha$ un multiensemble fini d'entiers naturels de support F, avec $0 \notin F$ et $\sum_{\alpha\in F} \frac{n_\alpha}{\alpha} = 1$. Si* $\operatorname{card} F \leq 2$*, alors le multiensemble n est idoine.*

5.4. Exemples. Nous illustrons les résultats de cette section en étudiant deux exemples particuliers.

Exemple 5.5. Considérons le cas du multiensemble n de support $F = \{4, 6, 8, 12, 24\}$ avec multiplicités respectives $n_4 = 1, n_6 = 2, n_8 = 1, n_{12} = 3$ et $n_{24} = 1$. Montrons que ce multiensemble n n'est pas idoine : soit en effet un coloriage de l'ensemble des sommets d'un tétraicosagone régulier en cinq couleurs, disons bleu, rouge, noir, vert et jaune, tel que les sommets bleus forment un hexagone régulier, les sommets rouges deux carrés, les sommets noirs un triangle équilatéral, les sommets verts trois diamètres, avec un unique sommet colorié en jaune. Alors les sommets de couleur bleue, rouge ou verte recouvrent dix diamètres, et ainsi ne laissent que deux diamètres pour les sommets coloriés en noir ou en jaune (voir Figure 5.1). Or il est clairement impossible de former un triangle équilatéral constitué de trois des quatre sommets de ces deux diamètres. Par conséquent, un tel coloriage ne peut exister, et donc la proposition 5.2 montre que le multiensemble n n'est pas idoine. Ainsi il ne peut exister de bijection quasi-affine de rapport $(4, 6, 6, 8, 12, 12, 12, 24)$.

Exemple 5.6. Considérons un multiensemble n de support $\{4, 6, 12\}$ tel que $\frac{n_4}{4} + \frac{n_6}{6} + \frac{n_{12}}{12} = 1$. On va montrer qu'une condition nécessaire et suffisante pour que n soit idoine est que $n_{12} \neq 1$.

En effet, si $n_{12} \neq 1$, la multiplicité n_{12} peut se mettre sous la forme $n_{12} = 2a + 3b$, où a et b sont éléments de $\mathbb{N}$. On a donc $\frac{n_4+b}{4} + \frac{n_6+a}{6} = 1$, de sorte que le multiensemble n' de support $\{4, 6\}$ donné par les multiplicités $n'_4 = n_4 + b$ et $n'_6 = n_6 + a$ est idoine par le corollaire 5.4 : on peut donc colorier les 12 sommets d'un dodécagone régulier de sorte que les sommets bleus recouvrent $n_4 + b$ triangles équilatéraux et les sommets rouges $n_6 + a$

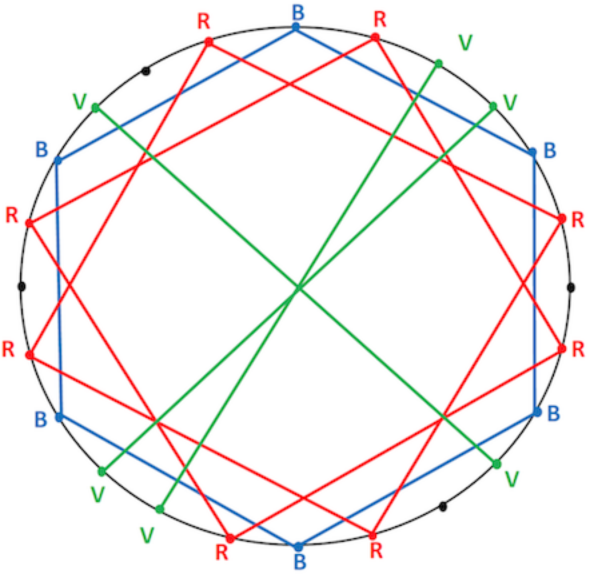

FIGURE 5.1.

diamètres. On prélève alors b triangles équilatéraux parmi les n_4+b bleus et a diamètres parmi les n_6+a rouges, et on colorie les sommets ainsi prélevés en vert : on obtient un coloriage des sommets du dodécagone en n_4 triangles équilatéraux bleus, n_6 diamètres rouges et $2a+3b=n_{12}$ sommets verts. L'existence de ce coloriage montre que le multiensemble n est idoine.

Réciproquement, si $n_{12}=1$, montrons par l'absurde que n ne peut être idoine. Si en effet on avait un coloriage en trois couleurs des sommets d'un dodécagone régulier tel que les sommets coloriés en bleu recouvrent n_4 triangles équilatéraux, ceux coloriés en rouge recouvrent n_6 diamètres et un seul sommet V est colorié en vert, alors le sommet V' diamétralement opposé au sommet vert est forcément bleu, alors que les sommets W_1 et W_2 formant avec ce sommet vert un triangle équilatéral sont forcément rouges. Or le sommet diamétralement opposé au sommet rouge W_2 forme avec le sommet bleu V' la base d'un triangle équilatéral, donc il serait à la fois bleu et rouge (voir Figure 5.2), ce qui est absurde.

Ainsi, il existe des bijections quasi-affines de largeur 6 et de rapport $(4,4,6,6,12,12)$, mais pas de bijection quasi-affine de largeur 5 et de rapport $(4,4,4,6,12)$.

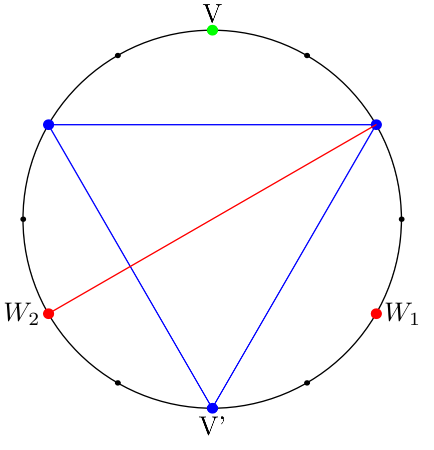

FIGURE 5.2.

Bibliographie

[1] A. AÏT-MOKHTAR, « Endomorphismes d'algèbres de suites », Thèse, Université de Limoges, France, 2008.

[2] ———, « Applications purement semi-affines et tressages », *C. R., Math., Acad. Sci. Paris* **348** (2010), nº 1-2, p. 1-4.

[3] A. AÏT-MOKHTAR, A. NECER & A. SALINIER, « Endomorphismes d'algèbres de suites », *J. Théor. Nombres Bordx.* **20** (2008), nº 1, p. 1-21.

[4] B. BENZAGHOU, « Algèbres de Hadamard », *Bull. Soc. Math. Fr.* **98** (1970), p. 209-252.

[5] J. BERSTEL & C. REUTENAUER, *Noncommutative rational series with applications*, Encyclopedia of Mathematics and Its Applications, vol. 137, Cambridge University Press, 2011, xiii+248 pages.

[6] N. BOURBAKI, *Eléments de mathématique. Algèbre Commutative. Chapitres 5 à 7*, Springer, 2006, 351 pages.

[7] A. CAYLEY, « Researches on the Partition of Numbers », *Philos. Trans. Roy. Soc. London* **146** (1856), p. 127-140.

[8] J.-L. CHABERT, « Anneaux de Fatou », *Enseign. Math.* **18** (1972), p. 141-144.

[9] L. COMTET, *Analyse combinatoire. Tome 1*, Le mathématicien, vol. 4, Presses Universitaires de France, 1970, 192 pages.

[10] E. EHRHART, *Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire*, International Series of Numerical Mathematics, vol. 35, Birkhäuser, 1977, 165 pages.

[11] R. ENGELKING, *General topology. A revised and enlarged translation*, Monografie Matematyczne., vol. 60, PWN-Polish Scientific Publishers, 1977, 626 pages.

[12] G. EVEREST, A. VAN DER POORTEN, I. SHPARLINSKI & T. WARD, *Recurrence Sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, 2003, xiii+318 pages.

[13] G. HANSEL, « Une démonstration simple du théorème de Skolem-Mahler-Lech », *Theor. Comput. Sci.* **43** (1986), nº 1, p. 91-98.

[14] R. G. LARSON & E. J. TAFT, « The algebraic structure of linearly recursive sequences under Hadamard product », *Isr. J. Math.* **72** (1990), nº 1-2, p. 118-132.

[15] I. NIVEN, « The asymptotic density of sequences », *Bull. Am. Math. Soc.* **57** (1951), nº 6, p. 420-434.

[16] G. PÓLYA, « Über ganzwertige ganze Funktionen », *Palermo Rend.* **40** (1915), p. 1-16.

[17] L. SCHWARTZ, *Analyse. 2e partie : Topologie générale et analyse fonctionnelle*, Collection Enseignement des Sciences, vol. 11, Hermann, 1970, 432 pages.

[18] R. P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, 1997, Corrected reprint of the 1986 hardback edition, xi+326 pages.

Razika Niboucha
Laboratoire ATN
Faculté de Mathématiques, USTHB
BP 82, Bab Ezzouar, Alger, Algérie
E-mail: rniboucha@usthb.dz

Alain Salinier
Pôle de Mathématiques et Informatique
Laboratoire XLIM (UMR CNRS 7252)
Université de Limoges,
123, avenue Albert Thomas, 87060 Limoges Cedex,France
E-mail: alain.salinier@unilim.fr