N° d'ordre : 16/2017-D/MT

République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifiques
Université des Sciences et de la Technologie Houari Boumediene
Faculté de Mathématiques

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

THESE

Présentée pour l'obtention du grade de DOCTORAT EN SCIENCES

En **: Mathématiques**

Spécialité **: Algèbre et Théorie des Nombres**

par : **NIBOUCHA Razika**

Thème

Composition d'applications quasi-polynomiales

Soutenue publiquement le 22/10/2017, devant le jury composé de :

M.BENZAGHOU Benali	**Pofesseur à l'USTHB**	**Président**
M. SALINIER Alain	**Professeur à l'université de Limoges**	**Directeur de thèse**
M. BETINA Kamel	**Professeur à l'USTHB**	**Co-directeur**
M. AIT-MOKHTAR Ahmed	**Maitre de conférence à l'ENS Kouba**	**Examinateur**
M. BAYAD Abdelmedjid	**Professeur à l'université d'Evry**	**Examinateur**
M.BELLAGH Abdelaziz	**Maitre de conférence à l' USTHB**	**Examinateur**

COMPOSITION D'APPLICATIONS QUASI-POLYNOMIALES

Razika NIBOUCHA

10 novembre 2017

Table des matières

Notations

A	Anneau commutatif unifère
$A[x]$	Algèbre des polynômes en la variable x
$A[x, x^{-1}]$	Algèbre des polynômes de Laurent
$\mathbf{a}$	Suite des rapports d'une application quasi-affine
$\widehat{\mathbf{a}}$	La suite $(a_{-m})_{m\in\mathbb{Z}}$, reflet de la suite $\mathbf{a}$
$\mathfrak{C}$	Application coloriage
$E_d(u_0, \ldots, u_{d-1})$	Emboîtement des suites $u_0, \ldots, u_{d-1}$
$End^c(S_{\mathbb{Z}}(A))$	Monoïde des endomorphismes continus de l'algèbre $S_{\mathbb{Z}}(A)$
F	Support du multiensemble n
(F_+, F_-)	couple de séries génératrices d'une suite bi-infinie
K	Corps commutatif
PQA	Monoïde des présentations d'applications quasi-affines
QA	Monoïde des applications quasi-affines
$QA*$	Groupe des bijections quasi-affines
QA_d	Ensemble des applications quasi-affines de largeur d
$r_{\mathbb{Z}}(A)$	Algèbre des suites bi-infinies récurrentes linéaires à valeurs dans A
$S_{\mathbb{Z}}(A)$	Algèbre des suites bi-infinies, à valeurs dans A
$T_A(u)$	La suite $(u(m+1))_{m\in\mathbb{Z}}$
$\vartheta_d(u)$	La suite $(u(dm))_{m\in\mathbb{Z}}$
φ	Application quasi-affine
$\kappa_{m,A}$	Projection canonique de $S_{\mathbb{Z}}(A)$ dans A

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

Dans le chapitre un, nous définissons par suite bi-infinie, toute suite indexée par $\mathbb{Z}$ l'ensemble des entiers rationnels. Pour chaque suite bi-infinie u, nous associons le couple de séries génératrices (F_+, F_-), tel que $F_-(u) = F_+(\widehat{u})$, où $\widehat{u}$ est définie comme la suite reflet de la suite u, par la relation $\widehat{u} = (u(-m))_m \in \mathbb{Z}$. Nous considérons aussi les séries génératrices des suites décalées $T^k(u), k \in \mathbb{Z}$, où les énoncés des propositions 1.2.2 et 1.2.3, nous ont permis de déterminer d'autres relations et résultats reliants les deux séries génératrices, qu'on trouvera dans les chapitres qui suivent. Au chapitre 2, nous étudions des propriétés de ces quasi-polynômes relativement à l'opération de composition des applications. 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 2.3.3). 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 2.4.6), c'est-à-dire combinaison linéaire à coefficients périodiques des deux fonctions 1 et $\mathrm{I}d_{\mathbb{Z}}$.

Le chapitre 3 est consacré aux propriétés de ces fonctions quasi-affines, qui constituent un sous-monoïde QA du monoïde de tous les quasi-polynômes arithmétiques (théorème 3.2.1). 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 3.2.2. La relation d'équivalence par laquelle on quotiente le monoïde PQA pour obtenir QA est précisée par l'énoncé de la proposition 3.3.1.

Dans le chapitre 4, la démonstration de la caractérisation de ces applications quasi-affines au moyen des endomorphismes continus de l'algèbre des suites reconnaissables est très proche de celle de [1] : c'est pourquoi nous avons omis de reprendre un certain nombre d'arguments en renvoyant pour leur exposé, á cet article lors-que 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 [16] 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.

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 le chapitre 5 des bijections quasi-affines, la condition (1) de la proposition 5.2.1 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 le domaine de départ est réunion disjointe de groupes.

Nous cherchons dans le chapitre 6 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 6.1.4). On cherche donc à caractériser les multiensembles associés aux rapports des bijections quasi-affines, dénommés multiensembles idoines. Nous montrons (proposition 6.2.1) que le caractère idoine d'un multiensemble $n : \alpha \mapsto n_\alpha$, avec $n_0 = 0$, est équivalent à l'existence d'un coloriage du groupe $\mathbb{Z}/N\mathbb{Z}$, où N est un multiple commun des éléments du support de n, 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. Une idée qui peut souvent être utile pour vérifier qu'un multiensemble donné est idoine est de se ramener à vérifier qu'un multiensemble plus simple l'est : c'est l'idée sous-jacente à la proposition 6.3.1. En particulier, cette idée permet de caractériser complètement les multiensembles idoines dont le support a au plus trois éléments (corollaire 6.3.7 et proposition 6.3.8).

1 Suites bi-infinies et leurs séries génératrices

Toute suite indexée par $\mathbb{Z}$ sera appelée une suite bi-infinie. Sur ces suites bi-infinies agissent deux opérations fondamentales, qui sont connus sous les noms de décalage et de réflexion.
Dans ce premier chapitre, nous introduisons en outre la notion nouvelle de couple de séries génératrices d'une suite bi-infinie u, noté par $(F_+(u), F_-(u))$, et nous caractérisons les couples de séries entières formelles qui sont couple de séries génératrices pour une suite bi-infinie. Nous explicitons l'action des puissances entières du décalage sur le couple $(F_+(u), F_-(u))$.

1.1 Notion de suite bi-infinie

Nous ne considérons dans le présent mémoire que des suites indexées par $\mathbb{Z}$. Nous donnons à ces suites un nom spécial.

Définition 1.1.1. Une *suite bi-infinie* est une suite indexée par l'ensemble $\mathbb{Z}$ des entiers rationnels, à valeurs dans l'ensemble A.

Nous fixons maintenant notre vocabulaire en distinguant deux opérations très importantes sur les suites bi-infinies, qui portent les noms de *décalage* et de *réflexion*.

Définition 1.1.2. Le *décalé* de la suite bi-infinie $u = (u(m))_{m\in\mathbb{Z}}$ est la suite $T(u) = (u(m+1))_{m\in\mathbb{Z}}$.

L'opération T prend le nom de *décalage*. On peut évidemment itérer l'opération unaire T : si k est un entier rationnel, le *décalé*

d'ordre k de la suite u est la suite $T^k(u) = (u(m+k))_{m\in\mathbb{Z}}$. En particulier, le décalage est bijectif, sa réciproque étant $T^{-1} : u \mapsto T^{-1}(u) = (u(m-1))_{m\in\mathbb{Z}}$.

Définition 1.1.3. Le *reflet* de la suite bi-infinie $u = (u(m))_{m\in\mathbb{Z}}$ est la suite $\widehat{u} = (u(-m))_{m\in\mathbb{Z}}$.

Ici, l'opération unaire $\mathscr{R} : u \mapsto \widehat{u}$ sur les suites bi-infinies est appelée la *réflexion*.

Proposition 1.1.4. *L'opération réflexion $\mathscr{R}$ est involutive. De plus, elle vérifie l'identité*

$$T^{-1}(\mathscr{R}(u)) = \mathscr{R}(T(u))\,. \tag{1}$$

Démonstration. Si u est une suite bi-infinie, il est clair que le reflet de $\widehat{u} = \mathscr{R}(u)$ est la suite u. Donc l'opération réflexion $\mathscr{R}$ est involutive. De plus, pour tout entier rationnel m, on vérifie que

$$\widehat{T(u)}(m) = (T(u))(-m) = u(-m+1) = \widehat{u}(m-1) = T^{-1}(\widehat{u})(m).$$

□

1.2 Séries génératrices d'une suite bi-infinie quelconque

1.2.1 Définition des séries génératrices

Comme nos suites sont indexées par $\mathbb{Z}$, il nous est impossible de les caractériser par une unique série génératrice. Nous utiliserons donc un couple de séries génératrices, comme le précise la définition suivante.

Définition 1.2.1. Étant donnée une suite bi-infinie $u = (u(m))_{m\in\mathbb{Z}}$ dont les termes sont éléments d'un anneau R où 2.1_R est inversible, on appelle *séries génératrices* de la suite u les deux séries entières formelles

$$F_+(u)(t) = \frac{u(0)}{2.1_R} + \sum_{n\geq 1} u(n)t^n \in R[\![\,t\,]\!]$$

et

$$F_-(u)(t) = \frac{u(0)}{2.1_R} + \sum_{n\geq 1} u(-n)t^n \in R[\![t]\!] .$$

Une façon équivalente de définir la série $F_-(u)(t)$ est fournie par la formule évidente

$$F_-(u)(t) = F_+(\widehat{u})(t) \tag{2}$$

où $\widehat{u} = (u(-m))_{m\in\mathbb{Z}}$ est la suite reflet de la suite u.

1.2.2 Caractérisation des séries génératrices

Soit R un anneau où 2 est inversible. On définit l'application $\mathscr{F}_R$ qui à toute suite bi-infinie u dont tous les termes sont éléments de R associe le couple de ses deux séries génératrices :

$$\mathscr{F}_R(u) = (F_+(u), F_-(u)) .$$

L'application $\mathscr{F}_R$ est évidemment bijective. De plus, l'image de $\mathscr{F}_R$ est exactement l'ensemble des couples $(f(t), g(t))$ d'éléments de l'anneau $R[\![t]\!]$ tels que $f(0) = g(0)$. Ceci permet de dire que tout énoncé concernant les suites bi-infinies est traduisible en un énoncé portant sur les couples de séries entières formelles.

1.2.3 Séries génératrices des suites décalées

On désire maintenant préciser l'effet du *décalage* $T : u \mapsto Tu = (u(m+1))_{m\in\mathbb{Z}}$ sur les séries génératrices de la suite bi-infinie u. Pour unifier l'expression du résultat, nous commençons par introduire une application $\gamma : \mathbb{Z}^2 \to \mathbb{Z}\left[\frac{1}{2}\right]$ en posant

$$\gamma(j,k) = \frac{1}{2}(\mathrm{sgn}(j) - \mathrm{sgn}(j-k)) ,$$

où la notation sgn est celle de la fonction signe, définie pour tout $x \in \mathbb{R}$ par :

$$\mathrm{sgn}(x) = \begin{cases} 1 & si \quad x > 0 \\ 0 & si \quad x = 0 \\ -1 & si \quad x < 0 \end{cases} .$$

Proposition 1.2.2. *Pour toute suite bi-infinie u dont les termes sont éléments d'un anneau R où 2 est inversible, et pour tout $k \in \mathbb{Z}$, on a*

$$F_+(T^{-k}u) = t^k F_+(u) + \sum_{j\in\mathbb{Z}} \gamma(j,k)u(j-k)t^j \ .$$

On remarquera que l'expression $\sum_{j\in\mathbb{Z}} \gamma(j,k)u(j-k)t^j$ a un sens, car, quand on fixe un entier k dans $\mathbb{Z}$, l'ensemble des entiers $j \in \mathbb{Z}$ tels que $\gamma(j,k) \neq 0$ est fini.

Démonstration. On part de la formule

$$F_+(u) = \sum_{m\in\mathbb{Z}} \frac{1+\mathrm{sgn}(m)}{2} u(m)t^m \ ,$$

qui a un sens dans l'anneau $R((t))$ des séries méromorphes formelles à coefficients dans R, car $1+\mathrm{sgn}(m) = 0$ pour $m < 0$. On en déduit, que pour un entier quelconque $k \in \mathbb{Z}$, on a d'une part

$$F_+(T^{-k}u) = \sum_{m\in\mathbb{Z}} \frac{1+\mathrm{sgn}(m)}{2} u(m-k)t^m \ , \tag{3}$$

et d'autre part

$$\begin{aligned} t^k F_+(u) &= \sum_{m\in\mathbb{Z}} \frac{1+\mathrm{sgn}(m)}{2} u(m)t^{m+k} \\ &= \sum_{m\in\mathbb{Z}} \frac{1+\mathrm{sgn}(m-k)}{2} u(m-k)t^m \end{aligned}$$

En soustrayant cette dernière égalité de l'équation (3), on trouve

$$F_+(T^{-k}u) = t^k F_+(u) + \sum_{j\in\mathbb{Z}} \frac{\mathrm{sgn}(j)-\mathrm{sgn}(j-k)}{2} u(j-k)t^j \ ,$$

ce qui est précisément l'identité à montrer. □

Proposition 1.2.3. *Pour toute suite bi-infinie u dont les termes sont éléments d'un anneau R où 2 est inversible, et pour tout $k \in \mathbb{Z}$, on a*

$$\begin{aligned} F_-(T^{-k}u) &= t^{-k} F_-(u) + \sum_{j\in\mathbb{Z}} \gamma(j,-k)u(-k-j)t^j \\ &= t^{-k} F_-(u) - \sum_{j\in\mathbb{Z}} \gamma(j+k,k)u(-k-j)t^j \ . \end{aligned}$$

Démonstration. On sait par la proposition 1.1.4 que $\widehat{T^{-k}u} = T^k\widehat{u}$. Par conséquent, par la proposition 1.2.2, on a

$$F_-(T^{-k}u) = F_+(T^k\widehat{u}) = t^{-k}F_+(\widehat{u}) + \sum_{j\in\mathbb{Z}} \gamma(j,-k)\widehat{u}(j+k)t^j \ .$$

On achève la démonstration en utilisant les identités $F_+(\widehat{u}) = F_-(u)$ et $\gamma(j,-k) = -\gamma(j+k,k)$. □

1.2.4 Séries génératrices et action d'un polynôme

Notation 1.2.4. Si $P(x) = \sum_{j=0}^{\ell} a_j x^j$ est un polynôme à coefficients dans un anneau R, et si $u = (u(m))_{m\in\mathbb{Z}}$ est une suite bi-infinie dont tous les termes appartiennent à R, on note $P(T)(u)$ la suite v de terme général $v(m) = \sum_{j=0}^{\ell} a_j u(m+j)$, et on note $P(T^{-1})(u)$ la suite w de terme général $w(m) = \sum_{j=0}^{\ell} a_j u(m-j)$.

Proposition 1.2.5. *Soit R un anneau commutatif où 2 est inversible. Soit h un entier naturel, et $q(x)$ un polynôme à coefficients dans l'anneau R, dont le degré est au plus h, de sorte que $q^*(x) = x^h q(x^{-1})$ est également un polynôme de degré au plus h. Si u est une suite bi-infinie dont tous les termes sont éléments de R, alors les différences*

$$q^*(t)F_+(u) - t^h F_+(q(T)(u)) \quad \text{et} \quad q^*(t)F_-(u) - t^h F_-(q(T^{-1})(u))$$

sont des polynômes en t, divisibles par $t^{h-\deg(q)}$, et de degré $\leq h$.

Démonstration. Écrivons $q(x) = \sum_{i=0}^{h} a_i x^i$, avec $a_i \in R$. Posons $q^*(x)$ le polynôme défini par : $q^*(x) = \sum_{i=0}^{h} a_i x^{h-i}$. À partir de la relation $q(T)(u)(m) = \sum_{i=0}^{h} a_i u(m+i)$, et compte tenu de la proposition 1.2.2, on a :

$$\begin{aligned} F_+(q(T)(u)) &= \sum_{i=0}^{h} a_i F_+(T^i u) \\ &= \sum_{i=0}^{h} a_i [t^{-i}F_+(u) + \sum_{j\in\mathbb{Z}} \gamma(j,-i)u(j+i)t^j] \\ &= (\sum_{i=0}^{h} a_i t^{-i})F_+(u) + \sum_{i=0}^{h}\sum_{j\in\mathbb{Z}} a_i\gamma(j,-i)u(j+i)t^j \ . \end{aligned}$$

Après multiplication par t^h, on obtient

$$t^h F_+(q(t)(u)) = q^*(t)F_+(u) + \sum_{i=0}^{h}\sum_{j\in\mathbb{Z}} a_i\gamma(j,-i)u(i+j)t^{j+h}.$$

Considérons la difference $q^*(t)F_+(u) - t^hF_+(q(T)(u))$, alors

$$q^*(t)F_+(u) - t^hF_+(q(T)(u)) = \\ -\sum_{m\in\mathbb{Z}}\left(\sum_{i=0}^{h} a_i\gamma(m-h,-i)u(i+m-h)\right)t^m.$$

Lorsque $m > h$, ou lorsque $m < 0$, du fait que $h \geq i \geq 0$, $\gamma(m-h,-i) = 0$. De même, lorsque $m \leq h$ et $0 \leq i < h-m$, on a $\gamma(m-h,-i) = 0$. L'égalité ci-dessus devient :

$$q^*(t)F_+(u) - t^hF_+(q(T)(u)) = \\ -\sum_{m=0}^{h}\left(\sum_{i=h-m}^{h} a_i\gamma(m-h,-i)u(i+m-h)\right)t^m\,,$$

expression dont on conclut que $q^*(t)F_+(u) - t^hF_+(q(T)(u))$ est un polynôme de degré au plus h. Ce polynôme est divisible par $t^{h-\deg(q)}$ car $a_i = 0$ dès que $i > \deg(q)$.

L'énoncé concernant la série $F_-(u)$ se déduit de celui concernant $F_+(u)$ en remplaçant la suite u par sa suite reflet, moyennant la remarque que, d'après l'identité (1), on a $\widehat{q(T_A^{-1})(u)} = q(T_A)(\widehat{u})$. □

Proposition 1.2.6. *Soit A un anneau où 2 est inversible. Soit $h \geq 1$ un entier naturel, et $q(x)$ un polynôme à coefficients dans l'anneau A, de degré h, de polynôme réciproque $q^*(x) = x^hq(x^{-1})$. Pour toute suite bi-infinie u sur A, considérons les produits de séries entières formelles*

$$L_+(t) = q^*(t)F_+(u) \qquad \text{et } L_-(t) = q(t)F_-(u)\,.$$

Pour tout entier $j \in \mathbb{Z}$, l'élément $q(T_A)(u)(-j)$ est la somme du coefficient de t^{h-j} dans $L_+(t)$ et du coefficient de t^j dans $L_-(t)$, avec la convention évidente que le coefficient d'une puissance de t d'exposant strictement négatif dans une série entière formelle est nul.

Démonstration. Soit $q(x) = \sum_{i=0}^{h} a_{h-i} t^i$ avec $a_0 \neq 0$ un polynôme de degré h dans $A[x]$, u une suite bi-infinie sur A et $j \in \mathbb{Z}$, alors

$$q(T_A)(u)(-j) = \sum_{i=0}^{h} a_{h-i} T_A^i(u)(-j) = \sum_{i=0}^{h} a_{h-i} u(i-j). \qquad (4)$$

D'autre part $q^*(x) = \sum_{i=0}^{h} a_i t^i$, de sorte que le coefficient de t^{h-j} dans la série entière formelle $L_+(t)$ vaut

$$\sum_{k=0}^{h-j-1} a_k u(h-j-k) + a_{h-j} \frac{u(0)}{2}.$$

De même, le coefficient de t^j dans la série entière formelle $L_-(t)$ est

$$\sum_{k=0}^{j-1} a_{h-k} u(k-j) + a_{h-j} \frac{u(0)}{2}.$$

La somme des deux coefficients précédents est donc

$$\sum_{k=0}^{h-j-1} a_k u(h-j-k) + \sum_{k=0}^{j-1} a_{h-k} u(k-j) + a_{h-j} u(0),$$

qui, par changement d'indices, devient

$$\sum_{i=j+1}^{h} a_{h-i} u(i-j) + \sum_{i=0}^{j} a_{h-i} u(i-j) = \sum_{i=0}^{h} a_{h-i} u(i-j). \qquad (5)$$

En comparant les expressions données par les relations (4) et (5), on obtient la relation voulue. □

2 Quasi-polynômes

Dans ce chapitre, nous commençons par rappeler la définition et les propriétés des nombres périodiques, en suivant Ehrhart [10]. L'étude du couple de séries « génératrices » que nous associons à un tel nombre périodique est nouvelle. Ensuite, nous introduisons la notion de quasi-polynôme déjà considérée par de nombreux auteurs [21, 10] : un quasi-polynôme est un polynôme dont les coefficients sont des nombres périodiques. Nous montrons que les quasi-polynômes à valeurs entières, que nous appelons les quasi-polynômes arithmétiques, sont exactement les solutions des récurrences d'un certain type, dites récurrences unimodulaires : ce résultat figure en substance chez Ehrhart [10]. Il nous permet aussi de caractériser les séries génératrices des quasi-polynômes. Nous montrons que le composé de deux quasi-polynômes arithmétiques est un quasi-polynôme arithmétique (théorème 2.3.3), puis que les quasi-polynômes arithmétiques bijectifs sont de degré un (théorème 2.4.6). La démonstration de ce dernier résultat s'appuie de façon cruciale sur la notion de densité naturelle d'une partie de $\mathbb{Z}$.

2.1 Les nombres périodiques

Il est nécessaire de reprendre les définitions et les résultats sur les nombres périodiques donnés par E.Ehrhart [10] afin de bien comprendre comment nous composons les quasi-polynômes arithmétiques.

2.1.1 Notion de nombre périodique

Définition 2.1.1. On appelle *nombre réel périodique*, ou en abrégé *périodique*, toute suite réelle $(a_m)_{m\in\mathbb{Z}}$, indexée par l'ensemble des entiers rationnels, admettant une période entière non nulle d, c'est-à dire telle que

$$\forall m \in \mathbb{Z}, \qquad a_{m+d} = a_m \,. \tag{6}$$

Le nombre périodique $(a_m)_{m\in\mathbb{Z}}$ est dit rationnel ou entier, si tous ses termes le sont.

La notation d'Ehrhart, pour le nombre réel périodique $a = (a_m)_{m\in\mathbb{Z}}$ est

$$a_m = [a_1, a_2, \cdots, a_d]. \tag{7}$$

Ainsi, dans cette notation, $[a_1, a_2, \cdots, a_d]$ est le terme de rang m de la suite de période d dont les d premiers termes de rang strictement positif sont $a_1, a_2, \cdots, a_d$. Comme Ehrhart le remarque : « Dans cette notation, la variable entière m n'apparaît pas explicitement ; elle doit donc être indiquée par le contexte ».

Exemples

1. Pour tout réel a, on note aussi a le nombre périodique $[a]$, c'est-à-dire la suite constante dont tous les termes valent a.
2. La notation $[-1, 1]$ désigne le terme de rang m de la suite $((-1)^m)_{m\in\mathbb{Z}}$.

2.1.2 Opérations sur les nombres périodiques

2.1.2.1 Somme et produit

On se donne $a = (a_m)_{m\in\mathbb{Z}}$ et $a' = \left(a'_m\right)_{m\in\mathbb{Z}}$ deux nombres périodiques de périodes respectives d et d'. On note $D = dq = d'q'$ le plus petit commun multiple de d et de d'. Alors on peut réduire à la même période D les deux périodiques en écrivant

$$\begin{aligned} a_m &= [a_1, a_2, \cdots, a_d, a_{d+1}, \cdots, a_D], \\ a'_m &= [a'_1, a'_2, \cdots, a'_{d'}, a'_{d'+1}, \cdots, a'_D], \end{aligned} \tag{8}$$

où les suites $a_1, a_2, \cdots, a_d$ et $a'_1, a'_2, \cdots, a'_d$ sont répétées q fois dans le premier crochet et q' fois dans le second.
La somme et le produit des nombres périodiques sont les opérations usuelles définies terme à terme. Ainsi on peut écrire

$$a_m + a'_m = [a_1 + a'_1, a_2 + a'_2, \cdots, a_D + a'_D],$$
$$a_m a'_m = [a_1 a'_1, a_2 a'_2, \cdots, a_D a'_D], \tag{9}$$

et s'ensuit le résultat suivant.

Proposition 2.1.2. *L'ensemble des nombres périodiques, muni de leur addition et de leur multiplication, est un anneau dont les éléments neutres pour les deux opérations sont respectivement 0 et 1.*

2.1.2.2 Décalage

Soit $a = (a_m)_{m\in\mathbb{Z}}$ un nombre périodique de période d. Il est clair que tous les décalés du périodique a sont des nombres périodiques de même période d. De plus, il est évident que $T^d(a) = a$.

La règle d'Ehrhart pour le calcul du décalé d'un périodique est la suivante.

Proposition 2.1.3. *Soit $a_m = [a_1, \cdots, a_d]$ le terme de rang m d'un nombre périodique de période d, et r un entier rationnel tel que $-d < r < d$. Si $r > 0$, alors le terme de rang m de son décalé d'ordre r est*

$$a_{m+r} = [a_{r+1}, \cdots, a_d, a_1, \cdots, a_r].$$

Si $r < 0$, alors le terme de rang m du décalé d'ordre r est

$$a_{m+r} = [a_{d+r+1}, \cdots, a_d, a_1, \cdots, a_{d+r}].$$

2.1.2.3 Réflexion

Il est immédiat que, si a est de période d, alors son reflet $\widehat{a}$ est un nombre périodique de même période d. La règle d'Ehrhart permettant le calcul du reflet est énoncée comme suit.

Proposition 2.1.4. *Soit $a_m = [a_1, \cdots, a_d]$ le terme de rang m d'un nombre périodique de période d. Alors le terme de rang m de son reflet est*

$$\widehat{a}_m = [a_{d-1}, a_{d-2}, \cdots, a_1, a_d].$$

2.1.3 Séries génératrices d'un nombre périodique

Le périodique $[a_1, a_2, \cdots, a_d] = [a_1, a_2, \cdots, a_{d-1}, a_0]$ admet pour première série génératrice

$$F_+(a) = \sum_{n\geq 0} [a_1, a_2, \cdots, a_d] t^n = \frac{a_0 \frac{1+t^d}{2} + a_1 t + a_2 t^2 + \cdots + a_{d-1} t^{d-1}}{1-t^d},$$

alors que sa deuxième série génératrice est

$$F_-(a) = \sum_{n\geq 0} [a_{d-1}, a_{d-2}, \cdots, a_1, a_d] t^n$$
$$= \frac{a_0 \frac{1+t^d}{2} + a_{d-1} t + a_{d-2} t^2 + \cdots + a_1 t^{d-1}}{1-t^d}.$$

On voit sur ces expressions que les deux séries génératrices d'un nombre périodique sont deux fractions rationnelles qui se correspondent dans l'involution $F(t) \mapsto -F(t^{-1})$ du groupe additif des fractions rationnelles.

Proposition 2.1.5. *Soit $(F_+(t), F_-(t))$ un élément de $\mathbb{R}[[t]]^2$. Pour que cet élément soit le couple de séries génératrices d'un nombre périodique $a = (a_m)_{m\in\mathbb{Z}}$, il faut et il suffit que les séries $F_+(t)$ et $F_-(t)$ vérifient les conditions suivantes :*

1. *F_+ et F_- sont des fractions rationnelles de degré ≤ 0,*
2. *tous les pôles de la série $F_+(t)$ sont simples et racines de l'unité,*
3. *$F_+(t^{-1}) = -F_-(t)$ et $F_+(0) + F_+(\infty) = 0$.*

Démonstration. Supposons que le couple $(F_+(t), F_-(t))$ est celui de séries génératrices d'une suite périodique $a = (a_m)_{m\in\mathbb{Z}}$. Alors, d'après les expressions précédemment obtenues pour les séries génératrices du périodique $[a_1, \cdots, a_d]$, on vérifie que

$$F_+(a)(t^{-1}) = -F_-(a)(t), \quad F_+(a)(0) + F_+(a)(\infty) = 0,$$

avec $deg(F_+(a)) \leq 0$. De plus, comme le dénominateur de la fraction $F_+(a)$ est égal au polynôme $1-t^d$, ainsi tous les pôles de cette fraction sont simples et racines de l'unité.

Réciproquement, supposons que le couple $(F_+(t), F_-(t))$ élément de $\mathbb{R}(t)^2$ vérifie les propriétés énoncées, alors il existe deux polynômes premiers entre eux f et g, à coefficients réels, tels que

$$F_+(t) = \frac{f(t)}{g(t)} \quad \text{et} \quad F_-(t) = -\frac{f(t^{-1})}{g(t^{-1})}.$$

Comme on sait que la fraction rationnelle $F_+(t)$ est de degré au plus zéro, on a $\deg f \leq \deg g$. Comme la fraction rationnelle $F_+(t)$ n'admet que des pôles simples qui sont tous racines de l'unité, il existe d un entier naturel non nul pour le quel $g(t)$ divise $1-t^d$. Ainsi on peut écrire

$$F_+(t) = \frac{f_1(t)}{1-t^d} \quad \text{et} \quad F_-(t) = -\frac{t^d f_1(t^{-1})}{1-t^d},$$

où $f_1(t) = \frac{c_0}{2} + c_1 t + c_2 t^2 + \cdots + \frac{c_d}{2} t^d$ est un polynôme de degré au plus d. Puisque $F_+(0) + F_+(\infty) = 0$, on voit que $c_0 = c_d$.
D'autre part,

$$\begin{aligned} F_+(t) &= \frac{\frac{c_d}{2} + c_1 t + c_2 t^2 + \cdots + \frac{c_d}{2} t^d}{1-t^d} \\ &= (\tfrac{c_d}{2} + c_1 t + c_2 t^2 + \cdots + \tfrac{c_d}{2} t^d) \textstyle\sum_{n\geq 0} t^{dn} \\ &= \tfrac{c_0}{2} + c_1 t + \cdots + c_{d-1} t^{d-1} + c_d t^d + c_1 t^{d+1} + \cdots \\ &= \tfrac{c_0}{2} + \textstyle\sum_{n\geq 1} [c_1, c_2, \cdots, c_d] t^n. \end{aligned}$$

Par un calcul analogue, on trouve que

$$F_-(t) = \frac{c_0}{2} + \sum_{n\geq 1} [c_{d-1}, c_{d-2}, \cdots, c_1, c_d] t^n .$$

Définissons la suite bi-infinie $\mathbf{a}$ de terme général $[c_1, \cdots, c_d]$, alors on a bien $F_+ = F_+(\mathbf{a})$ et $F_- = F_-(\mathbf{a})$. □

2.2 Notion de quasi-polynôme

2.2.1 Définitions

La notion de quasi-polynôme diffère d'un auteur à un autre. C'est pourquoi nous rappelons les différentes définitions données par Stanley [21] et Ehrhart [10], puis nous préciserons celle utilisée dans notre étude.

Définition 2.2.1 (Stanley)**.** Etant 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

$$\forall m \in \mathbb{Z}, \qquad f(m) = a_0(m) + a_1(m)m + \ldots + a_\ell(m)m^\ell, \qquad (10)$$

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.

De façon équivalente, f est un quasi-polynôme s'il existe un entier d période commune à tous les coefficients $a_j, j = 0, \cdots, \ell$ et des polynômes $f_i, i = 0, \cdots, d-1$ tel que

$$\forall m \in \mathbb{Z}, \quad f(m) = f_i(m), \text{ si } \quad m \equiv i (\text{mod } d)$$

Définition 2.2.2 (Ehrhart)**.** Soit ℓ un entier donné, un *polynôme arithmétique* de degré ℓ, aussi appelé un *polar*, est une fonction f de $\mathbb{Z}$ dans $\mathbb{C}$ à valeurs entières de la forme (10) avec $a_\ell \neq 0$, où chaque coefficient $a_j(m)$ est une fonction périodique de l'entier m. Le plus petit commun multiple des périodes des a_j est appelé la *pseudopériode* du polynôme arithmétique f. Le polar f est appelé *quasi-polynôme* lorsque a_0 est le seul coefficient non constant.

Dans tout ce qui suit, nous considérons des fonctions f de $\mathbb{Z}$ dans lui même. Comme les quasi-polynômes de R.Stanley [21] sont exactement les polynômes arithmétiques d'E.Ehrhart [10] à valeurs dans $\mathbb{Z}$, nous conviendrons d'utiliser partout le terme de *quasi-polynôme* au sens de la définition 2.2.1, tout en donnant la précision suivante.

Définition 2.2.3. Si f est un quasi-polynôme au sens de la définition 2.2.1 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*.

En tant qu'application de $\mathbb{Z}$ dans $\mathbb{Z}$, tout quasi-polynôme arithmétique f peut être identifié à la *suite bi-infinie* (c'est-à-dire indexée par l'ensemble $\mathbb{Z}$ des entiers rationnels) $(f(m))_{m\in\mathbb{Z}}$.

2.2.2 Propriétés

Nous citons et démontrons quelques résultats sur les quasi-polynômes que nous utiliserons dans les sections qui suivent.

Lemme 2.2.4. *Les fonctions périodiques $a_j : \mathbb{Z} \to \mathbb{C}$ figurant dans l'écriture (10) 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 pérodique de période d, est la fonction nulle, alors, pour tout entier $r \in [0..d[$, la fonction $m \mapsto a_0(r) + a_1(r)(r+dm) + \cdots + a_\ell(r)(r+dm)^\ell$ est une fonction polynomiale ne prenant que la valeur zéro ; par conséquent, tous ses coefficients $\sum_{k=j}^{\ell} a_k(r)\binom{k}{j} r^{k-j} d^j$, 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 $r \in [0..d[$. Par périodicité, il s'ensuit que les coefficients $a_j(m)$ sont nuls sur $\mathbb{Z}$. □

Lemme 2.2.5. *Soit $f : \mathbb{Z} \to \mathbb{Z}$ un quasi-polynôme arithmétique de degré ℓ et de quasi-période $d \in \mathbb{Z} \setminus \{0\}$, donné par $\ell + 1$ fonctions $a_j, 0 \le j \le \ell$ satisfaisant l'identité (10). Alors, pour tout indice $j \in [0..\ell]$, on a*

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

Démonstration. Envisageons d'abord le cas où $d = 1$, c'est-à-dire celui où les fonctions a_j sont constantes. On sait [19] 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 $d = 1$ en définissant, pour tout entier $r \in [0..d[$, un polynôme f_r par

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

avec $A_j = d^j \sum_{k=j}^{\ell} \binom{k}{j} a_k(r) r^{k-j}$. 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 $\ell! A_\ell = d^\ell \ell! a_\ell(r)$ est entier. Supposons qu'il existe un indice $j \in [0..\ell[$ tel que $d^\ell \ell! a_j(r) \notin \mathbb{Z}$. On peut choisir j le plus grand possible satisfaisant cette condition, de sorte que $d^\ell \ell! a_k(r)$

est entier pour tout indice $k \in]j..\ell]$. Alors

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

est entier, contrairement à l'hypothèse. □

2.2.3 Récurrence unimodulaire d'un quasi-polynôme arithmétique

Notation 2.2.6. Si $P(x) = \sum_{j=0}^{\ell} a_j x^j$ est un polynôme à coefficients a_j réels, et si $u = (u_m)_{m\in\mathbb{Z}}$ est une suite bi-infinie de nombres réels, on note $P(T)(u)$ la suite v de terme général $v_m = \sum_{j=0}^{\ell} a_j u_{m+j}$.

Définition 2.2.7. Soit u une suite bi-infinie de réels. S'il existe un polynôme non nul $P(x)$ à coefficients réels tel que $P(T)(u) = 0$, on dit que u est reconnaissable ou récurrente linéaire.

Définition 2.2.8. Le polynôme P à coefficients réels est dit *unimodulaire* s'il est de la forme $P(x) = \prod_{i=1}^{s}(x^{a_i} - 1)$, où s est un entier naturel, et où $(a_1, \ldots, a_s)$ est une suite d'entiers naturels non nuls.

Remarque 2.2.9. Cette notion de polynôme unimodulaire correspond à ce qu'Ehrhart [10, p. 17] appelle une récurrence unitaire.

Remarque 2.2.10. La somme des coefficients d'un polynôme unimodulaire $P(x)$ non constant est nulle, car ce polynôme est divisible par le polynôme $x - 1$.

Définition 2.2.11. Soit f un quasi-polynôme donné sous la forme (10). On appelle *grade* du quasi-polynôme f le plus petit entier k dans $\mathbb{N} \cup \{-1\}$ tel que, pour tout entier naturel $i > k$, le coefficient a_i est constant.

Remarque 2.2.12. Il résulte clairement de cette définition qu'un quasi-polynôme est de grade -1 si et seulement si c'est une fonction polynomiale au sens habituel.

Théorème 2.2.13. *Soit f un quasi-polynôme arithmétique de degré ℓ, de quasi-période d et de grade k. Alors f vérifie la relation de récurrence unimodulaire*

$$(T-1)^{\ell-k}(T^d-1)^{k+1}(f)=0.$$

Démonstration. [10, pp.18]

2.2.4 Séries génératrices d'un quasi-polynôme arithmétique

Comme tout quasi-polynôme arithmétique vérifie une relation de récurrence unimodulaire, les deux séries génératrices qui lui sont associées vont pouvoir s'exprimer en termes de cette relation de récurrence.

Lemme 2.2.14. *Si u est une suite bi-infinie à termes complexes vérifiant une relation de récurrence unimodulaire, alors ses deux séries génératrices $F_+(u)$ et $F_-(u)$ sont des fractions rationnelles de degré ≤ 0, satisfaisant l'identité*

$$F_+(u)(t)+F_-(u)(t^{-1})=0\,.$$

Démonstration. Par hypothèse, il existe un polynôme unimodulaire $P(x)=\sum_{i=0}^{h}a_{h-i}x^i$ dans $\mathbb{R}[x]$, tel que $P(T)(u)=0$. À partir de la définition 2.2.8, on déduit que $a_0=1$, et que $a_h=\mp 1$. D'autre part, $P(T)(u)=\sum_{i=0}^{h}a_{h-i}T^iu$, et donc

$$F_+(P(T)(u))=\sum_{i=0}^{h}a_{h-i}F_+(T^iu).$$

En utilisant le résultat de la proposition 1.2.2, et le fait que $\gamma(j,-i)\neq 0$ pour $-h\leq -i<j\leq 0$, on trouve :

$$\begin{aligned}
F_+(P(T)(u)) &= \sum_{i=0}^{h} a_{h-i}[t^{-i}F_+(u) + \sum_{j\in\mathbb{Z}} \gamma(j,-i)u(i+j)t^j] \\
&= (\sum_{i=0}^{h} a_{h-i}t^{-i})F_+(u) + \sum_{j\in\mathbb{Z}} t^j[\sum_{i=0}^{h} a_{h-i}\gamma(j,-i)u(i+j)] \\
&= t^{-h}P^*(t)F_+(u) + \sum_{j=-h}^{0} t^j \sum_{i=0}^{h} a_{h-i}\gamma(j,-i)u(i+j) \\
&= 0
\end{aligned}$$

Ainsi,

$$F_+(u)(t) = -\frac{\sum_{j=-h}^{0} t^{j+h} \sum_{i=0}^{h} a_{h-i}\gamma(j,-i)u(i+j)}{P^*(t)}\,. \tag{11}$$

Sur cette expression, on voit que $F_+(u)$ est une fraction rationnelle de degré ≤ 0. Il en est de même de $F_-(u) = F_+(\widehat{u})$, car l'annulateur de la suite reflet $\widehat{u}$ comprend le polynôme réciproque d'un polynôme non nul dans l'annulateur de u. Montrons maintenant que $F_+(u)(t) + F_-(u)(t^{-1}) = 0$. En appliquant la relation (11)à la suite reflet de u, on trouve :

$$F_+(\widehat{u})(t) = -\frac{\sum_{j=-h}^{0} t^{j+h} \sum_{i=0}^{h} a_i\gamma(j,-i)\widehat{u}(i+j)}{P(t)}\,.$$

Comme $F_-(u) = F_+(\widehat{u})$, on a ainsi

$$F_-(u)(t^{-1}) = F_+(\widehat{u})(t^{-1}) = -\frac{\sum_{j=-h}^{0} t^{-(j+h)} \sum_{i=0}^{h} a_i\gamma(j,-i)\widehat{u}(i+j)}{P(t^{-1})}$$

comme $P^*(t) = t^h p(t^{-1})$, on obtient :

$$F_-(u)(t^{-1}) = -\frac{\sum_{j=-h}^{0} t^{-j} \sum_{i=0}^{h} a_i\gamma(j,-i)u(-i-j)}{P^*(t)}$$

On peut écrire aussi

$$F_-(u)(t^{-1}) = -\frac{\sum_{j=0}^{h} t^{j} \sum_{i=0}^{h} a_i\gamma(-j,-i)u(-i+j)}{P^*(t)}$$

de même la relation (11) devient :

$$F_+(u)(t) = -\frac{\sum_{j=0}^{h} t^{h-j} \sum_{i=0}^{h} a_{h-i}\gamma(-j,-i)u(i-j)}{P^*(t)}\,.$$

$$F_+(u)(t) = -\frac{\sum_{j=0}^{h} t^{h-j} \sum_{i=0}^{h} a_{h-i}\gamma(-j,-i)\widehat{u}(j-i)}{P^*(t)}\,.$$

Ainsi on a

$$P^*(t)F_+(u)(t) = -\sum_{j=0}^{h} t^{h-j} \sum_{i=0}^{h} a_{h-i}\gamma(-j,-i)\widehat{u}(j-i);$$

et

$$P^*(t)F_-(u)(t^{-1}) = -\sum_{j=0}^{h} t^{j} \sum_{i=0}^{h} a_{i}\gamma(-j,-i)u(j-i).$$

On voit bien que les polynômes $P^*(t)F_-(u)(t^{-1})$, $P^*(t)F_+(u)(t)$ sont de degré au plus h, tel que le coefficient de t^h dans $P^*(t)F_+(u)(t)$ est obtenu lorsque $j = 0$; et il est égale à

$$-\sum_{i=0}^{h} a_{h-i}\gamma(0,-i)u(i);$$

où $\gamma(0,-i) = -\frac{1}{2}$ pour tout $i = 1,\cdots,h$ et $\gamma(0,0) = 0$. Ainsi

$$-\sum_{i=0}^{h} a_{h-i}\gamma(0,-i)u(i) = \frac{1}{2}\sum_{i=1}^{h} a_{h-i}u(i).$$

Comme $\gamma(-h,-i) = 0$, pour tout $i < h$ et $\gamma(-h,-h) = -\frac{1}{2}$, on a que

$$-\sum_{i=0}^{h} a_{i}\gamma(-h,-i)u(h-i) = \frac{1}{2}a_h u(0).$$

En sommant les coefficients de t^h des polynômes $P^*(t)F_+(u)(t)$ et $P^*(t)F_-(u)(t^{-1})$, on obtient :

$$\frac{1}{2}\sum_{i=0}^{h} a_{h-i}u(i) = 0.$$

Soit $k \in \mathbb{N}$, tel que $k < h$. Le coefficient de t^k dans le polynôme $P^*(t)F_-(u)(t)$ est $-\sum_{i=0}^{h} a_i\gamma(-k,-i)u(k-i)$, comme $\gamma(-k,-i)$ vaut 0 si $i < k$, -1 si $i > k$, et $-\frac{1}{2}$, lorsque $i = k$, on a

$$-\sum_{i=0}^{h} a_i\gamma(-k,-i)u(k-i) = \frac{1}{2}a_k u(0) + \sum_{i=k+1}^{h} a_i u(k-i).$$

Dans le polynôme $P^*(t)F_+(u)(t)$ le coefficient de t^k est obtenu pour $j = h-k$, et est égal à $-\sum_{i=0}^{h} a_{h-i}\gamma(k-h,-i)u(i+k-h)$. Or $\gamma(k-h,-i)$ est égal à 0 si $i < h-k$, -1 si $i > h-k$ et $-\frac{1}{2}$ lorsque $i = h-k$. Ainsi on a

$$\begin{aligned}\sum_{i=0}^{h} a_{h-i}\gamma(k-h,-i)u(i+k-h) &= \frac{1}{2}a_k u(0) + \sum_{i=h-k+1}^{h} a_{h-i}u(i+k-h)\\ &= \frac{1}{2}a_k u(0) + \sum_{i=0}^{k-1} a_i u(k-i).\end{aligned}$$

La somme des coefficients de t^k des deux polynômes $P^*(t)F_+(u)(t)$ et $P^*(t)F_-(u)(t^{-1})$ est donc égal à

$$\sum_{i=0}^{h} a_i u(k-i).$$

Comme la suite u est annulée par le polynôme $p(x) = \sum_{i=0}^{h} a_{h-i}x^i$, alors pour tout $m \in \mathbb{Z}$, on a

$$\sum_{i=0}^{h} a_{h-i}u(m+i) = 0,$$

donc pour $m = k-h$ on trouve

$$\sum_{i=0}^{h} a_{h-i}u(k-h+i) = \sum_{i=0}^{h} a_i u(k-i) = 0.$$

□

Théorème 2.2.15. *Soit $u : \mathbb{Z} \to \mathbb{Z}$ une suite bi-infinie d'entiers rationnels. Les énoncés suivants sont équivalents.*

1. *La fonction u est un quasi-polynôme arithmétique ;*
2. *la suite bi-infinie u vérifie une relation de récurrence unimodulaire ;*
3. *les deux séries génératrices $F_+(t)$ et $F_-(t)$ de u sont des fractions rationnelles de degré ≤ 0 dont tous les pôles sont racines de l'unité, et vérifient les relations $F_+(t^{-1}) = -F_-(t)$, $F_+(0) + F_+(\infty) = 0$.*

Démonstration. L'implication $1 \Rightarrow 2$ est le théorème 2.2.13.

Supposons que la suite bi-infinie u vérifie une récurrence unimodulaire, d'après le lemme 2.2.14 les séries génératrices $F_+(u)$ et $F_-(u)$ sont des fractions rationnelles de degré ≤ 0, vérifiant :
$F_+(u)(t) + F_-(u)(t^{-1}) = 0$.
Lorsque la variable $t = 0$, la relation 11 devient :

$$F_+(0) = \sum_{i=0}^{h} a_{h-i}\gamma(-h,-i)u(i-h).$$

Comme $\gamma(-h,-i) = 0$, pour tout $i < h$ et égale à $-\frac{1}{2}$ si $i = h$; en déduit que

$$F_+(0) = -\frac{1}{2}a_0u(0) = -\frac{u(0)}{2}.$$

D'autre part ; la relation 11 s'écrit pour $t = +\infty$:

$$\begin{aligned} F_+(+\infty) &= \frac{\sum_{i=0}^{h} a_{h-i}\gamma(0,-i)u(i)}{a_h} \\ &= -\frac{1}{2a_h}\sum_{i=1}^{h} a_{h-i}u(i) = -\frac{1}{2a_h}(-a_hu(0)) = \frac{u(0)}{2}, \end{aligned}$$

et donc on a bien

$$F_+(0) + F_+(+\infty) = 0.$$

Soit l'hypothèse 3 vérifiée. En particulier, si on considère la série génératrice $F_+(u)(t) = \frac{P(t)}{Q(t)}$, avec $Q^*(u)(t) = 0$, alors d'après [10, pp.23], la suite bi-infinie u est un quasi-polynôme arithmétique. □

Comme une conséquence du théorème 2.2.15, on a l'énoncé suivant.

Proposition 2.2.16. *Si u est un quasi-polynôme arithmétique vérifiant une récurrence unimodulaire de la forme $(T-1)^h(u)=0$, où h est un entier naturel, alors u est une fonction polynomiale de degré moindre que h.*

2.3 Composition de quasi-polynômes arithmétiques

2.3.1 Opérations sur les quasi-polynômes arithmétiques

Soient f et g deux quasi-polynômes arithmétiques ; comme la somme et le produit de deux périodiques est un périodique, il est immédiat que $f+g$ et fg sont aussi des quasi-polynômes arithmétiques en vertu de la proposition 2.1.2. Les éléments neutres pour l'addition et la multiplication des quasi-polynômes arithmétiques sont respectivement 0 et 1. On a donc le résultat suivant.

Proposition 2.3.1. *L'ensemble des quasi-polynômes arithmétiques, muni de leur addition et de leur multiplication, est un anneau.*

2.3.2 Composition de quasi-polynômes arithmétiques

Nous montrons maintenant que l'anneau des quasi-polynômes arithmétiques est stable pour la composition.

Lemme 2.3.2. *Si f est un quasi-polynôme arithmétique non nul de degré ℓ et de quasi-période d, 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 $L=d^{\max(1,\ell)}\ell!p$.*

Démonstration. On remarque que $L=d^{\max(1,\ell)}\ell!p$ est un multiple commun des entiers d et p. Par hypothèse, il existe $\ell+1$ fonctions $a_j:\mathbb{Z}\to\mathbb{C}, j=0\dots\ell$ de période d satisfaisant l'identité (10). 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

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

Comme les nombres $a_j(m)\ell!d^\ell$ sont entiers pour tout indice $j \in [1..\ell]$ par le lemme 2.2.5, on voit que les entiers $\ell!d^\ell(f(m+L)-f(m))$ sont des multiples de L. Par division par $\ell!d^\ell$, on en déduit que $f(m+L)-f(m)$ est divisible par p. □

Théorème 2.3.3. *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 d 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 $L = d^{\max(1,\ell)}\ell!p$ est une quasi-période de $g \circ f$.*

Démonstration. On sait [10] que les quasi-polynômes arithmétiques forment un anneau quand on les munit de l'addition et de la multiplication usuelles ; en particulier, le produit de deux quasi-polynômes arithmétiques 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 (10), 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 2.3.2, 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 ℓ' est un entier naturel, il existe $\ell'+1$ fonctions périodiques a_j, avec $j \in [0..\ell']$, telles que $g(m) = a_0(m)+a_1(m)m+\cdots+a_{\ell'}(m)m^{\ell'}$ pour tout $m \in \mathbb{Z}$, et donc pour tout entier rationnel m,

$$(g \circ f)(m) = a_0(f(m)) + a_1(f(m))f(m) + \cdots + a_{\ell'}(f(m))f(m)^{\ell'} .$$

Comme les fonctions $a_j \circ f$ sont périodiques de période L d'après le lemme 2.3.2, 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 $\ell\ell'$ et que L en est une quasi-période. □

2.4 Les quasi-polynômes bijectifs

2.4.1 Densité arithmétique ou asymptotique

Les deux définitions qui suivent sont équivalentes [18] :

Définition 2.4.1. Soit B une partie de $\mathbb{N}$. On appelle densité de B la limite quand elle existe de la suite de terme général

$$\frac{\text{card}(B \cap [1,n])}{n}.$$

Définition 2.4.2. Soit $B = \{a_1, a_2, a_3, \cdots\}$ avec $a_1 < a_2 < a_3 \cdots$, une partie infinie de $\mathbb{N}$. On appelle densité de B et on la note par dens(B) la limite suivante lorsqu'elle existe

$$\text{dens}(B) = \lim_{n\to+\infty} \frac{a_n}{n}.$$

La notion de densité arithmétique ou naturelle est définie pour une partie de $\mathbb{N}$, de manière analogue nous donnons une définition de la densité pour une partie de $\mathbb{Z}$.

Définition 2.4.3. Soit B une partie de $\mathbb{Z}$. On dit que la partie B a une densité si la suite de terme général

$$\frac{\text{card}(B \cap [-n,+n])}{2n+1} \tag{12}$$

admet une limite pour n tendant vers l'infini. Lorsque B a une densité, la densité (naturelle) de B, notée dens(B), est la limite de la suite (12).

On a évidemment l'énoncé suivant.

Lemme 2.4.4. *Si B_1 et B_2 sont deux parties disjointes de $\mathbb{Z}$ ayant toutes deux une densité, alors $B_1 \cup B_2$ a une densité, et la densité de $B_1 \cup B_2$ est la somme des densités de B_1 et de B_2.*

Lemme 2.4.5. *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 $\mathrm{c}d(f)$, 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 $k < \rho$.

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 $f(\mathbb{N}) \cup \mathbb{N}^*$ dans une suite strictement croissante $(a_n)_n \geq 1$. Il résulte de ce qui précéde l'équivalent

$$a_n \sim \mathrm{c}d(f) n^\ell \quad \text{pour } n \to +\infty ,$$

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 [18], on aboutit au résultat voulu. □

2.4.2 Les quasi-polynômes bijectifs

Théorème 2.4.6. *Un quasi-polynôme arithmétique bijectif est de degré un.*

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 2.4.4 et 2.4.5 :

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

Posons $N = ppcm\{a_r,\ r \in A\}$ 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'aprés le lemme 2.4.4, la densité

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

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.

□

3 Applications quasi-affines

Le contenu du présent chapitre est extrait sans modification de notre article [17]. La définition des fonctions quasi-affines de $\mathbb{Z}$ dans $\mathbb{Z}$ est inspirée de celle des applications purement semi-affines de $\mathbb{N}$ dans $\mathbb{N}$ introduite dans [2], elle-même cas particulier des applications semi-affines de $\mathbb{N}$ dans $\mathbb{N}$ définies dans [1]. Notons que l'appellation d'application semi-affine précédemment utilisée [1, 2] 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. Nous représentons chaque fonction quasi-affine par un triplet $(d, \mathbf{a}, \mathbf{b})$ appelé présentation. Nous montrons que l'ensemble des applications quasi-affines est un monoïde pour la composition des fonctions, et qu'une application quasi-affine peut admettre plusieurs présentations.

3.1 Présentations d'une application quasi-affine

3.1.1 Définitions et propriétés

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 généaliser la notion d'application affine de la manière suivante.

Définition 3.1.1. 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

$$\forall m \in \mathbb{Z}, \qquad \varphi(m+d) - 2\varphi(m) + \varphi(m-d) = 0\,. \tag{13}$$

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 3.1.2. Cette définition est l'analogue, pour les applications de $\mathbb{Z}$ dans $\mathbb{Z}$, de celle des applications purement semi-affines donnée par [2].

Proposition 3.1.3. *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

$$\varphi(m+kd) - \varphi(m) = k\,(\varphi(m+d) - \varphi(m))\,. \tag{14}$$

(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

$$\varphi\left(\frac{m+n}{2}\right) = \frac{\varphi(m) + \varphi(n)}{2}\,. \tag{15}$$

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

Pour montrer l'implication $(ii) \Rightarrow (iii)$, 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 $\varphi(m) - \varphi(r) = q\,(\varphi(r+d) - \varphi(r))$. Il vient alors :

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

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.

L'implication $(iv) \Rightarrow (i)$ résulte de la congruence $m + d \equiv m - d \bmod 2d$. □

Les deux lemmes suivants sont des conséquences immédiates des relations (14) et (15).

Lemme 3.1.4. *Soit $d \geq 1$ et $k \geq 1$ deux entiers naturels. Alors $\mathrm{QA}_d \subset \mathrm{QA}_{kd}$.*

Lemme 3.1.5. *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 3.1.6. 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.

3.1.2 Forme explicite d'une application quasi-affine

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

Proposition 3.1.7. *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 $\boldsymbol{a} = (a_i)_{0 \leq i < d} \in \mathbb{Z}^d$, $\boldsymbol{b} = (b_i)_{0 \leq i < d} \in \mathbb{Z}^d$, telles que*

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

   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

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

entraine 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 (14) :

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

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

Définition 3.1.8. Pour toute application quasi-affine φ, la donné du triplet $(d, \mathbf{a}, \mathbf{b})$ constitué de la largeur d et des suites finies $\mathbf{a} = (a_i)_{0 \le i < d} \in \mathbb{Z}^d$ et $\mathbf{b} = (b_i)_{0 \le i < d} \in \mathbb{Z}^d$ de la proposition 3.1.7 est appelé une *présentation* de φ. La suite finie $\mathbf{a} \in \mathbb{Z}^d$ est appelée le *rapport* de la présentation.

Remarque 3.1.9. 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 3.1.4, 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 3.1.7 sont uniquement déterminées : en effet, on a toujours $a_r = \varphi(r+d) - \varphi(r)$ et $b_r = \varphi(r)$ quelque soit l'entier $r \in [0..d[$.

3.2 Composition d'applications quasi-affines

Théorème 3.2.1. *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 2.3.3. □

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

Proposition 3.2.2. *Soit φ une application quasi-affine de présentation $(d, \boldsymbol{a}, \boldsymbol{b})$, et φ' une application quasi-affine de présentation $(d', \boldsymbol{a}', \boldsymbol{b}')$. Alors une présentation de l'application $\varphi'' = \varphi \circ \varphi'$ est le triplet $(dd', \boldsymbol{a}'', \boldsymbol{b}'')$, où $\boldsymbol{a}'' \in \mathbb{Z}^{dd'}$ et $\boldsymbol{b}'' \in \mathbb{Z}^{dd'}$ sont les suites, indexées par l'ensemble des entiers naturels plus petits que dd', données par*

$$\forall k \in \left[0..dd'\right[, \quad a''_k = a_{u(k)} a'_{s(k)} \quad \text{et}$$
$$b''_k = a_{u(k)} \left\lfloor \frac{a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)}}{d} \right\rfloor + b_{u(k)}, \quad (16)$$

avec

$$\forall k \in \left[0..dd'\right[, \; s(k) = d' \left\{ \frac{k}{d'} \right\} \quad \text{et} \quad u(k) = d \left\{ \frac{a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)}}{d} \right\}. \quad (17)$$

Démonstration. D'aprés le théoréme 3.2.1, l'application φ'' est quasi-affine de largeur dd' . La proposition 3.1.7 montre qu'il existe deux suites $\mathbf{a}'' = \left(a''_k\right)_{0 \le k < dd'}$ et $\mathbf{b}'' = \left(b''_k\right)_{0 \le k < dd'}$ d'entiers rationnels telles que

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

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

$$a''_k = \varphi''(k + dd') - \varphi''(k) \quad (18)$$

et

$$b''_k = \varphi''(k). \quad (19)$$

En appliquant la formule (14) à l'application quasi-affine φ' de largeur d', on a :

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

Par hypothèse

$$\varphi'(k) = a'_{s(k)} \left\lfloor \frac{k}{d'} \right\rfloor + b'_{s(k)} . \tag{20}$$

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 (14) 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

$$\varphi\left(\varphi'(k)\right) = a_{r(\varphi'(k))} \left\lfloor \frac{\varphi'(k)}{d} \right\rfloor + b_{r(\varphi'(k))} \tag{21}$$

et de même $\varphi\left(\varphi'(k)+d\right) = a_{r(\varphi'(k)+d)} \left\lfloor \frac{\varphi'(k)+d}{d} \right\rfloor + b_{r(\varphi'(k)+d)}$. Comme $r(\varphi'(k)+d) = r(\varphi'(k))$, et que l'équation (20) 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'aprés la relation (18), l'égalité $a''_k = a_{u(k)} a'_{s(k)}$ qu'on voulait montrer. En outre, la relation (21) 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 (20), on obtient, compte tenu de (19), l'expression voulue de b''_k. □

Remarque 3.2.3. On pourra comparer notre résultat à l'énoncé donné par [3, 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' ériture de b''_k.

Remarque 3.2.4. Introduisons le magma P*QA* d'ensemble sous-jacent $\coprod_{d\geq 1}\mathbb{Z}^{2d} = \cup_{d\geq 1}\{d\}\times\mathbb{Z}^{2d}$, 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 (16) et (17). En notant $\mathbb{N}^*$ le monoïde multiplicatif des entiers naturels non nuls, l'application de P*QA* dans $\mathbb{N}^*$ qui associe l'entier d à tout élément de $\mathbb{Z}^{2d}$ est un morphisme de magmas, et la proposition 3.2.2 signifie que l'application de P*QA* dans le monoïde Q*A* 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 3.1.7 est aussi un morphisme de magmas. Par conséquent, on a un morphisme de P*QA* dans $\mathbb{N}^*\times$ Q*A*. Ce morphisme est injectif d'aprés la remarque 3.1.9 ; en particulier, le magma P*QA* est un monoïde qui admet Q*A* comme un quotient.

3.3 Changement de présentations

3.3.1 Présentations équivalentes

Nous allons maintenant expliciter la relation d'équivalence sur le monoïde P*QA* par laquelle on quotiente pour obtenir Q*A*, 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 3.3.1. *On se donne deux entiers naturels $d\geq 1$ et $d'\geq 1$, et des suites finies $\boldsymbol{a}\in\mathbb{Z}^d,\boldsymbol{b}\in\mathbb{Z}^d,\boldsymbol{a}'\in\mathbb{Z}^{d'},\boldsymbol{b}'\in\mathbb{Z}^{d'}$. On note q le plus grand commun diviseur des entiers d et d'. Pour que les triplets $(d,\boldsymbol{a},\boldsymbol{b})$ et $(d',\boldsymbol{a}',\boldsymbol{b}')$ 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*

$$d'a_r = da'_{r'} \qquad et \qquad d(b_r - b'_{r'}) = a_r(r-r')\,.$$

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 :

$$\begin{aligned}\varphi(m) &= a_{r(m)} \left\lfloor \frac{m}{d} \right\rfloor + b_{r(m)} \\ &= a_{r(m)} \left(\frac{m}{d} - \left\{ \frac{m}{d} \right\} \right) + b'_{r'(m)} + \frac{a_{r(m)}}{d} (r(m) - r'(m)) \,. \quad (22)\end{aligned}$$

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'aprés la proposition 3.1.3, 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 3.1.3, 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

$$\begin{aligned} d'a_r &= d'(\varphi(r+d) - \varphi(r)) = c_1(r)dd' = dc_1(r')d' \\ &= d(\varphi(r'+d') - \varphi(r')) = da'_{r'} \end{aligned}$$

D'autre part :

$$\begin{aligned} d(b_r - b'_{r'}) &= d(\varphi(r) - \varphi(r')) = dc_1(r)(r - r') \\ &= (\varphi(r+d) - \varphi(r))(r - r') = a_r(r - r') \end{aligned}$$

□

3.3.2 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 3.3.2. 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 3.1.7 est appelée la *forme réduite* de φ.

Puisque $\mathbb{Z}$ est un anneau principal, la proposition 3.1.3 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 3.3.3. *Soit $(d, \boldsymbol{a}, \boldsymbol{b})$ 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 $\boldsymbol{a}$ et vérifiant de plus :*

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

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

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

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

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

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

$$a_{r+d'} = qa'_{r'} = a_r\ .$$

D'autre part :

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

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 $(0 \leq r < d)$, et que soient vérifiées les égalités

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

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

$$da'_{r'} = d'qa'_{r'} = d'a_{r'} = d'a_r$$

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

Exemple 3.3.4. 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 3.3.3 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 $d' = 3$.

4 Endomorphismes continus de l'algèbre des suites bi-infinies

Nous commençons par décrire la structure de l'ensemble de toutes les suites bi-infinies à coefficients dans un anneau fixé A : ces suites forment une algèbre $S_{\mathbb{Z}}(A)$ pour le produit de Hadamard. Le sous-ensemble $r_{\mathbb{Z}}(A)$ de $S_{\mathbb{Z}}(A)$, dont les éléments sont les suites récurrentes linéaires (ou reconnaissables) bi-infinies est une sous-algèbre dense de $S_{\mathbb{Z}}(A)$. On caractérise les séries génératrices des suites éléments de $r_{\mathbb{Z}}(A)$. Enfin, nous caractérisons les endomorphismes continus de l'algèbre $r_{\mathbb{Z}}(A)$, lorsque l'anneau A est une $\mathbb{Q}$-algèbre de caractéristique nulle qui est de Fatou au sens de Benzaghou, c'est-à-dire qui est un anneau complètement intégralement clos (théorème 4.3.5).

Dans le présent chapitre, le terme anneau est utilisé pour « anneau commutatif unifère ». L'élément unité d'un anneau A est noté 1_A ou simplement 1. 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.

4.1 L'algèbre des suites bi-infinies

4.1.1 Anneau produit

Soit A un anneau. On identifie le produit $A^{\mathbb{Z}}$ à l'ensemble de toutes les applications de $\mathbb{Z}$ dans A, c'est-à-dire l'ensemble de toutes les suites bi-infinies dont tous les termes sont éléments de A ; une telle suite bi-infinie est appelée pour abréger une *suite bi-infinie sur*

A. On note T_A l'application *décalage* de $A^{\mathbb{Z}}$ dans $A^{\mathbb{Z}}$ telle que

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

Définition 4.1.1. 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 1_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 4.1.2. *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.

Définition 4.1.3. La A-algèbre $S_{\mathbb{Z}}(A)$ est appelée l'*algèbre des suites bi-infinies sur A.*

4.1.2 Topologie produit

L' algèbre $S_{\mathbb{Z}}(A)$ est 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. Cette topologie produit est compatible avec les opérations algébriques de $S_{\mathbb{Z}}(A)$; elle possède les deux propriétés suivantes.

Proposition 4.1.4. *L' anneau produit $S_{\mathbb{Z}}(A)$ est un anneau topologique complet.*

Démonstration.[11, Théorèm 8.3.9]

Proposition 4.1.5. *L'anneau produit $S_{\mathbb{Z}}(A)$ est métrisable.*

Démonstration.[20, 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.

Définition 4.1.6. L'application $\mathscr{R}_A$ de $S_{\mathbb{Z}}(A)$ envoyant toute suite bi-infinie à son reflet est appelée *application réflexion en A*.

Proposition 4.1.7. *L'application réflexion en A est un automorphisme bicontinu de la A-algèbre $S_{\mathbb{Z}}(A)$.*

Démonstration. On a clairement $\kappa_{m,A} \circ \mathscr{R}_A = \kappa_{-m,A}$ pour tout $m \in \mathbb{Z}$, ce qui prouve que l'application $\mathscr{R}_A : S_{\mathbb{Z}}(A) \to S_{\mathbb{Z}}(A)$ est continue. Puisqu'elle est aussi involutive, elle est donc bicontinue. Il est facile de vérifier qu'elle est aussi un endomorphisme de la A-algèbre $S_{\mathbb{Z}}(A)$. □

4.2 Suites récurrentes linéaires

Parmi toutes les suites bi-infinies, nous nous intéresserons plus spécialement à celles qui satisfont une récurrence linéaire non triviale à coefficients constants. Nous caractériserons également leurs couples de séries génératrices. Nous verrons que certaines constructions simples préservent l'ensemble des suites bi-infinies satisfaisant de telles récurrences.

4.2.1 Définitions et propriétés

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

Définition 4.2.1. 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 4.2.2. 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], nous allons 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.

Proposition 4.2.3. *Une suite bi-infinie u sur A est récurrente linéaire si et seulement si il existe un sous-A-module de type fini de $S_{\mathbb{Z}}(A)$ qui comprend la suite u, et est stable par le décalage T_A.*

Démonstration. Soit u une suite bi-infinie sur A récurrente linéaire ; il existe un entier $h \in \mathbb{N}^*$ et des constantes $\alpha_i \in A$, pour $i \in [1..h]$, tels que

$$\forall m \in \mathbb{Z}, \quad u(m+h) = \alpha_1 u(m+h-1) + \cdots + \alpha_h u(m).$$

Ainsi, on peut écrire

$$T_A^h u(m) = \alpha_1 T_A^{h-1} u(m) + \cdots + \alpha_h u(m). \tag{23}$$

On considère le sous-A-module M de $S_{\mathbb{Z}}(A)$ engendré par les suites $u, T_A u, \cdots, T_A^{h-1} u$. Vérifions que le sous-A-module M est stable par l'application décalage. En effet, soit N l'image réciproque de M par le décalage T_A : comme ce décalage est une application A-linéaire, l'ensemble N est un sous-A-module de $S_{\mathbb{Z}}(A)$, qui comprend par définition les suites u, $T_A u, \ldots, T_A^{h-2} u$, mais qui comprend aussi $T_A^{h-1} u$ en vertu de la relation (23). Par conséquent, le sous-module M est contenu dans N, c'est-à-dire que $T_A(M) \subseteq M$.

Réciproquement, supposons qu'il existe un sous-A-module M de type fini de $S_{\mathbb{Z}}(A)$ stable par le décalage et comprenant la suite u. Alors il existe une suite finie $(\vartheta_i)_{i \in [1..d]}$ d'éléments de $S_{\mathbb{Z}}(A)$, dont les éléments engendrent le sous-A-module M. Comme u et chacune

des suites $T_A\vartheta_i$ sont des éléments du sous-A-module M, il existe des constantes éléments de A, λ_{ij}, pour tout $i \in [1..d]$ et $j \in [1..d]$, et ν_i, pour tout $i \in [1..d]$, telles que

$$T_A\vartheta_i = \sum_{j=1}^{d} \lambda_{ij}\vartheta_j \quad \text{et} \quad u = \sum_{i=1}^{d} \nu_i\vartheta_i.$$

Considérons A' le plus petit sous-anneau de A contenant les ν_i et les λ_{ij}, ainsi A' est un anneau noethérien du fait qu'il est de type fini. Soit M' le sous-A'-module de M engendré par $\vartheta_1, \cdots, \vartheta_d$. Par définition de A', on vérifie que $u \in M'$ car les ν_i sont des éléments de A'. Vérifions que M' est stable par T_A, soit $\omega \in M'$, c'est-à-dire $\omega = \sum_{j=1}^{d} a_j\vartheta_j$, avec $a_j \in A'$, alors

$$T_A\omega = \sum_{j=1}^{d} a_j T_A\vartheta_j = \sum_{j=1}^{d} a_j \sum_{k=1}^{d} \lambda_{jk}\vartheta_k = \sum_{j=1}^{d}\sum_{k=1}^{d} a_j\lambda_{jk}\vartheta_k = \sum_{k=1}^{d} \beta_k\vartheta_k,$$

où $\beta_k = \sum_{j=1}^{d} a_j\lambda_{jk} \in A'$. Ainsi on conclut que $T_A\omega \in M'$.
Construisons la suite croissante de sous- A'-modules $(N_i)_{i\geq 1}$ de M', telle que, pour tout entier naturel $i \geq 1$, le sous-A'-module N_i est engendré par $u, T_Au, T_A^2u, \cdots, T_A^{i-1}u$. Du fait que le sous-$A'$-module M' comprend la suite u et est stable par T_A, on a bien $N_i \subseteq M'$. Comme A' est un anneau noetherien, et que M' est un A'-module de type fini, il existe un entier naturel $i \geq 1$ tel que $N_i = N_{i+1}$. En particulier $T_A^i u \in N_{i+1} = N_i$, ainsi il existe une suite finie $\left(\alpha_j\right)_{0\leq j<i}$ d'éléments de A' telle que $T_A^i u = \sum_{j=0}^{i-1} \alpha_j T_A^j u$. Ceci implique que le polynôme unitaire $X^i - \sum_{j=0}^{i-1} \alpha_j X^j$ appartient à l'annulateur de la suite u. □

Théorème 4.2.4 (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 T_A.*

Démonstration. Soit u, v deux suites récurrentes linéaires. D'aprés la proposition 4.2.3, il existe M et N deux sous-A-modules de type fini de $S_{\mathbb{Z}}(A)$, comprenant respectivement u et v, qui sont stables par le décalage T_A.

On peut alors introduire la somme $M+N$, dont on vérifie immédiatement que c'est un sous-A-module de $S_{\mathbb{Z}}(A)$, de type fini et stable par T_A. Puisque $u+v$ est élément de $M+N$, la proposition 4.2.3 montre que $u+v$ est une suite récurrente linéaire.

De manière analogue, introduisons le produit MN, défini comme le sous-A-module de l'algèbre $S_{\mathbb{Z}}(A)$ qui est engendré par les produits d'un élément de M par un élément de N. Si le A-module M est engendré par une famille finie $(m_1,\dots,m_r)$, alors que le A-module N est engendré par une autre famille finie $(n_1,\dots,n_s)$, on voit que MN est engendré par les produits $m_i n_j$, avec $1\leq i\leq r$ et $1\leq j\leq s$, de sorte que MN est de type fini dès que M et N le sont. De plus, le produit MN est stable par T_A, car, puisque T_A est un endomorphisme de l'algèbre $S_{\mathbb{Z}}(A)$ et que M et N sont stables par décalage, le sous-A-module $T_A^{-1}(MN)$ comprend tous les produits d'un élément de M par un élément de N. Ainsi MN est un sous-A-module de type fini de $S_{\mathbb{Z}}(A)$, stable par décalage et comprenant le produit uv. De ce fait, en vertu de la proposition 4.2.3, le produit uv est une suite récurrente linéaire.

De plus, pour tout $a\in A$, la suite $\iota_A(a)=(a)_{m\in\mathbb{Z}}$, étant constante, est évidemment récurrente linéaire, de sorte que $r_{\mathbb{Z}}(A)$ est bien une sous-A-algèbre de $S_{\mathbb{Z}}(A)$.

Enfin, puisque M est stable par le décalage T_A, la suite $T_A(u)$ est élément du sous-A-module de type fini M de $S_{\mathbb{Z}}(A)$, et est stable par décalage. Donc, la proposition 4.2.3 entraîne que $T_A(u)$ est une suite récurrente linéaire. Ainsi $r_{\mathbb{Z}}(A)$ est stable par décalage. □

Définition 4.2.5. Nous appelons cette sous-algèbre $r_{\mathbb{Z}}(A)$ l'*algèbre des suites bi-infinies reconnaissables sur A*.

Proposition 4.2.6. *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 4.2.7. Cette preuve montre en fait un énoncé plus fort : l'ensemble des suites bi-infinies périodiques est dense dans $S_{\mathbb{Z}}(A)$.

4.2.2 Séries génératrices de suites reconnaissables

Lemme 4.2.8. *Soit A un anneau intègre où 2 est inversible. Si u est une suite bi-infinie sur A dont l'annulateur contient un polynôme non nul (en particulier, si u est reconnaissable), alors sa première série génératrice $F_+(u)$ est une fraction rationnelle n'ayant de pôle ni en zéro, ni à l'infini.*

Démonstration. Par hypothèse, la suite u admet dans son annulateur un élément non nul $q(x)$ qu'on peut choisir de degré minimal h. Comme le décalage $T_A : S_{\mathbb{Z}}(A) \to S_{\mathbb{Z}}(A)$ est bijectif, la minimalité du degré de q impose alors que $q(0) \neq 0$. Introduisons le polynôme réciproque $q^*(t) = t^h q(t^{-1})$ de $q(t)$: c'est un polynôme de degré h car $q(0) \neq 0$, et son terme constant est non nul. Comme $q(T_A)(u) = 0$, on sait par la proposition 1.2.5 que la série $q^*(t)F_+(u)$ est un polynôme de degré au plus h. Par conséquent $F_+(u)$ est le quotient des deux polynômes $q^*(t)F_+(u)$ et $q^*(t)$, c'est-à-dire une fraction rationnelle. Cette fraction rationnelle n'a pas de pôle en zéro car $q^*(0) \neq 0$, et non plus de pôle à l'infini, car le degré du numérateur $q^*(t)F_+(u)$ est au plus égal au degré h du dénominateur $q^*(t)$. □

Lemme 4.2.9. *Soit A un anneau intègre où 2 est inversible. Si u est une suite bi-infinie sur A dont l'annulateur contient un polynôme non nul (en particulier, si u est reconnaissable), alors ses deux séries génératrices $F_+(u)$ et $F_-(u)$ sont des fractions rationnelles satisfaisant l'identité*

$$F_+(u)(t) + F_-(u)(t^{-1}) = 0\,. \tag{24}$$

Démonstration. D'après le lemme précédent, on sait que $F_+(u)$ est une fraction rationnelle. Il en est de même de $F_-(u) = F_+(\widehat{u})$, car l'annulateur de la suite reflet $\widehat{u}$ comprend le polynôme réciproque d'un polynôme non nul dans l'annulateur de u. Soit $q(t)$ un élément

non nul de l'annulateur de u, et notons h le degré de $q(t)$. D'après la proposition 1.2.5, les séries

$$L_+(t) = q^*(t)F_+(u) \qquad \text{et } L_-(t) = q(t)F_-(u)$$

sont des polynômes de degré au plus h. Comme $q(T_A)(u)$ est la suite nulle, la proposition 1.2.6 entraîne que, pour tout indice $j \in [0..h]$, le coefficient de t^{h-j} dans le polynôme $L_+(t)$ est l'opposé du coefficient de t^j dans $L_-(t)$. Par conséquent, on a l'identité $L_+(t) = -t^h L_-(t^{-1})$. D'où

$$F_+(u) = \frac{L_+(t)}{q^*(t)} = -\frac{t^h L_-(t^{-1})}{t^h q(t^{-1})} = -\frac{L_-(t^{-1})}{q(t^{-1})} = -F_-(u)(t^{-1})\,.$$

□

Lorsque l'anneau A est un corps $\mathbb{K}$ 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 4.2.10. *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. *les séries génératrices $F_+(u)$ et $F_-(u)$ sont des fractions rationnelles de degré négatif ou nul, tel que la série $F_+(u)$ n'a pas de pôle en zéro et $F_-(u)(t^{-1}) = -F_+(u)(t)$;*
3. *il existe un entier naturel d, d éléments $\alpha_1, ..., \alpha_d$ non nuls de $\mathbb{K}$, et d polynômes $p_1, ..., p_d$ à coefficients dans $\mathbb{K}$, tels que*

$$\forall m \in \mathbb{Z}, \qquad u(m) = \sum_{i=1}^{d} p_i(m)\alpha_i^m. \tag{25}$$

Démonstration. L'implication $1 \Rightarrow 2$, est une conséquence des lemmes 4.2.8 et 4.2.9.

Afin de montrer l'implication $2 \Rightarrow 3$, on se donne une suite bi-infinie u dont la première série génératrice

$$F_+(u)(t) = \frac{u(0)}{2} + \sum_{n\geq 1} u(n)t^n$$

est une fraction rationnelle ne présentant de pôle ni en zéro, ni à l'infini, et dont la deuxième série génératrice $F_-(u)(t) = \frac{u(0)}{2} + \sum_{n\geq 1} u(-n)t^n$ est aussi une fraction rationnelle telle que $F_-(u)(t) = -F_+(u)(t^{-1})$. Il existe donc un polynôme $Q(t) \in \mathbb{K}[t]$ ne s'annulant pas en zéro tel que la série entière formelle $Q(t)F_+(t)$ soit un polynôme n'ayant avec $Q(t)$ aucune racine commune. Comme $\mathbb{K}$ est supposé algébriquement clos, le polynôme $Q(t)$ se factorise dans $\mathbb{K}[t]$ sous la forme

$$Q(t) = Q(0)\prod_{i=1}^{d}(1-\alpha_i t)^{n_i} ,$$

où la constante $Q(0) \in \mathbb{K}$ est non nulle, d est un entier naturel, les éléments $\alpha_1, \cdots, \alpha_d$ de $\mathbb{K}$ sont deux à deux distincts, et les exposants $n_1, \cdots, n_d$ sont des entiers naturels non nuls. Comme on sait de plus que la fraction $F_+(u)$ n'a pas de pôle à l'infini, il en résulte que la fraction rationnelle $F_+(u)$ se décompose en éléments simples sous la forme

$$F_+(u)(t) = F_+(u)(+\infty) + \sum_{i=1}^{d}\sum_{j=1}^{n_i}\frac{a_{i,j}}{(1-\alpha_i t)^j} ,$$

où les constantes $a_{i,j}$ sont éléments de $\mathbb{K}$.

En particulier, pour $t = 0$, on a

$$\frac{u(0)}{2} = F_+(u)(0) = F_+(u)(+\infty) + \sum_{i=1}^{d}\sum_{j=1}^{n_i} a_{i,j} .$$

Or, d'après l'hypothèse liant $F_+(u)$ et $F_-(u)$, on a

$$F_+(u)(+\infty) = -F_-(u)(0) = -\frac{u(0)}{2},$$

ainsi

$$F_+(u)(+\infty) = -\frac{1}{2}\sum_{i=1}^{d}\sum_{j=1}^{n_i} a_{i,j},$$

c'est-à-dire

$$F_+(u)(t) = \sum_{i=1}^{d}\sum_{j=1}^{n_i} a_{i,j}\left[\frac{1}{(1-\alpha_i t)^j} - \frac{1}{2}\right].$$

On connaît le développement en série entière formelle

$$(1-\alpha_i t)^{-j} = \sum_{n=0}^{+\infty} \binom{n+j-1}{j-1} \alpha_i^n t^n .$$

Par identification des coefficients, on en déduit que, pour tout entier naturel n, on a

$$u(n) = \sum_{i=1}^{d} \sum_{j=1}^{n_i} a_{i,j} \binom{n+j-1}{j-1} \alpha_i^n .$$

D'autre part la relation $F_+(u)(t^{-1}) = -F_-(u)(t)$ nous permet d'écrire

$$\begin{aligned} F_-(u)(t) &= \sum_{i=1}^{d} \sum_{j=1}^{n_i} a_{i,j} \left[\frac{1}{2} - \frac{1}{(1-\alpha_i t^{-1})^j} \right] \\ &= \sum_{i=1}^{d} \sum_{j=1}^{n_i} a_{i,j} \left[\frac{1}{2} - \left(\frac{t}{t-\alpha_i} \right)^j \right] . \end{aligned}$$

Or, on a dans $\mathbb{K}[\![t]\!]$ l'égalité

$$\left(\frac{t}{t-\alpha_i} \right)^j = -\sum_{n\geq 1} \binom{j-n-1}{j-1} \alpha_i^{-n} t^n ,$$

d'où par identification

$$\forall n \in \mathbb{N}^*, \qquad u(-n) = \sum_{i=1}^{d} \sum_{j=1}^{n_i} a_{i,j} \binom{j-n-1}{j-1} \alpha_i^{-n} .$$

Finalement, on a montré que, pour tout entier $m \in \mathbb{Z}$, on a

$$u(m) = \sum_{i=1}^{d} \sum_{j=1}^{n_i} a_{i,j} \binom{m+j-1}{j-1} \alpha_i^m .$$

Comme $\mathbb{K}$ est supposé de caractéristique nulle, on peut considérer le coefficient binomial $\binom{m+j-1}{j-1}$ comme un polynôme en m de degré $j-1$, on a donc une expression de la forme voulue pour $u(m)$.

Pour montrer $3 \Rightarrow 1$, et comme on sait que $r_{\mathbb{Z}}(\mathbb{K})$ est une $\mathbb{K}$-algèbre, il suffit de vérifier, d'une part, que les suites géométriques $(\alpha^m)_{m\in\mathbb{Z}}$, où $\alpha \in \mathbb{K}^*$, sont récurrentes linéaires, et d'autre part, que la suite $(m)_{m\in\mathbb{Z}}$ l'est aussi. Or, d'une part, le polynôme $X-\alpha$ est élément de l'idéal annulateur de la suite $(\alpha^m)_{m\in\mathbb{Z}}$, et, d'autre part $(X-1)^2$ est élément de l'idéal annulateur de la suite $(m)_{m\in\mathbb{Z}}$. □

4.2.3 Anneaux de Fatou

Définition 4.2.11. Si K est un corps, on appelle *fraction normalisée sur K* un couple $(P(X), Q(X))$ de polynômes à coefficients dans K, tel que (i) l'idéal de $K[X]$ engendré par ces polynômes est $K[X]$ tout entier ; (ii) $\deg(P) < \deg(Q)$; (iii) $Q(0) = 1$.

Proposition 4.2.12. *Soit A un anneau intègre de corps de fractions K. les deux propriétés suivantes sont équivalentes :*

1. *Pour toute fraction normalisée $(P(X), Q(X))$ sur K, si tous les coefficients du développement en série à l'origine du quotient $P(X)/Q(X)$ sont éléments de A, alors les coefficients de $Q(X)$ sont eux aussi dans A.*
2. *Si une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A vérifie une relation de récurrence de la forme*

$$\forall n \in \mathbb{N}, \quad u(n+h) = \alpha_1 u(n+h-1) + \cdots + \alpha_h u(n), \quad (26)$$

où les coefficients α_i sont éléments de K et où l'ordre h de la récurrence est minimal, alors les α_i sont éléments de A.

Démonstration. Montrons l'implication $1 \Rightarrow 2$. Pour ce faire, on se donne une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A et une liste finie $(\alpha_1, \ldots, \alpha_h)$ d'éléments de K satisfaisant la relation (26), et on suppose que l'entier h est minimal parmi les ordres de telles relations de récurrences vérifiées par la suite $(u_n)_{n\in\mathbb{N}}$. Considérons la série formelle $F(X) = \sum_{n\geq 0} u_n X^n \in A[[X]]$ et le polynôme unitaire $Q(X) = X^h - \alpha_1 X^{h-1} - \cdots - \alpha_h$, à coefficients dans K. Le polynôme réciproque $Q^*(X) = X^h Q(X^{-1})$ de $Q(X)$ est alors $Q^*(X) = 1 - \alpha_1 X - \alpha_2 X^2 - \cdots - \alpha_h X^h$. Alors $P(X) = Q^*(X)F(X)$ est un polynôme de degré $< h$.

L'idéal engendré par les polynômes $P(X)$ et $Q^*(X)$ est $K[X]$, car si $P(X) = D(X)P_1(X)$ et $Q^*(X) = D(X)G(X)$, avec $\deg D \geq 1$, on aura $G(X)F(X) = P_1(X)$, où $h_1 = \deg P_1 < \deg P < h$, ce qui montre que la suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A vérifie une relation de récurrence d'ordre h_1, ce qui est impossible puisque l'ordre h est supposé minimal. Comme $Q^*(0) = 1$, on voit que le couple $(P(X), Q^*(X))$ est une fraction normalisée. L'hypothèse entraîne alors que les coefficients du polynôme $Q^*(X)$ sont éléments de A, ce qu'il fallait montrer.

Réciproquement, soit $(P(X), Q(X))$ une fraction normalisée sur K, telle que tous les coefficients u_n du développement en série à l'origine du quotient

$$\frac{P(X)}{Q(X)} = \sum_{n\geq 0} u_n X^n$$

sont éléments de A. Soit h le degré du polynôme $Q(X)$. Comme $Q(X)\sum_{n\geq 0} u_n X^n$ est un polynôme de degré moindre que h, on voit que la suite $(u_n)_{n\in\mathbb{N}}$ satisfait la récurrence

$$\forall n \in \mathbb{N}, \qquad u_{n+h} = \alpha_1 u_{n+h-1} + \cdots + \alpha_h u_n \ ,$$

où $Q(X) = 1 - \alpha_1 X - \cdots - \alpha_h X^h$. Comme les polynômes $P(X)$ et $Q(X)$ n'ont pas de diviseur commun dans $K[X]$, on peut affirmer que h est l'ordre minimal d'une relation de récurrence satisfaite par la suite $(u_n)_{n\in\mathbb{N}}$. Par hypothèse, on conclut que tous les coefficients de $Q(X)$ sont dans A. □

La définition suivante, qui se trouve dans [8], est due en essence à Benzaghou [4].

Définition 4.2.13. Un anneau intègre A de corps de fractions K est dit de *Fatou* au sens de Benzaghou, lorsqu'une des propriétés de la proposition 4.2.12 est satisfaite.

Fatou [13] a démontré que $\mathbb{Z}$ l'anneau des entiers rationnels possède la proporiété 1 de la proposition 4.2.12.

La définition qui suit est celle donnée dans Bourbaki [6, p. 16].

Définition 4.2.14. Un anneau A est dit *complètement intégralement clos* s'il est intègre, et si la condition suivante est vérifiée : si un élément x du corps des fractions K de A est tel que toutes les puissances x^n, où $n \in \mathbb{N}$, soient contenues dans un sous-A-module de type fini de K, alors x appartient à A.

Notons qu'un anneau *complètement intégralement clos* est un anneau intégralement clos.

On sait que l'anneau $\mathbb{Z}$ des entiers rationnels est un anneau complètement intégralement clos. D'autres exemples d'anneaux complètement intégralement clos sont les anneaux de polynômes $A[X_1,$

$\cdots, X_n]$ ou les anneaux de séries entières formelles $A[[X_1, \cdots, X_n]]$, à condition que l'anneau de base A soit lui-même complètement intégralement clos [6, p. 16-17]. On a aussi l'exemple des anneaux d'entiers des corps de nombres :

Proposition 4.2.15. *Si K est une extension finie de $\mathbb{Q}$, alors son anneau des entiers $\mathcal{O}_K$ est un anneau complètement intégralement clos.*

Démonstration. [4, p.225]

Proposition 4.2.16. *Un anneau intègre est de Fatou si et seulement si il est complètement intégralement clos.*

Démonstration. [8]

Si A est un anneau, nous utiliserons la notation $S_{\mathbb{N}}(A)$ pour désigner la A-algèbre de Hadamard dont les éléments sont les suites $(u_n)_{n\in\mathbb{N}}$ d'éléments de A indexées par $\mathbb{N}$. Parmi ces suites, la sous-algèbre des suites satisfaisant une relation de récurrence linéaire telle que (26) est notée $r_{\mathbb{N}}(A)$. Lorsque l'anneau A est factoriel, la condition 2 de la proposition 4.2.12 peut se traduire par l'énoncé suivant.

Proposition 4.2.17. *Si un anneau intègre A de corps de fractions K est de Fatou, alors toute suite indexée par $\mathbb{N}$ récurrente linéaire sur K à valeurs dans A, est récurrente linéaire sur A; c'est -à-dire :*

$$r_{\mathbb{N}}(A) = r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A).$$

Réciproquement, si l'anneau A est factoriel et si $r_{\mathbb{N}}(A) = r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$, alors l'anneau A est de Fatou.

Démonstration. Supposons la condition 2 de la proposition 4.2.12 satisfaite et soit $u \in r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$. L'anneau $K[X]$ étant principal, il existe dans l'idéal annulateur de u un polynôme unitaire de degré minimal. D'après la condition 2, ce polynôme est à coefficients dans A, ainsi $u \in r_{\mathbb{N}}(A)$, ceci implique que l'intersection $r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$ est contenue dans $r_{\mathbb{N}}(A)$; l'inclusion réciproque étant immédiate, on a bien $r_{\mathbb{N}}(A) = r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$.
Réciproquement, supposons l'anneau A factoriel tel que $r_{\mathbb{N}}(A) =$

$r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$. On se donne une suite $u = (u_n)_{n\in\mathbb{N}}$ à valeurs dans A, et des éléments $\alpha_1, \cdots, \alpha_h$ de K en nombre fini h, tels que

$$\forall n \in \mathbb{N}, \qquad u_{n+h} = \alpha_1 u_{n+h-1} + \cdots + \alpha_h u_n,$$

et on suppose que l'ordre h de cette relation de récurrence est minimal. On voit que u est élément de l'intersection $r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$; par hypothèse, ceci entraîne que u est élément de $r_{\mathbb{N}}(A)$, c'est-à-dire qu'il existe un polynôme unitaire $P(X) = X^\ell - \beta_1 X^{\ell-1} - \cdots - \beta_\ell \in A[X]$ tel que

$$\forall n \in \mathbb{N}, \qquad u_{n+\ell} = \beta_1 u_{n+\ell-1} + \cdots + \beta_\ell u_n.$$

Considérons le polynôme $Q(X) = X^h - \alpha_1 X^{h-1} - \cdots - \alpha_h$ élément de $K[X]$. Par division euclidienne dans $K[X]$ de $P(X)$ par $Q(X)$, on obtient un reste $R(X) = \gamma_0 X^k - \gamma_1 X^{k-1} - \cdots - \gamma_k \in K[X]$ de degré $k < h$, tel que, si $R(X) \neq 0$, on aurait

$$\forall n \in \mathbb{N}, \qquad u_{n+k} = \frac{\gamma_1}{\gamma_0} u_{n+k-1} + \cdots + \frac{\gamma_k}{\gamma_0} u_n,$$

avec $k < h$. Par minimalité de h, on voit que $R(X) = 0$, ce qui prouve que $Q(X)$ est un diviseur de $P(X)$ dans l'anneau $K[X]$. Donc il existe $G(X) \in K[X]$ tel que $P(X) = Q(X)G(X)$. Puisque l'anneau A est factoriel, il existe un élément d non nul de A tel que le polynôme $dG(X)$ est un polynôme primitif de $A[X]$, et de même il existe un élément d' non nul de A tel que le polynôme $d'Q(X)$ est un polynôme primitif de $A[X]$. Le polynôme $dd'P(X) = (d'Q(X))(dG(X))$ est alors le produit de deux polynômes primitifs de $A[X]$. D'après le lemme de Gauss, il en résulte que $dd'P(X)$ est un polynôme primitif de $A[X]$. Or les coefficients de $P(X)$ sont éléments de A. Par conséquent, l'élément dd', qui divise tous les coefficients du polynôme $dd'P(X)$, doit être inversible dans A, ce qui entraîne que d et d' sont tous deux inversibles de A, et donc $Q(X) = d'^{-1}(d'Q(X))$ est à coefficients dans A. □

Remarque 4.2.18. Si l'anneau A n'est plus supposé factoriel, il est possible qu'on ait l'égalité $r_{\mathbb{N}}(A) = r_{\mathbb{N}}(K) \cap S_{\mathbb{N}}(A)$ sans que A soit de Fatou. Un exemple est celui de l'anneau $\mathbb{Z}[i\sqrt{3}]$. En effet l'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel puisque $4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$. Il n'est pas non plus de Fatou , puisqu'il n'est pas intégralement

clos (proposition 4.2.16), car le polynôme X^2+X+1 est un polynôme unitaire de $\mathbb{Z}[i\sqrt{3}][X]$ n'ayant pas de racines dans $\mathbb{Z}[i\sqrt{3}]$, mais qui est scindé sur son corps de fractions $\mathbb{Q}(i\sqrt{3})$. Par contre $r_{\mathbb{N}}(\mathbb{Z}[i\sqrt{3}]) = r_{\mathbb{N}}(\mathbb{Q}(i\sqrt{3}))\cap S_{\mathbb{N}}(\mathbb{Z}[i\sqrt{3}])$. En effet, soit $u=(u(n))_{n\in\mathbb{N}}$ un élément de l'intersection $r_{\mathbb{N}}(\mathbb{Q}(i\sqrt{3}))\cap S_{\mathbb{N}}(\mathbb{Z}[i\sqrt{3}])$. Alors u est aussi élément de l'algèbre $S_{\mathbb{N}}(\mathbb{Z}[j])$, où $j=\frac{-1+i\sqrt{3}}{2}$. Or $\mathbb{Z}[j]$ est l'anneau des entiers du corps quadratique $\mathbb{Q}(i\sqrt{3})$, donc est de Fatou par la proposition 4.2.15. Par conséquent u est élément de $r_{\mathbb{N}}(\mathbb{Z}[j])$, ce qui signifie qu'il existe un polynôme unitaire $R(x)\in\mathbb{Z}[j][x]$ tel que $R(T)(u)=0$. Soit $\overline{R}(x)$ le polynôme obtenu à partir de $R(x)$ en remplaçant ses coefficients par leurs conjugués. Alors le polynôme produit $R(x)\overline{R}(x)$ est un polynôme unitaire à coefficients dans $\mathbb{Z}\subset\mathbb{Z}[i\sqrt{3}]$ qui est un polynôme annulateur de la suite u : ceci achève de montrer que u est élément de $r_{\mathbb{N}}(\mathbb{Z}[i\sqrt{3}])$.

Voici une propriété des anneaux de Fatou relative aux suites bi-infinies (indexées par $\mathbb{Z}$), qui est analogue à celle vérifiée dans le cas des suites récurrentes linéaires indexées par $\mathbb{N}$.

Proposition 4.2.19. *Soit A un anneau de Fatou où 2 est inversible, et K son corps de fractions. Alors toute suite bi-infinie indexée par $\mathbb{Z}$, récurrente linéaire sur K et à valeurs dans A, est une suite récurrente linéaire sur A.*

Démonstration. Soit u une suite bi-infinie indexée par $\mathbb{Z}$, récurrente linéaire sur K à valeurs dans A et $F_+(u)(t)$ sa première série génératrice. D'après le lemme 4.2.8, il existe deux polynômes $P(t), Q(t)$ premiers entre eux dans $K[t]$ tels que $Q(0)=1$ et

$$F_+(u)(t)=\frac{P(t)}{Q(t)}.$$

Posons h le degré du polynôme $Q(t)$, $Q^*(t)=t^hQ(t^{-1})$ son polynôme réciproque et $P^*(t)=t^hP(t^{-1})$. Ainsi, par le lemme 4.2.9, $F_-(u)(t)=-\frac{P^*(t)}{Q^*(t)}$. Soit les polynômes

$$L_+(t)=Q(t)F_+(u)(t)=P(t)\ ,\quad L_-(t)=Q^*(t)F_-(u)(t)=-P^*(t),$$

en vertu de la proposition 1.2.6, la somme du coefficient de t^{h-j} dans $L_+(t)$ et du coefficient t^j dans $L_-(t)$ est égale à $Q^*(T_A)(u)(-j)$.

Or, puisque $P^*(t) = t^h P(t^{-1})$, cette somme est nulle. Donc le polynôme $Q^*(t)$ est dans l'annulateur de u. En outre, toujours par le lemme 4.2.9, on a

$$F_+(u)(+\infty) = -F_-(u)(0) = -\frac{u(0)}{2} = \frac{cd(P(t))}{cd(Q(t))}.$$

Ainsi, le polynôme $G(t) \in K[t]$ défini par

$$G(t) = \frac{u(0)}{2} Q(t) + P(t),$$

est de degré inférieur à h. Par conséquent $(G(t), Q(t))$ est une fraction normalisée. Or

$$\frac{G(t)}{Q(t)} = F_+(u)(t) + \frac{u(0)}{2} = \sum_{n \geq 0} u_n t^n \, .$$

Comme la suite u est à valeurs dans l'anneau A qui est de Fatou, alors $Q(t) \in A[t]$. Par conséquent les coefficients de son polynôme réciproque $Q^*(t)$, qui sont ceux d'un polynôme annulateur de la suite u, sont aussi éléments de A. □

4.2.4 Constructions préservant la reconnaissabilité

4.2.4.1 Applications décalage et réflexion

Lemme 4.2.20. *Soit $u = (u(m))_{m \in \mathbb{Z}}$ 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 4.2.21. *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 $X^h + q_1 X^{h-1} + \cdots + q_h$ de degré minimal h dans l'annulateur

de u. On a $u(n_0+h)+q_1u(n_0+h-1)+\ldots+q_hu(n_0)=0$, 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. □

Nous montrons par le résultat qui suit que l'algèbre $r_{\mathbb{Z}}(A)$ est stable par l'application réflexion $\mathscr{R}_A$.

Lemme 4.2.22. *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 dans $K[x]$ tel que $Q(T_A)(\widehat{u})(m)=0$ pour tout entier $m\in\mathbb{N}$. Comme $\widehat{u}$ est élément de l'algèbre $r_{\mathbb{Z}}(K)$, le lemme 4.2.21 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 $(\widehat{u}(m))_{m\in\mathbb{N}}$ 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 $r_{\mathbb{Z}}(A)$. □

4.2.4.2 Applications décimation et emboîtement

Définition 4.2.23. 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 $u=(u(m))_{m\in\mathbb{Z}}$ associe la suite bi-infinie $\vartheta_d(u)=(u(dm))_{m\in\mathbb{Z}}$;

- *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 4.2.24. On vérifie immédiatement que $T_A \circ \vartheta_d = \vartheta_d \circ T_A^d$.

Si $\mathbf{u} = (u_j)_{0\leq j<d}$ est élément de $S_{\mathbb{Z}}(A)^d$, alors il est facile de vérifier que $(T_A \circ E_d)(\mathbf{u}) = E_d(u_1, ..., u_{d-1}, T_A u_0)$, 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 4.2.25. *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 $u_0, ..., u_{d-1}$ sont des suites bi-infinies reconnaissables sur A, alors leur d-emboîtement $E_d(u_0, ..., u_{d-1})$ est une suite reconnaissable sur A.*

Démonstration. Compte tenu de la remarque précédente, elle est identique à celle de [1] qui traite le cas des suites indexées par $\mathbb{N}$. □

Proposition 4.2.26. *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 $\left(d, \mathbf{a} = (a_r)_{0\leq r<d}, \mathbf{b} = (b_r)_{0\leq r<d}\right)$ une présentation 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 4.2.20, 4.2.22, 4.2.25, chaque suite u_r est reconnaissable, donc aussi leur emboîtement $u \circ \varphi$. □

4.3 Endomorphismes continus d'algèbres de suites bi-infinies

Dans le cas où l'anneau A est intègre, les endomorphismes continus de l'algèbre $S_{\mathbb{Z}}(A)$ des suites bi-infinies ont été caractérisés dans [1], où se trouve démontré l'énoncé suivant.

Proposition 4.3.1. *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 4.3.2. *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 :*

$$\forall u \in r_{\mathbb{Z}}(A), \quad u \circ \varphi \in r_{\mathbb{Z}}(A)\,. \tag{27}$$

Démonstration. Puisque $r_{\mathbb{Z}}(A)$ est dense dans $S_{\mathbb{Z}}(A)$ par la proposition 4.2.6, 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 [20, Théorème XI, 3 ; 1, p. 132]. Par la proposition 4.3.1, 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 (27). Il est simple de vérifier que, réciproquement, si φ vérifie la condition (27), 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. □

4.3.1 Quelques lemmes

Lemme 4.3.3. *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 [1, Lemme 2.4]. □

Lemme 4.3.4. *Soit $\mathbb{K}$ une algèbre commutative sur le corps $\mathbb{Q}$ des nombres rationnels, 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 4.3.3, donc aussi reconnaissables sur $\mathbb{C}$. Puisque de plus elles sont évidemment non nulles, on voit par la proposition 4.2.10 que, pour tout $\epsilon \in \{-1, 1\}$, il existe un entier $d_\epsilon > 0$, une suite $\left(p_{i,\epsilon}\right)_{1 \le i \le d_\epsilon}$ de polynômes à coefficients dans $\mathbb{C}$, et une suite $\left(\alpha_{i,\epsilon}\right)_{1 \le i \le d_\epsilon}$ 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 $\forall n \ge 1, \epsilon\frac{\varphi(n)}{n} \le \log_2 c_1 + \frac{\log_2(\sum_{i=1}^{d_\epsilon} |p_{i,\epsilon}(n)|)}{n}$. Comme les deux suites $\left(\frac{\log_2(\sum_{i=1}^{d_\epsilon} |p_{i,\epsilon}(n)|)}{n}\right)_{n \ge 1}$, pour $\epsilon \in \{-1, 1\}$, convergent vers 0 quand n tend vers l'infini, elles 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 4.2.22 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 $\left(\frac{\varphi(-n)}{n}\right)_{n\geq 1}$ est borné, ce qui achève la démonstration. □

4.3.2 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'aprés les propositions 4.2.26 et 4.3.2, 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 (27) est quasi-affine.

Théorème 4.3.5. *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) ⇒ (2). Soit donc f un endomorphisme continu de l'algèbre $r_{\mathbb{Z}}(\mathbb{K})$. En vertu de la proposition 4.3.2, il existe une application φ de $\mathbb{Z}$ dans $\mathbb{Z}$ satisfaisant la condition (27) 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'aprés le lemme 4.3.3, 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 $\mathbb{Q}^{alg}$ de $\mathbb{Q}$ dans $\mathbb{C}$. A partir de la proposition 4.2.10, il existe un entier $d \in \mathbb{N}$, une suite $(\alpha_j)_{1\leq j\leq d}$ de nombres complexes algébriques non nuls, et une suite $(p_j)_{1\leq j\leq d}$ 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 $\left(\frac{\varphi(n)}{n}\right)_{n\geq 1}$ 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 [1, 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 $\mathbb{Q}^{alg}$ 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. □

5 Bijections quasi-affines

Nous associons dans ce chapitre à chaque présentation $(d, \mathbf{a}, \mathbf{b})$ d'une application quasi-affine, une application appelée son *empreinte* ; cette empreinte est à valeurs dans un groupe cyclique, et son ensemble de départ est une réunion disjointe de groupes cycliques. La bijectivité de l'empreinte et celle de l'application quasi-affine de départ sont étroitement liées. Nous déterminons à partir de là un critère qui caractérise les présentations des applications quasi-affines bijectives. En dernier, nous montrons que la réciproque d'une bijection quasi-affine est aussi quasi-affine.

5.1 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

$$c_r = \begin{cases} \frac{N}{|a_r|} & si \quad a_r \neq 0 \\ 0 & si \quad a_r = 0 \end{cases} \tag{28}$$

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

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

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

Proposition 5.1.2. *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 $a_r m + b_r \equiv a_r n + b_r \bmod N$. Puisque $a_r \neq 0$, on peut diviser cette congruence par a_r, ce qui conduit à l'égalié $m + c_r\mathbb{Z} = n + c_r\mathbb{Z}$, 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 $\varphi_r(m) = \varphi_s(n) + a_s k$. Or $\varphi_s(n) + a_s k = a_s n + b_s + a_s k = \varphi_s(n + k)$, 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. □

Proposition 5.1.3. *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 $(d, \boldsymbol{a}, \boldsymbol{b})$ est surjective, et si aucun des termes de $\boldsymbol{a}$ 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 $n = a_r m + b_r$. 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 $n \equiv a_r m + b_r \bmod N$. 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. □

5.2 Caractérisation des bijections quasi-affines

Proposition 5.2.1. *Une application quasi-affine de présentation* $(d, \boldsymbol{a}, \boldsymbol{b})$ *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 diffèrence* $b_s - b_r$.

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 5.1.2 et 5.1.3 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 5.1.2 et 5.1.3. □

5.3 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 5.3.1. *Soit $(d, \boldsymbol{a}, \boldsymbol{b})$ une présentation d'une bijection quasi-affine φ. On considère le plus petit commun multiple N des termes de la suite $\boldsymbol{a}$, 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 $(N, \boldsymbol{a}', \boldsymbol{b}')$ avec, pour tout entier naturel $s < N$:

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

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'aprés la proposition 3.1.3, 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

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

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 $b'_s = d\left\lfloor \frac{b'_s}{d} \right\rfloor + d\left\{\frac{b'_s}{d}\right\}$. □

A partir du théorème 3.2.1 et de la proposition 5.3.1, nous pouvons énoncer le résultat suivant :

Corollaire 5.3.2. *L'ensemble* QA^* *des applications quasi-affines bijectives est un groupe non abélien pour la composition.*

6 Caractérisation des rapports des bijections quasi-affines

Le problème que nous étudions dans ce chapitre, 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. Cette caractérisation s'exprime à l'aide d'un multiensemble d'entiers naturels déterminé par la suite finie $\mathbf{a}$: ce multiensemble donne pour multiplicité à un entier quelconque le nombre d'occurences de cet entier dans la suite des valeurs absolues des termes de la suite $\mathbf{a}$. Un tel multiensemble sera dit idoine s'il est associé à une suite finie qui est rapport d'une présentation d'une bijection quasi-affine. Un certain problème de coloriage des sommets de polygones réguliers donné dans la proposition 6.2.1, nous permet de caractériser les multiensembles idoines. Une idée qui nous permet de savoir si un multiensemble donné est idoine est de se réduire à l'idonéité d'un multiensemble plus simple (proposition 6.3.1). Nous démontrerons deux conditions suffisantes simples pour qu'un multiensemble donné soit idoine : c'est le cas si le support de ce multiensemble est totalement ordonné par la relation de divisibilité, ou encore si les plus grands diviseurs communs de deux éléments distincts du support sont tous égaux entre eux.

6.1 Multiensembles

6.1.1 Définitions et propriétés

Définition 6.1.1. Un multiensemble fini (d'entiers naturels) est 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.

Si pour tout $i \in [1..d]$, n_i est la multiplicité de l'élément α_i dans un multiensemble fini M de cardinal n où d est le nombre d'éléments distincts dans M, le nombre de permutations de M est égal au coefficient multinomial [15, page 23]

$$\binom{n}{n_1, n_2, \cdots, n_d} = \frac{n!}{n_1! n_2! \cdots n_d!}.$$

Si M et N sont deux multiensembles finis, $M \coprod N, M \cup N$ et $M \cap N$ sont aussi des multiensembles finis définis par : Si un élément se produit l fois dans M et k fois dans N, il se produit $l + k$ fois dans $M + N$, $max(l, k)$ fois dans $M \cup N$ et $min(l, k)$ fois dans $M \cap N$. [14, page 694]

Exemples 6.1.2.
1. La factorisation en nombres premiers d'un entier positif n, est un multiensemble fini N, dont les éléments sont des nombres premiers.
2. Les racines complexes d'un polynôme unitaire dans $\mathbb{C}[X]$ est un multiensemble fini.
3. Les combinaisons de k-éléments d'un ensemble fini S avec répétition est un multiensemble à valeurs dans S à k éléments.

6.1.2 Rapport de présentation d'une bijection quasi-affine

Une première observation est que la propriété, pour la suite finie $\mathbf{a} \in \mathbb{Z}^d$, d'être rapport dans une présentation d'une bijection quasi-affine de largeur d est en fait une propriété du multiensemble associé à la suite des valeurs absolues des éléments de la suite $\mathbf{a}$. Pour expliciter ce point, nous utiliserons la définition 6.1.1 [21].

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

$$n_\alpha = card\{r \in [0..d[, |a_r| = \alpha\}\ . \tag{29}$$

Remarque 6.1.3. Le cardinal $\sum_{\alpha \in \mathbb{N}} n_\alpha$ [21, page 25] de ce multiensemble $\alpha \mapsto n_\alpha$ n'est autre que l'entier d.

Proposition 6.1.4. *Soit $\boldsymbol{a}$ et $\boldsymbol{a}'$ deux suites appartenant à $\mathbb{Z}^d$ associées à un même multiensemble $\alpha \mapsto n_\alpha$. Alors $\boldsymbol{a}$ est le rapport dans une présentation d'une bijection quasi-affine de largeur d si et seulement si $\boldsymbol{a}'$ l'est aussi.*

Démonstration. Par hypothèse, il existe pour tout $\alpha \in \mathbb{N}$ une bijection entre l'ensemble des indices $r \in [0..d[$ tels que $|a_r| = \alpha$ et l'ensemble des indices $r' \in [0..d[$ tels que $|a'_{r'}| = \alpha$. En recollant ces bijections, on obtient une permutation σ de l'ensemble $[0..d[$ telle que $|a_{\sigma(r')}| = |a'_{r'}|$ pour tout indice $r' \in [0..d[$. Si $\mathbf{b} \in \mathbb{Z}^d$ est une suite finie telle que $(d, \mathbf{a}, \mathbf{b})$ est présentation d'une bijection quasi-affine, alors les propriétés (1) et (2) de la proposition 5.2.1 sont satisfaites. On a alors $a'_{r'} \neq 0$ pour tout $r' \in [0..d[$ et

$$\sum_{r'=0}^{d-1} \frac{1}{|a'_{r'}|} = \sum_{r'=0}^{d-1} \frac{1}{|a_{\sigma(r')}|} = \sum_{r=0}^{d-1} \frac{1}{|a_r|} = 1 \,,$$

de sorte que la suite $\mathbf{a}'$ satisfait également la propriété (1) de la proposition 5.2.1. On définit d'autre part une suite $\mathbf{b}' \in \mathbb{Z}^d$ par

$$\forall r' \in [0..d[, \qquad b'_{r'} = b_{\sigma(r')} \,.$$

Si $r' \neq s'$ sont deux indices dans $[0..d[$, alors on a $\sigma(r') \neq \sigma(s')$, donc par la propriété (2) de la proposition 5.2.1, le plus grand commun diviseur des entiers $a_{\sigma(r')}$ et $a_{\sigma(s')}$ ne divise pas la différence $b_{\sigma(s')} - b_{\sigma(r')}$. Ceci revient à dire que le plus grand commun diviseur des entiers $a'_{r'}$ et $a'_{s'}$ ne divise pas $b'_{s'} - b'_{r'}$, ce qui prouve que la présentation $(d, \mathbf{a}', \mathbf{b}')$ vérifie la même propriété (2). En utilisant la proposition 5.2.1, on en déduit que cette présentation $(d, \mathbf{a}', \mathbf{b}')$ est aussi la présentation d'une bijection quasi-affine. □

Définition 6.1.5. nous conviendrons, pour abréger, d'appeler multiensemble idoine tout multiensemble $\alpha \mapsto n_\alpha$ d'entiers naturels qui est associé par la formule (29) au rapport d'une présentation d'une bijection quasi-affine.

On va chercher à caractériser les multiensembles idoines.

6.2 Un problème de coloriage

On commence par réduire le problème à la construction d'une certaine application.

Proposition 6.2.1. *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) $\forall \alpha \in \mathbb{N}^*, \quad card\,(\mathfrak{C}^{-1}(\alpha)) = n_\alpha \frac{N}{\alpha}$;

(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 (29). Soit $N_0 = \frac{N}{k}$ le plus petit commun multiple des éléments de F. Par les propositions 5.1.2 et 5.1.3, 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 (29) 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 égal 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 $O_r \cap O_s = \emptyset$, 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

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

On en conclut que la présentation $(d, \mathbf{a}, \mathbf{b})$ satisfait les conditions (1) et (2) de la proposition 5.2.1, et est donc la présentation d'une bijection quasi-affine. □

Exemple 6.2.2. Considérons le multiensemble n de support $F = \{2, 4, 12\}$ avec mulitplicités respectives $n_2 = 1, n_4 = 1$ et $n_{12} = 3$. Voici le coloriage de l'ensemble des sommets d'un dodécagone ($N = 12$) associée à la suite des rapports $\mathbf{a} = (2, 4, 12, 12, 12)$. Les sommets de couleur bleue associés à la valeur $\alpha = 2$(FIGURE 1), sont en nombre $n_2 \frac{12}{2} = 6$, et forment un hexagone régulier. Les sommets de couleur rouge associés à la valeur $\alpha = 4$, sont en nombre $n_4 \frac{12}{4} = 3$, et forment un triangle équilatérale. Tandis que les sommets de couleur verte, associés à la valeur $\alpha = 12$, sont en nombre $n_{12} \frac{12}{12} = 3$,

où chaque sommet constitue un polygone à un seul sommet. Ainsi la suite des rapports $\mathbf{a} = (2, 4, 12, 12, 12)$ est celle d'une bijection quasi-affine, autrement dit le multiensemble n est idoine.

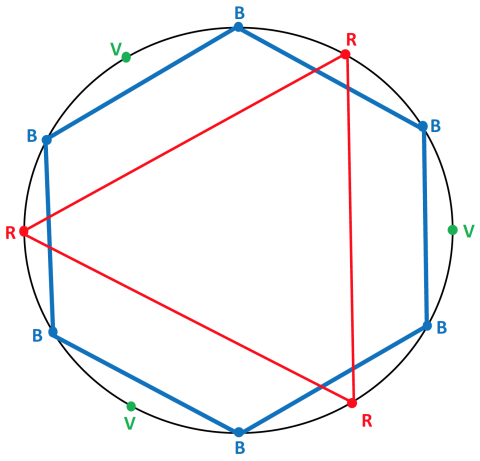

FIGURE 1 –

6.3 Passage à d'autres multiensembles

Pour un ensemble fini F d'entiers naturels non nuls, on définit une application $t = t_F$ de $F \times F$ dans $\mathbb{N}^*$ en posant

$$\forall (\alpha, \beta) \in F \times F, \qquad t(\alpha, \beta) = \mathrm{p}pcm\{\gamma, \gamma \in F \setminus \{\alpha, \beta\}\} .$$

Pour deux éléments distincts $\alpha \neq \beta$ de l'ensemble fini F d'entiers naturels, on note

$$S(\alpha, \beta) = \mathrm{p}gcd(\alpha, \mathrm{p}gcd\{t(\alpha, \eta); \eta \neq \alpha, \eta \neq \beta\}),$$

Dans ces notations, on utilisera si nécessaire les conventions usuelles $\mathrm{p}ppcm\, \varnothing = 1$, $\mathrm{p}gcd\, \varnothing = 0$ et $\mathrm{p}gcd(\alpha, 0) = \alpha$.

Proposition 6.3.1. *Soit $n : \alpha \mapsto n_\alpha$ un multiensemble fini d'entiers naturels de support F, avec $0 \notin F$ et $\mathrm{c}ardF \geq 2$. On note $\Delta_F = \{(\alpha, \alpha), \alpha \in F\}$. Pour que le multiensemble n soit idoine, il faut et il suffit qu'il existe une application $\lambda : F \times F \setminus \Delta_F \to \mathbb{N}$ telle que :*

a. $\forall \alpha \in F, \qquad n_\alpha = \sum_{\beta \in F \setminus \{\alpha\}} \lambda(\alpha, \beta) \frac{\alpha}{S(\alpha, \beta)}$;

b. le multiensemble s d'entiers naturels défini par

$$\forall \sigma \in \mathbb{N}, \qquad s(\sigma) = \sum_{S(\alpha, \beta) = \sigma} \lambda(\alpha, \beta)$$

est idoine.

Démonstration. Montrons que la condition indiquée est nécessaire. Supposons que le multiensemble n soit idoine, et soit N le plus petit commun multiple des éléments de F. D'aprés la proposition 6.2.1, il existe une application $\mathfrak{C}$ de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{N}^*$ satisfaisant les conditions (i) et (ii). On a alors le

Lemme 6.3.2. *Soit $\overline{m}$ un élément de $\mathbb{Z}/N\mathbb{Z}$ et $(\alpha, \eta) \in F \times F$. Si $\mathfrak{C}(\overline{m}) = \alpha$, alors pour tout entier $\ell \in \mathbb{Z}$, l'élément $\mathfrak{C}(\overline{m} + \ell\, t(\alpha, \eta) + N\mathbb{Z})$ appartient à $\{\alpha, \eta\}$.*

Ce lemme sera montré par la suite. Pour (α, β) élément de $F \times F \setminus \Delta_F$, soit $X_{\alpha,\beta}$ la partie de $\mathbb{Z}/N\mathbb{Z}$ telle que

$$X_{\alpha,\beta} = \{\overline{m} \in \mathbb{Z}/N\mathbb{Z} \mid \forall \eta \in F \setminus \{\alpha, \beta\}, \forall \ell \in \mathbb{Z}, \mathfrak{C}(\overline{m} + \ell\, t(\alpha, \eta) + N\mathbb{Z}) = \mathfrak{C}(\overline{m}) = \alpha\} . \quad (30)$$

En particulier, la réunion des $X_{\alpha,\beta}$ lorsque β décrit $F\backslash\{\alpha\}$ est incluse dans $\mathfrak{C}^{-1}(\alpha)$. Montrons maintenant que cette inclusion est en fait une égalité. Soit en effet $\overline{m}$ tel que $\mathfrak{C}(\overline{m}) = \alpha$ et supposons que $\overline{m}$ n'appartienne à aucun des ensembles $X_{\alpha,\beta}(\beta \in F\backslash\{\alpha\})$. Cela signifie que pour tout élément $\beta \neq \alpha$ dans F, il existe un élément $\eta(\beta) \neq \beta$ dans $F\setminus\{\alpha\}$ et un entier ℓ_β dans $\mathbb{Z}$ tels que $\mathfrak{C}(\overline{m} + \ell_\beta t(\alpha, \eta(\beta)) + N\mathbb{Z}) \neq \alpha$. Le lemme 6.3.2 entraîne alors que $\mathfrak{C}(\overline{m} + \ell_\beta t(\alpha, \eta(\beta)) + N\mathbb{Z}) = \eta(\beta)$ pour tout élément $\beta \in F\setminus\{\alpha\}$. Puisque $t(\alpha, \eta(\eta(\beta)))$ est un multiple de $\eta(\beta)$, la condition (ii) de la proposition 6.2.1 entraîne alors que

$$\mathfrak{C}(\overline{m} + \ell_\beta t(\alpha, \eta(\beta)) + \ell_{\eta(\beta)} t(\alpha, \eta(\eta(\beta))) + N\mathbb{Z}) = \eta(\beta). \qquad (31)$$

Mais d'autre part, on sait par le même argument que

$$\mathfrak{C}(\overline{m} + \ell_{\eta(\beta)} t(\alpha, \eta(\eta(\beta))) + N\mathbb{Z}) = \eta(\eta(\beta)).$$

Donc, puisque $t(\alpha, \eta(\beta))$ est un multiple de $\eta(\eta(\beta))$, la condition (ii) montre que

$$\mathfrak{C}(\overline{m} + \ell_\beta t(\alpha, \eta(\beta)) + \ell_{\eta(\beta)} t(\alpha, \eta(\eta(\beta))) + N\mathbb{Z}) = \eta(\eta(\beta)). \quad (32)$$

Comparant les relations (31) et (32), on voit que $\eta(\beta) = \eta(\eta(\beta))$, ce qui contredit la définition de $\eta(\eta(\beta))$. Cette contradiction montre l'égalité

$$\forall \alpha \in F, \qquad \mathfrak{C}^{-1}(\alpha) = \bigcup_{\beta \in F\backslash\{\alpha\}} X_{\alpha,\beta}.$$

Fixons $\alpha \in F$; si β et β' sont deux éléments distincts de $F\setminus\{\alpha\}$, alors l'intersection $X_{\alpha,\beta} \bigcap X_{\alpha,\beta'}$ est l'ensemble des éléments $\overline{m}$ de $\mathbb{Z}/N\mathbb{Z}$ tels que, pour tout $\eta \in (F\setminus\{\alpha,\beta\}) \cup (F\setminus\{\alpha,\beta'\}) = F\setminus\{\alpha\}$, et pour tout entier $\ell \in \mathbb{Z}$, on a $\mathfrak{C}(\overline{m} + \ell t(\alpha, \eta) + N\mathbb{Z}) = \mathfrak{C}(\overline{m}) = \alpha$. Ceci montre que l'intersection $X_{\alpha,\beta} \bigcap X_{\alpha,\beta'}$ est la même pour tous les choix du couple (β, β') d'éléments distincts de $F\setminus\{\alpha\}$. Choisissons alors un élément $\beta_0 \neq \alpha$, ce qui est possible en vertu de l'hypothèse $card F \geq 2$. Posons alors, pour tout $\beta \in F\setminus\{\alpha\}$:

$$Y_{\alpha,\beta} = \begin{cases} X_{\alpha,\beta_0} & \text{si} \quad \beta = \beta_0 \\ X_{\alpha,\beta} \setminus X_{\alpha,\beta_0} & \text{si} \quad \beta \neq \beta_0 \end{cases}.$$

Puisque l'intersection $X_{\alpha,\beta} \bigcap X_{\alpha,\beta'}$ est indépendante du couple (β,β'), on a $Y_{\alpha,\beta} \bigcap Y_{\alpha,\beta'} = \varnothing$ si $\beta \neq \beta'$; de plus $\mathfrak{C}^{-1}(\alpha) = \bigcup_{\beta\in F\setminus\{\alpha\}} Y_{\alpha,\beta}$.

Montrons ensuite que, pour tout couple (α,β) d'éléments distincts de F, la partie $Y_{\alpha,\beta}$ est stable par toutes les translations $\overline{m} \mapsto \overline{m} + t(\alpha,\gamma) + N\mathbb{Z}$, où $\gamma \in F\setminus\{\alpha,\beta\}$.

On commence par vérifier que $X_{\alpha,\beta}$ est stable par ces translations : on a donc à vérifier que, pour tout entier $\ell \in \mathbb{Z}$, et pour tout $\eta \in F\setminus\{\alpha,\beta\}$, on a la double égalité

$$\mathfrak{C}(\overline{m} + t(\alpha,\gamma) + \ell t(\alpha,\eta) + N\mathbb{Z}) = \mathfrak{C}(\overline{m} + t(\alpha,\gamma) + N\mathbb{Z}) = \alpha.$$

Pour cela, on considère deux cas. Tout d'abord, si $\gamma = \eta$, la double égalité à vérifier résulte directement du fait que $\overline{m}$ appartient à $X_{\alpha,\beta}$. Supposons donc que $\gamma \neq \eta$; comme $\overline{m}$ est élément de $X_{\alpha,\beta}$, et que γ et η appartiennent à $F\setminus\{\alpha,\beta\}$, on a $\mathfrak{C}(\overline{m}+t(\alpha,\gamma)+N\mathbb{Z}) = \alpha = \mathfrak{C}(\overline{m}+\ell t(\alpha,\eta)+N\mathbb{Z})$. Par le lemme 6.3.2, on a les relations $\mathfrak{C}(\overline{m}+t(\alpha,\gamma)+\ell t(\alpha,\eta)+N\mathbb{Z}) \in \{\alpha,\gamma\}$ et $\mathfrak{C}(\overline{m}+\ell t(\alpha,\eta)+t(\alpha,\gamma)+N\mathbb{Z}) \in \{\alpha,\eta\}$. Puisque $\gamma \neq \eta$, on trouve que $\mathfrak{C}(\overline{m}+\ell t(\alpha,\eta)+t(\alpha,\gamma)+N\mathbb{Z}) = \alpha$, comme on voulait l'établir. En particulier $Y_{\alpha,\beta_0} = X_{\alpha,\beta_0}$ satisfait la propriété voulue, de sorte qu'on suppose dorénavant que $\beta \neq \beta_0$, et donc que F contient au moins les trois éléments α,β,β_0 deux à deux distincts.

Si $\beta \neq \beta_0$, on passe de la stabilité de $X_{\alpha,\beta}$ à celle de $Y_{\alpha,\beta}$ en distinguant deux nouveaux cas. Si $\gamma \neq \beta_0$, alors $X_{\alpha,\beta}$ et X_{α,β_0} sont stables par la translation $\overline{m} \mapsto \overline{m} + t(\alpha,\gamma) + N\mathbb{Z}$, donc $Y_{\alpha,\beta}$ est stable par cette translation en tant que différence ensembliste de deux parties stables. Si maintenant $\gamma = \beta_0$, alors de deux choses l'une. Ou bien $cardF \geq 4$, de sorte qu'il existe $\beta_1 \in F\setminus\{\alpha,\beta,\beta_0\}$, et alors on peut écrire $Y_{\alpha,\beta} = X_{\alpha,\beta}\setminus\big(X_{\alpha,\beta}\cap X_{\alpha,\beta_0}\big) = X_{\alpha,\beta}\setminus\big(X_{\alpha,\beta}\cap X_{\alpha,\beta_1}\big) = X_{\alpha,\beta}\setminus X_{\alpha,\beta_1}$, ce qui fait là aussi apparaître $Y_{\alpha,\beta}$ comme différence ensembliste de deux parties stables par la translation considérée. Ou bien $F = \{\alpha,\beta,\beta_0\}$ est un ensemble à trois éléments. Dans ce dernier cas, on a $t(\alpha,\gamma) = t(\alpha,\beta_0) = \beta$ et $t(\alpha,\beta) = \beta_0$. On a alors

$$X_{\alpha,\beta} \bigcap X_{\alpha,\beta_0} = \{\overline{m} \in \mathbb{Z}/N\mathbb{Z} \mid \forall(\ell,\ell') \in \mathbb{Z}^2, \mathfrak{C}(\overline{m} + \ell\beta + N\mathbb{Z}) = \mathfrak{C}(\overline{m} + \ell'\beta_0 + N\mathbb{Z}) = \mathfrak{C}(\overline{m}) = \alpha\} . \quad (33)$$

Soit $\overline{m}$ un élément de l'intersection $X_{\alpha,\beta} \bigcap X_{\alpha,\beta_0}$. Alors on a visiblement pour tout $\ell \in \mathbb{Z}$ la double égalité $\mathfrak{C}(\overline{m}+\beta+\ell\beta+N\mathbb{Z}) = \mathfrak{C}(\overline{m}+$

$\beta+N\mathbb{Z}) = \alpha$. En outre, pour tout entier ℓ', on a $\mathfrak{C}(\overline{m}+\ell'\beta_0+N\mathbb{Z}) = \alpha$, et le lemme 6.3.2 entraîne alors que $\mathfrak{C}(\overline{m}+\beta+\ell'\beta_0+N\mathbb{Z}) \in \{\alpha, \beta_0\}$. De même, comme $\mathfrak{C}(\overline{m}+\beta+N\mathbb{Z}) = \alpha$, on a par le lemme 6.3.2 la relation $\mathfrak{C}(\overline{m}+\beta+\ell'\beta_0+N\mathbb{Z}) \in \{\alpha, \beta\}$. Par conséquent $\mathfrak{C}(\overline{m}+\beta+\ell'\beta_0+N\mathbb{Z}) = \alpha$, ce qui signifie que $\overline{m}+\beta+N\mathbb{Z}$ est élément de l'intersection $X_{\alpha,\beta} \bigcap X_{\alpha,\beta_0}$. On en conclut à nouveau que $Y_{\alpha,\beta} = X_{\alpha,\beta} \backslash \left(X_{\alpha,\beta} \bigcap X_{\alpha,\beta_0}\right)$ est stable par la translation $\overline{m} \mapsto \overline{m} + \beta + N\mathbb{Z}$.

Montrons de même que, pour tout couple (α, β) d'éléments distincts de F, la partie $Y_{\alpha,\beta}$ est stable par la translation $\overline{m} \mapsto \overline{m} + \alpha + N\mathbb{Z}$. Pour vérifier d'abord que $X_{\alpha,\beta}$ est stable par cette translation, on a à vérifier que, pour tout entier $\ell \in \mathbb{Z}$, on a pour tout $\eta \in F \backslash \{\alpha, \beta\}$ la double égalité

$$\mathfrak{C}(\overline{m} + \alpha + \ell\, t(\alpha, \eta) + N\mathbb{Z}) = \mathfrak{C}(\overline{m} + \alpha + N\mathbb{Z}) = \alpha,$$

conséquence immédiate de la double égalité

$$\mathfrak{C}(\overline{m} + \ell\, t(\alpha, \eta) + N\mathbb{Z}) = \mathfrak{C}(\overline{m}) = \alpha$$

en utilisant la condition (ii) de la proposition 6.2.1. Maintenant, il en résulte que $Y_{\alpha,\beta}$ est stable par la translation voulue, car c'est, pour $\beta \neq \beta_0$ la différence ensembliste de deux parties stables.

De tout ceci il résulte par définition de $S(\alpha, \beta)$ que, pour tout couple (α, β) d'éléments distincts de F, la partie $Y_{\alpha,\beta}$ est stable par la translation $\overline{m} \mapsto \overline{m} + S(\alpha, \beta) + N\mathbb{Z}$.

Comme la réunion des parties deux à deux disjointes $Y_{\alpha,\beta}$ quand β décrit $F \backslash \{\alpha\}$ est $\mathfrak{C}^{-1}(\alpha)$, on a $card(\mathfrak{C}^{-1}(\alpha)) = \sum_{\beta \in F\backslash\{\alpha\}} card\ Y_{\alpha,\beta}$. Puisque la partie $Y_{\alpha,\beta}$ est stable par la translation $\overline{m} \mapsto \overline{m}+S(\alpha, \beta)+N\mathbb{Z}$, elle est réunion d'orbites sous l'action du groupe engendré par cette translation. Le nombre d'éléments d'une telle orbite étant $N/S(\alpha, \beta)$, désignons par $\lambda(\alpha, \beta)$ le nombre de ces orbites qui sont contenues dans $Y_{\alpha,\beta}$; on a alors $card\ Y_{\alpha,\beta} = \lambda(\alpha, \beta)(N/S(\alpha, \beta))$.

Alors, en utilisant la condition (i) de la proposition 6.2.1, on obtient

$$n_\alpha \frac{N}{\alpha} = card\ (\mathfrak{C}^{-1}(\alpha)) = \sum_{\beta \in F\backslash\{\alpha\}} card\ Y_{\alpha,\beta} = \sum_{\beta \in F\backslash\{\alpha\}} \lambda(\alpha, \beta) \frac{N}{S(\alpha, \beta)},$$

ce qui implique que la relation (a) est vérifiée.

Il reste à montrer que le multiensemble s est idoine. Les éléments du support de s sont nécessairement de la forme $S(\alpha,\beta)$ pour au moins un élément (α,β) de $F\times F\setminus\Delta_F$. Comme $S(\alpha,\beta)$ divise toujours α, l'entier naturel N est un multiple commun des éléments du support de s. Comme $\mathbb{Z}/N\mathbb{Z}$ est réunion disjointe des $Y_{\alpha,\beta}$ quand le couple (α,β) décrit $F\times F\setminus\Delta_F$, il existe une unique application $\mathfrak{C}_s$ telle que

$$\forall\alpha\in F,\forall\beta\in F\setminus\{\alpha\},\forall\overline{m}\in Y_{\alpha,\beta},\qquad \mathfrak{C}_s(\overline{m})=S(\alpha,\beta)\,.$$

On a donc $\mathfrak{C}_s(\overline{m})=\sigma$ si et seulement si il existe un couple $(\alpha,\beta)\in F\times F\setminus\Delta_F$ tel que $\sigma=S(\alpha,\beta)$ et $\overline{m}\in Y_{\alpha,\beta}$. Par conséquent

$$\mathfrak{C}_s^{-1}(\sigma)=\bigcup_{S(\alpha,\beta)=\sigma}Y_{\alpha,\beta}$$

ce qui entraîne

$$card;(\mathfrak{C}_s^{-1}(\sigma))=\sum_{S(\alpha,\beta)=\sigma}\lambda(\alpha,\beta)\frac{N}{S(\alpha,\beta)}=s(\sigma)\frac{N}{\sigma}\,.$$

Soit d'autre part $\overline{m}$ élément de $\mathbb{Z}/N\mathbb{Z}$ et $\sigma\in\mathbb{N}^*$ tel que $\mathfrak{C}_s(\overline{m})=\sigma$, de sorte qu'il existe un couple $(\alpha,\beta)\in F\times F\setminus\Delta_F$ tel que $\sigma=S(\alpha,\beta)$ et $\overline{m}\in Y_{\alpha,\beta}$. Comme $Y_{\alpha,\beta}$ est stable par la translation $\overline{m}\mapsto\overline{m}+\sigma+N\mathbb{Z}$, on voit que $\overline{m}+\sigma+N\mathbb{Z}$ est élément de $\mathfrak{C}_s^{-1}(\sigma)$. Ainsi l'application $\mathfrak{C}_s$ de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{N}^*$ satisfait les conditions (i) et (ii) de la proposition 6.2.1, ce qui montre que le multiensemble s est idoine.

Réciproquement, supposons que le multiensemble s défini par

$$\forall\sigma\in\mathbb{N},s(\sigma)=\sum_{S(\alpha,\beta)=\sigma}\lambda(\alpha,\beta)=\sum_{(\alpha,\beta)\in S^{-1}(\sigma)}\lambda(\alpha,\beta)$$

est idoine et que $\forall\alpha\in F,n_\alpha=\sum_{\beta\in F\setminus\{\alpha\}}\lambda(\alpha,\beta)\frac{\alpha}{S(\alpha,\beta)}$. Définissons N comme le plus petit commun multiple des éléments de F, qui est aussi un multiple commun des éléments $S(\alpha,\beta)$ pour (α,β) décrivant l'ensemble $F\times F\setminus\Delta_F$: en effet $S(\alpha,\beta)$ est toujours diviseur de α. Puisque s est supposé être idoine, selon la proposition 6.2.1, il existe une application $\mathfrak{C}_s$ de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{N}^*$ vérifiant les conditions (i) et (ii). Pour tout $\sigma\in\mathbb{N}^*$, la condition (ii) signifie que $\mathfrak{C}_s^{-1}(\sigma)$

est réunion d'orbites sous l'action par translation du sous-groupe engendré par $\sigma + N\mathbb{Z}$. D'aprés la condition (i), on voit que $\mathfrak{C}_s^{-1}(\sigma)$ est réunion de précisément $\sum_{S(\alpha,\beta)=\sigma} \lambda(\alpha,\beta)$ telles orbites. On peut donc choisir des parties $Z_{\alpha,\beta}$ deux à deux disjointes, pour (α,β) décrivant l'ensemble $F\times F\setminus\Delta_F$, telles que $Z_{\alpha,\beta}$ est réunion de $\lambda(\alpha,\beta)$ orbites sous l'action par translation du sous-groupe engendré par

$$\mathfrak{C}_s^{-1}(\sigma) = \bigcup_{S(\alpha,\beta)=\sigma} Z_{\alpha,\beta}\ .$$

Définissons alors l'application $\mathfrak{C} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{N}^*$ par

$$\forall \overline{m} \in Z_{\alpha,\beta}, \qquad \mathfrak{C}(\overline{m}) = \alpha.$$

On a alors $\mathfrak{C}^{-1}(\alpha) = \bigcup_{\beta\in F\setminus\{\alpha\}} Z_{\alpha,\beta}$, de sorte que

$$\begin{aligned} card\ (\mathfrak{C}^{-1}(\alpha)) = \sum_{\beta\in F\setminus\{\alpha\}} card\ Z_{\alpha,\beta} &= \sum_{\beta\in F\setminus\{\alpha\}} \lambda(\alpha,\beta)\frac{N}{S(\alpha,\beta)} \\ &= \frac{N}{\alpha}\sum_{\beta\in F\setminus\{\alpha\}} \lambda(\alpha,\beta)\frac{\alpha}{S(\alpha,\beta)}. \quad (34) \end{aligned}$$

Or, par hypothèse, on a $n_\alpha = \sum_{\beta\in F\setminus\{\alpha\}} \lambda(\alpha,\beta)\frac{\alpha}{S(\alpha,\beta)}$, ce qui implique que $card\ (\mathfrak{C}^{-1}(\alpha)) = n_\alpha\frac{N}{\alpha}$. D'autre part, puisque la partie $Z_{\alpha,\beta}$ est stable par la translation $\overline{m} \mapsto \overline{m} + S(\alpha,\beta) + N\mathbb{Z}$, et comme α est un multiple de $S(\alpha,\beta)$, cette même partie $Z_{\alpha,\beta}$ est également stable par la translation $\overline{m} \mapsto \overline{m}+\alpha+N\mathbb{Z}$. Donc, pour tout $\overline{m} \in \mathbb{Z}/N\mathbb{Z} = \cup Z_{\alpha,\beta}$, on a l'égalité $\mathfrak{C}(\overline{m} + \mathfrak{C}(\overline{m}) + N\mathbb{Z}) = \mathfrak{C}(\overline{m})$. Par la même proposition 6.2.1, on en conclut que le multiensemble n est idoine, ce qui achève la démonstration. □

Démonstration du Lemme 6.3.2 . Supposons au contraire que $\mathfrak{C}(\overline{m} + \ell t(\alpha,\eta) + N\mathbb{Z}) = \gamma$, où $\gamma \neq \alpha$ et $\gamma \neq \eta$, ainsi $t(\alpha,\eta)$ est un multiple de γ. Selon la propriété (ii) de la proposition 6.2.1, on a

$$\forall \ell' \in \mathbb{Z}, \qquad \mathfrak{C}(\overline{m} + \ell t(\alpha,\eta) + \ell'\gamma + N\mathbb{Z}) = \gamma.$$

Puisque γ est un diviseur de N et de $t(\alpha,\eta)$, il existe $\ell' \in \mathbb{Z}$ tel que l'entier $\ell t(\alpha,\eta)+\ell'\gamma$ soit divisible par N ; avec un tel choix de ℓ', on obtient $\mathfrak{C}(\overline{m}) = \gamma$. Or, par hypotèse, $\mathfrak{C}(\overline{m}) = \alpha$, d'où contradiction du fait que $\alpha \neq \gamma$. □

Corollaire 6.3.3. *Soit $n : \alpha \mapsto n_\alpha$ un multiensemble fini d'entiers naturels de support F, avec $0 \notin F$ et $cardF \geq 2$. Pour que le multiensemble n soit idoine, il est nécessaire que, pour tout $\alpha \in F$, l'entier naturel n_α soit un multiple du plus grand commun diviseur des entiers de l'ensemble $\left\{\frac{\alpha}{S(\alpha,\beta)}, \beta \in F \setminus \{\alpha\}\right\}$.*

6.3.1 Un exemple

Exemple 6.3.4. 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 $n_{24} = 1$. On vérifie que $\sum_{\alpha \in F} \frac{n_\alpha}{\alpha} = 1$. En essayant d'appliquer la proposition 6.3.1, le calcul de la fonction t étant immédiat, on peut calculer les valeurs de S, ce qui conduit au tableau suivant pour $S(\alpha, \beta)$.

α \ β	4	6	8	12	24
4		4	4	4	4
6	6		6	6	6
8	4	4		4	8
12	12	12	12		12
24	12	12	24	12	

Cherchant à appliquer la proposition 6.3.1, on est ramené à chercher des entiers naturels $\lambda(\alpha, \beta)$, où le couple (α, β) décrit l'ensemble $F \times F \setminus \Delta_F$, qui satisfassent les équations

$$\lambda(4,6) + \lambda(4,8) + \lambda(4,12) + \lambda(4,24) = 1 \tag{35a}$$
$$\lambda(6,4) + \lambda(6,8) + \lambda(6,12) + \lambda(6,24) = 2 \tag{35b}$$
$$2\lambda(8,4) + 2\lambda(8,6) + 2\lambda(8,12) + \lambda(8,24) = 1 \tag{35c}$$
$$\lambda(12,4) + \lambda(12,6) + \lambda(12,8) + \lambda(12,24) = 3 \tag{35d}$$
$$2\lambda(24,4) + 2\lambda(24,6) + \lambda(24,8) + 2\lambda(24,12) = 1 \tag{35e}$$

pour se ramener à l'étude du multiensemble s telle que $s(\sigma) = \sum_{S(\alpha,\beta)=\sigma} \lambda(\alpha, \beta)$. D'aprés la table ci-dessus, on a $s(4) = \lambda(4,6) + \lambda(4,8) + \lambda(4,12) + \lambda(4,24) + \lambda(8,4) + \lambda(8,6) + \lambda(8,12)$. D'aprés l'équation (35c), on a $\lambda(8,4) = \lambda(8,6) = \lambda(8,12) = 0$, de sorte

que l'équation (35a) donne $s(4) = 1$. De même $s(12) = \lambda(12,4) + \lambda(12,6) + \lambda(12,8) + \lambda(12,24) + \lambda(24,4) + \lambda(24,6) + \lambda(24,12)$, alors que l'équation (35e) impose $\lambda(24,4) = \lambda(24,6) = \lambda(24,12) = 0$, d'où $s(12) = 3$ d'aprés l'équation (35d). Par l'équation (35b), on voit que $s(6) = \lambda(6,4) + \lambda(6,8) + \lambda(6,12) + \lambda(6,24) = 2$. D'aprés l'équation (35c), on a $s(8) = \lambda(8,24) = 1$. Enfin, on a $s(24) = \lambda(24,8)$, d'où $s(24) = 1$ d'aprés l'équation (35e). Ainsi le multiensemble s est égal au multiensemble n. On est ainsi dans une situation où l'application de la proposition 6.3.1 ne peut apporter aucun renseignement sur le caractère idoine ou non du multiensemble donné. Cependant, il est facile de s'assurer que le multiensemble n que nous considérons 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. 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 6.2.1 montre que le multiensemble n n'est pas idoine. Ainsi il ne peut exister de bijection quasi-affine de rapport $(4,6,6,8,12,12,12,24)$.

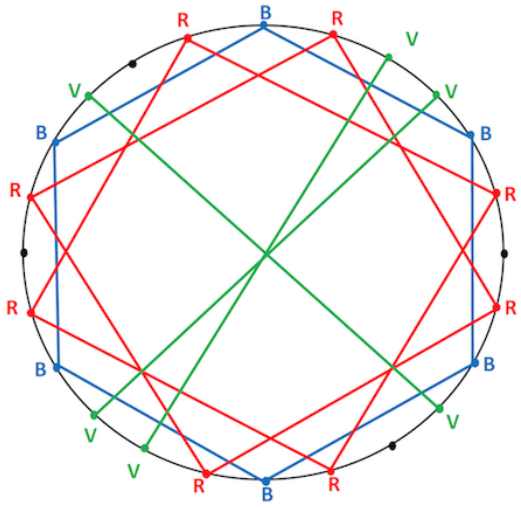

FIGURE 2 –

6.3.2 Conditions suffisantes

On va donner des conditions suffisantes sur le support F d'un multiensemble n pour que celui-ci soit idoine.

Proposition 6.3.5. *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 F est totalement ordonné par divisibilité, alors le multiensemble n est idoine.*

Démonstration. Raisonnons par récurrence sur le nombre d'éléments de F. Puisque $\sum_{\alpha \in F} \frac{n_\alpha}{\alpha} = 1$, ce nombre d'éléments est au moins 1. Pour initialiser la récurrence, supposons que $card F = 1$. Alors $F = \{\beta\}$, $n_\beta = \beta$ et $n_\alpha = 0$ si $\alpha \neq \beta$. L'application constante $\mathfrak{C} : \mathbb{Z}/\beta\mathbb{Z} \to \mathbb{N}^*$ de valeur β satisfait évidemment les conditions (i) et (ii) de la proposition 6.2.1, donc le multiensemble $\alpha \mapsto n_\alpha$ est idoine.

On fait donc dorénavant l'hypothèse que $card\ F \geq 2$, et que tout multiensemble dont le support est totalement ordonné par divisibilité et dont le nombre d'éléments est moindre que $card F$ est idoine. Soit N le plus petit multiple commun des éléments de F. Comme F est totalement ordonné par divisibilité, on a $N = \max F$; puisque $card F \geq 2$, l'ensemble $F' = F \setminus \{N\}$ est une partie non vide de $\mathbb{N}^*$ totalement ordonnée par divisibilité, de sorte que $N' = \max F'$ est le

plus petit multiple commun des éléments de F'. Par hypothèse, on a la relation $\sum_{\alpha\in F}\frac{n_\alpha}{\alpha}=1$, d'où $\sum_{\alpha\in F}n_\alpha c_\alpha=N$, où $c_\alpha=\frac{N}{\alpha}\in\mathbb{N}$; en particulier $c_N=1$, ce qui entraîne que n_N est divisible par l'entier $\frac{N}{N'}$. On considère alors l'application $\lambda : F\times F\setminus\Delta_F\to\mathbb{N}$ telle que :

$$\lambda(\alpha,\beta)=\begin{cases} n_\alpha & \text{si} \quad \alpha<N \ et \ \beta=N \\ n_N/(\frac{N}{N'}) & \text{si} \quad \alpha=N \ et \ \beta=N' \\ 0 & \text{sinon} \end{cases} .$$

Pour $\alpha<N$, on a ainsi

$$\sum_{\beta\in F\setminus\{\alpha\}}\lambda(\alpha,\beta)\frac{\alpha}{S(\alpha,\beta)}=n_\alpha\frac{\alpha}{S(\alpha,N)};$$

or $S(\alpha,N)=\min(\alpha,\min\{t(\alpha,\eta),\eta\in F\setminus\{\alpha,N\}\})$, avec $t(\alpha,\eta)=\max(F\setminus\{\alpha,\eta\})=N$ pour tout $\eta\in F\setminus\{\alpha,N\}$, d'où $S(\alpha,N)=\alpha$. En définitive, on trouve pour $\alpha<N$ l'égalité

$$\sum_{\beta\in F\setminus\{\alpha\}}\lambda(\alpha,\beta)\frac{\alpha}{S(\alpha,\beta)}=n_\alpha .$$

Pour $\alpha=N$, on a semblablement

$$\sum_{\beta\in F\setminus\{N\}}\lambda(N,\beta)\frac{N}{S(N,\beta)}=\frac{n_N}{(N/N')}\frac{N}{S(N,N')};$$

or $S(N,N')=\min(N,\min\{t(N,\eta),\eta\in F\setminus\{N,N'\}\})$, avec $t(N,\eta)=\max(F\setminus\{N,\eta\})=N'$ pour tout $\eta\in F\setminus\{N,N'\}\}$, d'où $S(N,N')=N'$. En définitive, on obtient

$$\sum_{\beta\in F\setminus\{N\}}\lambda(N,\beta)\frac{N}{S(N,\beta)}=n_N .$$

On a ainsi montré que l'application λ vérifie la condition (a) de la proposition 6.3.1.

Soit d'autre part s le multiensemble de support contenu dans $F'=F\setminus\{N\}$ tel que :

$$\forall\sigma\in F',\qquad s(\sigma)=\sum_{(\alpha,\beta)\in S^{-1}(\sigma)}\lambda(\alpha,\beta)=\begin{cases} n_\sigma & \text{si} \quad \sigma<N' \\ n_{N'}+\frac{n_N}{(N/N')} & \text{si} \quad \sigma=N' \end{cases} .$$

On a

$$\sum_{\sigma\in F\setminus\{N\}} \frac{s(\sigma)}{\sigma} = \sum_{\sigma<N'} \frac{s(\sigma)}{\sigma} + \frac{s(N')}{N'} = \sum_{\alpha\in F} \frac{n_\alpha}{\alpha} = 1.$$

Le support de s est strictement inclus dans F, en particulier il est totalement ordonné par divisibilité ; donc l'hypothèse de récurrence montre que le multiensemble s est idoine.

Ainsi la condition (b) de la proposition 6.3.1 est également satisfaite, ce qui montre que le multiensemble n est idoine. □

Proposition 6.3.6. *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 $D = \mathrm{pgcd}(\alpha,\beta)$ pour tout $(\alpha,\beta) \in F\times F \setminus \Delta_F$. 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_γ 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

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

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

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

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'aprés la proposition 6.2.1, on en déduit que le multiensemble n est idoine. □

Corollaire 6.3.7. *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 $cardF \leq 2$, alors le multiensemble n est idoine.*

6.3.3 Caractérisation dans le cas d'un support à trois éléments

Quand le support F du multiensemble fini n est de cardinal 3, on peut obtenir une condition nécessaire et suffisante simple pour que n soit idoine.

Proposition 6.3.8. *Soit n un multiensemble d'entiers naturels dont le support F a 3 éléments $\alpha_1 \neq 0, \alpha_2 \neq 0, \alpha_3 \neq 0$ de multiplicités respectives n_1, n_2, n_3. On suppose que $\frac{n_1}{\alpha_1} + \frac{n_2}{\alpha_2} + \frac{n_3}{\alpha_3} = 1$. Pour tout $i \in \{1,2,3\}$, on note δ_i le plus grand commun diviseur des entiers α_j et α_k, où j et k sont définis par la condition $\{1,2,3\} = \{i,j,k\}$. Pour que le multiensemble n soit idoine il faut et il suffit que pour tout $i \in \{1,2,3\}$, l'entier naturel n_i soit élément du sous-monoïde additif de $\mathbb{N}$ engendré par les deux entiers naturels $\frac{\alpha_i}{\delta_j}$ et $\frac{\alpha_i}{\delta_k}$, avec encore $\{1,2,3\} = \{i,j,k\}$.*

Démonstration. La condition de l'énoncé équivaut pour le multiensemble n à la condition (a) de la proposition 6.3.1 : en effet, si i et j sont deux éléments distincts de $\{1,2,3\}$, on a $S(\alpha_i,\alpha_j) = \delta_k$, où $\{1,2,3\} = \{i,j,k\}$. D'aprés la proposition 6.3.1, elle est donc nécessaire. Reste à montrer qu'elle est aussi suffisante, c'est-à-dire que la condition (b) de la proposition 6.3.1 est également satisfaite. Soit donc s le multiensemble d'entiers naturels défini par

$$\forall \sigma \in \mathbb{N}, \qquad s(\sigma) = \sum_{S(\alpha_i,\alpha_j)=\sigma} \lambda(\alpha_i,\alpha_j)\,,$$

où les $\lambda(\alpha_i,\alpha_j)$ sont tels que

$$\forall i \in \{1,2,3\}, \qquad n_i = \lambda(\alpha_i,\alpha_j)\frac{\alpha_i}{\delta_k} + \lambda(\alpha_i,\alpha_k)\frac{\alpha_i}{\delta_j}\,.$$

On voit donc que $s(\sigma) = 0$ dés que $\sigma \notin \{\delta_1, \delta_2, \delta_3\}$. Or le plus grand commun diviseur D des 3 entiers $\alpha_1, \alpha_2, \alpha_3$ est tel que $D = pgcd(\delta_i, \delta_j)$ dés que i et j sont deux éléments distincts de $\{1, 2, 3\}$. Donc le multiensemble s est idoine par la proposition 6.3.6, ce qui veut dire que la condition (b) de la proposition 6.3.1 est satisfaite. □

Exemple 6.3.9. Considérons le cas $\alpha_1 = 4$, $\alpha_2 = 6$ et $\alpha_3 = 12$. Alors $\delta_1 = 6$, $\delta_2 = 4$ et $\delta_3 = 2$. On a donc $\frac{\alpha_1}{\delta_2} = \frac{\alpha_2}{\delta_1} = 1$, de sorte que pour $i \in \{1, 2\}$, le sous-monoïde additif de $\mathbb{N}$ engendré par $\frac{\alpha_i}{\delta_j}$ et $\frac{\alpha_i}{\delta_k}$ est $\mathbb{N}$ tout entier. Pour qu'un multiensemble n de support $\{4, 6, 12\}$ tel que $\frac{n_1}{4} + \frac{n_2}{6} + \frac{n_3}{12} = 1$ soit idoine, il est donc nécessaire et suffisant que la multiplicité n_3 de 12 dans n soit élément du sous-monoïde additif de $\mathbb{N}$ engendré par 2 et 3, qui est en fait $\mathbb{N}\setminus\{1\}$. Ainsi, il faut et il suffit que $n_3 \neq 1$. Par conséquent, 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 $(4, 4, 4, 6, 12)$.

En particulier, on voit que la condition nécessaire pour qu'un multiensemble n soit idoine du corollaire 6.3.3 n'est pas suffisante, et que la condition suffisante de la proposition 6.3.5 n'est pas nécessaire.

Bibliographie

[1] A. AÏT-MOKHTAR, A. NECER, A. SALINIER. *Endomorphismes d'algèbres de suites,* J. Théor. Nombres Bordeaux, **2**0, n°1 (2008), 1-21.

[2] A. AÏT-MOKHTAR. *Endomorphismes d'algèbres de suites,* Thèse de Doctorat de l'université de Limoges, 2008.

[3] A. AÏT-MOKHTAR. *Applications purement semi-affines et tressages,* C. R. Math. Acad. Sci. Paris **3**48 (2010), n° 1-2, 1-4.

[4] B. BENZAGHOU. *Algèbre de Hadamard,* Bull. Soc. Math. France, **9**8 (1970), 209-252.

[5] J. BERSTEL, C. REUTENAUER. *Noncommutative rational series with applications,* Encyclopedia of Mathematics and Its Applications **1**37, Cambridge University Press, Cambridge, 2011. xiv+248 pp.

[6] N. BOURBAKI. *Éléments de mathématique. Algèbre Commutative. Chapitres 5 à 7,*
N. Bourbaki et Springer-Verlag, Berlin Heidelberg, 2006.

[7] A. CAYLEY. *Researches on the Partition of Numbers,* Philos. Trans. Roy. Soc. London, **1**46 (1856), pp. 127-140.

[8] J.-L. CHABERT. *Anneaux de Fatou,* Ens. Math., **1**8 (1972), 141-144.

[9] L. COMTET. *Analyse combinatoire, tome premier,* Collection Sup : "Le Mathématicien" **4**, Presses Universitaires de France, 1970, 192 pp.

[10] E. EHRHART. *Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire,* Birkhäuser Verlag, Basel und Stuttgart, 1977.

[11] R. ENGELKING. *General Topology,* Monografie Matematyczne 60, Polska Akademia Nauk, PWN-Polish Scientific Publishers, Warszawa, 1977.

[12] G. EVEREST, A. VAN DER POORTEN, I. SHPARLINSKI, T. WARD. *Recurrence Sequences,* Mathematical Surveys and Monographs, **1**04, American Mathematical Society, Providence, RI, 2003. xiv+318 pp.

[13] P. FATOU. *Séries trigonométriques et séries de Taylor,* Acta Math., Uppsala **3**0 (1906), 335-400.

[14] D. E. KNUTH. *The Art of Computer Programming,*Volume **2** Seminumerical Algorithms, Third edition, Addison-Wesley, Reading, Mass., 1981.

[15] D. E. KNUTH. *The Art of Computer Programming,*Volume **3** Sorting and Searching, Addison-Wesley, Reading, Mass., 1973.

[16] R. G. LARSON, E. J. TAFT. *The algebraic structure of linearly recursive sequences under Hadamard product,* Israel Journal of Math., **7**2 (1990), N^{os} 1-2, 118-132.

[17] R. NIBOUCHA, A. SALINIER. *Composition d'applications quasi-polynomiales,* J. Théor. Nombres Bordeaux, 29 no. 2 (2017), 569-601.

[18] I. NIVEN. *The asymptotic density of sequences.* Bull. Amer. Math. Soc., **5**7 (1951), n° 6, 420-434.

[19] G. POLYA. *Über ganzwertige ganze Funktionen.* Rend. Circ. Mat. Palermo **4**0 (1915), 1-16.

[20] L. SCHWARTZ. *Topologie générale et analyse fonctionnelle,* Deuxième édition revue et corrigée, Collection Enseignement des Sciences **1**1, Hermann, Paris, 1970, 440 pp.

[21] R. P. STANLEY. *Enumerative combinatorics. Vol. 1,* with a foreword by Gian-Carlo Rota. Corrected reprint of the 1986 original. Cambridge Studies in Advanced Mathematics, **4**9. Cambridge University Press, Cambridge, 1997. xii+325 pp.