G. RAUZY

Des mots en arithmétique

Publications du Département de Mathématiques de Lyon, 1984, fascicule 6B
« Théorie des langages et complexité des algorithmes », , p. 103-113

<http://www.numdam.org/item?id=PDML_1984___6B_A5_0>

DES MOTS EN ARITHMETIQUE

par C. RAUZY

Les suites infinies à termes dans un ensemble fini ou, si l'on préfère, les mots infinis sur un alphabet fini interviennent sous divers aspects en arithmétique qu'il serait illusoire de vouloir recenser en un court exposé.

Il a donc fallu choisir et c'est bien dommage, car la notion de complexité d'algorithme, implicite dans diverses branches des mathématiques, n'est sans doute pas ressentie de la même manière chez les uns et les autres (songer par exemple à l'écriture décimale d'un nombre réel tel que $\sqrt{2}$)

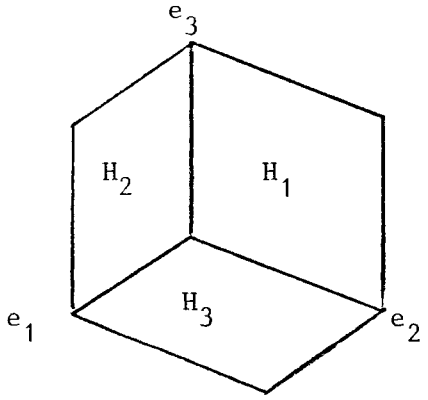
Nous commençons donc par un problème (espérant qu'un modèle existe déjà que nous ne connaissons pas, pour y apporter une réponse) lié sans qu'il soit facile d'expliciter pourquoi à l'extension en dimension 2 de la théorie des fractions continues et aux difficultés qu'on y rencontre, et illustrons ensuite sur un exemple quelques méthodes de type combinatoire efficaces en dimension 1.

1. UN PROBLEME.

. Soient e_1, e_2, e_3 3 vecteurs de $\mathbb{R}^2$ Q-linéairement indépendants et vérifiant sur $\mathbf{R}$ une relation :

$$c_1e_1 + c_2e_2 + c_3e_3 = 0$$

où c_1, c_2, c_3 sont de même signe.



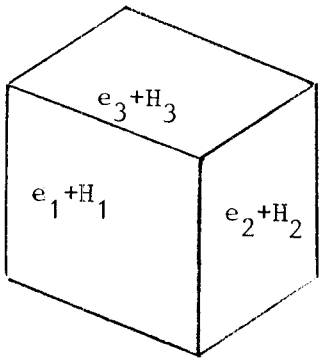
Cette relation assure que les trois parallélogrammes "semi-ouverts" :

$$H_1 = \{ x,\ \exists x_2,x_3 \quad x = x_2e_2 + x_3e_3 \quad 0 \leqslant x_2 < 1 \ ,\ 0 < x_3 < 1 \}$$

$$H_2 = \{ x,\ \exists x_3,x_1 \quad x = x_3e_3 + x_1e_1 \quad 0 < x_3 \leqslant 1 \ ,\ 0 < x_1 \leqslant 1 \}$$

$$H_3 = \{ x,\ \exists x_1,x_2 \quad x = x_1e_1 + x_2e_2 \quad 0 < x_1 \leqslant 1 \ ,\ 0 \leqslant x_2 < 1 \}$$

sont deux à deux disjoints et que l'hexagone $H = H_1 \cup H_2 \cup H_3$ est un domaine fondamental pour le réseau Λ de vecteurs de base e_2-e_1 , e_3-e_1.



Elle assure en outre que e_1+H_1 , e_2+H_2 , e_3+H_3 sont contenus dans H permettant de définir une transformation T de H en lui-même par :

$$Tx = x+e_k \quad \text{si} \quad x \in H_k$$

Nous voulons ici étudier l'orbite d'un point x de H par T, c'est-à-dire, la suite $(T^n x)_{n \in \mathbb{N}}$.

Définissant alors une application ν de H dans $\{1,2,3\}$ par :

$$\nu(x) = k \quad \text{si} \quad x \in H_k$$

une suite plus "simple" à étudier que l'orbite de x sera ce que nous appellerons "l'itinéraire" de x , c'est-à-dire, la suite $(\nu(T^n x))_{n \in \mathbb{N}}$ à termes dans l'ensemble fini $\{1,2,3\}$.

. Remarquons tout d'abord que l'application T est en fait si l'on identifie H à $\mathbb{R}^2/\Lambda$ la translation modulo Λ qui à x associe $x+e_1$ et que la $\mathbb{Q}$-linéaire indépendance des vecteurs e_1, e_2, e_3 assure en vertu du théorème de Kronecker que toute orbite selon T est dense dans H.

Soient alors x,y deux points de H $u = (u_n)$, $v = (v_n)$ leurs itinéraires respectifs.

Quelque soit l'entier N, il existe un parallélogramme non vide P dont l'un des sommets est y tel que :

$$\forall z \in P \quad \forall n = 0,\ldots,N \qquad \nu(T^n z) = \nu(T^n y)$$

(et donc $T^n z \subset T^n y + z-y$)/

Par suite de la densité de la suite $(T^n x)_{n \in \mathbb{N}}$, il existe un entier M tel que : $T^M x \in P$.

Il en résulte que :

$$\forall N \ \exists M \quad \forall n = 0,\ldots,N \qquad u_{n+M} = v_n .$$

Bien entendu, le même résultat subsiste en intervertissant les rôles de u et v.

Soit alors L l'ensemble des mots sur l'alphabet $\{1,2,3\}$ figurant dans u, c'est-à-dire des mots $A = a_o \ldots a_N$ tels que

$$\exists M \quad \forall n = 0,\ldots,N \qquad u_{M+n} = a_n .$$

De la propriété précédente nous pouvons en conclure que L est indépendant du point x de départ : c'est ce qu'il y a de commun à tous les itinéraires.

Réciproquement, d'ailleurs, une analyse plus fine montrerait que toute suite u telle que l'ensemble des mots y figurant soit L est l'itinéraire d'un point x (modulo éventuellement un choix différent pour la frontière de H).

. Bien entendu, l'ensemble L dépend des données initiales, c'est-à-dire, des vecteurs e_1, e_2, e_3 . Il reste cependant invariant si l'on effectue sur ces vecteurs une même transformation affine.

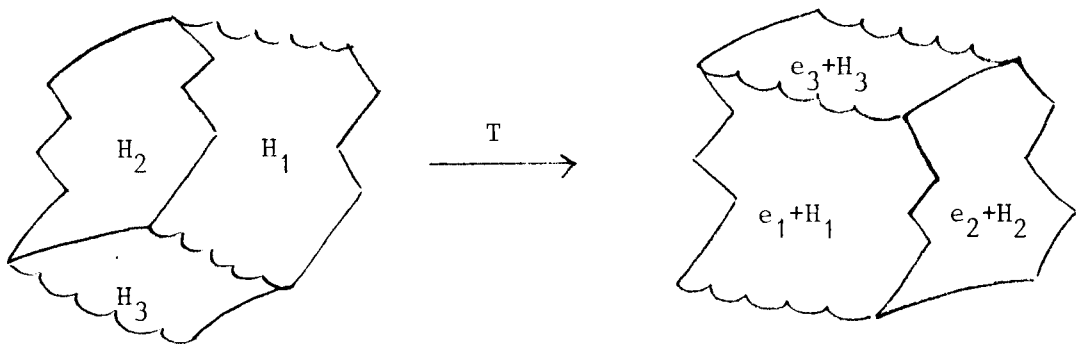
Indiquons maintenant une propriété commune à tous les ensembles L ainsi définis. Soit p(n) le nombre de mots de L de longueur n : p(n) est le nombre de "morceaux" de H délimités par les lignes $T^{-k}F$ k : 0,...,n-1, où F est l'ensemble des lignes frontières de H_1 ,H_2, H_3.

On constate alors que quels que soient les vecteurs e_1, e_2, e_3 de départ on a :

$$p(n) = n^2+n+1 \ .$$

. Nous pouvons maintenant formuler notre problème : parmi les parties L de $\{1,2,3\}^*$ vérifiant $p(n) = n^2+n+1$, quelles sont les propriétés combinatoires supplémentaires qui assurent que L est du type précédent ? où si l'on préfère, quelles "machines" peuvent produire des suites du type itinéraire au sens ci-dessus.

. Il n'est pas certain, a priori, que cette question ait une réponse. Indiquons cependant pourquoi elle n'est pas totalement dénuée de sens. Au lieu de partir des parallélogrammes H_1, H_2, H_3 nous aurions pu partir de parallélogrammes "gondolés" comme indique sur la figure :



Tout ce qui précède resterait valable, sauf éventuellement la valeur de p(n), car les frontières des "parallélogrammes" pourraient être choisies de manière à se correspondre au moins partiellement par la transformation T.

Cela est effectivement possible : pour un choix convenable de H_1, H_2, H_3 et pour un système de vecteurs e_1, e_2, e_3 particulier, on peut montrer [3] que l'un des itinéraires est la suite :

$w = 121312112...$

point fixe de la substitution π définie par

$\pi(1) = 2$, $\pi(2) = 13$, $\pi(3) = 1$.

Pour cette suite w une analyse combinatoire directe montre aisément que, cette fois :

$p(n) = 2n+1$.

"Point fixe d'une substitution" est une notion en quelque sorte "réplicative" : une partie de la structure est isomorphe à la structure tout entière. Dans l'exemple cité, cette notion se traduit par le fait que la frontière de "l'hexagone" H pris pour domaine fondamental est un fractal [2].

. On peut même donner une réciproque partielle au résultat précédent. Soit w une suite vérifiant $p(n) = 2n+1$ et une condition combinatoire $\mathscr{C}$ que nous préciserons ultérieurement. Alors, il existe des vecteurs e_1, e_2, e_3 et des "parallélogrammes gondolés" H_1, H_2, H_3 tels que u soit un itinéraire au sensprécédent [4].

Cependant, e_1, e_2, e_3 étant donnés, il n'existe pas nécessairement de tels parallélogrammes, ce qui d'une autre manière justifie la question posée.

Ajoutons qu'un résultat analogue (totalement élucidé !) existe en dimension 1 où les suites intervenenant sont cette fois les suites "sturmiennes" [1] où $p(n) = n+1$.

2. UN EXEMPLE.

Nous allons retrouver ici une autre suite vérifiant $p(n) = 2n+1$ ce qui nous permettra d'expliciter la condition $\mathscr{C}$ du paragraphe précédent, en

en même temps que de montrer pourquoi substitutions et points fixes de substitution interviennent naturellement dans ces questions.

. Soit X l'intervalle $[0,1[$, α le nombre $\frac{\sqrt{3}-1}{2}$ et T la transformation de X en lui même définie par :

$$Tx = x + \alpha - [x+\alpha]$$

(où $[y]$ désigne la partie entière de y, c'est-à-dire l'entier immédiatement inférieur ou égal à y).

Nous nous intéressons ici à l'orbite de 0 par T, ou plutôt à l'ensemble des n tels que $T^n 0 \in [o,1/2[$.

Dans le même esprit que précédemment, nous appelons X_o et X_1 respectivement les intervalles $X_o = [o,1/2[$, $X_1 = [1/2,1[$ ν la fonction de X dans $\{0,1\}$ qui à x associe k si $x \in X_k$, et nous voulons décrire l'itinéraire de 0 selon la partition X_o, X_1 c'est-à-dire la suite $u = (\nu(T^n 0))_{n \in \mathbb{N}}$ à termes dans $\{o,1\}$.

Le résultat est alors le suivant.

Soit v la suite à termes dans $\{1,2,3\}$ point fixe de la substitution τ définie par :

$\tau(1) = 13$, $\tau(2) = 13223$, $\tau(3) = 1323$

et soit σ la substitution de $\{1,2,3\}$ dans $\{0,1\}^*$ définie par

$\sigma(1) = 0$, $\sigma(2) = 011$, $\sigma(3) = 01$.

Alors on a : $u = \sigma(v)$.

Cela signifie que puisque $v = \tau(v)$ on a :

$v = \underbrace{13}\ \underbrace{1323}\ \underbrace{13}\ \underbrace{1323}\ \underbrace{13223}\ \ldots$

et donc : $u = \underbrace{0}\ \underbrace{01}\ \underbrace{0}\ \underbrace{01}\ \underbrace{011}\ \ldots$

. Avant d'esquisser la démonstration de ce résultat, faisons une remarque.

Soit L l'ensemble des mots figurant dans v, et soit comme précédemment p(n) le nombre de mots de longueur n.

Avec un peu de patience et raisonnant par récurrence il n'est pas trop difficile de voir que : $p(n) = 2n+1$.

Le plus simple pour cela est d'examiner comment un mot de L de longueur n se prolonge en un mot de L de longueur n+1. De manière plus précise posons pour un mot A de L :

$$\partial^+(A) = \text{Card } \{a \in \{1,2,3\} \ , \ Aa \in L\} \ .$$

Dans le graphe orienté dont les sommets sont les mots de L de longueur n et dont les arêtes sont les couples (A,B) tels qu'il existe un mot C de longueur n-1 , deux lettres a et b de {1,2,3} vérifiant :

$$A = aC \ , \ B = Cb \ , \ aCb \in L$$

∂^+ est ce que l'on appelle un demi-degré.

On a évidemment :

$$p(n+1) = \sum_{A \in L_n} \partial^+(A)$$

(en appelant L_n l'ensemble des mots de A de longueur n) d' où l'on tire

$$p(n+1)-p(n) = \sum_{A \in L_n} (\partial^+(A)-1)$$

Compte tenu du fait que p(1) = 3 , il suffit donc de montrer que p(n+1)-p(n) = 2. et pour cela d'établir par récurrence la propriété suivante :

$$\mathscr{C}'_+ \quad \begin{cases} \text{(i)} \quad \exists A,B \in L_n \quad A \neq B \quad \text{et} \quad \partial^+(A) = \partial^+(B) = 2 \\ \text{(ii)} \quad \forall C \in L_n \quad C \notin \{A,B\} \Rightarrow \partial^+(C) = 1. \end{cases}$$

Revenons maintenant à la suite w du premier paragraphe point fixe de la substitution π où $\pi(1) = 12$, $\pi(2) = 13$, $\pi(3) = 1$. Elle vérifie comme on l'a dit : p(n) = 2n+1. Mais cette fois les conditions (i) et (ii) précédentes sont à remplacer par :

$$\mathscr{C}_+ \quad \begin{cases} \text{(i)} \quad \exists A \in L_n \quad \partial^+(A) = 3 \\ \text{(ii)} \quad \forall C \in L_n \quad C \neq A \Rightarrow \partial^+(C) = 1 \end{cases}$$

. Nous n'avons jusqu'ici suggéré que des démonstrations combinatoires des propriétés $\mathscr{C}'_+$ ou $\mathscr{C}_+$. En fait, et ceci me semble important, <u>l'interprétation géométrique que nous avons donnée des suites correspondantes conduit beaucoup plus simplement au même résultat</u> : dans le premier cas par exemple p(n) s'interprétait comme un certain nombre de morceaux de

l'hexagone H ; dans le morcellement correspondant à l'étape suivante (passage de n à n+1), un seul de ces morceaux éclate en 3 celui qui contient le seul point frontière commun à H_1, H_2, H_3;

. Soit maintenant une suite quelconque vérifiant p(n) = 2n+1. Pour chaque n l'une des conditions $\mathscr{C}_+$ ou $\mathscr{C}'_+$. Mais, si la condition $\mathscr{C}_+$ est vérifiée pour une valeur de n, elle l'est évidemment pour toute valeur inférieur (par troncature du mot vérifiant $\partial^+(A) = 3$).

Donc ou bien $\mathscr{C}_+$ est toujours vérifiée, ou bien $\mathscr{C}'_+$ est toujours vérifiée à partir d'un certain rang.

Bien entendu nous pouvons définir de manière analogue (avec une légère restriction toutefois sur les suites employées - celle de pouvoir être "prolongée" à gauche) une fonction ∂^- par :

$\partial^-(A)$ = card $\{a \in \{1,2,3\}$, $a A \in L\}$

et des conditions $\mathscr{C}_-$ et $\mathscr{C}'_-$ associées.

Si on considère comme équivalentes deux suites obtenues par substitution à partir d'une même troisième, nous voyons qu'il existe donc quatre classes de suites telles que p(n) = 2n+1 (ou plus généralement p(n+1) - p(n) = 2 dès que n assez grand).

La suite v vérifie $\mathscr{C}'_-$ et $\mathscr{C}'_+$. La suite w vérifie $\mathscr{C}_-$ et $\mathscr{C}_+$.

La condition $\mathscr{C}$ du premier paragraphe est simplement $\mathscr{C}_-$ et $\mathscr{C}_+$.

Un exemple de suite vérifiant $\mathscr{C}'_+$ et $\mathscr{C}_-$ est donné par le point fixe de la substitution : 1 → 12, 2 → 123 , 3 → 1 .

En lisant cette suite "à l'envers" (ce qui est possible car chaque mot y figurant, y figure une infinité de fois) on obtient un exemple de suite vérifiant $\mathscr{C}'_-$ et $\mathscr{C}_+$.

. QUESTIONS : - La suite précédente est-elle susceptible d'une interprétation géométrique simple dans le même esprit ?

- Qu'en est-il pour les suites vérifiant p(n+1)-p(n) = k (k > 3) ? Les deux cas extrêmes sont encore susceptibles d'interprétations analogues (échanges de k intervalles, translation dans $\mathbf{R}^k$ modulo $\mathbf{Z}^k$).

3. DEMONSTRATION RELATIVE A L'EXEMPLE

. Si x est un point de X_o, la suite $(T^n x)$ étant dense (toujours le théorème de Kronecker) dans X, il en résulte que :

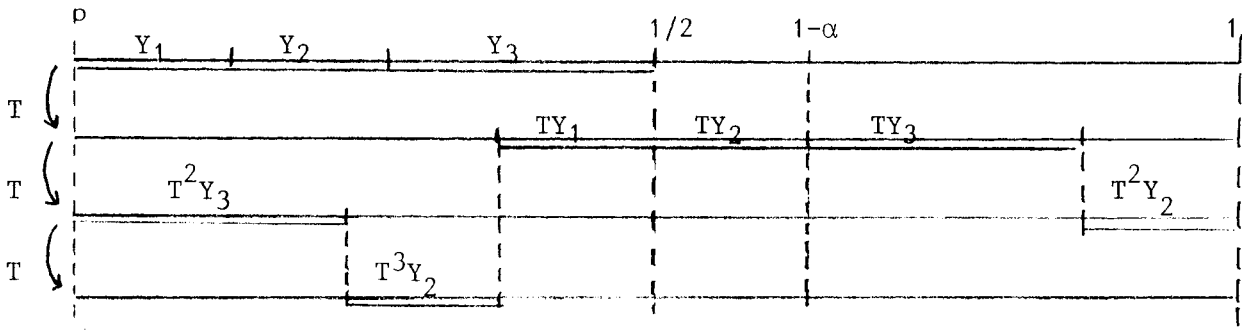
$$\exists\, n \geqslant 1 \qquad T^n x \in X_o$$

Nous appelons r(x) le plus petit entier $n \geqslant 1$ tel que $T^n x \in X_o$.

C'est le "temps de premier retour" sur X_o. Nous définissons de la même manière une "transformation de premier retour" S de X_o en lui même par :

$$Sx = T^{r(x)}x.$$

Précisons sur une figure cette transformation :



On voit ainsi que $X_o = [0,1/2[$ se trouve partagé en trois intervalles semi-ouverts y_1, y_2, y_3 de longueurs respectives $\frac{2-\sqrt{3}}{2}$, $\frac{2-\sqrt{3}}{2}$, $\frac{2\sqrt{3}-3}{2}$

que si $x \in Y_1$, $r(x) = 1$ et donc $Sx = Tx$
$x \in Y_2$, $r(x) = 3$ et donc $Sx = T^3x$
$x \in Y_3$, $r(x) = 2$ et donc $Sx = T^2x$.

La transformation S a donc pour restriction à chacun des intervalles Y_1, Y_2, Y_3, une translation aisée à préciser : elle consiste à "découper" X_o selon ces 3 intervalles et à les "remplacer dans l'ordre Y_3, Y_2, Y_1.

. De même que nous avions défini l'itinéraire d'un point x de X pour la transformation T relativement à la partition X_o, X_1 , nous pouvons définir l'itinéraire d'un point x de X_o pour la transformation S relativement à la partition Y_1, Y_2, Y_3 en introduisant la fonction μ définie par $\mu(x) = 1$ si $x \in Y_1$, 2 si $x \in Y_2$, 3 si $x \in Y_3$.

L'itinéraire d'un point x sera alors la suite $(\mu(S^n x))_{n \in \mathbb{N}}$.

. Partons alors d'un point x de X_o. Nous avons deux suites :

$u = (\nu(T^n x))$, $v = (\mu(S^n x))$.

Supposons, par exemple, que v = 2 3 1 ... .

Que peut-on dire de u.

Tout d'abord $v_o = 2$ implique $x \in Y_2$ donc $Sx = T^3 x$

de même $v_1 = 3$ " $Sx \in Y_3$ " $S^2x = T^2Sx = T^5x$

" $V_2 = 1$ " $S^2x \in Y_1$ " $S^3x = TS^2x = T^6x$

.....

En particulier, du fait que x, Sx, S^2x, S^3x .... appartient à Y_o on en déduit que $u_o = u_3 = u_5 = u_6 = 0$.

En outre, $v_o = 2$ implique également que $Tx \in Y_1$, $T^2x \in X_1$

de même $v_1 = 3$ " $T^4x \in Y_2$.

Finalement nous avons donc : $u_o = 0$, $u_1 = 1$, $u_2 = 1$; $u_3 = 0$, $u_4 = 1$ $u_5 = 0$ $u_6 = \ldots$.

De manière générale il est aisé de prouver par un raisonnement analogue que la suite u s'obtient à partir de la suite v par la substitution σ que nous avons introduite dans le deuxième paragraphe.

. Pour démontrer que v est point fixe de la substitution τ nous allons recommencer la même procédure pour la transformation S, c'est-à-dire, considérer la transformation R de premier retour sur l'intervalle Y_1.

La figure est cette fois un peu plus compliquée ; décrivons seulement le résultat (on engage le lecteur à la faire, mais attention aux longueurs respectives des intervalles!

La transformation R obtenue est du même type que la transformation S c'est-à-dire que l'intervalle Y_1 se subdivise en 3 intervalles Z_1, Z_2, Z_3 R consistant à échanger ces intervalles et les remettre dans l'ordre Z_3, Z_2, Z_1.

En outre : si $x \in Z_1$ $\quad Rx = S^2x$

si $x \in Z_2$ $\quad Rx = S^5x$

si $x \in Z_3$ $\quad Rx = S^4x$

De plus : $Z_1 \subset Y_1$, $SZ_1 \subset Y_3$

$Z_2 \subset Y_2$, $SZ_2 \subset Y_3$, $S^2Z_2 \subset Y_2$, $S^3Z_2 \subset Y_2$, $S^4Z_2 \subset Y_3$

$Z_3 \subset Y_3$, $SZ_2 \subset Y_3$, $S_2Z_2 \subset Y_2$, $S^3Z_2 \subset Y_3$.

Ceci, par un raisonnement analogue à celui qui précède nous assure que l'itinéraire d'un point x de Y_1 pour la transformation S relativement à la partition Y_1, Y_2, Y_3 , s'obtient à partir de l'itinéraire de ce même point pour la transformation R relativement à la partition Z_1, Z_2, Z_3 précisément au moyen de la substitution du deuxième paragraphe.

. Nous pouvons donc affirmer que, en particulier pour la suite v de ce paragraphe correspondant à l'itinéraire de 0 selon S, on a :

$$v = \tau(v')$$

v' étant cette fois l'itinéraire de 0 selon R.

. On pourrait bien sûr continuer, c'est-à-dire, prendre la transformation de premier retour sur Z_1. Oh miracle ! elle est encore du même type et de surcroît la substitution associée est encore τ .

Miracle, non, puisque l'exemple a été choisi pour cela : très exactement les diverses inclusions écrites sur les $T^i Z_j \subset Y_k$ (ainsi que le fait que tous ces ensembles sont disjoints et recouvrent X_0) montrent que l'on a :

$$\begin{pmatrix} |Y_1| \\ |Y_2| \\ |Y_3| \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} |Z_1| \\ |Z_2| \\ |Z_3| \end{pmatrix}$$

où l'on désigne par $|J|$ la longueur de l'intervalle J.

Le choix $\alpha = \frac{\sqrt{3}-1}{2}$ a alors été fait de manière que $|Z_1|$, $|Z_2|$, $|Z_3|$ soit vecteur propre de cette matrice correspondant à sa plus grande valeur propre (qui est à coordonnées positives d'après le théorème de Perron-Frobenius):

ainsi, $|Z_1|$, $|Z_2|$, $|Z_3|$ sont proportionnels à $|Y_1|$, $|Y_2|$, $|Y_3|$. En d'autres termes la figure formée par (Y_1,Y_2,Y_3) est homothétique de celle formée par (Z_1,Z_2,Z_3).

Les transformations S et R ayant même définition une fois ces intervalles fixés, il en résulte que l'orbite du centre d'homothétie, c'est-à-dire, le point 0 selon S se déduit par cette homothétie de l'orbite du même point selon R.

En particulier, les itinéraires correspondants sont les mêmes et donc :

$$v' = v$$

ce qui termine la démonstration.

Remarquons que, d'une part, en changeant α et donc les substitutions intervenant dans les transformations de permier retour, on pourrait fournir de nombreux exemples analogues, d'autre part que le morcellement associé à la définition de p(n) est dans ce cas constitué d'intervalles dont deux d'entre eux seulement sont à chaque étape divisés en deux chacuns.

BIBLIOGRAPHIE.

[1] E. COVEN, G.A. HEDLUND, Sequences with minimal block growth, Math. Syst. Theory 7 - (138-155), 1973.

[2] F.M. DEKKING, Replicative superfigures and endomorphisms of free groups, J. of Combinatorial Theory - Series A - Vol. 32 n° 3, May 1982.

[3] G. RAUZY, Nombres algébriques et substitutions, Bull. Soc. Math. de France, Tomme 110 - Fascicule 2 - Année 1982.

[4] G. RAUZY, Polyèdres à restes bornés. Aparaître in Séminaire de théorie des nombres de Paris (1982-1983).