Astérisque

MICHEL LAURENT

Équations exponentielles polynômes et suites récurrentes linéaires

Astérisque, tome 147-148 (1987), p. 121-139

<http://www.numdam.org/item?id=AST_1987__147-148__121_0>

Société Mathématique de France
Astérisque 147-148 (1987), p. 121-139.

ÉQUATIONS EXPONENTIELLES POLYNÔMES ET SUITES RÉCURRENTES LINÉAIRES

par Michel LAURENT

1. Introduction et plan.

Il s'agit ici d'étudier l'ensemble des zéros entiers d'un système général d'équations exponentielles-polynômes. Le théorème 1 montre qu'une solution quelconque d'un tel système est proche de certains sous-groupes explicitement décrits dans le §2, et fournit une version quantitative du résultat principal de [8] . Cet énoncé général permet en particulier d'étudier les équations algébriques reliant les valeurs d'une ou plusieurs suites récurrentes linéaires. Nous examinons ainsi dans le §3 quelques cas particuliers liés aux notions de répétition et d'intersection. Il est important de noter que les démonstrations de tous les résultats présentés ici se fondent sur le "théorème du sous-espace" de W. Schmidt et sur sa généralisation p-adique due à H.P. Schlickewei. Ce théorème intervient de façon essentielle dans la preuve du théorème 1, voir [4] . Il s'ensuit en particulier que les démonstrations proposées ont un caractère ineffectif. On trouvera dans [9] un exposé détaillé des résultats effectifs sur les suites récurrentes linéaires, obtenus grâce à la théorie des formes linéaires de logarithmes. Retournant enfin à des questions générales, nous proposons dans le §5 une conjecture concernant la distribution globale de l'ensemble des solutions d'un système d'équations exponentielles-polynômes. On fait ensuite le lien avec deux conjectures classiques, dues respectivement à Hadamard et à Pisot.

2. Un théorème de décomposition.

Soit $r \geqslant 1$ un entier fixé. Nous appellerons fonction

exponentielle-polynôme toute application

$$F : \mathbb{Z}^r \to \mathbb{C}$$

de la forme

$$F(m_1, \ldots, m_r) = \sum_\ell P_\ell(m_1, \ldots, m_r) \prod_{k=1}^{r} a_{k\ell}^{m_k} ,$$

où les P_ℓ désignent des polynômes à coefficients complexes, et les $a_{k\ell}$ des nombres complexes non nuls donnés, ℓ décrivant un ensemble fini d'indices. Notons pour simplifier χ_ℓ la fonction exponentielle

$$\chi_\ell(m_1, \ldots, m_r) = \prod_{k=1}^{r} a_{k\ell}^{m_k} .$$

Il sera commode de considérer F comme une combinaison linéaire

$$F = \sum P_\ell \chi_\ell$$

de caractères $\chi_\ell : \mathbb{Z}^r \to \mathbb{C}^\star$ du groupe $\mathbb{Z}^r$, à coefficients polynomiaux P_ℓ. On notera qu'une telle écriture est unique si l'on suppose de plus que les caractères χ_ℓ sont distincts 2 à 2 et que les coefficients P_ℓ sont non nuls.

On s'intéresse à l'ensemble $S \subseteq \mathbb{Z}^r$, des zéros communs d'une famille finie F_i, $i \in I$, de fonctions exponentielles-polynômes. Nous allons montrer que la forme d'une solution $\mu \in S$, dépend essentiellement des caractères χ_ℓ qui interviennent dans la décomposition des fonctions F_i. Avant de donner le théorème de structure général, examinons les deux cas particuliers suivants.

Dans le cas particulier $r = 1$, le théorème de Skolem-Mahler affirme que S est réunion finie de sous-groupes affines de $\mathbb{Z}$ (c'est-à-dire de sous-ensembles de $\mathbb{Z}$ de la forme $a\mathbb{Z} + b$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$). Lorsque $r \geqslant 2$, il n'existe pas nécessairement une telle décomposition de S comme le montre l'exemple simple (et déjà examiné dans [6]) de l'équation

$$m\, 2^m = 2^n \quad , \quad (m,n) \in \mathbb{Z}^2$$

dont les solutions sont

$$\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} 2^h \\ h+2^h \end{pmatrix} \quad , \quad h \text{ entier} \geqslant 0$$

$$\mu = \underbrace{\begin{pmatrix} 0 \\ h \end{pmatrix}}_{\mu'} + \underbrace{\begin{pmatrix} 2^h \\ 2^h \end{pmatrix}}_{\mu''}$$

On remarque néanmoins que le deuxième terme μ'' appartient à la diagonale de $\mathbb{Z}^2$, c'est-à-dire à un sous-groupe propre de $\mathbb{Z}^2$ et que $|\mu'| << \log |\mu|$, où de façon générale nous noterons

$$|\mu| = \max |m_i| \quad , \text{ si } \quad \mu = (m_1, \ldots, m_r) \in \mathbb{Z}^r \quad .$$

Nous allons montrer que l'existence d'une telle décomposition est un fait général. Commençons par fixer quelques notations.

Soit L un ensemble fini d'indices. Pour chaque $\ell \in L$, soient P_ℓ un polynôme non nul en r variables à coefficients complexes et χ_ℓ un caractère du groupe $\mathbb{Z}^r$ (on ne suppose pas ici que les χ_ℓ sont distincts 2 à 2). Supposons que L est muni d'une partition $L = \coprod_{i \in I} L_i$ et considérons le système d'équations exponentielles-polynômes

$$(\star) \quad \sum_{\ell \in L_i} P_\ell(\mu) \ \chi_\ell(\mu) = 0 \quad , \quad i \in I \quad .$$

Pour toute partition $\mathcal{P}$ de L, induisant sur chacun des sous-ensembles L_i des partitions $L_i = \coprod_{j \in J_i} L_{ij}$, considérons le système obtenu en tronquant les équations de $(\star)$ suivant la partition $\mathcal{P}$:

$$(\star)_{\mathcal{P}} \quad \sum_{\ell \in L_{ij}} P_\ell(\mu) \ \chi_\ell(\mu) = 0 \quad , \quad i \in I \ , \ j \in J_i \quad .$$

Nous dirons qu'une solution $\mu \in S$ est compatible avec la partition $\mathcal{P}$ si μ est solution du système tronqué $(\star)_{\mathcal{P}}$. Si de plus, μ n'est compatible avec aucune partition de L plus fine que $\mathcal{P}$, nous dirons que μ est compatible maximal avec $\mathcal{P}$. Notons alors $S_{\mathcal{P}}$ l'ensemble des solutions compatibles maximales avec $\mathcal{P}$. Il est clair que S est réunion (non nécessairement disjointe) des sous-ensembles $S_{\mathcal{P}}$. Désignons enfin par $H_{\mathcal{P}}$ le sous-groupe de $\mathbb{Z}^r$ obtenu en égalant tous les caractères χ_ℓ qui apparaissent dans une même équation du système tronqué $(\star)_{\mathcal{P}}$, autrement dit

$$H_{\mathcal{P}} = \{\mu \in \mathbb{Z}^r / \chi_\ell(\mu) = \chi_m(\mu) \quad , \quad \forall \ell, m \in L_{ij} \quad , \quad \forall i \in I \ , \quad \forall j \in J_i\}$$

On a alors le

Théorème 1 :

i) Supposons que tous les polynômes P_ℓ soient constants. Alors $S_{\mathcal{P}}$ est réunion finie de sous-groupes affines modulo $H_{\mathcal{P}}$ (autrement dit, de translatés de $H_{\mathcal{P}}$).

ii) Soit μ un élément de $S_{\mathcal{P}}$ tel que tous les coefficients $P_\ell(\mu)$, $(\ell \in L)$, soient $\neq 0$. Alors il existe $\mu' \in Z^r$, $\mu'' \in H_{\mathcal{P}}$ vérifiant :

$$\mu = \mu' + \mu''$$
$$|\mu'| << \log |\mu|$$

Il s'ensuit en particulier que le théorème de Skolem-Mahler se généralise en dimension $r > 1$ dans le cas particulier des combinaisons linéaires de caractères. On trouvera dans le §8 de [4] une démonstration complète de ce théorème. En particulier, la partie i) démontre et précise une conjecture de Chabauty dont on trouvera l'historique dans l'introduction de [4] .

3. Application aux suites récurrentes linéaires.

Nous appellerons suite récurrente linéaire, toute suite de nombres complexes $(u_n)_{n \in \mathbb{Z}}$, non identiquement nulle, vérifiant une relation de la forme

$$u_{n+d} = a_1 u_{n+d-1} + \ldots + a_d u_n \quad , \quad n \in \mathbb{Z} \ ,$$

où $a_1, \ldots, a_d$ désignent des nombres complexes indépendants de n. Classiquement, on s'intéresse plutôt aux valeurs de la suite u_n sur les entiers $n \geqslant 0$.

Supposons que la relation ci-dessus soit de longueur d minimale et considérons le polynôme

$$1 - a_1 X - \ldots - a_d X^d = \prod_{i=1}^{k} (1 - \alpha_i X)^{d_i+1}$$

où les $\alpha_i \in \mathbb{C}^\star$ sont 2 à 2 distincts. Il est alors facile de vérifier que la suite u_n s'écrit de façon unique sous la forme

$$u_n = \sum_{i=1}^{k} f_i(n)\, \alpha_i^n \quad , \quad n \in \mathbb{Z} \quad ,$$

où f_i est un polynôme de degré d_i, autrement dit, u_n est la suite des valeurs d'une fonction exponentielle-polynôme en une variable, non identiquement nulle. Les nombres $\alpha_1, \ldots \alpha_k$ s'appellent les fréquences de u_n et on dira que la suite récurrente linéaire u_n est non dégénérée si le rapport de deux fréquences distinctes n'est jamais une racine de l'unité.

Ainsi un système de relations algébriques entre une ou plusieurs suites récurrentes linéaires détermine un système d'équations exponentielles-polynômes dont les solutions sont essentiellement décrites par les sous-groupes $H_{\mathcal{P}}$ correspondants et dans certains cas particuliers, on peut en déduire des énoncés de finitude. On trouvera dans [2] un rapport et une abondante bibliographie sur ce sujet. Voir aussi [7] , ainsi que [5] dans le cas particulier des suites binaires à coefficients complexes. Voici quelques exemples d'application concrets.

Etudions d'abord les rapports u_m/u_n des valeurs d'une suite récurrente linéaire $(u_n)_{n \in \mathbb{Z}}$, non dégénérée.

On supposera que le nombre k de ses fréquences distinctes est $\geqslant 2$. Pour tout nombre complexe $\lambda \neq 0$, désignons par S_λ l'ensemble des couples $(m,n) \in \mathbb{Z}^2$, solution de l'équation $u_m = \lambda u_n$. On a alors le

Théorème 2 : Il existe un entier $r \in \mathbb{Z}$, indépendant de λ, tel que

i) S_1 est réunion d'un ensemble fini, de la diagonale de $\mathbb{Z}^2$, et éventuellement d'un sous-groupe affine contenu dans la droite $m+n = r$.

ii) Si λ est une racine de l'unité $\neq 1$, S_λ est réunion d'un ensemble fini, et éventuellement d'un sous-groupe affine contenu dans la droite $m+n = r$.

iii) Si λ n'est pas une racine de l'unité, S_λ est un ensemble fini.

En particulier, S_λ est toujours réunion finie de sous-groupes affines de $\mathbb{Z}^2$, de dimension 0 ou 1. On notera que la droite $m+n = r$ peut effectivement contenir une infinité de solutions, comme le montre l'exemple simple de la suite de Fibonacci

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n \quad , \quad n \in \mathbb{Z} \quad .$$

On a alors $F_{-n} = F_n$ si n est impair et $F_{-n} = -F_n$ si n est pair. La détermination de l'entier r, en fonction de la suite (u_n), est tout-à-fait explicite. Il en est de même pour le sous-groupe affine éventuellement associé à λ et il n'y a qu'un nombre fini de valeurs de λ pour lesquelles ce sous-groupe apparaît. Il s'agit simplement de déterminer les valeurs de r et de λ telles que la suite récurrente linéaire $u_{-n+r} - \lambda u_n$ s'annule identiquement sur un sous-groupe affine non-trivial de $\mathbb{Z}$.

Comme corollaire du théorème 2, on retrouve un résultat dû à Schlickewei et à Van der Poorten [8] : le nombre de répétitions dans une telle suite u_n, restreinte aux entiers $n \geqslant 0$, est fini ;

$$\text{card } \{(m,n) \in \mathbb{N}^2 \ , \ m \neq n \ , \ u_m = u_n\} < +\infty \quad .$$

Lorsque la suite u_n est à valeurs rationnelles, Evertse [3] a démontré que le plus grand facteur premier du quotient u_m/u_n (c'est-à-dire le plus grand nombre premier intervenant effectivement

dans la décomposition en facteurs premiers du numérateur et du dénominateur réduit du nombre rationnel u_m/u_n) tendait vers l'infini lorsque $\max(m,n)$ tendant vers l'infini, en supposant que $m \geqslant 0$, $n \geqslant 0$ et $m \neq n$. Il est probable que l'on puisse remplacer cette dernière condition par $m \neq n$, $m+n \neq r$.

Etudions maintenant "l'intersection" de deux suites récurrentes linéaires u_n et v_n, autrement dit, considérons l'équation exponentielle-polynôme plus générale

$$u_m = v_n \quad , \quad (m,n) \in \mathbb{Z}^2 \quad .$$

On supposera que les deux suites u_n et v_n sont non dégénérées. Soit alors

$$u_n = \sum_{i=1}^{k} f_i(n)\ \alpha_i^n \quad , \quad v_n = \sum_{j=1}^{\ell} g_j(n)\ \beta_j^n \quad , \quad n \in \mathbb{Z} \quad ,$$

l'écriture canonique de ces deux suites, comme ci-dessus. Quitte à remplacer u_n par u_{-n} et v_n par v_{-n}, on peut se restreindre à examiner les solutions $(m,n) \in \mathbb{N}^2$. On a alors le

Théorème 3 : Supposons que $k \geqslant 2$, $\ell \geqslant 2$ et que l'équation $u_m = v_n$ ait une infinité de solutions $(m,n) \in \mathbb{N}^2$. Alors $k = \ell$ et il existe deux entiers $r > 0$, $s > 0$, tels que, après réindexation éventuelle des α_i et des β_j, on ait

$$\alpha_i^r = \beta_i^s \quad , \quad 1 \leqslant i \leqslant k \quad .$$

De plus, à un nombre fini d'exceptions près, tout couple $(m,n) \in \mathbb{N}^2$ solution de $u_m = v_n$, vérifie alors le système d'équations binaires

$$f_i(m)\ \alpha_i^m = g_i(n)\ \beta_i^n \quad , \quad 1 \leqslant i \leqslant k \quad .$$

En fait, il est facile de préciser la forme de l'ensemble des solutions d'un tel système binaire. Toujours à un nombre fini

d'exceptions près, ou bien c'est la trace sur $\mathbb{N}^2$ d'un sous-groupe affine de $\mathbb{Z}^2$, ou bien on peut paramétrer cet ensemble par des fonctions exponentielles-polynômes en une variable, comme dans l'exemple $m2^m = 2^n$. Notons que Van der Poorten a énoncé dans [10] un résultat analogue. Le théorème 3 est cependant plus général car il autorise l'un des α_i et l'un des β_j à être une racine de l'unité. De plus, M. Mignotte a démontré dans [6] une version effective de ce théorème lorsque les ensembles de fréquences $(\alpha_1, \ldots, \alpha_k)$ et $(\beta_1, \ldots, \beta_\ell)$ contiennent chacun un élément de valeur absolue dominante.

Il reste à étudier le cas $k = 1$, $\ell \geqslant 2$. L'intersection de u_n et de v_n est alors finie, sauf si α_1 est une racine de l'unité, auquel cas, il se peut qu'elle soit infinie.

4. Démonstrations.

Le principe de démonstration des théorèmes 2 et 3 est le suivant. A chacun de ces deux énoncés est associée une équation exponentielle-polynôme en deux variables et il s'agit d'analyser les dégénérescences possibles (suivant la terminologie de [8]) de ses solutions. En d'autres termes, il s'agit de déterminer les partitions $\mathcal{P}$ du support L de l'équation correspondante telles que l'ensemble $S_{\mathcal{P}}$ des solutions compatibles maximales avec $\mathcal{P}$ soit susceptible de contenir une infinité d'éléments. Des arguments combinatoires simples, joints au théorème 1, permettent alors de prédire la forme de ces partitions.

Donnons par exemple une preuve complète du théorème 3, la démonstration du théorème 2 étant de même nature.

Il s'agit d'étudier l'ensemble S des solutions de l'équation

$$u_m = v_n \quad , \quad (m,n) \in \mathbb{N}^2 \quad ,$$

où

$$u_m = \sum_{i=1}^{k} f_i(m)\, \alpha_i^m \quad , \quad v_n = \sum_{i=1}^{\ell} g_i(n)\, \beta_i^n \quad ,$$

en supposant $k \geqslant 2$, $\ell \geqslant 2$. Le support L de cette équation com-

porte $k + \ell$ éléments qu'il sera commode d'écrire sous la forme

$$L = \{1, 2, \ldots, k, \overline{1}, \overline{2}, \ldots, \overline{\ell}\}$$

où les k premiers termes numérotent les termes correspondants de la somme u_m, tandis que les ℓ derniers numérotent ceux de v_n.

Commençons par les deux lemmes combinatoires suivants.

Lemme 1 : Soit $L = \coprod_{j \in J} L_j$ une partition $\mathcal{P}$ de L vérifiant les propriétés :

i) pour tout j dans J, le cardinal de L_j est $\geqslant 2$,

ii) le sous-groupe associé $H_{\mathcal{P}}$ est non nul.

Alors $k = \ell$ et après avoir éventuellement renuméroté les ensembles de fréquences $(\alpha_1, \ldots, \alpha_k)$ et $(\beta_1, \ldots, \beta_k)$, on peut supposer que

$$J = \{1, \ldots, k\} \quad , \quad L_j = \{j, \overline{j}\} \quad , \quad 1 \leqslant j \leqslant k \quad .$$

De plus, si (r,s) est un élément non nul de $H_{\mathcal{P}}$, on a $rs \neq 0$ et

$$\alpha_j^r = \beta_j^s \quad , \quad 1 \leqslant j \leqslant k \quad .$$

Preuve : Commençons par montrer que les coordonnées r et s d'un élément non nul de $H_{\mathcal{P}}$ sont toutes deux non nulles.

Supposons par exemple que $r \neq 0$, $s = 0$. Soit i un entier compris entre 1 et k. En tant qu'élément de L, cet entier i appartient à un sous-ensemble L_j qui contient un autre élément de L, nécessairement d'une des deux formes :

$$i_1 \ , \ 1 \leqslant i_1 \leqslant k \quad \text{où} \quad \overline{i}_2 \ , \ 1 \leqslant i_2 \leqslant \ell \quad .$$

Par définition du groupe $H_{\mathcal{P}}$, on a alors l'une des deux relations

$$\alpha_i^r = \alpha_{i_1}^r \quad \text{ou} \quad \alpha_i^r = \beta_{i_2}^s = 1 \quad .$$

La première relation est impossible par non-dégénérescence de la suite u_n . Quant à la deuxième relation, elle entraîne que α_i est une racine de l'unité pour $i = 1, \ldots, k$. Comme $k \geqslant 2$, il y a de nouveau contradiction avec la non-dégénérescence de u_n .

Par symétrie, on démontre de même que $r \neq 0$.

Montrons maintenant que chaque sous-ensemble L_j contient au plus un des k premiers (resp. ℓ derniers) éléments de L .

Supposons en effet que

$$i_1, i_2, \ 1 \leqslant i_1 < i_2 \leqslant k \ , \ (\text{resp. } \bar{i}_1, \bar{i}_2, \ 1 \leqslant i_1 < i_2 \leqslant \ell)$$

appartiennent à L_j . Soit (r,s) un élément non nul de $H_{\mathcal{P}}$. On a alors

$$\alpha_{i_1}^r = \alpha_{i_2}^r \quad , \quad (\text{resp. } \beta_{i_1}^s = \beta_{i_2}^s) \quad .$$

Puisque $rs \neq 0$, la non-dégénérescence des suites u_n et v_n montre que ces deux égalités sont impossibles.

Il s'ensuit que L_j contient exactement un des k premiers éléments de L et un des ℓ derniers éléments de L . On a donc

$$k = \ell \quad , \quad \text{card } J = k \quad .$$

Rénumérotant alors les éléments de L , on peut supposer sans restriction que

$$L_j = \{ j \ , \ \bar{j} \} \quad , \quad 1 \leqslant j \leqslant k \quad .$$

Le lemme est donc démontré.

Remarque : Si l'on suppose que $k = 1$, $\ell \geqslant 2$ et que α_1 n'est pas une racine de l'unité, les mêmes arguments montrent qu'il n'existe alors aucune partition $\mathcal{P}$ de L satisfaisant les conditions i) et

ii) du lemme 1. Il s'ensuit que dans ce cas particulier, l'équation

$$u_m = v_n \quad , \quad (m,n) \in \mathbb{Z}^2 \ ,$$

n'a qu'un nombre fini de solutions.

Lemme 2 : Il existe au plus une partition $\mathcal{P}$ de L satisfaisant les conditions i) et ii) du lemme 1, et telle que le sous-groupe associé $H_{\mathcal{P}}$ contienne un élément de coordonnées positives.

Preuve : Soit $\mathcal{P}$ une telle partition. Fixons une numérotation des ensembles de fréquences $(\alpha_1 , \ldots , \alpha_k)$ et $(\beta_1 , \ldots , \beta_k)$ fournie par le lemme 1 , de telle sorte que la partition $\mathcal{P}$ s'écrive

$$L = \coprod_{j=1}^{k} \{j, \overline{j}\} \quad .$$

Si $\mathcal{P}'$ désigne une autre partition de L vérifiant le lemme 2, il existe une permutation σ de l'ensemble des k premiers entiers telle que $\mathcal{P}'$ s'écrive

$$L = \coprod_{j=1}^{k} \{j, \overline{\sigma(j)}\} \quad .$$

Il s'agit de démontrer que σ est l'identité.

Soient alors r, r', s, s' des entiers > 0 tels que (r,s) et (r',s') appartiennent respectivement aux sous-groupes $H_{\mathcal{P}}$ et $H_{\mathcal{P}'}$. Par définition de ces sous-groupes, on a alors les égalités :

$$\alpha_j^r = \beta_j^s \quad , \quad \alpha_j^{r'} = \beta_{\sigma(j)}^{s'} \quad , \quad 1 \leqslant j \leqslant k \quad .$$

On en déduit que

$$\beta_j^a = \beta_{\sigma(j)}^b \quad , \quad 1 \leqslant j \leqslant k \quad ,$$

où $a = r's$ et $b = rs'$ sont des entiers > 0 . Si $a = b$, la non-dégénérescence de la suite v_n montre que σ est l'identité.

Supposons donc que $a \neq b$. Par itération de l'égalité ci-dessus, on vérifie par récurrence sur $n \geqslant 1$ que l'on a

$$\beta_j^{a^n} = \beta_{\sigma^n(j)}^{b^n} \quad , \quad 1 \leqslant j \leqslant k \quad , \quad n \geqslant 1 \quad .$$

En particulier, si n désigne l'ordre de la permutation σ dans le groupe symétrique à k éléments, on a

$$\beta_j^{(a^n-b^n)} = 1 \quad , \quad 1 \leqslant j \leqslant k \quad .$$

L'exposant a^n-b^n est un entier non nul. Il s'ensuit que les fréquences β_j sont toutes des racines de l'unité. Ce dernier cas est donc impossible.

On notera que l'idée de considérer des itérés de σ est due à J.H. Evertse [3] .

Preuve du théorème 3 : Pour chaque partition $\mathcal{P}$ de L , désignons par $S_{\mathcal{P}}$ l'ensemble des solutions de l'équation

$$u_m = v_n \quad , \quad (m,n) \in \mathbb{N}^2 \quad ,$$

qui sont compatibles maximales avec la partition $\mathcal{P}$.

Nous allons montrer qu'il existe une et une seule partition $\mathcal{P}$ de L pour laquelle $S_{\mathcal{P}}$ est un ensemble infini et que cette partition vérifie les conditions des lemmes 1 et 2 ci-dessus. Comme S est réunion de ses sous-ensembles $S_{\mathcal{Q}}$, $\mathcal{Q}$ décrivant l'ensemble des partitions de L , le théorème 3 sera clairement établi. Tout d'abord, puisque S est supposé infini, il existe nécessairement une partition $\mathcal{P}$ de L telle que $S_{\mathcal{P}}$ soit infini. Soit

$$L = \coprod_{j \in J} L_j$$

une telle partition.

Montrons que le cardinal de chacun des sous-ensembles L_j est $\geqslant 2$. En effet, si pour un indice j , on a

$$L_j = \{i\} \quad , \quad (\text{resp. } L_j = \{\bar{i}\}) \quad ,$$

où i désigne un entier compris entre 1 et k (resp. 1 et ℓ), tout élément (m,n) de $S_{\mathcal{P}}$ vérifie l'équation

$$f_i(m)\ \alpha_i^m = 0 \qquad (\text{resp. } g_i(n)\ \beta_i^n = 0) \quad .$$

Il s'ensuit que les entiers m (resp. n) ne prennent qu'un nombre fini de valeurs lorsque (m,n) décrit $S_{\mathcal{P}}$. On est ainsi ramené à un nombre fini d'équations en une variable de la forme

$$v_n = a \quad , \quad (\text{resp. } u_m = b) \quad .$$

Par le théorème de Skolem-Mahler, nous savons que les suites récurrentes linéaires u_n et v_n ne prennent qu'un nombre fini de fois la même valeur.

Montrons maintenant que le sous-groupe $H_{\mathcal{P}}$ associé est de rang un et est engendré par un élément de coordonnées positives.

Le théorème 1 montre tout d'abord que le groupe $H_{\mathcal{P}}$ ne peut être nul. En effet, dans le cas contraire, l'assertion ii) de ce théorème implique l'inégalité

$$\max(m,n) << \operatorname{logmax}(m,n) \quad ,$$

valable pour tout élément (m,n) de $S_{\mathcal{P}}$; d'où provient la contradiction lorsque $\max(m,n)$ est suffisamment grand. Les conditions du lemme 1 sont ainsi satisfaites. Il s'ensuit que le sous-groupe $H_{\mathcal{P}}$ est de rang un car ce sous-groupe de $\mathbb{Z}^2$ ne possède aucun élément non nul ayant l'une de ses deux coordonnées nulle. Désignons alors par (r,s) un générateur de $H_{\mathcal{P}}$ et montrons que r et s ont nécessairement le même signe. Pour cela, utilisons de nouveau le théorème 1 . Tout élément (m,n) de $S_{\mathcal{P}}$ se décompose sous la forme :

$$m = qr + m' \quad , \quad n = qs + n'$$

où q, m', n' désignent des entiers tels que

$$\max(|m'|, |n'|) << \operatorname{logmax}(m,n) \quad .$$

Il s'ensuit en particulier que

$$|rn - sm| \ll \log\max(m,n) \quad .$$

Puisque m et n sont des entiers $\geqslant 0$, il est clair que r et s ont nécessairement le même signe.

Remplaçant éventuellement (r,s) par $(-r, -s)$, on peut supposer sans restriction que $r > 0$, $s > 0$. Ainsi la partition $\mathcal{P}$ considérée vérifie bien les conditions des lemmes 1 et 2 et le théorème 3 est démontré.

5. Questions de densité.

Nous nous intéressons maintenant aux propriétés globales de l'ensemble des solutions d'un système d'équations exponentielles-polynômes. En fait, il s'agit là d'un problème très général puisqu'il contient, entre autre, l'étude de l'ensemble des points entiers d'une variété affine quelconque. Nous examinerons ici des questions de densité, en analogie avec le cas algébrique et les résultats du type "théorème d'irréductibilité de Hilbert".

Etendons tout d'abord la notion de fonction exponentielle-polynôme. Si G est un groupe libre de type fini, on désignera ainsi toute application de G dans $\mathbb{C}$ qui s'exprime par une fonction exponentielle-polynôme en les coordonnées du point dans une base affine de G (c'est-à-dire, non nécessairement centrée à l'origine de G). On notera que cette propriété est indépendante de la base affine choisie. En particulier, la notion de fonction exponentielle-polynôme est bien définie sur toute classe modulo un sous-groupe libre, contenue dans un groupe abélien quelconque.

Reprenons les notations du §2. Fixons une partition $\mathcal{P}$ de L et désignons par Π la projection canonique

$$\Pi : \mathbb{Z}^r \to \mathbb{Z}^r/H \quad .$$

Au vu du théorème 1, il est naturel d'étudier l'image par Π de l'ensemble S des solutions du système $(\star)_{\mathcal{P}}$. Dans le cas particulier de l'équation $m2^m = 2^n$, on peut identifier cette

projection Π à l'application

$$\mathbb{Z}^2 \to \mathbb{Z} \quad , \quad (m,n) \mapsto n-m \quad ,$$

et l'image $\Pi(S)$ est alors égale à $\mathbb{N} \subseteq \mathbb{Z}$. On constate de plus que l'application :

$$\mathbb{Z} \to \mathbb{C}^2 \quad , \quad h \mapsto (2^h , h+2^h) \quad ,$$

formée de deux fonctions exponentielles-polynômes, définit une section de Π au-dessus de $\mathbb{N}$, à valeurs dans l'ensemble S . Dans le cas général, il me semble que la seule manière de construire un ensemble de solutions de $(\star)_{\mathcal{P}}$, dont la projection par Π remplit une large partie de $\mathbb{Z}^r/H_{\mathcal{P}}$, consiste à utiliser une telle section fonctionnelle de Π . La conjecture ci-dessous n'est rien d'autre que la formalisation de cet exemple.

Transformons tout d'abord $(\star)_{\mathcal{P}}$ en un système équivalent de la façon suivante. Pour chaque $i \in I$, $j \in J_i$, choisissons un indice $\ell_{ij} \in L_{ij}$, et divisons l'équation d'indices i,j par $\chi_{\ell_{ij}}$. Par définition du groupe H , pour tout indice $\ell \in L_{i,j}$, le caractère quotient $\chi_\ell/\chi_{\ell_{ij}}$ est égal à 1 sur $H_{\mathcal{P}}$, et se factorise donc par un caractère ψ_ℓ du groupe $\mathbb{Z}^r/H_{\mathcal{P}}$. On peut donc réécrire le système $(\star)_{\mathcal{P}}$ sous la forme

$$(\star)_{\mathcal{P}} \quad : \quad \sum_{\ell \in L_{ij}} P_\ell(\mu)\ \psi_\ell \circ \Pi(\mu) = 0 \quad , \quad i \in I \quad , \quad j \in J_i \quad .$$

Désignons par $\Pi_{\mathbb{C}}$ l'application linéaire

$$\mathbb{C}^r \to (\mathbb{Z}^r/H_{\mathcal{P}}) \otimes \mathbb{C}$$

déduite de Π par extension des scalaires de $\mathbb{Z}$ à $\mathbb{C}$. Il s'ensuit que toute solution μ du système $(\star)_{\mathcal{P}}$, située au-dessus de $\nu = \Pi(\mu)$ vérifie le système d'équations

$$(\star\star)_{\mathcal{P}} \quad \begin{cases} \sum_{\ell \in L_{ij}} P_\ell(\mu)\ \psi_\ell(\nu) = 0 \ , \ i \in I \ , \ j \in J_i \ , \\ \\ \overline{\nu} = \Pi_{\mathbb{C}}(\mu) \end{cases}$$

où $\overline{\nu} = \nu \otimes 1$ désigne l'image de ν dans $(\mathbb{Z}^r/H_{\mathcal{P}}) \otimes \mathbb{C}$.

Pour $\nu \in \mathbb{Z}^r/H_{\mathcal{P}}$ fixé, on a maintenant un système d'équations polynomiales en μ , définissant une sous-variété affine de $\mathbb{C}^r$, dont on recherche les points entiers. Soient alors G un sous-groupe libre de $\mathbb{Z}^r/H_{\mathcal{P}}$, de rang > 0 , et $\Gamma = aG$ une classe modulo G . Par analogie avec le cas algébrique, nous supposerons que la fibre au-dessus d'un point $\nu \in \Gamma$ est en général de dimension 0 , disons pour tout $\nu \in \Gamma$, sauf peut-être sur un sous-ensemble propre réunion finie de sous-groupes affines de Γ . C'est là une hypothèse qui sera vérifiée dans les cas particuliers que nous avons en vue. Supposons aussi qu'il existe un corps de nombres de K , tel que les polynômes P_ℓ soient à coefficients dans K , et que les caractères ψ_ℓ soient à valeurs dans $K^\star$. On peut alors formuler la

Conjecture : Soit T un ensemble fini de places de K , contenant toutes les places archimédiennes de K . Supposons que pour tout élément ν d'un sous-ensemble $N \subset \Gamma$, il existe un r-uplet μ , dont les coordonnées sont des T-entiers de K , vérifiant le système $(\star\star)_{\mathcal{P}}$. Alors si N est "suffisamment dense", (en un sens à définir), il existe un r-uplet σ de fonctions exponentielles-polynômes, définies sur Γ et à valeurs dans K , telles que $\mu = \sigma(\nu)$ soient une solution du système $(\star\star)_{\mathcal{P}}$ pour tout $\nu \in \Gamma$..

Si N est égal à Γ tout entier, ou même à sa "moitié" (c'est-à-dire : $N = a\,\mathbb{N}^s$ après avoir identifié G à $\mathbb{Z}^s$ par le choix d'une base) comme dans l'exemple $m\,2^m = 2^n$, on peut raisonnablement espérer que N est "suffisamment dense" pour que la conjecture soit vraie. Une hypothèse de répartition est néanmoins nécessaire, comme on s'en convaincra aisément.

Pour revenir au problème initial de la structure de l'ensemble S des solutions du système $(\star)_{\mathcal{P}}$, la conjecture s'applique lorsque $\Pi(S) \cap \Gamma$ est "suffisamment dense" dans la classe Γ. Il existe alors une section fonctionnelle σ du système associé $(\star\star)_{\mathcal{P}}$ et cette section, restreinte au sous-ensemble $M \subset \Gamma$ (qui peut-etre vide) des points où σ est à valeurs entières et est une section de Π, fournit une famille de "solutions génériques" du système $(\star)_{\mathcal{P}}$.

L'énoncé conjectural ci-dessus contient les deux conjectures classiques suivantes, qui ont été vérifiées sous certaines hypothèses restrictives (voir par exemple [1]).

Conjecture du quotient de Hadamard : Soient u_n et v_n deux suites récurrentes linéaires, à valeurs dans $\mathbb{Z}$. On suppose que le quotient u_n/v_n est un entier pour tout $n \geqslant 0$ tel que $v_n \neq 0$. Alors il existe une suite récurrente linéaire w_n telle que $u_n = v_n w_n$.

Conjecture de Pisot : Soient h un entier $\geqslant 1$ et u_n une suite récurrente linéaire, tels que u_n soit la puissance h-ième d'un entier pour tout $n \geqslant 0$. Alors il existe une suite récurrente linéaire v_n telle que $u_n = v_n^h$.

On notera que Van der Poorten a annoncé une preuve complète de la conjecture de Hadamard.

Ces deux conjectures sont associées respectivement aux deux équations exponentielles-polynômes à deux variables :

$$u_n = m\, v_n \quad , \quad (m,n) \in \mathbb{Z}^2 \quad ,$$

$$u_n = m^h \quad , \quad (m,n) \in \mathbb{Z}^2 \quad .$$

Désignons par $\mathcal{P}$ la partition triviale (réduite à une seule partie) du support de l'équation correspondante. Le sous-groupe $H_{\mathcal{P}}$ contient toujours le point $(1,0)$ et l'on peut supposer sans restriction que $H_{\mathcal{P}} = \mathbb{Z}(1,0)$, (en effet lorsque l'inclusion est stricte, les deux conjectures ci-dessus sont faciles à vérifier directement).

On peut alors identifier $\mathbb{Z}^2/H_\varphi$ à $\mathbb{Z}$ par l'application

$$\Pi : \mathbb{Z}^2 \to \mathbb{Z} \quad , \quad (m,n) \mapsto n \quad .$$

La conjecture ci-dessus fournit alors une section de $\Pi_{\mathbb{C}}$ au-dessus de $\mathbb{Z}$, autrement dit dans ce cas particulier, une application de $\mathbb{Z}$ dans $\mathbb{C}^2$ de la forme $\sigma(n) = (f(n), n)$, où $f(n)$ désigne une suite récurrente linéiare, vérifiant l'équation correspondante.

BIBLIOGRAPHIE

[1] J.P. BEZIVIN. - Factorisation de suites récurrentes linéaires et applications. Bull. Soc. Math. France, t. 112, 1984, p. 365-376.

[2] L. CERLIENCO, M. MIGNOTTE, F. PIRAS. - Suites récurrentes linéaires, propriétés algébriques et arithmétiques. Publication de l'Université Louis Pasteur, Strasbourg, 1984, 253/P. 141.

[3] J.H. EVERTSE. - On sums of S-units and linear recurrences. Compositio Math., t. 53, 1984, p. 225-244.

[4] M. LAURENT. - Equations diophantiennes exponentielles. Invent. Math., t. 78, 1984, p. 299-327.

[5] D.J. LEWIS, J. TURK. - Repetitiveness in binary sequences. J. Reine angew. Math., t. 356, 1985, p. 19-48.

[6] M. MIGNOTTE. - Une extension du théorème de Skolem-Mahler ; C.R.A.S., t. 288, 1979, p. 233-235.

[7] M. MIGNOTTE, T.N. SHOREY, R. TIJDEMAN. - The distance between terms of an algebraic recurrence sequence ; J. Reine angew. Math., t. 349, 1984, p. 63-76.

[8] H.P. SCHLICKEWEI, A.J. VAN DER POORTEN. - The growth conditions for recurrence sequences. Report 82.0041, Macquarie University, N.S.W. Australia, 1982.

[9] T.N. SHOREY, R. TIJDEMAN. - Exponential diophantine equations, Cambridge University Press, à paraître.

[10] A.J. VAN DER POORTEN. - Identification of rational functions : lost and regained ; C.R. Math. Rep. Acad. Sci. Canada, vol. 4, 1982, n° 5.

Michel LAURENT
Institut Henri Poincaré, UA 763,
11, rue Pierre et Marie Curie
75005 PARIS