ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

JACQUES LABEYRIE

Factorisation de Ritt pour les polynômes exponentiels formels

Annales de la faculté des sciences de Toulouse 5^e série, tome 4, n° 3-4 (1982), p. 281-289
<http://www.numdam.org/item?id=AFST_1982_5_4_3-4_281_0>

Annales Faculté des Sciences Toulouse
Vol IV, 1982, P 281 à 289

FACTORISATION DE RITT POUR LES POLYNOMES EXPONENTIELS FORMELS

Jacques Labeyrie *(1)*

(1) Centre Océanologique de Bretagne, B.P. 337, 29273 Brest Cédex - France.

Résumé : Le théorème de factorisation démontré en 1928 par J.F. Ritt pour les sommes exponentielles dans $\mathbb{C}$, est ici généralisé aux polynômes exponentiels formels dans un corps de caractéristique zéro. Soit exp X la série formelle $\sum_{n=0}^{\infty} \frac{X^n}{n!}$ et $F(X) = \sum_{\ell=1}^{q} a_\ell(X) \exp(\lambda_\ell X)$ avec $a_\ell(X) \in K[X]$. Alors F(X) est dit simple si le $\mathbb{Q}$-espace vectoriel engendré par les λ_i est de dimension 1. On montre que F(X) se factorise sous la forme $\prod_{i=1}^{m} F_i(X) \prod_{j=1}^{n} G_j(X)$ où les F_i sont simples et les G_j irréductibles. De plus cette factorisation est unique si pour tous $i \neq i'$, le $\mathbb{Q}$-espace vectoriel engendré par les $\lambda_{\ell,i}$ de F_i et les $\lambda'_{\ell',i'}$ de $F_{i'}$ n'est pas de dimension 1. (Les résultats sont en fait démontrés en plusieurs variables). L'anneau des polynômes exponentiels est alors un anneau de Gauss non factoriel.

Summary : The Ritt factorization theorem proved in 1928 for exponential sums in $\mathbb{C}$ is now generalized to exponential polynomials in any algebraically closed field K of characteristic zero. Let exp X be the formal series $\sum_{n=0}^{\infty} \frac{X^n}{n!}$ and $F(X) = \sum_{\ell=1}^{q} a_\ell(X) \exp(\lambda_\ell X)$ with $a_\ell(X) \in K[X]$. Then F(X) is said to be *simple* if the $\mathbb{Q}$-linear space generated by the λ_i has dimension 1. We prove then F has a factorization in the form $\prod_{i=1}^{m} F_i(X) \prod_{j=1}^{n} G_j(X)$ with the F_i simple and the G_j irreductible. Such a factorization is unique provited the $\mathbb{Q}$-linear space generated by the $\lambda_{\ell,i}$ of F_i and the $\lambda_{\ell',i'}$ of $F_{i'}$ is not of dimension 1, whenever $i \neq i'$. (Actually results are proved in several variables). The ring of the exponential polynomials is then a Gauss ring but not a factorization ring.

INTRODUCTION

Rappelons qu'un polynôme exponentiel complexe est dit simple si le $\mathbb{Q}$-espace engendré par ses fréquences est de dimension 1. Le théorème établi par J.F. Ritt [2] en 1927, permet de factoriser tout polynôme exponentiel complexe en un nombre fini de facteurs simples et de facteurs irréductibles. Nous proposons ici une généralisation de ce théorème à l'anneau E_m des polynômes exponentiels formels de K^m, valable dans tout corps K de caractéristique nulle. Nous utilisons pour cela une nouvelle démonstration qui évite tout usage de la structure d'espace de dimension 2 sur IR de $\mathbb{C}$. Il en résulte que E_m est un anneau de Gauss non noethérien.

1. - GENERALITES

Soit K[[Y]] l'algèbre des séries formelles à coefficients dans K, on notera

$$\exp(Y) = \sum_{n \geqslant o} \frac{Y^n}{n!} \text{ la série exponentielle formelle.}$$

Soient

$$\alpha = (\alpha_1,...,\alpha_m) \qquad \text{et} \qquad \nu = (n_1,...,n_m) \in \mathbb{N}^m.$$

Dans l'anneau des polynômes $K[X_1,...,X_m]$, on notera

$$<\alpha,X> = \alpha_1 X_1 + ... + \alpha_m X_m ,$$

$$X^\nu = X_1^{n_1} X_2^{n_2} ... X_m^{n_m}$$

et

$$\nu ! = n_1 ! n_2 ! ... n_m ! ;$$

on a alors

$$\exp(<\alpha,X>) = \sum_{\nu \in \mathbb{N}^m} \frac{X^\nu \alpha^\nu}{\nu !}$$

Dans l'algèbre $K[[X_1,...,X_m]]$ des séries formelles à m indéterminées, on appelle *polynôme exponentiel formel* de K^m une série entière formelle à m indéterminée de la forme

$$f(X) = a_o(X) \exp(<\alpha_o,X>) + ... + a_n(X) \exp(<\alpha_n,X>),$$

$\alpha_i \in K^m$, $\alpha_i \neq \alpha_j$ $\forall\, i \neq j$, $a_i(X)$ est un élément non nul de K[X]. Les α_i sont appelés *les fréquences* de f(X), et les polynômes $a_i(X)$ *les coefficients* de f(X).

L'ensemble E_m des polynômes exponentiels formels de K^m est clairement une sous-algèbre de l'algèbre $K[[X_1,...,X_m]]$.

Les inversibles de E_m sont de la forme $\lambda \exp(<\alpha,X>)$ où $\lambda \in K^*$ et $\alpha \in K^m$.

Un élément $f(X)$ de E_m à coefficients dans K est dit *simple* si les fréquences de $f(X)$ engendrent un $\mathbb{Q}$-espace de dimension 1. Deux éléments simples de E_m tels que leurs fréquences engendrent un Q-espace de dimension deux sont dits *incommensurables.*

REMARQUE 1. *Si le corps* K *est algébriquement clos, on voit qu'un élément simple de* E_m *n'est jamais irréductible dans* E_m.

En effet, soit $P(Y) \in K[Y]$ et pour tout $h \in \mathbb{N}^*$, soit $P_h(Y) = P(Y^h)$. Alors $P(\exp(<\alpha,X>)) = P_h(\exp(<\frac{\alpha}{h},x>))$.

Les éléments qui sont à la fois simples et irréductibles seront caractérisés au § 4.

2. - DIVISIBILITE DANS E_m ET FREQUENCES

Pour établir le théorème de Ritt, on appliquera la proposition 1 qui va suivre. On dira qu'un élément de E_m est *de la forme* ($\mathscr{F}$) s'il s'écrit

$$a_0(X) + a_1(X) \exp(<\alpha_1,X>) + ... + a_n(X) \exp(<\alpha_n,X>),$$

et si le $\mathbb{Q}$-espace W_f engendré par $\alpha_1,...,\alpha_n$ admet une base $w_1,...,w_q$ dans laquelle chaque α_i a toutes ses composantes rationnelles non négatives. Enfin, on notera E'_m le sous-ensemble des éléments de E_m dont l'une au moins des fréquences est nulle.

PROPOSITION 1. *Soit* $f(X)$ *un élément de* E_m *de la forme* ($\mathscr{F}$) *et soit* $g(X) \in E'_m$. *Alors il existe une base de* W_f, *telle que :*

si $f(X)$ *se factorise sous la forme* $g(X) \cdot h(X)$ *où* $h \in E'_m$, *les composantes dans cette base de chaque fréquence de* $g(X)$ *soient rationnelles* $\geqslant 0$.

Preuve. Soit $f(X) \in E_m$ de la forme ($\mathscr{F}$). Soit $g(X) \in E'_m$,

$$g(X) = b_0(X) \exp(<\beta_0,X>) + ... + b_r(X) \exp(<\beta_r,X>) \text{ ; où } \beta_0 = 0.$$

Soit $h(X) \in E'_m$ tel que l'on ait $f(X) = h(X) \cdot g(X)$, et écrivons

$$h(X) = c_0(X) \exp(<\gamma_0,X>) + ... + c_\ell(X) \exp(<\gamma_\ell,X>) \text{ où } \gamma_0 = 0.$$

Si on note θ_u, $o \leqslant u \leqslant t$, l'ensemble des valeurs $\beta_j + \gamma_k$, $o \leqslant j \leqslant r$, $o \leqslant k \leqslant \ell$, alors on voit que pour tout $i = o,...,n$

$$a_i(X) = \sum_{\substack{j,k \\ \beta_j + \gamma_k = \alpha_i}} b_j(X)\, c_k(X)$$

et que

$$\sum_{\substack{j,k \\ \beta_j + \gamma_k = \theta_u}} b_j(X)\, c_k(X) = 0 \text{ si } \theta_u \notin \{\alpha_o,...,\alpha_n\}$$

a) Supposons qu'il existe un certain β_j, noté w_o, n'appartenant pas à W_f. Grâce au théorème de la base incomplète on peut trouver une base

$$w_o, w_1, ..., w_q, ..., w_s$$

du $\mathbb{Q}$-espace U engendré par l'ensemble des fréquences de f(X), g(X) et h(X). On note $\geqslant$ l'ordre lexicographique dans U relatif à la base $w_o,...,w_s$.

Soit β (resp γ) le plus grand des éléments $\beta_o,...,\beta_r$ (resp $\gamma_o,...,\gamma_\ell$) pour l'ordre $\geqslant$. On pose $\theta = \beta + \gamma$, et on voit que :

$$\sum_{\beta_j + \gamma_k = \theta} b_j(X)\, c_k(X) = b_\beta(X) \,.\, c_\gamma(X) \neq 0$$

Ainsi θ est une fréquence de f(x) qui a une composante non nulle sur w_o, d'où la contradiction. Par suite on a $U = W_f$.

b) Supposons que pour $j = j_o$ l'élément β_j admette une composante négative sur la base $w_1,...,w_q$; il existe donc une permutation σ du groupe symétrique Σ_q telle que β_{j_o} soit négatif pour l'ordre lexicographique dans W_f relatif à la base $w_{\sigma(1)},...,w_{\sigma(q)}$ (noté $\geqslant$).

Soit β' (resp γ') le plus petit des éléments $\beta_o,...,\beta_r$ (resp $\gamma_o,...,\gamma_\ell$) pour l'ordre $\geqslant$. On pose $\theta' = \beta' + \gamma'$ et on voit que,

$$\sum_{\beta_j + \gamma_k = \theta'} b_j(X)\, c_k(X) = b_{\beta'}(X) \,.\, c_{\gamma'}(X) \neq 0$$

Ainsi θ' est une fréquence de f(x) qui a une composante négative sur $w_{\sigma(1)}$ d'où la contradiction.

3. - THEOREME DE FACTORISATION DE RITT

On se propose de démontrer dans K^m le théorème de Ritt.

THEOREME 1. *Tout élément de* E_m *se factorise de façon unique, à un facteur inversible près, sous la forme*

$$(f_1(X)...f_\ell(X))\ (g_1(X)...g_n(X))$$

où les $f_i(X)$ *sont des éléments de* E_m *simples, deux à deux incommensurables, et les* $g_i(X)$ *sont des éléments de* E_m *irréductibles, non associés à un élément simple.*

On aura besoin, tout d'abord, de la proposition suivante :

PROPOSITION 2. *Soit* V *un espace vectoriel sur* K. *Pour tout* $v \in V$, *soit* t_v *la translation de* $V : x \to x + v$. *Soit* S *une partie finie de* V.
Alors il existe $v \in S$ *et une base* $\mathscr{B}$ *du* $\mathbb{Q}$*-espace* W *engendré par* $t_{-v}(S)$ *tels que chaque élément de* $t_{-v}(S \setminus \{v\})$ *ait dans la base* $\mathscr{B}$ *toutes ses composantes rationnelles positives.*

La démonstration de la propriété 2 est immédiate à partir des deux lemmes qui suivent.

LEMME 1. *Soit* T *une partie finie de* $\mathbb{Q}^\ell$.

Pour qu'il existe une base $\mathscr{B}_0$ *de* $\mathbb{Q}^\ell$ *dans laquelle chaque élément de* T *ait toutes ses coordonnées positives il suffit qu'il existe une base* $\mathscr{B}_1$ *de* $\mathbb{Q}^\ell$ *dans laquelle tous les éléments de* T *aient leur n-uplet de coordonnées positif pour l'ordre lexicographique.*

Preuve. Soit $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant \ell \\ 1 \leqslant j \leqslant \ell}}$ une matrice carrée régulière à coefficients rationnels positifs. Soient $t_1,...,t_\ell$ des rationnels.

On note A' la matrice carrée

$$(a'_{i,j})_{\substack{1 \leqslant i \leqslant \ell \\ 1 \leqslant j \leqslant \ell}} \quad \text{où} \quad a'_{i,j} = t_j\, a_{ij}$$

On montre qu'il existe alors des rationnels tous non nuls $t_1,...,t_\ell$ tels que la base $\mathscr{B}_0$ de $\mathbb{Q}^\ell$, pour laquelle la matrice de changement de base de $\mathscr{B}_0$ à $\mathscr{B}_1$ est la matrice A', satisfasse la condition du lemme.

LEMME 2. *Soit* T *une partie finie de* $\mathbb{Q}^\ell$. *S'il existe une base* $\mathscr{B}_o$ *de* $\mathbb{Q}^\ell$ *dans laquelle les éléments de* T *ont leurs coordonnées positives, alors il existe une base* $\mathscr{B}$ *du sous-espace* W *engendré par* T *dans laquelle les éléments de* T *ont leurs coordonnées positives.*

Preuve. Soit $\mathscr{B}_o = (e_1,...,e_\ell)$ et soient $\varphi_1,...,\varphi_\ell$ les fonctions coordonnées associées à la base $\mathscr{B}_o$, alors on voit que pour tout $\alpha \in T$ on a :

$$\alpha = \sum_{1 \leqslant i \leqslant \ell} \varphi_i(\alpha) \cdot e_i \quad \text{où} \quad \varphi_i(\alpha) > o, \quad 1 \leqslant i \leqslant \ell.$$

Soit W* le dual de W et soit $\varphi_i^* \in W^*$ défini comme la restriction de φ_i à W ; alors il existe une permutation σ du groupe symétrique Σ_ℓ, et une base $\mathscr{B} = (f_1,...,f_q)$ de W dont les fonctions coordonnées sont les formes $\varphi^*_{\sigma(1)},...,\varphi^*_{\sigma(q)}$.

Par suite chaque élément de T a dans la base $\mathscr{B}$ de W toutes ses composantes rationnelles positives.

Preuve du Théorème 1. Tout d'abord on va mettre en évidence un problème polynômial équivalent au problème de la factorisation d'un élément de E_m.

Soit $V = K^m$, soit f(X) un élément de E_m, et soit S le système des fréquences de f(X). Si on applique la proposition 2, il est alors clair que f(X) admet un associé de la forme ($\mathscr{F}$).

On peut donc se ramener au cas où f(X) est de la forme ($\mathscr{F}$).

On note W_f le Q-espace engendré par S, et on note $w_1,...,w_q$ une base de W_f dans laquelle chaque fréquence de f(X) a toutes ses composantes non négatives que l'on supposera entières (quitte à remplacer w_i par un de ses multiples rationnels que l'on note encore w_i).

On pose $Y_i = \exp(< w_i,x >)$ $1 \leqslant i \leqslant q$, et par suite f(X) s'identifie à un élément $Q(Y_1,...,Y_q)$ de $K[X][Y_1,...,Y_q]$.

Supposons maintenant que f(X) se factorise dans E'_m sous la forme

$$f_1(X) \ldots f_\ell(X),$$

alors d'après la proposition 1 on voit que les composantes des fréquences de chaque $f_i(X)$ dans la base $w_1,...,w_q$ sont rationnelles non négatives ; par conséquent on peut trouver des entiers positifs $t_1,...,t_q$ et des éléments

$$Q_1(Y_1,...,Y_q),...,Q_\ell(Y_1,...,Y_q) \text{ de } K[X][Y_1,...,Y_q]$$

tels que l'on ait :

$$Q(Y_1^{t_1},...,Y_q^{t_q}) = Q_1(Y_1,...,Y_q) \dots Q_\ell(Y_1,...,Y_q)$$

Réciproquement, si pour des entiers positifs $t_1,...,t_q$ il existe une décomposition de

$Q(Y_1^{t_1},...,Y_q^{t_q})$ de la forme $Q_1,...,Q_\ell$.

Où pour tout $i = 1,...,\ell$ on a $Q_i(Y_1,...,Y_q) \in K[X][Y_1,...,Y_q]$, il est alors clair que $f(X)$ se factorise dans E'_m sous la forme $f_1,...,f_\ell$, où pour tout $i = 1,...,\ell$ on a

$$f_i(X) = Q_i(\exp(<\frac{w_1}{t_1}, X>),..., \exp(<\frac{w_q}{t_q}, X>)$$

On est donc ramené au problème suivant, qui est purement algébrique : *Etant donné un polynôme* $Q(Y_1,...,Y_q)$ *que l'on peut supposer irréductible, pour quels entiers positifs* $t_1,...,t_q$ *le polynôme* $Q(Y_1^{t_1},...,Y_q^{t_q})$ *n'est-il pas irréductible ?*

On résoud ce problème en raisonnant sur des polynômes primaires en suivant, dans ses grandes lignes, la méthode de Ritt [2] (une démonstration détaillée est donnée dans [1]).

4. - APPLICATIONS

Rappelons qu'un anneau commutatif A est appelé *anneau de Gauss* si tout couple d'éléments de A admet un PGCD.

THEOREME 2. *L'anneau* E_m *est un anneau de Gauss non factoriel et non noetherien.*

Preuve. Le théorème 1 permet de montrer que E_m est un anneau de Gauss. Pour voir que E_m n'est pas factoriel il suffit de considérer :

$$f = 1 - \exp(Y) = (1 - \exp(\frac{Y}{2^n})) \prod_{h=1}^{n} (1 + \exp(\frac{Y}{2^h})), \quad n \in \mathbb{N}.$$

Par ailleurs on peut maintenant caractériser les éléments simples irréductibles.

THEOREME 3. *Un élément simple* $P(\exp < \alpha,x >)$ *est irréductible si et seulement si* $P_h(Y)$ *est irréductible dans* $K[Y]$ *pour tout* $h \in \mathbb{N}^*$.

Preuve. Supposons d'abord qu'il existe $h \in \mathbb{N}^*$ tel que P_h ne soit pas irréductible :

$P_h(Y) = R(Y)T(Y)$ où $R, T \in K[Y] \setminus K$. Alors l'élément $g(X) = R(\exp < \frac{\alpha}{h}, X >)$ est un diviseur propre de f dans E_m. Réciproquement supposons que $f(X) = g(X)\, \ell(X)$ où g, ℓ sont non inversibles dans E_m. Alors d'après la proposition 1, les fréquences de g et ℓ appartiennent à αQ_+ et on peut donc écrire $\ell(X)$ sous la forme $R(\exp < \frac{\alpha}{h}, X >)$ et $g(X)$ sous la forme $T(\exp < \frac{\alpha}{h}, X >)$ où $R,T \in K[Y] \setminus K$ et on voit que $P_h(Y) = R(Y)\, T(Y)$ n'est pas irréductible.

COROLLAIRE. *Soit* A *un anneau factoriel de caractéristique nulle et qui n'est pas un corps. Soit* K *le corps des fractions de* A. *Alors l'anneau* E_m *contient des éléments simples irréductibles.*

Preuve. On considère $P(Y) = Y^n + q \in A[Y]$ où q est un élément premier de A ; alors d'après le critère d'Eisenstein on sait que $P_h(Y)$ est irréductible dans K[Y] pour tout $h \in \mathbb{N}^*$ et on voit donc que pour tout $\alpha \in K^m$, l'élément $P(\exp < \alpha, X >)$ de E_m est simple et irréductible d'après le théorème 3.

REFERENCES

[1] J. LABEYRIE. *«Polynômes exponentiels ultramétriques»*. Thèse de 3ème cycle, Université de Bordeaux I (1981).

[2] J.F. RITT. *«A factorization theory for functions* $\sum_{1 \leqslant i \leqslant n} a_i \exp(\alpha_i z)$*»*. Trans. Amer. Math. Soc. 29 (1927), pp. 584-596.

(Manuscrit reçu le 3 février 1982)