

JACQUES LABEYRIE

**Factorisation de Ritt pour les polynômes exponentiels formels**

*Annales de la faculté des sciences de Toulouse 5<sup>e</sup> série*, tome 4, n° 3-4 (1982), p. 281-289

[http://www.numdam.org/item?id=AFST\\_1982\\_5\\_4\\_3-4\\_281\\_0](http://www.numdam.org/item?id=AFST_1982_5_4_3-4_281_0)

© Université Paul Sabatier, 1982, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## FACTORISATION DE RITT POUR LES POLYNOMES EXPONENTIELS FORMELS

Jacques Labeyrie <sup>(1)</sup>

(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  $\lambda_i$  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  $\lambda_i$  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  $G_j$  irreducible. Such a factorization is unique provided 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  $\mathbb{R}$  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

$$\exp(Y) = \sum_{n \geq 0} \frac{Y^n}{n!} \text{ la série exponentielle formelle.}$$

Soient

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

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

$$\langle \alpha, X \rangle = \alpha_1 X_1 + \dots + \alpha_m X_m,$$

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

et

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

on a alors

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

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

$$f(X) = a_0(X) \exp(\langle \alpha_0, X \rangle) + \dots + a_n(X) \exp(\langle \alpha_n, X \rangle),$$

$\alpha_i \in K^m$ ,  $\alpha_i \neq \alpha_j \quad \forall i \neq j$ ,  $a_i(X)$  est un élément non nul de  $K[X]$ . Les  $\alpha_i$  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  $K[[X_1, \dots, X_m]]$ .

Les inversibles de  $E_m$  sont de la forme  $\lambda \exp(\langle \alpha, X \rangle)$  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  $\mathbb{Q}$ -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  $P(\exp(\langle \alpha, X \rangle)) = P_h(\exp(\langle \frac{\alpha}{h}, X \rangle))$ .

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 (  $\mathcal{F}$  ) s'il s'écrit

$$a_0(X) + a_1(X) \exp(\langle \alpha_1, X \rangle) + \dots + a_n(X) \exp(\langle \alpha_n, X \rangle),$$

et si le  $\mathbb{Q}$ -espace  $W_f$  engendré par  $\alpha_1, \dots, \alpha_n$  admet une base  $w_1, \dots, w_q$  dans laquelle chaque  $\alpha_i$  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 (  $\mathcal{F}$  ) 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  $\geq 0$ .

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

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

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

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

Si on note  $\theta_u$ ,  $0 \leq u \leq t$ , l'ensemble des valeurs  $\beta_j + \gamma_k$ ,  $0 \leq j \leq r$ ,  $0 \leq k \leq \ell$ , alors on voit que pour tout  $i = 0, \dots, n$

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

et que

$$\sum_{\substack{j,k \\ \beta_j + \gamma_k = \theta_u}} b_j(X) c_k(X) = 0 \text{ si } \theta_u \notin \{\alpha_0, \dots, \alpha_n\}$$

a) Supposons qu'il existe un certain  $\beta_j$ , noté  $w_0$ , n'appartenant pas à  $W_f$ . Grâce au théorème de la base incomplète on peut trouver une base

$$w_0, w_1, \dots, w_q, \dots, w_s$$

du  $\mathbb{Q}$ -espace  $U$  engendré par l'ensemble des fréquences de  $f(X)$ ,  $g(X)$  et  $h(X)$ . On note  $\geq$  l'ordre lexicographique dans  $U$  relatif à la base  $w_0, \dots, w_s$ .

Soit  $\beta$  (resp  $\gamma$ ) le plus grand des éléments  $\beta_0, \dots, \beta_r$  (resp  $\gamma_0, \dots, \gamma_\ell$ ) pour l'ordre  $\geq$ . On pose  $\theta = \beta + \gamma$ , et on voit que :

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

Ainsi  $\theta$  est une fréquence de  $f(x)$  qui a une composante non nulle sur  $w_0$ , d'où la contradiction. Par suite on a  $U = W_f$ .

b) Supposons que pour  $j = j_0$  l'élément  $\beta_j$  admette une composante négative sur la base  $w_1, \dots, w_q$  ; il existe donc une permutation  $\sigma$  du groupe symétrique  $\Sigma_q$  telle que  $\beta_{j_0}$  soit négatif pour l'ordre lexicographique dans  $W_f$  relatif à la base  $w_{\sigma(1)}, \dots, w_{\sigma(q)}$  (noté  $\geq$ ).

Soit  $\beta'$  (resp  $\gamma'$ ) le plus petit des éléments  $\beta_0, \dots, \beta_r$  (resp  $\gamma_0, \dots, \gamma_\ell$ ) pour l'ordre  $\geq$ . On pose  $\theta' = \beta' + \gamma'$  et on voit que,

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

Ainsi  $\theta'$  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*

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

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  $V : x \rightarrow x + v$ . Soit  $S$  une partie finie de  $V$ .*

*Alors il existe  $v \in S$  et une base  $\mathcal{B}$  du  $\mathbb{Q}$ -espace  $W$  engendré par  $t_{-v}(S)$  tels que chaque élément de  $t_{-v}(S \setminus \{v\})$  ait dans la base  $\mathcal{B}$  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  $\mathcal{B}_0$  de  $\mathbb{Q}^\ell$  dans laquelle chaque élément de  $T$  ait toutes ses coordonnées positives il suffit qu'il existe une base  $\mathcal{B}_1$  de  $\mathbb{Q}^\ell$  dans laquelle tous les éléments de  $T$  aient leur  $n$ -uplet de coordonnées positif pour l'ordre lexicographique.*

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

$t_1, \dots, t_\ell$  des rationnels.

On note  $A'$  la matrice carrée

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

On montre qu'il existe alors des rationnels tous non nuls  $t_1, \dots, t_\ell$  tels que la base  $\mathcal{B}_0$  de  $\mathbb{Q}^\ell$ , pour laquelle la matrice de changement de base de  $\mathcal{B}_0$  à  $\mathcal{B}_1$  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  $\mathcal{B}_0$  de  $\mathbb{Q}^\ell$  dans laquelle les éléments de  $T$  ont leurs coordonnées positives, alors il existe une base  $\mathcal{B}$  du sous-espace  $W$  engendré par  $T$  dans laquelle les éléments de  $T$  ont leurs coordonnées positives.

Preuve. Soit  $\mathcal{B}_0 = (e_1, \dots, e_\ell)$  et soient  $\varphi_1, \dots, \varphi_\ell$  les fonctions coordonnées associées à la base  $\mathcal{B}_0$ , alors on voit que pour tout  $\alpha \in T$  on a :

$$\alpha = \sum_{1 \leq i \leq \ell} \varphi_i(\alpha) \cdot e_i \text{ où } \varphi_i(\alpha) > 0, \quad 1 \leq i \leq \ell.$$

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

Par suite chaque élément de  $T$  a dans la base  $\mathcal{B}$  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  $(\mathcal{F})$ .

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

On note  $W_f$  le  $\mathbb{Q}$ -espace engendré par  $S$ , et on note  $w_1, \dots, w_q$  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  $Y_i = \exp(\langle w_i, x \rangle)$   $1 \leq i \leq q$ , et par suite  $f(X)$  s'identifie à un élément  $Q(Y_1, \dots, Y_q)$  de  $K[X][Y_1, \dots, Y_q]$ .

Supposons maintenant que  $f(X)$  se factorise dans  $E_m^1$  sous la forme

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

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

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

tels que l'on ait :

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

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

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

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

$$f_i(X) = Q_i(\exp\langle \frac{w_1}{t_1}, X \rangle, \dots, \exp\langle \frac{w_q}{t_q}, X \rangle)$$

On est donc ramené au problème suivant, qui est purement algébrique : *Etant donné un polynôme  $Q(Y_1, \dots, Y_q)$  que l'on peut supposer irréductible, pour quels entiers positifs  $t_1, \dots, t_q$  le polynôme  $Q(Y_1^{t_1}, \dots, Y_q^{t_q})$  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  $P(\exp\langle \alpha, x \rangle)$  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  $g(X) = R(\exp \langle \frac{\alpha}{h}, X \rangle)$  est un diviseur propre de  $f$  dans  $E_m$ . Réciproquement supposons que  $f(X) = g(X) \ell(X)$  ou  $g, \ell$  sont non inversibles dans  $E_m$ . Alors d'après la proposition 1, les fréquences de  $g$  et  $\ell$  appartiennent à  $\alpha Q_+$  et on peut donc écrire  $\ell(X)$  sous la forme  $R(\exp \langle \frac{\alpha}{h}, X \rangle)$  et  $g(X)$  sous la forme  $T(\exp \langle \frac{\alpha}{h}, X \rangle)$  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  $P(\exp \langle \alpha, X \rangle)$  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  $\sum_{1 \leq i \leq n} a_i \exp(\alpha_i z)$* ». Trans. Amer. Math. Soc. 29 (1927), pp. 584-596.

(Manuscrit reçu le 3 février 1982)