RAIRO. INFORMATIQUE THÉORIQUE

GUY VIRY

Factorisation des polynômes à plusieurs variables

RAIRO. Informatique théorique, tome 14, n° 2 (1980), p. 209-223

<http://www.numdam.org/item?id=ITA_1980__14_2_209_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 14, n° 2, 1980, p. 209 à 223)

FACTORISATION DES POLYNÔMES A PLUSIEURS VARIABLES (*)

par Guy VIRY (1)

Communiqué par J. BERSTEL

Résumé. — *On donne un algorithme généralisant celui de Musser et Wang aux polynômes à plusieurs variables à coefficients dans* $\mathbb{K}$ *où* $\mathbb{K}=\mathbb{Z}$, $\mathbb{R}$ *ou* $\mathbb{C}$. *Le polynôme donné* $P(x_1, \ldots, x_n)$ *est d'abord transformé en un polynôme unitaire* $\overline{P}(x_1, \ldots, x_n)$, *puis on factorise* $\overline{P}(x_1, 0, \ldots, 0)$; *à chacun des diviseurs obtenus* $q_i \in \mathbb{K}[x_1]$ *on associe* $Q_i \in \mathbb{K}[x_1, \ldots, x_n]$ *tel que tout diviseur* Q *de* $\overline{P}$ *soit égal à un produit* $Q_{i_1} \ldots Q_{i_m}$. *La recherche des diviseurs de* $\overline{P}$ *est facilitée grâce à un critère de divisibilité qui permet de vérifier si* $Q_{i_1} \ldots Q_{i_m}$ *divise* $\overline{P}$ *sans effectuer la division.*

Abstract. — *We give an algorithm that generalizes the algorithm of Musser and Wang to the multivariate polynomials over* $\mathbb{K}$ *where* $\mathbb{K}=\mathbb{Z}$, $\mathbb{R}$ *or* $\mathbb{C}$. *The given polynomial* $P(x_1, \ldots, x_n)$ *is first reduced to a monic polynomial* $\overline{P}(x_1, \ldots, x_n)$, *then we factorize* $\overline{P}(x_1, 0, \ldots, 0)$; *we use the factors* q_i *of* $\overline{P}(x_1, 0, \ldots, 0)$ *to construct polynomials* $Q_i \in \mathbb{K}[x_1, \ldots, x_n]$ *such that each factor* Q *of* $\overline{P}$ *is equal to a product* $Q_{i_1} \ldots Q_{i_m}$. *The search for the factors of* $\overline{P}$ *is simplified by a theorem that allows to test if* $Q_{i_1} \ldots Q_{i_m}$ *is a factor of* $\overline{P}$ *without executing the division.*

1. INTRODUCTION

La factorisation des polynômes à plusieurs variables à coefficients entiers et à coefficients dans une extension algébrique finie de $\mathbb{Q}$ a été étudiée par [3, 5 à 8]; l'algorithme est implémenté sur ordinateur dans le système MACSYMA (projet MAC, M.I.T.), mais il se complique lorsque le polynôme n'est pas unitaire; de plus la recherche des diviseurs réels du polynôme est longue.

La méthode proposée ici est valable lorsque les coefficients du polynôme sont entiers, réels ou complexes. On transforme d'abord le polynôme donné en un polynôme unitaire. On utilise une méthode de factorisation des polynômes à une variable. Pour les polynômes à coefficients entiers on choisit la méthode de Berlekamp [1] et pour les polynômes à coefficients réels ou complexes on choisit une méthode d'analyse numérique, par exemple les méthodes de Bairstow et de

(*) Reçu mai 1979, et dans sa forme définitive octobre 1979.
(1) Département de Mathématiques, Faculté des Sciences, Abidjan.

Newton. Une des étapes de la factorisation consiste à décomposer des fractions rationnelles en éléments simples; on utilise la méthode proposée par Kung et Tang dans [2]. On traite entièrement un exemple de factorisation d'un polynôme à trois variables, puis on étudie la complexité des calculs en majorant le nombre d'opérations dans le cas des polynômes à coefficients entiers.

2. FACTORISATION D'UN POLYNÔME P

Dans la suite on considère les polynômes de $\mathbb{K}[x, x_1, \ldots, x_n]$ où $\mathbb{K}=\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$. Pour tout polynôme P de $\mathbb{K}[x, x_1, \ldots, x_n]$ on note ∂P le degré de P suivant x. Supposons que P soit ordonné suivant les puissances croissantes de x. On dit que P est *unitaire* en x si le coefficient du monôme de degré le plus élevé en x est égal à 1. Rendre P unitaire en x revient en fait à l'écrire sous la forme $P=A x^r+B(x_1, \ldots, x_n)x^{r-1}+\ldots+D(x_1, \ldots, x_n)$ où $A\in\mathbb{K}$; en effet si P s'écrit sous cette forme on peut le rendre facilement unitaire en le divisant par A lorsque $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ et en prenant $x'=A x$ comme nouvelle variable lorsque $\mathbb{K}=\mathbb{Z}$.

Considérons un polynôme P de $\mathbb{A}[x_1, \ldots, x_n]$ où $\mathbb{A}=\mathbb{K}[x]$. On note δ le degré de P suivant $x_1, \ldots, x_n$ et on écrit P sous la forme $P^0+P^1+\ldots+P^\delta$ où P^i est une forme de degré i de $\mathbb{A}[x_1, \ldots, x_n]$. On veut décomposer P en un produit de s polynômes irréductibles $Q_1 \ldots Q_s$. On a la relation

$$P^0+\ldots+P^i+\ldots=(Q_1^0+Q_1^1+\ldots)(Q_2^0+Q_2^1+\ldots)\ldots(Q_s^0+Q_1^1+\ldots). \quad (1)$$

La relation (1) est équivalente au système suivant :

$$\left.\begin{aligned} Q_1^0 Q_2^0 \ldots Q_s^0 &= P^0, \\ Q_1^1 Q_2^0 \ldots Q_s^0+Q_1^0 Q_2^1 Q_3^0 \ldots Q_s^0+\ldots+ &= P^1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ Q_1^k Q_2^0 \ldots Q_s^0+Q_1^0 Q_2^k Q_3^0 \ldots Q_s^0+\ldots &= \overline{P}^k, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \end{aligned}\right\} \quad (2)$$

où

$$\overline{P}^k=P^k-\sum_{\substack{0\leq i_1, \ldots, i_s<k \\ i_1+\ldots+i_s=k}} Q_1^{i_1} Q_2^{i_2} \ldots Q_s^{i_s}.$$

La méthode de factorisation consiste d'abord à factoriser P^0 en un produit de facteurs premiers; alors chacun des polynômes cherchés Q_i^0 est un produit de un

ou plusieurs des facteurs premiers de P^0. La factorisation de P revient à résoudre des équations de la forme

$$Q_1^k Q_2^0 \dots Q_s^0 + Q_1^0 Q_2^k Q_3^0 \dots Q_s^0 + \dots = \overline{P}^k. \tag{3}$$

Les deux membres de (3) sont des polynômes homogènes de $\mathbb{A}[x_1, \dots, x_n]$; en identifiant leurs coefficients on obtient des équations de la forme

$$b_1^k Q_2^0 \dots Q_s^0 + Q_1^0 b_2^k Q_3^0 \dots Q_s^0 + \dots = \bar{a}^k, \tag{4}$$

où $b_1^k, \dots, \bar{a}^k, Q_1^0, \dots, Q_s^0 \in \mathbb{K}[x]$.

En divisant les deux membres par $Q_1^0 \dots Q_s^0$ on obtient :

$$\frac{b_1^k}{Q_1^0} + \dots + \frac{b_s^k}{Q_s^0} = \frac{\bar{a}^k}{Q_1^0 \dots Q_s^0}. \tag{5}$$

On doit d'abord résoudre les équations (5) pour tous les polynômes $\bar{a}^k$ de $\mathbb{A}$ qui sont coefficients des monômes $x_1^{\beta_1} \dots x_n^{\beta_n}$ dans $\overline{P}^k$: alors b_i^k est le coefficient de $x_1^{\beta_1} \dots x_n^{\beta_n}$ dans Q_i^k. On résoud d'abord ces équations pour $k=1$, on en déduit :

$$\overline{P}^2 = P^2 - \sum_{i,j} Q_1^0 \dots Q_i^1 \dots Q_j^1 \dots Q_s^0,$$

puis on continue la résolution des équations (3) jusqu'à $k=\delta$.

3. CONDITIONS IMPOSÉES AU POLYNÔME P

Pour que les résolutions successives des équations (3) ne donnent pas d'indéterminations il faut que les équations (5) admettent une solution unique. Il suffit pour cela que le premier membre de (5) soit la décomposition en éléments simples de la fraction rationnelle $\bar{a}^k / Q_1^0 \dots Q_s^0$.

Les deux conditions suivantes doivent donc être vérifiées :

1° les polynômes $Q_1^0, \dots, Q_s^0$ sont deux à deux premiers entre eux;

2° $d^0 b_i^k < d^0 Q_i^0$ pour $i=1, \dots, s$.

La première condition signifie que P^0 n'a pas de facteur carré. On impose pour cela la condition :

(i) P n'a pas de facteur carré

Remarquons que si P avait un facteur carré on pourrait l'obtenir facilement en calculant PGCD $(P, \partial P/\partial x)$. De plus si (i) est vérifié, on verra au théorème 1 ci-

dessous qu'avec un changement de variables on peut se ramener au cas où P^0 est lui aussi sans facteur carré.

La deuxième condition $d^0 b_i^k < d^0 Q_i^0$, s'écrit encore $\partial Q_i^k < \partial Q_i^0$ (∂ désignant le degré suivant x). Cette inégalité est vérifiée si Q_i est unitaire en x. Il suffit pour cela que P vérifie la condition :

(ii) P **est unitaire en** x

On définit dans le paragraphe 4 ci-dessous un changement de variable $x_1' = x_1 + a_1 x, \ldots, x_n' = x_n + a_n x$ permettant de transformer P en un polynôme unitaire.

L'algorithme de Wang [5] impose comme ici la condition (i) mais pas la condition (ii); il utilise un autre changement de variable $x_1' = x_1 + a_1, \ldots, x_n' = x_n + a_n$ qui ne rend pas P unitaire et les diviseurs Q_i obtenus ne sont pas entièrement définis.

En résumé, si P est unitaire et sans facteur carré on sait déterminer une décomposition $Q_1 \ldots Q_s$ de P à partir d'une décomposition $Q_1^0 \ldots Q_s^0$ de P^0. Afin de ne pas recommencer les calculs pour toute décomposition de P^0 on part de la décomposition de P^0 en facteurs premiers $Q_1 \ldots Q_r$. Alors les diviseurs Q de P seront obtenus à partir d'un produit extrait de $Q_1 \ldots Q_r$. Le problème restant à résoudre étant de tester rapidement si un produit extrait de $Q_1 \ldots Q_r$ correspond bien à un diviseur de P.

4. TRANSFORMATION DE P EN POLYNÔME UNITAIRE

L'application $U : P(x, x_1, \ldots, x_n) \to \tilde{P}(x, x_1, \ldots, x_n)$ où

$$\tilde{P}(x, x_1, \ldots, x_n) = P(x, x_1 + a_1 x, \ldots, x_n + a_n x)$$

est un isomorphisme de $\mathbb{K}[x, x_1, \ldots, x_n]$:

$$U(P.Q) = U(P).U(Q) \qquad \text{et} \qquad U^{-1}(P) = P(x, x_1 - a_1 x, \ldots, x_n - a_n x).$$

La factorisation de P se ramène donc à celle de $U(P)$.

Remarquons que si l'un des diviseurs $Q_1^0, \ldots, Q_r^0$ de P^0 divise P on l'obtient en calculant PGCD (P, P^0). Dans la suite on suppose que ce PGCD est égal à 1.

THÉORÈME 1 : *Soit P un polynôme sans facteur carré de $\mathbb{K}[x, x_1, \ldots, x_n]$ tel qu'aucun facteur de P^0 ne divise P. Désignons par ∂_i le degré de P suivant x_i.*

Il existe un changement de variable

$$x_1' = x_1 + a_1 x, \ldots, x_1' = x_i + a_i x, \ldots, x_n' = x_n + a_n x,$$

où a_i est un entier naturel inférieur à $(\partial_i + 1)^2$ tel que

$\tilde{P}(x, x_1, \ldots, x_n) = P(x, x'_1, \ldots, x'_n)$ *vérifie les propriétés suivantes :*

(I) $\tilde{P}$ *est unitaire et* $\partial \tilde{P}^k \leqq \partial \tilde{P}^0 - k$ *pour* $k \geqq 0$;

(II) $\tilde{P}^0 = P(x, a_1 x, \ldots, a_n x)$ *n'a pas de facteur carré.*

La démonstration du théorème utilise le lemme suivant qui se vérifie facilement par récurrence sur n :

LEMME : *Soit P un polynôme non nul de* $\mathbb{K}[x_1, \ldots, x_n]$ *et* E_i *des ensembles de* $\partial_i + 1$ *entiers. Il existe au moins une valeur* a_i *de* E_i *pour* $i = 1, 2, \ldots, n$ *telle que* $P(a_1, \ldots, a_n) \neq 0$.

Démonstration du théorème : $P(x, x_1 + a_1 x, \ldots, x_n + a_n x)$ est une somme de polynômes homogènes $p_i = \mu_i x^\alpha (x_1 + a_1 x)^{\beta_1} \ldots (x_n + a_n x)^{\beta_n}$ et la forme de degré k en $x_1, \ldots, x_n$ de p_i notée p_i^k vérifie $\partial p_i^k + k = \partial p_i$. Donc $P = \sum_i p_i$ vérifie aussi $\partial P^k + k \leqq \partial P = \partial P^0$ à condition toutefois que la somme des coefficients $\mu_i a_1^{\beta_1} \ldots a_n^{\beta_n}$ des monômes de degré maximal en x ne soit pas nulle, c'est-à-dire que $P(1, a_1, \ldots, a_n)$ ne soit pas nul. Si on suppose que $P(1, x_1, \ldots, x_n) \neq 0$ (autrement P admettrait le diviseur $x - 1$ qui diviserait aussi P^0) il résulte du lemme qu'il existe pour tout i compris entre 1 et n et tout q positif des entiers $a_{q,i}$ dans l'intervalle $[q(\partial_i + 1), (q+1)(\partial_i + 1)[$ tels que $P(1, a_{q,1}, \ldots, a_{q,n})$ soit non nul, c'est-à-dire que (I) soit vérifié. Soit E_i l'ensemble des entiers $\{a_{0,i}, a_{1,i}, \ldots, a_{\partial_i, i}\}$.

Supposons que $P(x, a_{q,1} x, \ldots, a_{q,n} x)$ ait un facteur au carré pour certaines valeurs de q; cela signifie que le discriminant $\Delta(a_{q,1}, \ldots, a_{q,n}) \in \mathbb{K}[a_{q,1}, \ldots, a_{q,n}]$ de $P(x, a_{q,1}, \ldots, a_{q,n})$ est nul pour ces valeurs de q. Comme $P(x, x_1, \ldots, x_n)$ n'a pas de facteur carré, alors Δ est un élément non nul de $\mathbb{K}[a_{q,1}, \ldots, a_{q,n}]$, d'après le lemme il existe au moins une valeur a_i de E_i pour $i = 1, \ldots, n$ telle que $\Delta(a_{q,1}, \ldots, a_{q,n})$ soit non nul. Le théorème est donc vérifié pour ces valeurs a_i.

APPLICATION : Pour rendre P unitaire on considère d'abord les changements de variables $x'_1 = x_1 + a_1 x, \ldots, x'_n = x_n + a_n x$ où $a_i = 0$, 1 ou -1.

Si aucun d'eux ne convient on prend successivement $|a_i| = 2, |a_i| = 3, \ldots$ On est assuré que l'un de ces choix vérifie le théorème pour $|a_i| < (\partial_i + 1)^2/2$.

5. ALGORITHME DE DÉCOMPOSITION DE P EN UN PRODUIT $Q_1 \ldots Q_r$

1° On factorise P^0 en $Q_1^0 \ldots Q_r^0$ où $Q_1^0, \ldots, Q_r^0$ sont irréductibles.

2° On décompose en éléments simples les fractions rationnelles $x^j / Q_1^0 \ldots Q_r^0$

sous la forme

$$\frac{U_1^j}{Q_1^0}+\ldots+\frac{U_r^j}{Q_r^0} \quad \text{pour} \quad 0<j<\partial P^0.$$

Cette décomposition d'une fraction rationnelle est obtenue à l'aide de l'algorithme de Kung et Tang [2].

3° On détermine Q_i^k (forme de degré k du diviseur Q_i) en utilisant la technique définie par Wang dans [5] qui consiste à remplacer dans $\overline{P}^k$, x^j par U_i^j pour $j=0, 1, \ldots, \partial P^k$. La différence étant qu'ici on ne travaille pas sur des entiers modulo B.

On obtient ainsi pour i compris entre 1 et r :

$$Q_i=Q_i^0+Q_i^1+\ldots+Q_i^k+\ldots+Q_i^q.$$

On dit que Q_i est déterminé à l'ordre q. On poursuit les calculs jusqu'à $q=\partial P^0+1$.

On sait que les formes Q_i^k vérifient le système (2). En faisant la somme des premiers membres et des seconds membres de ce système on obtient une relation de la forme

$$(Q_1^0+Q_1^1+\ldots+Q_1^q)(Q_2^0+Q_2^1+\ldots+Q_2^q)\cdots(Q_r^0+Q_r^1+\ldots+Q_r^q)-E_q = P^0+P^1+\ldots+P^q,$$

où E_q est une somme de monômes dont le degré suivant $x_1, \ldots, x_n$ est supérieur à q. Par suite on a

$$Q_1.Q_2.\ldots.Q_r-E_q=P.$$

On convient d'écrire cette relation sous la forme

$$P\equiv Q_1.Q_2.\ldots.Q_r \text{ modulo } (x_1, \ldots, x_n)^q.$$

Vérifions que tout diviseur Q de P est défini par les polynômes Q_i déterminés ci-dessus. Il est clair que Q^0 divise P^0, donc que Q^0 est un produit de facteurs premiers de P^0 noté $Q_1^0 \ldots Q_m^0$. En appliquant l'algorithme de factorisation de P en partant de $P^0=Q^0.Q_{m+r}^0.\ldots.Q_r^0$ au lieu de $P^0=Q_1^0 \ldots Q_m^0 \ldots Q_r^0$ on obtient les relations

$$\frac{\bar{a}^k}{P^0}=\frac{\bar{b}^k}{Q^0}+\frac{b_{m+1}^k}{Q_{m+1}^0}+\ldots+\frac{b_r^k}{Q_r^0},$$

au lieu de

$$\frac{\bar{a}^k}{P^0}=\frac{b_1^k}{Q_1^0}+\ldots+\frac{b_m^k}{Q_m^0}+\ldots+\frac{b_r^k}{Q_r^0}.$$

Il résulte de l'unicité de la décomposition des fractions rationnelles que

$$\frac{\bar{b}^k}{\bar{Q}^0} = \frac{b_1^k}{Q_1^0} + \ldots + \frac{b_m^k}{Q_m^0}.$$

Par suite on a $Q \equiv Q_1 \ldots Q_m$ modulo $(x_1, \ldots, x_n)^q$. Ainsi comme q est supérieur au degré de Q suivant $x_1, \ldots, x_n$, alors Q est obtenu à partir du polynôme $Q_1 \ldots Q_m$ en supprimant les monômes de degré supérieur à q. Donc tout diviseur Q de P est associé à un produit $Q_1 \ldots Q_m$.

6. DÉTERMINATION DES DIVISEURS DE P

Soient $Q_1, \ldots, Q_r$ les polynômes déterminés par l'algorithme jusqu'à l'ordre $q = \partial P^0 + 1$. On note $Q_{i_1} \ldots Q_{i_m}$ un produit extrait du produit $Q_1 \ldots Q_r$ et on cherche à quelles conditions le produit $Q_{i_1} \ldots Q_{i_m}$ est associé à un diviseur de P.

THÉORÈME 2 : *On suppose que P est un polynôme unitaire vérifiant la relation* (iii) $\partial P^k \leqq \partial P^0 - k$ *pour* $k \geqq 0$. *Les deux propriétés suivantes sont équivalentes :*

1. *Le polynôme $Q = Q_{i_1} \ldots Q_{i_m}$ est associé à un diviseur de P.*
2. *Le polynôme Q vérifie la relation*

(iii) $$\partial Q^k \leqq \partial Q^0 - k \qquad \text{pour} \quad 0 \leqq k \leqq \partial P^0.$$

On note R le produit des polynômes Q_i où $1 \leqq i \leqq r$ et où i est distinct de $i_1, \ldots, i_m$. On note $\overline{Q}$ et $\overline{R}$ les polynômes déduits de Q et R en supprimant les monômes de degré suivant $x_1, \ldots, x_n$ supérieur à ∂P^0. La propriété 1 du théorème signifie que $P = \overline{Q}.\overline{R}$.

Pour la démonstration du théorème on utilise la représentation polyédrale des polynômes présentée dans Ostrowski [4]. A tout monôme $m = A x^a x_1^{a_1} \ldots x_n^{a_n}$ on associe le point M de $\mathbb{Z}^{n+1}$ de coordonnées $(a, a_1, \ldots, a_n)$. On appelle polyèdre associé au polynôme P l'enveloppe convexe $\Pi(P)$ des points M associés aux monômes de P. On montre que si $P = Q.R$, alors $\Pi(P)$ est égal à la somme vectorielle des polyèdres $\Pi(Q)$ et $\Pi(R)$ ([4], th. 6). On note $\Pi(P)_v$ l'intersection de $\Pi(P)$ avec l'hyperplan d'appui perpendiculaire à la direction v (v étant orienté vers l'extérieur du polyèdre); on a alors la relation :

(*a*) $$\Pi(P)_v = \Pi(Q)_v + \Pi(R)_v \quad \text{[[4], relation (43)]}.$$

Enfin on a la propriété suivante :

(*b*) tout sommet de $\Pi(P)$ est la somme de deux sommets de $\Pi(Q)$ et de $\Pi(R)$, mais n'est pas la somme d'autres points de $\Pi(Q)$ et de $\Pi(R)$.

Les monômes de P associés aux sommets de $\Pi(P)$ sont appelés monômes

extrêmes de P. La relation (iii) $\hat{c}P^k \leqq \partial P^0 - k$ signifie que $\Pi(P)$ est situé en dessous de l'hyperplan d'équation $a + a_1 + \ldots + a_n = \hat{c}P^0$.

Démonstration du théorème : Supposons que 1 soit vérifié et que 2 ne le soit pas. Il existe k_0 dans l'intervalle $[0, \hat{c}P^0]$ tel que

$$(c) \qquad \hat{c}Q^{k_0} > \hat{c}Q^0 - k_0.$$

Choisissons k_0 minimal. Supposons que R vérifie la relation (iii) pour $0 \leqq k \leqq \hat{c}P$. La relation (1) du paragraphe 2 donne en effectuant le produit

$$Q^0 R^{k_0} + Q^1 R^{k_0 - 1} + \ldots + Q^{k_0} R^0 = P^{k_0}.$$

D'autre part on a

$$(d) \quad \hat{c}(Q^{k_0} R^0) > \partial Q^0 + \partial R^0 - k_0$$
$$> (\partial Q^0 - i) + (\partial R^0 - (k_0 - i)) \qquad \text{où} \qquad 0 \leqq i < k_0$$
$$> \partial Q^i + \hat{c}R^{k_0 - i} = \hat{c}(Q^i R^{k_0 - i}).$$

Par suite $\partial(Q^{k_0} R^0) = \partial P^{k_0} \leqq \partial Q^0 + \partial R^0 - k_0$, ce qui est en contradiction avec (d). On a établit la propriété suivante :

$$(e) \qquad \begin{cases} \text{Si } P \equiv Q.R \text{ modulo } (x_1, \ldots, x_n)^q \text{ et que } Q \text{ ne vérifie pas} \\ \text{(iii) pour } 0 \leqq k \leqq \partial P \text{ alors } R \text{ ne le vérifie pas non plus.} \end{cases}$$

Notons k_1 et k_2 les entiers inférieurs à ∂P^0 tels que $\partial \overline{Q}^{k_1} + k_1 = \partial Q^{k_1} + k_1$ noté λ_1 et $\partial \overline{R}^{k_2} + k_2 = \partial R^{k_2} + k_2$ noté λ_2 soient maximaux. Les hyperplans d'appui H_1, H_2 et H de $\Pi(\overline{Q})$, $\Pi(\overline{R})$ et $\Pi(P)$ perpendiculaires au vecteur $v(1, 1, \ldots, 1)$ ont comme équations $a + a_1 + \ldots + a_n = \lambda_1$, $a + a_1 + \ldots + a_n = \lambda_2$ et $a + a_1 + \ldots + a_n = \lambda$. D'après (a) on a $H = H_1 + H_2$, donc $\lambda = \lambda_1 + \lambda_2$. Soit m un monôme extrême de P associé à un point de H. Alors d'après (b), m s'écrit de façon unique $m_1 . m_2$ où m_1 et m_2, sont des monômes de $\overline{Q}$ et de $\overline{R}$; de plus m_1 et m_2 ont leurs points associés dans H_1 et H_2. D'après (c) et (e) on a

$$\lambda_1 = \partial Q^{k_1} + k_1 > \partial Q^0 \qquad \text{et} \qquad \lambda_2 = \partial R^{k_2} + k_2 > \partial R^0.$$

Donc

$$\lambda = \lambda_1 + \lambda_2 > \partial Q^0 + \partial R^0 = \partial P^0.$$

Si k désigne le degré de m suivant $x_1, \ldots, x_n$ et ∂m le degré de m suivant x, alors on obtient $\lambda = k + \partial m < k + \partial P^k$. Par suite $\partial P^0 < k + \partial P^k$ ce qui est en contradiction avec les hypothèses du théorème. Il en résulte que 1 implique 2.

Supposons maintenant que 2 soit vérifié. Alors d'après (e) on a également $\partial R^k \leqq \partial R^0 - k$ pour $0 \leqq k \leqq \partial P^0$. Il en résulte que pour $\partial Q^0 \leqq k \leqq \partial P$ (resp. $\partial R^0 \leqq k \leqq \partial P$) on a $\overline{Q}^k = Q^k = 0$ (resp. $\overline{R}^k = R^k = 0$). Par suite le degré maximal suivant $x_1, \ldots, x_n$ des monômes de $P - \overline{Q}.\overline{R}$ est égal à $\partial Q^0 + \partial R^0 = \partial P^0$.

D'autre part on a $P-\overline{Q}.\overline{R}\equiv 0$ modulo $(x_1, \ldots, x_n)^{\partial P^0+1}$; donc $P-\overline{Q}.\overline{R}=0$ et par suite 1 est vérifié.

7. ALGORITHME DE RECHERCHE DES DIVISEURS DE P

Soit $Q=Q_{i_1}\ldots Q_{i_m}$ un produit associé à un diviseur de P. Alors d'après les relations du paragraphe 2. On a

$$Q^k=Q^k_{i_1}Q^0_{i_2}\ldots Q^0_{i_m}+Q^{k-1}_{i_1}Q^1_{i_2}Q^0_{i_3}\ldots Q^0_{i_m}+\ldots+Q^0_{i_1}\ldots Q^0_{i_{m-1}}Q^k_{i_m}.$$

Les polynômes $Q^k_{i_j}$ sont obtenus par décomposition de fractions rationnelles en éléments simples de dénominateurs $Q^0_{i_j}$; ils s'écrivent donc sous la forme

$$Q^k_{i_j}=\sum_{\omega_1+\ldots+\omega_n=k}(A^\omega_j x^{q-1}+B^\omega_j x^{q-2}+\ldots+C^\omega_j)\,x_1^{\omega_1}\ldots x_n^{\omega_n},$$

où $\omega=(\omega_1, \ldots, \omega_n)$ et où $q=\partial Q^0_{i_j}$. Comme Q^k doit vérifier la relation (iii) $\partial Q^k\leqq\partial Q^0-k$, alors pour $k>\partial Q^0$, $Q^k=0$ donc la somme des monômes de degré ∂Q^0-1 en x de Q^k est nulle.

Or les monômes de degré ∂Q^0-1 en x de Q^k ne peuvent provenir que des produits $Q^0_{i_1}\ldots Q^0_{i_{j-1}}Q^k_{i_j}Q^0_{i_{j+1}}\ldots Q^0_{i_m}$ (les autres produits étant de degré en x inférieur à ∂Q^0-1). Comme les polynômes $Q^0_{i_1}, \ldots, Q^0_{i_m}$ sont unitaires, les coefficients des monômes de Q^k de degré ∂Q^0-1 sont égaux aux coefficients A^ω_j des monômes de $Q^k_{i_j}$ de degré $q-1$ en x. On a donc la relation

(iv) $$\sum_{1\leqq j\leqq m} A^\omega_j=0 \quad \text{pour tout } \omega=(\omega_1, \ldots, \omega_n)$$

tel que $\omega_1+\ldots+\omega_n>\partial Q^0$.

La relation (iv) est une condition nécessaire pour que le produit $Q_{i_1}\ldots Q_{i_m}$ soit associé à un diviseur de P. L'algorithme de recherche des diviseurs de P aura deux parties :

A I. on détermine les sous-ensembles $S=\{Q_{i_1}, \ldots, Q_{i_m}\}$ de $E=\{Q_1, \ldots, Q_r\}$ vérifiant (iv) pour un diviseur Q de P de degré minimal;

A II. on vérifie (iii) en calculant le produit $Q_{i_1}\ldots Q_{i_m}$ uniquement pour les sous-ensembles S de E vérifiant (iv).

Dans la partie A I, le diviseur Q cherché a un degré majoré par ∂Q^0 qui est lui-même majoré par $E(\partial P^0/2)$. Les n-uples $\omega=(\omega_1, \ldots, \omega_n)$ pour lesquels (iv) est vérifié sont donc tels que

(I) $$E\left(\frac{\partial P^0}{2}\right)<\omega_1+\ldots+\omega_n\leqq\partial P^0 \qquad \text{où} \quad \omega_1, \ldots, \omega_n\geqq 0.$$

Le polynôme P rendu unitaire par le changement de variable défini dans le théorème 1 est presque toujours dense. Le nombre K des monômes

$Ax^{\alpha}x_1^{\omega_1}\ldots x_n^{\omega_n}$ de P tels que $(\omega_1, \ldots, \omega_n)$ vérifie (I) est donc de l'ordre $(\partial P^0)^n = d^n$ si on note d le degré total de P.

Considérons la matrice θ de coefficients A_j^{ω} à K lignes et r colonnes, les colonnes correspondant aux r polynômes $Q_1, \ldots, Q_r$, et les lignes aux K monômes de P dont les degrés $\omega_1, \ldots, \omega_n$ suivant $x_1, \ldots, x_n$ vérifient (I). La partie A I de l'algorithme revient alors à trouver les ensembles d'indices $\{i_1, \ldots, i_m\}$ dont les colonnes dans θ ont une somme nulle et tels que $\partial Q_{i_1}^0 + \ldots + \partial Q_{i_m}^0$ soit inférieur à $E(\partial P^0/2)$. Pour cette recherche de colonnes de θ dont la somme est nulle, on peut transformer θ en ajoutant à une ligne une combinaison linéaire des autres lignes. En utilisant la méthode du pivot de résolution des systèmes d'équations linéaires on peut transformer θ en une matrice θ' de la forme

$$\theta' = \begin{pmatrix} 0 & 0 & 1 & \ldots & a_s & a_{s+1} & \ldots & a_r \\ 1 & 0 & 0 & \ldots & b_s & b_{s+1} & \ldots & b_r \\ 0 & 1 & 0 & \ldots & c_s & c_{s+1} & \ldots & c_r \\ \cdot & \cdot & \cdot & \ldots & \cdot\cdot & \ldots\ldots & \ldots & \cdot\cdot \\ 0 & 0 & 0 & \ldots & g_s & g_{s+1} & \ldots & g_r \end{pmatrix}$$

Comme r majoré par d est très inférieur à $K = d^n$, le nombre s de lignes linéairement indépendantes est majoré par r et à partir d'un certain rang toutes les lignes de θ' sont nulles. On ne poursuit donc pas les calculs transformant θ en θ' pour toutes les lignes de θ. L'ordre de grandeur des calculs de cette transformation de θ en θ' est proportionnel à r^3.

Algorithme A I

1° Construction d'une matrice θ à r colonnes et K lignes de coefficients A_j^{ω} où les ω correspondent aux monômes de P vérifiant (I).

2° Pour chacune des colonnes d'indices 1, 2, 3, ... choisir un pivot dans cette colonne et annuler les autres termes de la colonne; si aucun choix de pivot n'est possible on passe à la colonne suivante.

3° Choix d'une colonne c_{i_1} n'ayant pas de pivot et pour chaque composante non nulle de c_{i_1}, recherche de colonnes $c_{i_2}, \ldots, c_{i_m}$ telles que $c_{i_1} + c_{i_2} + \ldots + c_{i_m} = 0$ et telles que $\partial Q_{i_1}^0 + \ldots + \partial Q_{i_m}^0$ soit inférieur à $E(\partial P^0/2)$.

Remarquons que la recherche de colonnes au 3° de l'algorithme est facilitée par le fait que la matrice θ est réduite sous la forme θ'.

Notons $S = \{Q_{i_1}, \ldots, Q_{i_m}\}$ un ensemble de polynômes défini par l'algorithme A I.

Algorithme A II

1° Calcul du produit $Q = Q_{i_1} \dots Q_{i_m}$ en ne gardant que les monômes de degré en $x_1, \dots, x_n$ inférieur à $\partial P^0 + 1$.

2° On vérifie que les monômes de Q de degré supérieur à ∂Q^0 s'annulent tous.

3° On vérifie que pour les monômes de Q dont le degré k en $x_1, \dots, x_n$ est majoré par ∂Q^0 et dont le degré en x est noté ∂ on a la relation $\partial \leqq \partial Q^0 - k$.

4° Si Q vérifie 2° et 3° alors c'est un diviseur de P sinon on détermine un autre sous-ensemble $\{Q_{i_1}, \dots, Q_{i_m}\}$ à l'aide de l'algorithme A I.

8. EXEMPLE

$$U = 6x^4 + 2x^3 + 5x^2 - 4 + 2y(3x^2 - 2x) + z(2x^4 + 2x^3 + 3x^2 + 5x - 2) + xz^2 + 2x^2 yz.$$

U n'est pas unitaire : le coefficient de x^4 est $6 + 2z$. Faisons le changement de variable $z \to z - x$; U est transformé en

$$U' = -2x^5 + 4x^4 + 2x - 4 + 2y(-2x^3 + 3x^2 - 2x) + z(2x^4 + 2x^3 + x^2 + 5x - 2) + xz^2 + 2x^2 yz.$$

On élimine le coefficient -2 de x^5 en faisant le changement de variable $z \to 2z$ dans U', puis en divisant par -2; on obtient :

$$P = x^5 - 2x^4 - x + 2 + y(2x^3 - 3x^2 + 2x) - z(2x^4 + 2x^3 + x^2 + 5x - 2) - 2xz^2 - 2x^2 yz.$$

Si Q est un diviseur de P, on obtient le diviseur correspondant de U par les changements de variables $z \to z/2$ (puis on multiplie par -2) et $z \to z + x$.

On factorise $P^0 = x^5 - 2x^4 - x + 2$; $P^0 = (x+1)(x-1)(x-2)(x^2+1)$.

On décompose en éléments simples les fractions rationnelles suivantes :

$$\frac{1}{x^5 - 2x^4 - x + 2} = \frac{1}{12(x+1)} - \frac{1}{4(x-1)} + \frac{1}{15(x-2)} + \frac{x+2}{10(x^2+1)},$$

$$\frac{x}{x^5 - 2x^4 - x + 2} = \frac{-1}{12(x+1)} - \frac{1}{4(x-1)} + \frac{2}{15(x-2)} + \frac{2x-1}{10(x^2+1)},$$

$$\frac{x^2}{x^5 - 2x^4 - x + 2} = \frac{1}{12(x+1)} - \frac{1}{4(x-1)} + \frac{4}{15(x-2)} - \frac{x+2}{10(x^2+1)},$$

$$\frac{x^3}{x^5 - 2x^4 - x + 2} = \frac{-1}{12(x+1)} - \frac{1}{4(x-1)} + \frac{8}{15(x-2)} + \frac{-2x+1}{10(x^2+1)},$$

$$\frac{x^4}{x^5 - 2x^4 - x + 2} = \frac{1}{12(x+1)} - \frac{1}{4(x-1)} + \frac{16}{15(x-2)} + \frac{x+2}{10(x^2+1)}.$$

On détermine les monômes en y et z des diviseurs Q_i en remplaçant dans les coefficients de y et z de P^1, x^j par le numérateur A_i de la fraction A_i/Q_i^0 du développement de x^j/P^0 en éléments simples. On obtient :

$$Q_1 = x+1+\frac{1}{2}z-\frac{1}{2}y,$$
$$Q_2 = x-1+2z,$$
$$Q_3 = x-2-4z,$$
$$Q_4 = x^2+1+\frac{1}{2}(-x+1)z+\frac{1}{2}(x+1)y.$$

On calcule $\overline{P}^2 = P^2 - \text{monômes en } y^2,\ yz \text{ et } z^2 \text{ de } Q_1 Q_2 Q_3 Q_4$:

$$\overline{P}^2 = -2xz^2-2x^2yz-z^2\left(\frac{33}{4}x^3+7x^2+\frac{37}{4}x+\frac{15}{2}+2x\right)$$
$$-yz\left(-\frac{1}{2}x^3+\frac{3}{2}x^2-2x^2-x\right)-y^2\left(\frac{1}{4}x^3-\frac{1}{2}x^2-\frac{1}{4}x+\frac{1}{2}\right)$$
$$=z^2\left(\frac{33}{4}x^3+7x^2+\frac{37}{4}x+\frac{15}{2}\right)+yz\left(-\frac{1}{2}x^3+\frac{3}{2}x^2-x\right)$$
$$+y^2\left(\frac{1}{4}x^3-\frac{1}{2}x^2-\frac{1}{4}x+\frac{1}{2}\right).$$

On détermine les monômes en y^2, yz et z^2 des diviseurs Q_i en remplaçant dans les coefficients de y^2, yz et z^2 de $\overline{P}^2$, x^j par le numérateur A_i de la fraction A_i/Q_i^0 du développement de x^j/P^0 en éléments simples.

On obtient :

$$Q_1 = x+1+\frac{1}{2}z-\frac{1}{2}y-\frac{1}{4}z^2+\frac{1}{4}yz,$$
$$Q_2 = x-1+2z-8z^2,$$
$$Q_3 = x-2+4z+8z^2,$$
$$Q_4 = x^2+1-\frac{1}{2}(x-1)z+\frac{1}{2}(x-1)y+\frac{1}{4}xz^2+\frac{1}{4}y^2-\frac{1}{4}(x+1)yz.$$

La matrice θ associée s'écrit :

$$\theta = \begin{array}{c} \\ y^2 \\ yz \\ z^2 \end{array}\begin{pmatrix} Q_1 & Q_2 & Q_3 & Q_4 \\ 0 & 0 & 0 & 0 \\ \frac{1}{4} & 0 & 0 & -\frac{1}{4} \\ -\frac{1}{4} & -8 & 8 & \frac{1}{4} \end{pmatrix}.$$

Après transformation de θ par la méthode du pivot on obtient :

$$\theta' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}.$$

La seule partition de $\{Q_1, Q_2, Q_3, Q_4\}$ vérifiant (iv) est $\{Q_1, Q_4\}$ et $\{Q_2, Q_3\}$, donc les seuls diviseurs possibles de P sont associés à $\{Q_2, Q_3\}$ et à $\{Q_1, Q_4\}$. On en déduit :

$$Q = Q_2 . Q_3 \equiv x^2 - 3x + 2 - 2xz \quad \text{modulo } (y, z)^3,$$
$$R = Q_1 . Q_4 \equiv x^3 + x^2 + x + 1 + z + xy \quad \text{modulo } (y, z)^3.$$

On vérifie que $Q.R$ est bien égal à P.

9. ÉVALUATION DES CALCULS DANS LE CAS OÙ $\mathbb{K} = \mathbb{Z}$

Dans la suite P est un polynôme à $n+1$ variables de degré total égal à d. Tous les logarithmes sont pris dans la base 2.

Les calculs importants sont causés par les opérations suivantes :

(1) Transformation de P en polynôme unitaire

Le changement de variable $x_i' = x_i + a_i x$ exige d'effectuer des produits $(x_1 + a_1 x)^{\beta_1} \ldots (x_n + a_n x)^{\beta_n}$. Pour chacun de ces produits on doit effectuer $(1+\beta_1) \ldots (1+\beta_n)$ multiplications où $\beta_1 + \ldots + \beta_n \leqq d$. On a au total $\Pi = \sum (1+\beta_1) \ldots (1+\beta_n)$ multiplications à effectuer. On peut montrer que $\Pi = (d+1)^{2n}/(2n)$.

Remarquons que ce changement de variable ne modifie pas le degré total d de P, mais augmente le degré de P suivant x et le rend égal à d. Ce changement de variable exige donc des calculs du même ordre que celui de l'algorithme de Wang.

(2) Factorisation de P^0

La méthode de Berlekamp exige des opérations de l'ordre de $d^3 H (\log H)$ où H est la hauteur de P^0.

(3) Décomposition des fractions rationnelles x^j / P^0

La décomposition d'une telle fraction exige d'après Kung et Tang [2] des calculs de l'ordre de $(\partial P)(\log \partial P)^2 < d (\log d)^2$.

On a donc des calculs de l'ordre de $d^2 (\log d)^2$ pour l'ensemble des décompositions.

(4) Calcul de $\overline{P}^k$ pour $k=2, 3, \ldots, d$

Ce calcul demande d'effectuer les produits de la somme

$$\sum_{\substack{0 \leqslant i_1, \ldots, i_s < k \\ i_1 + \ldots + i_s = k}} Q_1^{i_1} \ldots Q_s^{i_s},$$

ce qui revient à chaque étape k à calculer les monômes de degré k de

$$(Q_1^0 + Q_1^1 + \ldots + Q_1^i + \ldots)(Q_2^0 + Q_2^1 + \ldots) \ldots (Q_s^0 + Q_s^1 + \ldots),$$

c'est-à-dire à effectuer $s-1$ produits de la forme $(S^0 + S^1 + \ldots)(Q_i^0 + Q_i^1 + \ldots)$ en ne prenant que les monômes de degré k en $x_1, \ldots, x_n$. Les calculs sont dominés par ceux de la dernière étape, qui reviennent à faire $s-1$ produits de polynômes de degré d à n variables. Si on utilise la transformation de Fourier les calculs sont de l'ordre de $(s-1)n(d+1)^n \log(d+1)$, alors que sans la transformation de Fourier les calculs sont de l'ordre de $(s-1)(d+1)^{2n}$.

(5) Recherche des diviseurs de P

La transformation de la matrice θ sous la forme θ' exige comme on l'a vu plus haut des opérations de l'ordre de $r^3 < d^3$.

Pour chaque produit $Q_{I_1} \ldots Q_{i_m}$ vérifiant (iv) donné par l'algorithme A I, on doit vérifier que les monômes de degré en $x_1, \ldots, x_n$ supérieur à $\partial Q_{i_1}^0 + \ldots + \partial Q_{i_m}^0$ sont nuls. Le calcul des produits $Q_{I_1} \ldots Q_{i_m}$ de m polynômes à $n+1$ variables de degré d exige avec la transformation de Fourier $m(n+1)(d+1)^{n+1} \log(d+1)$ multiplications et $m(d+1)^{2(n+1)}$ multiplications sans utiliser la transformation de Fourier. Si l'algorithme A I définit plusieurs produits $Q_{i_1} \ldots Q_{i_m}$ vérifiant (iv) à partir de la matrice θ on doit effectuer chacun de ces produits, ce qui accroît les calculs.

10. CONCLUSION

On peut diminuer les calculs de l'algorithme en ne développant les polynômes $Q_i = Q_{i_1}^0 + \ldots + Q_i^k$ que jusqu'à $k = k_0 < \partial P^0$. Les calculs de (4) sont alors de l'ordre de $(k_0+1)^{2n}$. Puis on cherche les partitions $\{Q_{i_1}, \ldots, Q_{i_m}\}$ vérifiant (iv). S'il y en a peu on vérifie aussitôt si certaines partitions correspondant à des diviseurs de P. Sinon on continue le développement de Q_i pour $k = k_0 + 1$, puis on cherche des partitions moins fines que les précédentes vérifiant (iv). On peut ainsi trouver des diviseurs de P sans avoir à calculer les produits $Q_1^{i_1} \ldots Q_s^{i_s}$ pour $i_1 + \ldots + i_s = \partial P$ et lorsque P est irréductible on le sait lorsqu'aucune partition de $\{Q_1, \ldots, Q_r\}$ ne vérifie (iv).

Remarquons enfin que l'algorithme proposé a pour conséquence des résultats généraux sur la factorisation des polynômes, comme le suivant :

THÉORÈME 3 : *Soit* $P(x, x_1, \ldots, x_n)$ *un polynôme unitaire en* x *ayant un monôme constant et à coefficients dans* $\mathbb{Q}$. *Supposons que* P *se factorise sur une extension de* $\mathbb{Q}$ *en un produit* $Q_1 \ldots Q_i \ldots Q_s$ *et que les polynômes* $Q_i(x, 0, \ldots, 0)$ *aient leurs coefficients dans* $\mathbb{Q}$ *et soient deux à deux premiers entre eux sur* $\mathbb{Q}[x]$. *Alors les polynômes* $Q_i(x, x_1, \ldots, x_n)$ *ont aussi leurs coefficients dans* $\mathbb{Q}$.

Ce théorème résulte de l'algorithme de construction de $Q_i(x, x_1, \ldots, x_n)$ à partir de $Q_i(x, 0, \ldots, 0)$ uniquement par des opérations rationnelles.

BIBLIOGRAPHIE

1. E. R. BERLEKAMP, *Algebraic Coding Theory*, MacGraw-Hill, New York, 1968, p. 146-150.
2. H. T. KUNG et D. M. TONG, *Fast Algorithms for Partial Fraction Decomposition*, S.I.A.M. J. Comput., vol. 6, n° 3, 1977, p. 582-593.
3. D. R. MUSSER, *Multivariate Polynomial Factorization*, J. Ass. Comp. Mach., vol. 22, n° 2, 1975, p. 291-308.
4. A. M. OSTROWSKI, *On Multiplication and Factorization of Polynomials*, Aequationes Math., 13, 1975, p. 201-228.
5. P. S. WANG et L. P. ROTHSCHILD, *Factoring Multivariate Polynomials over the Integers*, Math. of Comp., vol. 29, n° 131, 1975, p. 935-950.
6. P. S. WANG, *Factoring Multivariate Polynomials over Algebraic Number Fields*, Math. of Comp., vol. 30, n° 134, 1976, p. 324-336.
7. P. S. WANG, *An Improved Multivariate Polynomial Factoring Algorithm*, Math. of Comp., vol. 32, n° 144, 1978, p. 1215-1231.
8. P. S. WANG, *Analysis of the p-adic Construction in Polynomial Factorization*, Lecture Notes in Comp. Sc., n° 72, p. 291.