HARRIS HANCOCK

Méthode de décomposition des polynomes entiers

Annales scientifiques de l'É.N.S. 3e série, tome 17 (1900), p. 89-102
<http://www.numdam.org/item?id=ASENS_1900_3_17__89_0>

MÉTHODE

DE

DÉCOMPOSITION DES POLYNOMES ENTIERS

À PLUSIEURS VARIABLES

EN FACTEURS IRRÉDUCTIBLES,

PAR M. HARRIS HANCOCK.

Le professeur Max Mandl (*Journal de Crelle*, t. 113, p. 252) a donné une méthode pour décomposer un polynome entier à une variable à coefficients entiers en facteurs irréductibles ([1]). La méthode suivante est une généralisation de celle que le professeur Mandl a donnée pour les polynomes à une seule variable.

Je vais d'abord montrer comment un polynome entier à k variables et à coefficients entiers peut être transformé en un polynome entier à k nouvelles variables ne contenant que des coefficients entiers et *positifs*.

Considérons d'abord le cas le plus simple, celui des polynomes à deux variables

$$(1)\qquad f(x_1, x_2) = a_0 + a_1 x_1 + a_2 x_1^2 + \ldots + a_n x_1^n = \sum_{\pi=0}^{\pi=n} a_\pi x_1^\pi,$$

où n est le degré de $f(x_1, x_2)$ en x_1, et où $a_\pi (\pi = 0, 1, 2, \ldots, n)$ sont des polynomes entiers en x_2 à coefficients entiers.

([1]) Ces facteurs sont des polynomes entiers à coefficients entiers. Nous ne considérerons, par conséquent, dans ce qui suit, que des polynomes de cette forme.

Nous pourrons donc écrire

$$(1)\qquad \begin{cases} a_0 = a_{0,0} + a_{1,0}x_2 + a_{2,0}x_2^2 + \ldots + a_{n_0,0}x_2^{n_0}, \\ a_1 = a_{0,1} + a_{1,1}x_2 + a_{2,1}x_2^2 + \ldots + a_{n_1,1}x_2^{n_1}, \\ a_2 = a_{0,2} + a_{1,2}x_2 + a_{2,2}x_2^2 + \ldots + a_{n_2,2}x_2^{n_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_n = a_{0,n} + a_{1,n}x_2 + a_{2,n}x_2^2 + \ldots + a_{n_n,n}x_2^{n_n}, \end{cases}$$

ou

$$a_\pi = \sum_{\nu=0}^{\nu=n_\pi} a_{\nu,\pi}x_2^\nu$$

$$(\pi = 0, 1, \ldots, n),$$

où n_π est le degré en x_2 du polynome $a_\pi\,(\pi = 0, 1, 2, \ldots, n)$ et où $a_{\nu,\pi}\begin{pmatrix}\nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n\end{pmatrix}$ sont entiers. Parmi les entiers $a_{n_\pi}(\pi = 0, 1, \ldots, n)$, c'est-à-dire les entiers correspondant aux plus hautes puissances de x_2 dans les expressions de a_π, il peut y en avoir qui soient précédés du signe *moins*. Nous les multiplierons par -1, ce qui nous obligera à placer le signe *moins* devant un certain nombre de a dans (I); mais nous garderons le signe *plus* devant a_n dans (I) en multipliant par -1, si cela est nécessaire.

En écrivant $x_2 = x_2' + h_\pi$ dans (1) et choisissant le nombre entier positif h_π suffisamment grand, nous pourrons changer a_π en

$$\bar{a}_\pi = \sum_{\nu=0}^{\nu=n_\pi} \bar{a}_{\nu,\pi}x_\pi'^\nu$$

$$(\pi = 0, 1, \ldots, n),$$

où toutes les quantités $a_{\nu,\pi}\begin{pmatrix}\nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n\end{pmatrix}$ sont des entiers positifs ou nuls.

Une limite inférieure pour h_π sera déterminée par la méthode donnée ci-après. Dès lors, prenant pour h un entier positif supérieur au plus grand des entiers $h_\pi(\pi = 0, 1, \ldots, n)$ et écrivant

$$x_2 = x_2' + h,$$

nous changeons a_π en

$$a'_\pi = \sum_{\nu=0}^{\nu=n_\pi} a'_{\nu,\pi} x'^{\nu}_2$$

$$(\pi = 0, 1, \ldots, n),$$

où toutes les quantités $a'_{\nu,\pi} \begin{pmatrix} \nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n \end{pmatrix}$ sont des nombres positifs non nuls.

L'expression (I) devient alors

$$(\mathrm{I}') \qquad f(x_1, x'_2 + h) = a'_n x_1^n \pm a'_{n-1} x_1^{n-1} \pm \ldots \pm a'_0.$$

Si le second terme de l'expression n'est pas déjà précédé du signe *plus*, il peut toujours être rendu positif en écrivant $-x$ à la place de x, et changeant ensuite le signe de l'expression tout entière, si n est un nombre impair. Nous pouvons donc considérer le second terme de (I') comme positif.

Dans (I') nous faisons la substitution

$$x_1 = x'_1 + k(x'_2)$$

ou

$$k(x'_2) = \alpha_\rho x'^{\rho}_2 + \alpha_{\rho-1} x'^{\rho-1}_2 + \ldots + \alpha_{02},$$

et choisissons les entiers ρ, $\alpha_\lambda (\lambda = 0, 1, \ldots, \rho)$ suffisamment grands pour que l'expression résultant de cette substitution

$$(\mathrm{II}) \qquad \mathrm{F}(x'_1, x'_2) = c_0 + c_1 x'_1 + c_2 x'^2_1 + \ldots + c_n x'^n_1$$

ait tous ses termes positifs, les c étant des polynomes entiers en x'_2 à coefficients entiers positifs.

Les raisons pour lesquelles nous pouvons choisir ainsi ces quantités résultent de ce qui suit. Prenons le cas le plus défavorable, dans lequel a'_n est positif, $a'_{n-1} = 0$, tandis que $a_\nu (\nu = 0, 1, \ldots, n-2)$ sont tous négatifs.

Nous pouvons alors écrire (I') sous la forme

$$a'_n x_1^n - (a'_{n-2} x_1^{n-2} + a'_{n-3} x_1^{n-3} + \ldots + a'_0).$$

Soit μ un entier inférieur ou égal à tout nombre du système des entiers

$$a'_{0,n}, \quad a'_{1,n}, \quad \ldots, \quad a'_{n_n,n},$$

qui entrent dans a'_n de la même manière que les entiers correspondants non accentués entrent dans les formules (1), et soient M_i des entiers égaux ou plus grands que ceux du système de nombres

$$a'_{0,i}, \quad a'_{1,i}, \quad \ldots, \quad a'_{n_i,i};$$

et soit, de plus, M un entier supérieur ou égal aux entiers $M_i (i = n-2, n-3, \ldots, 0)$.

Formons l'expression

$$(a) \qquad \mu \Sigma (x'_2)^{n_n} x_1^n - M[\Sigma (x'_2)^{n_{n-2}} x_1^{n-2} + \Sigma (x'_2)^{n_{n-3}} x_1^{n-3} + \ldots + \Sigma (x'_2)^{n_1} x_1 + \Sigma (x'_2)^{n_0}],$$

où

$$\Sigma (x'_2)^\nu = x_2'^\nu + x_2'^{\nu-1} + x_2'^{\nu-2} + \ldots + x'_2 + 1$$
$$(\nu = n_n, n_{n-2}, n_{n-3}, \ldots, n_0).$$

Nous voyons que l'expression

$$\Sigma (x'_2)^i - \Sigma (x'_2)^j$$

ne contient que des termes positifs tant que $i > j$.

Supposons que n_λ soit supérieur ou égal aux entiers

$$n_{n-2}, \quad n_{n-3}, \quad \ldots, \quad n_0,$$

et, pour abréger, posons

$$\Sigma (x'_2)^{n_\lambda} = k(x'_2).$$

Formons maintenant l'expression

$$(b) \qquad \mu x_1^n - M k(x'_2)(x_1^{n-2} + x_1^{n-3} + \ldots + x_1 + 1).$$

En vertu de l'identité

$$x_1^n = x_1 + x_1(x_1 - 1)(x_1^{n-2} + x_1^{n-3} + \ldots + x_1 + 1),$$

l'expression (b) peut s'écrire

$$(b') \qquad \mu x_1 + [\mu x_1 (x_1 - 1) - M k(x'_2)][x_1^{n-2} + x_1^{n-3} + \ldots + x_1 + 1].$$

Si dans (b') nous posons $x_1 = x'_1 + 1 + \alpha k'(x'_2)$, expression dans laquelle $k'(x'_2) = \Sigma(x'_2)^\pi$, où $\pi = \frac{n_\lambda}{2}$ si n_λ est pair et $\frac{n_\lambda + 1}{2}$ si n_λ est impair, et si, de plus, nous choisissons l'entier α de telle manière que l'on ait $\mu\alpha^2 > \mathrm{M}$, nous aurons une expression dans laquelle il n'entrera que des termes positifs. Dès lors, *a fortiori*, cette substitution rendra positifs tous les termes de (a) et aussi, par suite, les termes de (I').

Si maintenant le polynome (I) est décomposable en facteurs, de façon que l'on ait

$$f(x_1, x_2) = \varphi(x_1, x_2)\,\psi(x_1, x_2),$$

où φ et ψ désignent des polynomes à coefficients entiers, on peut écrire

$$\begin{aligned} f[x'_1 + k(x'_2), x'_2 + h] &= \mathrm{F}(x'_1, x'_2) \\ &= \varphi[x'_1 + k(x'_2), x'_2 + h]\,\psi[x'_1 + k(x'_2), x'_2 + h] \\ &= \Phi(x'_1, x'_2)\,\Psi(x'_1, x'_2); \end{aligned}$$

où $\Phi(x'_1, x'_2)$ et $\Psi(x'_1, x'_2)$ sont entiers en x'_1, x'_2 et à coefficients entiers; et *réciproquement* si $\mathrm{F}(x'_1, x'_2) = \mathrm{P}(x'_1, x'_2)\,\mathrm{Q}(x'_1, x'_2)$ où P et Q désignent des polynomes à coefficients entiers, on a aussi

$$\mathrm{F}[x_1 - k(x_2 - h), x_2 - h] = \mathrm{P}[x_1 - k(x_2 - h), x^2 - h]\,\mathrm{Q}[x_2 - k(x_2 - h), x_2 - h],$$

ou

$$f(x_1, x_2) = p(x_1, x_2)\,q(x_1, x_2),$$

où $p(x_1, x_2)$ et $q(x_1, x_2)$ sont des polynomes entiers en x_1, x_2 à coefficients entiers.

Dès lors, si $f(x_1, x_2)$ est décomposable en facteurs, $\mathrm{F}(x'_1, x'_2)$ est aussi décomposable en facteurs; et, à tout facteur irréductible de l'un des polynomes, correspond un facteur irréductible de l'autre.

Notre problème revient donc à trouver les facteurs d'un polynome tel que

$$\mathrm{F}(x_1, x_2) = c_0 + c_1 x_1 + c_2 x_1^2 + \ldots + c_n x_1^n,$$

où les c sont tous des polynomes entiers en x_2 à coefficients entiers.

Considérons maintenant un polynome à trois variables $f(x_1, x_2, x_3)$; il peut être écrit sous la forme donnée pages 91 et 92, mais maintenant les quantités

$$a_{\nu,\pi} \qquad \begin{pmatrix} \nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n \end{pmatrix}$$

ne sont plus des entiers, mais des polynomes entiers en x_3 à coefficients entiers. Nous pouvons écrire, par exemple,

$$a_{1,n} = a_{0,1,n} + a_{1,1,n} x_3 + a_{2,1,n} x_3^2 + \ldots + a_{n_{1,n},1,n} x_3^{n_{1,n}},$$

où $n_{1,n}$ est le degré de $a_{1,n}$ en x_3; et nous avons, en général,

$$a_{\nu,\pi} = \sum_{\mu=0}^{\mu=n_{\nu,\pi}} a_{\mu,\nu,\pi} x_3^\mu$$

$$\begin{pmatrix} \nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n \end{pmatrix},$$

où $n_{\nu,\pi}$ est le degré de $a_{\nu,\pi}$ en x_3, et où les nombres

$$a_{\mu,\nu,\pi} \qquad \begin{pmatrix} \mu = 0, 1, \ldots, n_{\nu,\pi} \\ \nu = 0, 1, \ldots, n_\pi \\ \pi = 0, 1, \ldots, n \end{pmatrix}$$

sont entiers.

Dans le polynome

$$f(x_1, x_2, x_3) = a_0 + a_1 x_1 + a_2 x_1^2 + \ldots + a_n x_1^n,$$

faisons les substitutions

$$x_3 = x'_3 + h_0,$$
$$x_2 = x'_2 + h_1(x'_3),$$

et choisissons h_0 et $h_1(x'_3)$ de telle façon que, dans l'expression transformée

$$\varphi(x_1, x'_2, x'_3) = a'_n x_1^n + a'_{n-1} x_1^{n-1} \pm a'_{n-2} x_1^{n-2} \pm \ldots \pm a'_0,$$

les quantités $a'_n, a'_{n-1}, \ldots, a'_0$ soient des polynomes à coefficients entiers et positifs en x'_2, x'_3, et tels que tous les termes possibles existent (puisque aucun terme n'est détruit par les opérations effectuées plus haut) et que tous les coefficients soient positifs.

Posant maintenant

$$x_1 = x'_1 + h_2(x'_2, x'_3),$$

nous pouvons transformer cette expression en une autre dans laquelle tous les termes sont positifs.

Si le degré de la plus haute puissance de x'_2 qui entre dans $\varphi(x_1, x'_2, x'_3)$ est D_2 tandis que celui de x'_3 est D_3, et si l'entier M est supérieur ou égal aux coefficients des termes négatifs qui entrent dans cette expression lorsque l'entier μ est inférieur ou égal aux entiers qui entrent dans a'_n, il est certain que la substitution suivante a la propriété voulue

$$x_1 = x'_1 + 1 + \alpha(1 + x'_2)^{d_2}(1 + x'_3)^{d_3}$$

où

$$d_2 = \frac{D_2}{2} \quad \text{ou} \quad \frac{D_2 + 1}{2},$$
$$d_3 = \frac{D_3}{2} \quad \text{ou} \quad \frac{D_3 + 1}{2},$$

suivant que D_2 et D_3 sont pairs ou impairs, et ceci lorsque $\mu\alpha^2 > M$.

En général il est clair que nous pouvons déterminer nos quantités de telle façon que, si dans la fonction $f(x_1, x_2, \ldots, x_k)$, nous faisons successivement les substitutions

$$\begin{aligned}
x_k &= x'_k + h_0,\\
x_{k-1} &= x'_{k-1} + h_1(x'_k),\\
x_{k-2} &= x'_{k-2} + h_2(x'_k, x'_{k-1}),\\
x_{k-3} &= x'_{k-3} + h_3(x'_k, x'_{k-1}, x'_{k-2}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
x_2 &= x'_2 + h_{k-2}(x'_k, x'_{k-1}, \ldots, x'_3),\\
x_1 &= x'_1 + h_{k-1}(x'_k, x'_{k-1}, \ldots, x'_2),
\end{aligned}$$

tous les termes peuvent être rendus positifs.

En effet, si D_λ est le degré de la plus haute puissance de x'_λ $(\lambda = 2, 3, \ldots, k)$ qui est précédée du signe *moins*, et si l'on a $d_\lambda = \frac{D_\lambda}{2}$ ou $\frac{D_\lambda + 1}{2}$ suivant que D_λ est pair ou impair, les substitutions (¹) suivantes ont la propriété voulue [*voir* la formule (b'), p. 92]:

$$x_k = x'_k + 1 + \alpha,$$

$$x_i = x'_i + 1 + \alpha \prod_{\lambda=i+1}^{\lambda=k} (1 + x'_\lambda)^{p_\lambda},$$

$$(i = 2, \ldots, k-1),$$

$$\mu\alpha > M,$$

$$x_1 = x'_1 + 1 + \alpha \prod_{\lambda=2}^{\lambda=k} (1 + x'_\lambda)^{d_\lambda},$$

$$\mu\alpha^2 > M,$$

où l'entier M est supérieur ou égal aux coefficients des termes négatifs qui y entrent, tandis que l'entier μ est supérieur aux entiers qui entrent dans a'_n.

Il en résulte aussi que l'on a inversement

$$\begin{aligned}
x'_k &= x_k - h_0 = \xi_k,\\
x'_{k-1} &= x_{k-1} - h_1(x_k - h_0) = x_{k-1} - h_1(\xi_k) = \xi_{k-1},\\
x'_{k-2} &= x_{k-2} - h_2(\xi_k, \xi_{k-1}) = \xi_{k-2},\\
x'_{k-3} &= x_{k-3} - h_3(\xi_k, \xi_{k-1}, \xi_{k-2}) = \xi_{k-3},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
x'_2 &= x_2 - h_{k-2}(\xi_k, \xi_{k-1}, \ldots, \xi_3) = \xi_2.\\
x'_1 &= x_1 - h_{k-1}(\xi_k, \xi_{k-1}, \ldots, \xi_2) = \xi_1.
\end{aligned}$$

Comme dans le cas de deux variables considéré plus haut, il est évident, ici encore, que, à tout facteur irréductible du polynome donné, correspond un facteur irréductible du polynome transformé, et que, à tout facteur irréductible du polynome transformé, correspond un facteur irréductible du polynome donné. Il suffit donc de considérer les facteurs irréductibles du polynome

$$\text{(II)} \qquad (x_1, x_2, \ldots, x_k) = c_0 + c_1 x_1 + c_2 x_1^2 + \ldots + c_n x_1^n,$$

(¹) Puisque dans le développement suivant l'une des variables, par exemple x_1, nous pouvons toujours supposer que les coefficients de la plus haute puissance et le coefficient de la puissance suivante en x_1 sont tous deux positifs.

où les c sont des polynomes entiers à coefficients entiers positifs.

Avec le professeur Mandl, considérons le polynome $f(x)$ comme un produit de facteurs linéaires. Si γ désigne une racine réelle, et $\alpha + i\beta$ une racine imaginaire de $f(x) = 0$, ce polynome peut s'écrire

$$f(x) = A_0 \Pi(x-\gamma)\Pi[(x-\alpha)^2 + \beta^2],$$

où A_0 est le coefficient de la plus haute puissance de x dans $f(x)$.

Si nous posons ensuite $x = x' + h$, l'expression ci-dessus devient

$$f(x'+h) = F(x') = A_0 \Pi(x'+h-\gamma)\,\Pi[(x'+h-\alpha)^2 + \beta^2].$$

En donnant à h une valeur entière et positive qui ne soit pas plus petite que la limite supérieure des parties réelles positives des racines de $f(x) = 0$, nous voyons que $F(x')$ et tous les facteurs réels de $F(x')$ ont des coefficients entiers et *positifs*.

Pour déterminer cette limite supérieure, posons

$$f(x) = A_0 x^n + A_1 x^{n-1} + \ldots + A_n,$$

et soit $x = \rho(\cos\theta + i\sin\theta)$ une racine de l'équation $f(x) = 0$, la partie réelle $\rho\cos\theta$ étant positive.

En substituant cette valeur de x dans $f(x)$, nous avons

$$A_0\rho^n + A_1\rho^{n-1}\cos\varphi + A_2\rho^{n-2}\cos 2\varphi + \ldots + A_n \cos n\varphi = 0,$$

et l'on a la limite supérieure cherchée en prenant pour ρ une valeur satisfaisant à l'inégalité

$$A_0\rho^n - |A_1|\rho^{n-1} - |A_2|\rho^{n-2} \ldots - |A_n| \geqq 0.$$

Le professeur Mandl donne une méthode qui permet souvent de trouver de plus petites valeurs de ρ.

On voit donc ainsi que nous pouvons donner à l'entier h qui entre dans la formule

$$f(x_1, x'_2 + h) = a'_n x_1^n \pm a'_{n-1} x_1^{n-1} \pm \ldots \pm a'_0$$

une valeur telle que les coefficients a'_k $(k = 0, 1, \ldots, n)$ soient des polynomes entiers en x'_2 à coefficients entiers et positifs, et que tous leurs facteurs réels soient aussi des polynomes entiers en x'_2 à coefficients entiers positifs.

De même, si, dans l'expression

$$a'_n x_1^n \pm a'_{n-1} x_1^{n-1} \pm \ldots \pm a'_0,$$

nous donnons à x_1 la valeur $\sigma(\cos\psi + i\sin\psi)$, nous pouvons déterminer une limite supérieure de σ, soit $\sigma = k(x'_2)$, telle que, lorsque nous ferons la substitution

$$x_1 = x'_1 + k(x'_2)$$

l'expression (II)

$$F(x'_1, x'_2) = c_0 + c_1 x'_1 + \ldots + c_n x_1'^n$$

non seulement ait tous ses termes positifs, mais, de plus, soit de telle nature que tous ses facteurs contiennent des termes positifs.

De même, dans les substitutions de la page 95, nous pouvons déterminer les quantités

$$h_0, \quad h_1(x'_k), \quad h_2(x'_k, x'_{k-1}), \quad \ldots, \quad h_{k-1}(x'_k, x'_{k-1}, \ldots, x'_2)$$

de façon que, lorsqu'on fait ces substitutions dans le polynome $f(x_1, x_1, \ldots, x_k)$, le polynome qui en résulte, non seulement ait tous ses termes positifs, mais, de plus, soit de telle nature que tous ses facteurs réels ne contiennent que des termes positifs.

Si, de même, le polynome

$$F(x_1, x_2, \ldots, x_k) = c_0 + c_1 x_1 + c_1 x_1^2 + \ldots + c_n x_1^n,$$

qui a été formé comme on l'a dit plus haut, est égal au produit des deux polynomes

$$\Phi(x_1, x_2, \ldots, x_k) = a_0 + a_1 x_1 + a_2 x_1^2 + \ldots + a_\nu x_1^\nu,$$
$$\Psi(x_1, x_2, \ldots, x_k) = b_0 + b_1 x_1 + b_2 x_1^2 + \ldots + b_{n-\nu} x_1^{n-\nu},$$

il en résulte que l'on a

$$\text{(III)} \qquad c_r = \sum_{k=0}^{k=r} a_k b_{r-k}$$
$$(r = 0, 1, \ldots, n).$$

Nous avons donc à déterminer les deux systèmes de polynomes entiers à coefficients entiers

$$a_0,\quad a_1,\quad a_2,\quad \ldots;\quad b_0,\quad b_1,\quad b_2,\quad \ldots,$$

qui satisfont à (III).

Le fait que nous pouvons supposer tous ces polynomes entiers par rapport aux variables résulte de l'extension d'un théorème dû à Gauss (*Disquisitiones arithmeticæ,* p. 42) d'après lequel, si un polynome entier en x_1 dont les coefficients sont des polynomes entiers en x_2, x_3, ..., x_k est décomposable en deux facteurs qui sont entiers en x_1 et à coefficients rationnels en x_2, x_3, ..., x_k, il est aussi décomposable en deux facteurs qui sont entiers en tous les x.

Comme la méthode employée pour la résolution du système d'équations (III) est au fond la même que celle donnée par le professeur Mandl, je ne ferai que l'indiquer brièvement.

Nous écrivons le système (III) sous la forme

$$\text{(IV)}\qquad \begin{cases} a_0 b_0 = c_0, \\ a_0 b_r + a_r b_0 = C_r, \end{cases}$$

où

$$C_r = c_r - \sum_{k=1}^{k=r-1} a_k b_{r-k}.$$

Il en résulte que

$$a_0 b_1 + a_1 b_0 = C_1 = c_1,$$
$$a_0 b_2 + a_2 b_0 = C_2 = c_2 - a_1 b_1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Afin que les équations (IV) puissent être résolues, nous remarquerons d'abord que C_r ne peut contenir que des termes positifs, puisque les a et les b ne contiennent que des termes positifs, et, de plus, que C_r doit être divisible par le plus grand commun diviseur entre a_0 et b_0. Ce diviseur peut toujours être déterminé par l'algorithme du plus grand commun diviseur.

Supposant pour le moment que a_0 et b_0 n'ont pas de facteur commun, nous déterminons un polynome entier des mêmes variables, à coefficients entiers et positifs d tel que

$$a_0 \mathrm{B} + b_0 \mathrm{A} = d,$$

où A et B sont des polynomes entiers à coefficients entiers (non forcément positifs).

Nous en déduisons les expressions

$$(\mathrm{V}^{(0)}) \qquad \begin{cases} da_r = -\mathrm{A}b_r + a_0 \mathrm{K}^{(0)}, \\ db_r = \quad \mathrm{B}b_r - b_0 \mathrm{K}^{(0)}, \end{cases}$$

où

$$\mathrm{K}^{(0)} = \mathrm{A}b_r + \mathrm{B}b_r,$$

et où $\mathrm{K}^{(0)}$ est par conséquent un polynome entier à coefficients entiers.

Puisque da_r et db_r ne contiennent pas de coefficients négatifs, il en résulte que $-\mathrm{A}b_r + a_0\mathrm{K}^{(0)}$ et $\mathrm{B}b_r - b_0\mathrm{K}^{(0)}$ ne peuvent contenir que des coefficients positifs.

Supposons alors que l'on pose

$$\mathrm{A}b_r = q^{(0)} a_0 + r^{(0)},$$

où $q^{(0)}$ est un polynome à coefficients entiers, et où $r^{(0)}$ est un polynome de même nature et formé de tous les termes de $\mathrm{A}b_r$ qui ne peuvent pas être arrangés de façon à avoir a_0 en facteur, l'autre facteur étant aussi entier par rapport aux mêmes variables, et à coefficients entiers. Dès lors les coefficients de $q^{(0)}$ doivent être inférieurs ou égaux aux coefficients correspondants de $\mathrm{K}^{(0)}$, ce qui détermine une limite inférieure pour les coefficients de $\mathrm{K}^{(0)}$.

Nous pouvons écrire de même

$$(\alpha) \qquad \mathrm{B}b_r = \mathrm{Q}^{(0)} b_0 + \mathrm{R}^{(0)}.$$

Il est clair que les coefficients de $\mathrm{Q}^{(0)}$ doivent être supérieurs ou égaux aux coefficients correspondants de $\mathrm{K}^{(0)}$, ce qui détermine une limite supérieure pour les coefficients de $\mathrm{K}^{(0)}$.

Nous pouvons donc écrire

$$\mathrm{K}^{(0)} = \mathrm{Q}^{(0)} - \mathrm{K}^{(1)},$$

où $K^{(1)}$ peut être nul et est aussi, comme $K^{(0)}$, un polynome entier à coefficients entiers.

Dès lors, nous avons

$$da_r = -AC_r + a_0 \frac{BC_r - R^{(0)}}{b_0} - a_0 K^{(1)}$$

ou

$$(V^{(1)}) \qquad \begin{cases} da_r = \dfrac{dC_r - a_0 R^{(0)}}{b_0} - a_0 K^{(1)}, \\ db_r = R^{(0)} + b_0 K^{(1)}, \\ K^{(1)} = Q^{(0)} - K^{(0)} = Q^{(0)} - (Ab_r + Ba_r). \end{cases}$$

De même nous pouvons écrire

$$(\beta) \qquad \frac{dC_r - a_0 R^{(0)}}{b_0} = Q^{(1)} a_0 + R^{(1)},$$

où $Q^{(1)}$ et $R^{(1)}$ sont des polynomes de même nature que les polynomes $Q^{(0)}$ et $R^{(0)}$ définis plus haut. Comme conséquence de cette identité nous avons la relation $Q^{(1)} \gtreqless K^{(1)}$, de sorte que l'on a

$$K^{(2)} = Q^{(1)} - K^{(1)},$$

où $K^{(2)}$ a un sens analogue à celui déjà donné pour $K^{(0)}$ et $K^{(1)}$.

Nous en déduisons

$$(V^{(2)}) \qquad \begin{cases} da_r = R^{(1)} + a_0 K^{(2)}, \\ db_r = \dfrac{dC_r - b_0 R^{(1)}}{a_0} - b_0 K^{(2)}, \\ K^{(2)} = Q^{(1)} - K^{(1)} = Q^{(1)} - Q^{(0)} + (Ab_r + Ba_r). \end{cases}$$

Si nous écrivons

$$\frac{dC_r - b_0 R^{(1)}}{a_0} = b_0 Q^{(2)} + R^{(2)},$$

on voit que $R^{(2)} = R^{(0)}$, et les expressions écrites plus haut commencent à se reproduire elles-mêmes.

Des relations $(V^{(0)})$, $(V^{(1)})$ et $(V^{(2)})$ nous déduisons des systèmes de limites supérieures pour les coefficients de $K^{(0)}$, $K^{(1)} = Q^{(0)} - K^{(0)}$ et $K^{(2)} = Q^{(1)} - Q^{(0)} + K^{(0)}$. Nous choisissons le système qui donne les plus petites valeurs pour les limites supérieures des coefficients de $K^{(0)}$.

Une limite inférieure de ces coefficients a été déterminée plus haut.

Si les limites supérieures sont plus grandes que les limites inférieures correspondantes, nous chercherons entre ces deux limites les systèmes de coefficients qui satisfont à ($V^{(0)}$). Les valeurs des coefficients qui sont les mêmes pour la limite inférieure et la limite supérieure sont fixés dans $K^{(0)}$.

Si un ou plusieurs des coefficients correspondant à la limite inférieure sont plus grands que le ou les coefficients correspondant à la limite supérieure, le problème n'a pas de solution et le polynome $F(x_1, x_2, \ldots, x_k)$ est irréductible.

Si, enfin, les polynomes a_0 et b_0 ont pour plus grand commun diviseur D, de sorte que $a_0 = a'_0 D$, $b_0 = b'_0 D$ et $C_r = C'_r D$, nous remplacerons dans les expressions ($V^{(0)}$), ($V^{(1)}$) et ($V^{(2)}$) a_0, b_0, C_r par a'_0, b'_0, C'_r et nous multiplierons le résultat final par D.