Factorise $f(x,\dots z) \in \mathbb{Z}[x\dots z]$ dans $\mathbb{Q}[x\dots z]$

conditions sur f :
a) facteurs x^α.. sortis
b) pas de facteurs multiples : $\text{pgcd}\left(f, \frac{df}{dx_i}\right) = 0$
c) $f(x\dots z) = \text{red}(f, x_i)$
d) f n'est pas homogène.
e) f dépend de plus de 2 littéraux

Sorties soit S1 : f est irreductible
S2 : $f = A(x\dots z) * B(x\dots z)$ où A et B sont irreductibles
S3 : $f = A(x\dots z) * B(x\dots z)$ où A est irreductible mais B peut être réductible

F1 **Choix du littéral x** . Pour $f = \sum f_{\alpha\beta\dots} x^\alpha y^\beta \dots$

a) $\exists$ x tel que $\deg(f,x) = 1$ oui → S1

b) Pour chaque littéral x déterminer le degré m, et les littéraux $y_1 \dots y_k$ à transformer qu'aurait g :
B1 $y_0 = x$, $k = 1$
B2 $m = \deg\{f$ en $y_0 y_1 \dots y_k$

soient $y_{k+1} \dots y_{k'}$ les littéraux tels que il le monome
$y_0^{\alpha_0} \dots y_k^{\alpha_k} y_j^{\alpha}$ avec $\alpha_0 + \dots + \alpha_k = m$ et $\alpha \neq 0$
soit présent dans f
si $k \neq k'$ faire $k = k'$ et retourner en B1
si $k = k'$ le degré est $\underline{m}$

c) Transformation : choisir x de degré m (déterminé en b) minimum
C1 $a_i = 1$ poser $a_i = 0$ pour $i > k$
C2 $g(x,y,z\dots) = \text{subs}\left(f, y_1 = y_1 + x^{a_1}, y_2 = y_2 + x^{a_2}, \dots y_k = y_k + x^{a_k}\right)$
C3 tant que $m \neq \deg(g,x)$
Choisir un i au hasard dans $[1,k]$ et $a_i := \begin{cases} 1 - a_i & \text{si } a_i \leq 0 \\ -a_i & \text{si } a_i > 0 \end{cases}$
poser $g = \text{subs}(g, y_i = y_i + \Delta a_i x)$

F2 Ici $g(x, y_1 \dots y_s) = \lambda x^m + \dots$ où λ est entier

Choix des point d'évaluation $(y_1 \dots y_s) = (b_1 \dots b_s)$

Poser $G(x\, y_1 \dots y_s) = g(x \dots y_s)$

Pour $i = 1$ à s : d1] $b_i = 0$

d2] si $\psi = \text{subs}(G, y_i = b_i)$ est sans facteur répété :

$$\text{pgcd}\left(\psi, \frac{d\psi}{dx}\right) = 1$$

poser $G = \psi$

sinon $\begin{cases} b_i = 1 - b_i & \text{si } b_i \leq 0 \\ b_i = -b_i & \text{si } b_i > 0 \end{cases}$ (on essaie $b_i = 0, 1, -1, 2, -2, 3, -3$ etc)

et reprendre en d2

On obtient ainsi $G(x) \in \mathbb{Z}(x)$ de degré m et sans facteur répétés

F3 Factoriser $G(x)$: poser $\lambda = \text{cont}(G(x))$

factoriser $\frac{G}{\lambda} = g_1(x) \dots g_t(x)$

[et reporter le facteur λ sur $g_1(x)$] inutile

Si $t = 1$: f était irréductible sortie S1

Poser $h(x, y_1 \dots y_s) = \text{subs}(g, y_1 = y_1 + b_1, \dots y_s = y_s + b_s)$

F4 Pour tous les sous ensembles $i_1, i_2 \dots i_p$ de $\{1, 2, 3 \dots t\}$,

rangés à p croissant $(p = 1, 2 \dots [\frac{t}{2}])$

E1][Recommencer]

Poser $A_0(x) = g_{i_1}(x)\, g_{i_2}(x) \dots g_{i_p}(x)$

$B_0(x) = G / A_0(x)$ on a $\text{pgcd}(A_0, B_0) = 1$

Calculer $a(x)$ et $b(x)$ $\in \mathbb{Z}(x)$

$$b(x) A_0(x) + a(x) B_0(x) = 1 \in \mathbb{Z}$$

$$H(x, y_1 \dots y_s) = h(x, y_1 \dots y_s) - A_0(x)\, B_0(x)$$

$$A(x) = A_0(x)$$

$$B(x) = B_0(x)$$

E1.1 déterminer les degrés max $D_1 = \deg(H, y_1)$, $D_2 = \deg(H, y_2) \dots D_s = \deg(H, y_s)$

E2] Déterminer le monome à lifter :

soit $\alpha_1, \dots, \alpha_s$ la plus petite suite (ordre $\alpha > \beta$)

telle que $\underbrace{y_1^{\alpha_1} \cdots y_s^{\alpha_s}}_{\nu} x^{\alpha}$ $(\alpha > q q)$ soit un monome de H.

Poser $u(x) = \text{coef}(H, y_1, \alpha_1, y_2, \alpha_2 \dots, y_s, \alpha_s)$

On cherche $\hat{A}(x)$, $\hat{B}(x)$ tels que :

- $(A + \hat{A}(x))(B + \hat{B}(x))$ ne contienne plus $u(x)\nu$

il faut : $A_0(x)\hat{B}(x) + B_0(x)\hat{A}(x) = u(x) y_1^{\alpha_1} \cdots y_s^{\alpha_s}$

d'où $\hat{A}(x) = \text{mod}(a(x)u(x), B_0(x)) \; y_1^{\alpha_1} \cdots y_s^{\alpha_s}$

$\hat{B}(x) = \text{mod}(b(x)u(x), B_0(x)) \; y_1^{\alpha_1} \cdots y_s^{\alpha_s}$

Calculs $\Delta = \hat{A}(x) * B$

$A(x) = A(x) + \hat{A}(x)$

$\Delta = \Delta + A(x) * \hat{B}(x)$

$B(x) = B(x) + \hat{B}(x)$

- Si tous les monomes de Δ sont majorés par un monome de H (si $x^{\alpha} \cdots y^{\beta} z^{\gamma}$ de Δ $\exists$ $x^{\alpha'} \cdots y^{\beta'} z^{\gamma'}$ dans H avec $\alpha' \geq \alpha$, $\beta' \geq \beta \dots \gamma' \geq \gamma$) nain

si $\deg_{y_i}(\Delta) \leq D_i$ pour $y_i = 1 \dots s$

$H = H - \Delta$

Si $H = 0$ [fin du lifting] aller en F5

Sinon reprendre E2

E2 sortie :

- Si un monome de Δ est trop grand : changer le sous ensemble $i_1 \dots i_p$ s'il n'y en a plus sortie → S1

F5] On a trouvé A et B : $h = A \cdot B$

$u(x, y_1, \dots y_s) = \text{red}(\text{subs}(A, y_1 = y_1 - a_1 x - b_1, y_2 = y_2 - a_2 x - b_2 \dots))$

$v = q_h / u$ $\quad p' = t - p$ si $p' \leq 2(p-1)$

si $\varphi \in \frac{t}{2}$ ou si $p = \left[\frac{t}{2}\right]$ avec $p \neq 1$ → Sortie S2

sinon sortie S3

Factorise $f(x \dots z) \in \mathbb{Z}[x \dots z]$

conditions sur f : a), b) et c) de l'algorithme F

Sortie : $u_1, u_2 \dots u_k$ irréductibles : $f(x \dots z) = u_1 \dots u_k$

G1 f univariée ?
si oui factoriser par XMFINT

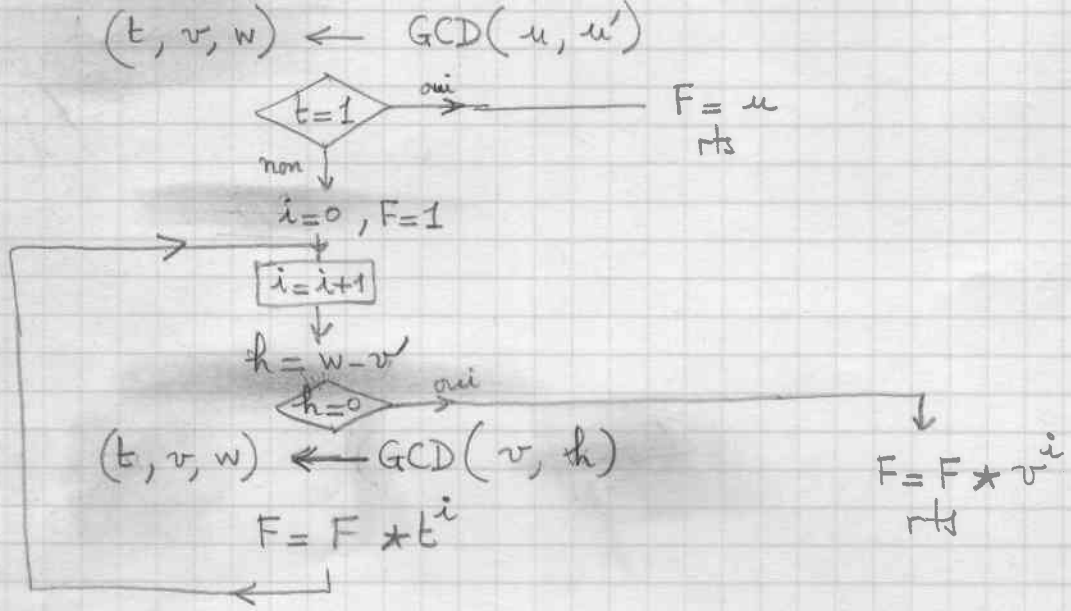
G2 f homogène ?
si oui factoriser $f' = \text{subs}(f, z=1)$: $f' = u'_1 \dots u'_k$
si $k=1$ → sortie $f = u_1$ (irreductible)
si $k>1$ $f = \text{homog}(u'_1, z)\ \text{homog}(u'_2, z) \dots$

G3 Sinon : appliquer **F**
si f irreductible sortie $f = u_1$
si $f = A \cdot B$ A et B irred sortie $f = A \cdot B$
si $f = A \cdot B$ poser $u_1 = A$
et factoriser B par G :
$B = u_2^* \dots u_k$
et sortir $u_1 * u_2 \dots u_k$

Décompose $u(x) = u_1(x)\, u_2^2(x) \cdots u_e^e(x)$ [$u(x,y,z\ldots)$ si on veut]

Knuth ex. 4.6.2.34 p 631

Note : $GCD(a,b) = \left(pgcd(a,b),\ \frac{a}{pgcd(a,b)},\ \frac{b}{pgcd(a,b)} \right)$



Test macsyma

$$x^6 y^3 z^2 \left(3z^3 + 2wz - 8xy^2 + 14w^2 y^2 - y^2 + 18x^3 y\right)$$

$$\left(12w^2 x y z^3 - w^2 z^3 - 3xy^2 - 29x + w^2\right)$$

MACSYMA: factorisé en 2 minutes

BASALG: // ~~208 secondes~~ ?

(TT) 1344 s → ne factorise pas

Série $A \sin(x^3) + \dfrac{B \log(x^2 - x + 1)}{x^5}$ en 365 mn :

$$= -\frac{B}{x^4} + \frac{B}{2x^3} + \cdots + \frac{(6B + A)\, x^{15}}{120}$$