UFR Sciences
M2 Calcul Formel
Option Maths approfondies

2012–2013
M. WEIMANN

Factorisation dans $\mathbb{Q}[t, x]$

Nous allons maintenant nous intéresser au problème de la factorisation des polynômes bivariés à coefficients dans $\mathbb{Q}$. L'objectif de ce chapitre est de développer un algorithme qui, étant donné $F \in \mathbb{Q}[t, x]$, retourne la liste $[(F_1, m_1), \ldots, (F_s, m_s)]$ des paires (facteurs irréductibles, multiplicités). L'idée est la même que pour la factorisation sur $\mathbb{Z}[x]$ avec cette fois l'anneau $\mathbb{Q}[t]$ jouant le rôle de l'anneau $\mathbb{Z}$, la réduction modulo (t) remplaçant la rédution modulo (p).

1. Factoriser F modulo (t).
2. Remonter cette factorisation modulo (t^k) pour une précision k suffisamment grande.
3. Recombiner les facteurs modulaires en des facteurs dans $\mathbb{Q}[t, x]$.

Avec l'algorithme de factorisation sur $\mathbb{Z}[x]$ et le lemme de Hensel à notre disposition, on a de fait tous les ingrédients pour écrire un algorithme de factorisation dans $\mathbb{Q}[t, x]$. C'est l'objet de la Section 1. On a vu dans le cas de $\mathbb{Z}[x]$ que le nombre de recombinaisons à tester peut-être exponentiel en le degré. L'enjeu de la section 2 est de montrer que l'on peut profiter de la richesse de l'anneau des coefficients $\mathbb{Q}[t]$ pour réduire le problème des recombinaisons à un problème d'algèbre linéaire, de complexité polynomiale en le degré de F.

1 L'approche naïve

1.1 Réduction au cas séparable unitaire

Comme d'habitude, la première chose à faire est de se ramener au cas où F est sans facteurs carrés. Pour ce faire on considère $F \in \mathbb{Q}[t, x] \simeq \mathbb{Q}[t][x]$ comme un polynôme en x à coefficient dans $\mathbb{Q}[t]$ et on mime ce que l'on a fait dans le cas des polynômes à coefficients dans $\mathbb{Z}$:

1. Réduction au cas primitif
2. Réduction au cas unitaire
3. Réduction au cas séparable

On supposera donc désormais que F est de la forme

$$F(t, x) = x^d + \sum_{i=0}^{d-1} a_i(t) x^i,$$

avec $\mathrm{Res}(F, \partial_x F, x) \neq 0$. On note ici ∂_x la dérivée partielle par rapport à x. On a $d := \deg_x(F)$ et on notera $e := \deg_t(F)$ le degré en t de F.

1.2 Réduction au cas $F(0,x)$ séparable

Pour remonter une factorisation modulo (t) à une factorisation modulo (t^k), on peut utiliser le lemme de Hensel dès lors que F est réduit modulo (t) ; on montre ici que l'on peut toujours se ramener à cette situation par un "shift" $t := t - a$ de la variable t.

Le polynôme $F(a,x)$ est réduit de degré d si et seulement si a n'est pas racine du discriminant par rapport à x

$$\Delta_x = \mathrm{Res}(F, \partial_x F, x).$$

(discriminant et résultant coïncident car F est supposé unitaire. Sinon, il faut diviser le résultant par le coefficient dominant de F vu comme polynôme en x). On a donc un nombre fini

$$\deg_t(\Delta_x) = \deg_t \mathrm{Res}(F, \partial_x F, x) \leq e(2d-1)$$

de mauvaises valeurs de t et il suffit de faire un changement de variable $FF(t,x) := F(t-a,x)$ pour $a \in \mathbb{Q}$ tel que $t-a$ ne divise pas Δ_x pour se ramener au cas $F(0,x)$ séparable. Si GG est un facteur de FF on retrouve le facteur correspondant G de F en posant $G(t,x) := G(t+a,x)$.

1.3 Remontée de Hensel et recombinaisons

On se place maintenant dans l'hypothèse

$$(H) \qquad \begin{cases} \deg(F(0,x)) = d \\ \mathrm{Res}(F(0,x), \partial_x F(0,x)) \neq 0, \\ F \text{ unitaire vu dans } \mathbb{Q}[t][x]. \end{cases}$$

Considérons la factorisation *analytique* de F dans $\mathbb{Q}[[t]][x]$

$$F = \mathcal{F}_1 \times \cdots \times \mathcal{F}_s.$$

D'après (H), le lemme de Hensel permet de calculer les $\mathcal{F}_i$ à une précision modulo (t^k) arbitrairement grande à partir de la factorisation irréductible de F modulo (t)

$$F(0,x) = \mathcal{F}_1(0,x) \times \cdots \times \mathcal{F}_s(0,x).$$

Considérons maintenant

$$F = F_1 \times \cdots \times F_r$$

la factorisation irréductible de F dans $\mathbb{Q}[t,x]$. Chaque $\mathcal{F}_i$ divise un unique F_j dans $\mathbb{Q}[[t]][x]$ et comme F est supposé réduit, il existe une unique collection $\mu_1, \ldots, \mu_r$ de vecteurs $\mu_i \in \{0,1\}^s$ tels que

$$\mathcal{F}_1^{\mu_{i1}} \times \cdots \times \mathcal{F}_s^{\mu_{is}} = F_i, \quad i = 1, \ldots, r. \tag{1}$$

Le *problème des recombinaisons* consiste à calculer les μ_i.

Comme les facteurs F_i sont de degré au plus $e = \deg_t(F)$ en t, ils suffit de calculer les $\mathcal{F}_i$ avec précision (t^{e+1}), puis de tester quelles combinaisons multiplicatives des $\mathcal{F}_i$ tronqués divisent F dans $\mathbb{Q}[t,x]$. Attention, rappelons que l'anneau $\mathbb{Q}[t][x]$ n'est pas euclidien. Cependant, on peut faire des divisions euclidiennes par rapport à x car les $\mathcal{F}_i$ sont supposés unitaires en x.

On a ainsi tous les ingrédients pour écrire un algorithme de factorisation dans $\mathbb{Q}[t,x]$. Cependant, on a vu dans le cas de $\mathbb{Z}[x]$ que le nombre de recombinaisons à tester peut-être exponentiel en le degré. L'enjeu du paragraphe suivant est de montrer que l'on peut profiter de la richesse de l'anneau des coefficients $\mathbb{Q}[t]$ pour réduire le problème des recombinaisons à un problème d'algèbre linéaire de complexité polynomiale en le degré de F.

2 Recombinaisons en temps polynômial

Pour réduire le problème des recombinaisons à un problème d'algèbre linéaire, on va considérer les μ_i comme des inconnues dans l'espace vectoriel $\mathbb{Q}^s$ plutôt que dans l'ensemble fini $\{0,1\}^s$.

2.1 La méthode des dérivées logarithmiques

Pour ramener les combinaisons multiplicative (1) en des combinaisons linéaires additives, on utilise le morphisme de *dérivation logarithmique*

$$\begin{array}{rcl} d\log : (k(x)^*, \times) & \longrightarrow & (k(x), +) \\ f & \longmapsto & f'/f \end{array}$$

agissant sur les polynômes univariés à coefficients dans un corps k. C'est un morphisme du groupe, transformant le produit en addition :

$$d\log(fg) = d\log(f) + d\log(g).$$

En regardant les F_i et les $\mathcal{F}_j$ dans $\mathbb{Q}((t))(x)$ et en appliquant $d\log$ à (1), on obtient

$$\sum_{j=1}^{s} \mu_{ij} \frac{\partial_x \mathcal{F}_j}{\mathcal{F}_j} = \frac{\partial_x F_i}{F_i}, \quad i = 1, \ldots, r.$$

En multipliant par F, on obtient une égalité dans $\mathbb{Q}[[t]][x]$:

$$\sum_{j=1}^{s} \mu_{ij} \hat{\mathcal{F}}_j \partial_x \mathcal{F}_j = \hat{F}_i \partial_x F_i, \quad i = 1, \ldots, r. \tag{2}$$

où

$$\hat{\mathcal{F}}_j = \prod_{k \neq j} \mathcal{F}_k \quad \text{et} \quad \hat{F}_i = \prod_{k \neq i} F_k$$

désignent les quotients respectifs de F par $\mathcal{F}_j$ et par F_i dans $\mathbb{Q}[[t]][x]$. Comme les membres de droite de (2) sont dans $\mathbb{Q}[t,x]$ de degré au plus e, l'égalité (2) équivaut à

$$\sum_{j=1}^{s} \mu_{ij} G_j = \hat{F}_i \partial_x F_i, \quad i = 1, \ldots, r. \tag{3}$$

où G_j désigne le reste de la division euclidienne de $\hat{\mathcal{F}}_j \partial_x \mathcal{F}_j$ par t^{e+1}. Il est donc naturel de définir le sous-espace vectoriel $V \subset \mathbb{Q}^s$

$$V := \left\{ (l_1, \ldots, l_s) \in \mathbb{Q}^s, \ \sum_{j=1}^{s} l_j G_j \in \left\langle \hat{F}_1 \partial_x F_1, \ldots, \hat{F}_r \partial_x F_r \right\rangle_{\mathbb{Q}} \right\}. \tag{4}$$

2.2 Base échelonnée réduite

Une matrice est dite échelonnée réduite (en lignes) si le nombre de zéros précédant la première valeur non nulle d'une ligne augmente ligne par ligne jusqu'à ce qu'il ne reste plus que des zéros. Voici un exemple de matrice échelonnée (les $*$ désignent des coefficients arbitraires, les $\oplus$ des pivots, coefficients non nuls) :

$$\begin{pmatrix} \oplus & * & * & * & * & * & * & * & * \\ 0 & 0 & \oplus & * & * & * & * & * & * \\ 0 & 0 & 0 & \oplus & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \oplus & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \oplus \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

La matrice est dite échelonnée réduite ou canonique si les les pivots valent 1 et les autres coefficients dans les colonnes des pivots sont nuls. En voici un exemple :

$$\begin{pmatrix} 1 & * & 0 & 0 & * & * & 0 & * & 0 \\ 0 & 0 & 1 & 0 & * & * & 0 & * & 0 \\ 0 & 0 & 0 & 1 & * & * & 0 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Toute matrice à coefficient dans $\mathbb{Q}$ admet une unique matrice équivalente sous forme échelonnée réduite. Il existe des algorithmes rapides qui renvoient une base d'un sous espace vectoriel sous sa forme échelonnée réduite. La fonction *Nullspace* de Maxima renvoie toujours la base d'un noyau sous sa forme échelonnée réduite. On a le lemme suivant :

Lemme 1 Le sous-espace vectoriel V admet $(\mu_1, \ldots, \mu_r)$ pour base échelonnée réduite (*i.e* forment une matrice échelonnée réduite quitte à réordonner les μ_i).

Preuve. Par construction on a $\mu_i \in V$ pour tout $i = 1, \ldots, r$. Comme $F(0, x)$ est séparable, les polynômes $\hat{\mathcal{F}}_j \partial_x \mathcal{F}_j(0, x)$, $j = 1, \ldots, s$ sont linéairement indépendants sur $\mathbb{Q}$, donc les $\hat{\mathcal{F}}_j \partial_x \mathcal{F}_j$ le sont, donc les G_j le sont. Par le même argument, les $\hat{F}_i \partial_x F_i$ le sont aussi. Il s'ensuit que $\dim V = r$. Comme les $\mu_i \in V$, $i = 1, \ldots, r$ sont deux à deux orthogonaux et à coefficients 0 ou 1, ils forment (mis dans le bon ordre) la base échelonnée réduite de V. $\square$.

On a donc caractérisé les μ_i comme base d'un sous-espace vectoriel de $\mathbb{Q}^s$. Bien sûr, on ne connaît pas les F_i, donc on ne peut pas déduire directement de (4) des équations explicites de V. On va utiliser pour cela la décomposition en éléments simples.

2.3 Décomposition en élément simple

On se fixe pour toute la suite $(l_1, \ldots, l_s) \in \mathbb{Q}^s$ et $G = \sum l_i G_i$. Soient $\phi_1, \ldots, \phi_d$ les racines de F dans $\bar{\mathbb{Q}}[[t]]$, où $\bar{\mathbb{Q}}$ désigne une clôture algébrique de $\mathbb{Q}$. On a donc

$$F = (x - \phi_1) \times \cdots \times (x - \phi_d)$$

et la décomposition en élément simple de G/F dans $\bar{\mathbb{Q}}[[t]][x]$ est

$$\frac{G}{F} = \frac{\rho_1}{x - \phi_1} + \cdots + \frac{\rho_d}{x - \phi_d}, \tag{5}$$

où les *résidus* $\rho_i \in \bar{\mathbb{Q}}[[t]]$ sont donnés par

$$\rho_i := res_{\phi_i}\Big(\frac{G}{F}\Big) = \frac{G(t, \phi_i)}{\partial_x F(t, \phi_i)}. \tag{6}$$

On a la proposition clé suivante :

Proposition 1 On a $(l_1, \ldots, l_s) \in V$ si et seulement si $\rho_i \in \bar{\mathbb{Q}}$ pour tout $i = 1, \ldots, d$.

Preuve. Si $l \in V$, alors G est par définition combinaison linéaire des $\hat{F}_i \partial_x F_i$. Comme

$$res_{\phi_i}\Big(\frac{\hat{F}_i \partial_x F_i}{F}\Big) \;=\; res_{\phi_i}\Big(\frac{\partial_x F_i}{F_i}\Big) \;=\; 1,$$

les résidus ρ_i de G/F sont donc constants pour tout i. Montrons l'implication inverse. On suppose maintenant les ρ_i constants. En substituant $t = 0$ dans (5) puis dans la définition de G, on obtient

$$\frac{G(0,x)}{F(0,x)} \;=\; \sum_{i=1}^{d} \frac{\rho_i(0)}{x - \phi(0)} \;=\; \sum_{j=1}^{s} l_j \frac{\partial_x \mathcal{F}_j(0,x)}{\mathcal{F}_j(0,x)}. \tag{7}$$

Par définition (6) du résidu, on a

$$res_{\phi_i(0)}\Big(\frac{\partial_x \mathcal{F}_j(0,x)}{\mathcal{F}_j(0,x)}\Big) \;=\; \begin{cases} 1 & \text{si} \quad \mathcal{F}_j(0, \phi_i(0)) = 0 \\ 0 & \text{sinon} \end{cases}$$

on déduit en appliquant $res_{\phi_i(0)}$ à (7) que $l_j = \rho_i(0)$ pour tout i tel que $\mathcal{F}_j(0, \phi_i(0)) = 0$, soit encore $l_j = \rho_i$ car ρ_i est supposé constant. Combiné avec (5), on obtient

$$G = \sum_{j=1}^{s} l_j \hat{\mathcal{F}}_j \partial_x \mathcal{F}_j \tag{8}$$

(on est ainsi passé d'une égalité modulo (t^{e+1}) à une égalité dans $\mathbb{Q}[[t]][x]$). Soient maintenant $\mathcal{F}_i$ et $\mathcal{F}_j$ divisant un même facteur irréductible F_k de F. Il suit de (8) que

$$\mathcal{F}_i \quad \text{divise} \quad l_i \partial_x F - G \quad \text{dans} \quad \mathbb{Q}[[t]][x].$$

Comme le membre de droite vit dans $\mathbb{Q}[t, x]$, cela force

$$\mathcal{F}_j \quad \text{divise} \quad l_i \partial_x F - G \quad \text{dans} \quad \mathbb{Q}[[t]][x]$$

car $\mathcal{F}_i$ et $\mathcal{F}_j$ sont conjugués (*i.e* facteurs irréductibles dans $\mathbb{Q}[[t]][x]$ d'un même polynôme irréductible dans $\mathbb{Q}[t, x]$). Comme $\mathcal{F}_j$ divise également $l_j \partial_x F - G$, il suit que

$$\mathcal{F}_j \quad \text{divise} \quad (l_i - l_j) \partial_x F \tag{9}$$

dans $\mathbb{Q}[[t]][x]$. Par hypothèse $\partial_x F$ est premier avec F, donc il est inversible modulo $\mathcal{F}_j$ et (9) force $l_i = l_j$. Ainsi, $l_i = l_j$ dés que $\mathcal{F}_i$ et $\mathcal{F}_j$ divisent un même facteur irréductible de F. Autrement dit, l est combinaison linéaire de $\mu_1, \ldots, \mu_s$, soit encore $l \in V$ d'après le lemme précédant. □

2.4 Conditions pour que les résidus soient constants

Puisque nous sommes en caractéristique nulle, les résidus ρ_i de G/F sont constants si et seulement si leurs dérivées sont nulles :

$$\rho_i' = \frac{d}{dt}\Big(\frac{G(t, \phi_i(t))}{\partial_x F(t, \phi_i(t))}\Big) = 0$$

On calcule la dérivée ρ_i' en utilisant la règle de dérivation des fonctions composées

$$\frac{d}{dt}\big(H(t, \phi(t))\big) = \partial_t H(t, \phi(t)) + \phi'(t) \partial_x H(t, \phi(t)).$$

et en utilisant l'égalité

$$\phi_i'(t) = -\frac{\partial_t F(t,\phi_i(t))}{\partial_x F(t,\phi_i(t))}$$

obtenue en dérivant la fonction identiquement nulle $F(t,\phi_i(t)) \equiv 0$. On trouve

$$\rho_i'(t) = \frac{D(G)(t,\phi_i(t))}{\partial_x F(t,\phi_i(t))^3}$$

où $D : \mathbb{Q}[t,x] \to \mathbb{Q}[t,x]$ est l'application $\mathbb{Q}$-linéaire définie par

$$D(G) := \big(\partial_t G \partial_x F - \partial_x G \partial_t F\big)\partial_x F - \Big(\partial^2_{tx} F \partial_x F - \partial^2_{xx} F \partial_t F\Big) G, \tag{10}$$

avec les notations $\partial^2_{xt} F = \partial_t(\partial_x F)$, etc. Ainsi, on a $\rho_i' = 0$ pour tout $i = 1,\ldots,d$ si et seulement si $D(G)(t,\phi_i(t)) \equiv 0$ pour tout $i = 1,\ldots,d$, si et seulement si F divise $D(G)$ dans $\mathbb{Q}[t][x]$ (la division euclidienne par F dans $\mathbb{Q}[t][x]$ est bien définie car F est supposé unitaire).

Bien que l'on n'ait aucune borne *a priori* sur le degré en t du reste de la division euclidienne de $D(G)$ par F, le lemme suivant permet de ramener le critère de divisibilité de $D(G)$ par F à un nombre fini d'équations linéaires. Pour un polynôme $H = \sum c_{ij} t^i x^j \in \mathbb{Q}[t,x]$, et deux entiers $0 \le k < l$, on définit les polynômes tronqués

$$[H]^l = \sum_{i<l} c_{ij} t^i x^j, \quad \text{et} \quad [H]^l_k = \sum_{k \le i < l} c_{ij} t^i x^j.$$

On a le lemme suivant :

Lemme 2 Soit $D(G) = QF + R$ la division euclidienne de $D(G)$ par F dans $\mathbb{Q}[t][x]$. On a $R = 0$ si et seulement si $[Q]^{3e}_{2e} = [R]^{3e} = 0$.

Preuve. Comme $\deg_x(G) \le d-1$ et $\deg_e(G) \le e$, on vérifie aisément que (10) implique les majorations suivantes

$$\deg_t(D(G)) \le 3e-1 \quad \text{et} \quad \deg_x(D(G)) \le 3d-3.$$

Ainsi, si $R = 0$, on a $D(G) = QF$ et

$$\deg_t Q = \deg_t D(G) - \deg_t F \le 2e-1$$

d'où $[Q]^{3e}_{2e} = [R]^{3e} = 0$. Inversement, si $[Q]^{3e}_{2e} = [R]^{3e} = 0$, on a $D(G) \equiv [Q]^{2e} F$ modulo (t^{3e}). Comme les polynômes $[Q]^{2e}F$ et $D(G)$ sont chacun de degré en t au plus $3e-1$, il suit que l'on a l'égalité $D(G) = [Q]^{2e}F$ dans $\mathbb{Q}[t,x]$. □

Ce lemme motive la définition de l'application linéaire suivante

$$\begin{array}{rcl} L : \mathbb{Q}^s & \longrightarrow & \mathbb{Q}[t,x]_{e-1,2d-3} \times \mathbb{Q}[t,x]_{3e-1,d-1} \\ l & \longmapsto & \Big([Q]^{3e}_{2e} \,/\, t^{2e} \quad , \quad [R]^{3e} \Big) \end{array}$$

où Q et R sont les restes de la division euclidienne de $D(G)$ par F, avec $G = \sum l_i G_i$ et $D(G)$ comme ci-dessus. La notation $\mathbb{Q}[t,x]_{k,l}$ désigne l'espace vectoriel de dimension finie des polynômes de degrés $\le k$ en t et $\le l$ en x. On obtient finalement le théorème suivant :

Théorème 1 Le noyau $\ker(L)$ admet $(\mu_1,\ldots,\mu_s)$ comme base échelonnée réduite.

Preuve. Découle des résultats précédants. □

3 L'algorithme

En suivant exactement la même procédure que dans le cas $\mathbb{Z}[x]$, on se ramène au cas où $F \in \mathbb{Q}[t,x]$ est séparable unitaire en x, ce que l'on supposera désormais pour alléger l'algorithme.

FactoBivariée(F) :

Entrée : $F \in \mathbb{Q}[t,x]$ séparable unitaire en x.
Sortie : La liste des facteurs irréductibles unitaires de F.

1. *Rédution au cas $F(0,y)$ séparable.* On effectue un changement de variable $F(t,x) := F(t-a,x)$ pour $a \in \mathbb{Q}$ tel que $t-a$ ne divise pas le discriminant de F par rapport à x.

2. *Factorisation modulo (t).* On utilise un algorithme de factorisation dans $\mathbb{Z}[x]$ pour factoriser F modulo (t).

3. *Remontée de Hensel.* On réitère le lemme de Hensel pour remonter la factorisation modulo (t) en une factorisation $F = \mathcal{F}_1 \times \cdots \times \mathcal{F}_s$ à la précision (t^{d+1}).

4. *Recombinaisons.* On fabrique la matrice de l'application linéaire L définie précédamment :

4.1. On calcule le quotient $\hat{\mathcal{F}}_i$ de F par $\mathcal{F}_i$ à la précision (t^{d+1}).

4.2. On calcule les $G_i := \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i$ à la précision (t^{d+1}).

4.3. On calcule $L(G_1), \ldots, L(G_s)$.

4.4. On en déduit la matrice de l'application L.

4.5. On calcule la base échelonnée réduite $(\mu_1, \ldots, \mu_r)$ de $\ker(L)$.

5. *Calcul des facteurs.* On calcule les produits $F_i = \prod_{j=1}^{s} \mathcal{F}_i^{\mu_{ij}}$.

6. *Translation et retour.* On renvoie la liste $[F_1(t+a,x), \ldots, F_r(t+a,x)]$.

Théorème 2 L'algorithme **FactoBivariée(F)** est correct. Il utilise une factorisation univariée dans $\mathbb{Z}[x]$ de degré d et $\tilde{\mathcal{O}}\big((de)^{\frac{\omega+1}{2}}\big)$ opérations arithmétiques dans $\mathbb{Q}$.

Preuve. L'algorithme est correct d'après le théorème 1. La complexité de l'algorithme découle des complexités des différentes sous-procédures mises en jeux (Hensel multifacteurs, division euclidienne, pgcd, résultant, noyau de matrice, multiplication polynômiale multifacteurs). Voir la référence pour plus dedétails.

Comme $2 < \omega < 3$, cet algorithme *déterministe* est de complexité *sous-quadratique* en la taille $\mathcal{O}(de)$ du polynôme d'entrée (modulo bien sûr la factorisation univariée probabiliste de degré d). Cette complexité est la meilleure connue actuelle pour les polynômes denses. Cet algorithme est récent (2010) et n'est pas encore implémenté dans tous les logiciels de calcul formel (je crois que Maxima utilise une variante plus ancienne...)

Références : G. Lecerf, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Appl. Alg. in Eng., Comm. and Comp. 21, no 2 (2010), pp 151-176.

4 Exercices et TP

Exercice 1 Ecrire une procédure **Test**(F) qui donné $F \in \mathbb{Q}[t,x]$ retourne *Vrai* si F est unitaire en x et $F(0,x)$ est séparable, et retourne *Faux* sinon. Choisir un polynôme test Ex de degré raisonnable (environ 10) tel que **Test**$(Ex) = Vrai$, ayant 2 ou 3 facteurs irréductibles sur $\mathbb{Q}[t,x]$ et 4 ou 5 facteurs modulo (t). On s'aidera de ce polynôme Ex pour tester les différentes procédures dans la suite du TP.

Exercice 2 Ecrire une procédure **Mod**(F,k) qui renvoie le reste de la division euclidienne de F par t^k, puis adapter les procédures **Hensel** et **EtapeHensel** du cas $\mathbb{Z}[x]$ au cas $\mathbb{Q}[t,x]$.

Exercice 3 En s'inspirant de la procédure du même nom décrite dans le cas $\mathbb{Z}[x]$, écrire une procédure **FactoModulaire**(F) qui, étant donné $F \in \mathbb{Q}[t,x]$ unitaire en x et séparable modulo (t), retourne les facteurs analytiques $\mathcal{F}_1, \ldots, \mathcal{F}_s$ de F calculés à la précision (t^{e+1}), où $e = \deg_t(F)$.

Exercice 4 En déduire une procédure **ListeG**(F, FM) qui, donné F et FM la liste des facteurs modulaires, retourne la liste des polynômes $G_1, \ldots, G_s$ décrits dans le cours.

Exercice 5 En déduire une procédure **Recombinaisons**(F, LG) qui donnés F et LG la liste des G_i, retourne la base échelonnée réduite $(\mu_1, \ldots, \mu_r)$ du noyau $\ker(L)$ de l'application L décrite dans le cours..

Exercice 6 En déduire une procédure **FactoBivariée**(F) qui, donné $F \in \mathbb{Q}[t,x]$, retourne **Faux** si F n'est pas unitaire en x et séparable modulo (t) et retourne la liste $[F_1, \ldots, F_r]$ de ses facteurs irréductibles sinon.

Exercice 7 Enrichir la procédure **FactoBivariée**(F) de compteurs temps qui renvoie les temps d'exécution des sous-procédures **FactoModulaire**(F), **Recombinaisons**(F, FM) et le temps total d'exécution de **FactoBivariée**(F).