Université Claude Bernard LYON 1
Master MAIM Mathématiques générales
Algèbre et calcul formel

Corrigé de la fiche de TD 2

Exercice 1.

Etant donnés des polynômes non nuls $f = \sum_{j=0}^{m} a_j X^j$ et $g = \sum_{j=0}^{n} b_j X^j$ de degrés m et n avec $m \geq n$, à coefficients dans un corps K, considérons l'algorithme d'Euclide :

$$\begin{array}{rcl}
A_1 & = & f \\
A_2 & = & g \\
A_1 & = & Q_1\, A_2 + A_3 \text{ avec } \deg(A_3) < \deg(A_2) \\
\vdots & & \\
A_k & = & Q_k\, A_{k+1} + A_{k+2} \text{ avec } \deg(A_{k+2}) < \deg(A_{k+1}) \\
\vdots & & \\
A_{t-2} & = & Q_{t-2}\, A_{t-1} + A_t \text{ avec } \deg(A_t) < \deg(A_{t-1}) \\
A_{t-1} & = & Q_{t-1}\, A_t \text{ avec } \deg(A_t) < \deg(A_{t-1})
\end{array}$$

$(Q_1, \cdots, Q_{t-1}, A_t)$ est la *représentation euclidienne* du couple de polynômes (f, g).
Les *quotients successifs* de l'algorithme d'Euclide permettent de retrouver la fraction rationnelle :

$$\frac{f}{g} = Q_1 + \cfrac{1}{Q_2 + \cfrac{1}{Q_3 + \cfrac{}{\ddots + \cfrac{1}{Q_{t-1}}}}}$$

et si on rajoute le pgcd $A_t = \text{pgcd}(f, g)$ on retrouve les polynômes f et g.
On posera $n_k = \deg(A_k)$ pour $1 \leq k \leq t$, $d_k = \deg(Q_k)$ pour $1 \leq k \leq t-1$ et $d_t = n_t$.

1. Montrer que $\deg(A_k) = \sum_{j=k}^{t} d_j$.
2. Soient $A, B \in K[X]$ des polynômes non nuls ; on considère la division euclidienne $A = BQ + R$ de A par B ; montrer que si $R \neq 0$ on a :

$$R_X(A, B) = (-1)^{\deg(A)\deg(B)} \text{lc}(B)^{\deg(A) - \deg(R)} R_X(B, R)$$

   indication utiliser la *formule de Poisson* (cours chap 1 prop 2 ou fiche TD1 ex2 3.)
3. En déduire que pour $1 \leq k \leq t-2$ on a :

$$R_X(A_k, A_{k+1}) = (-1)^{n_k n_{k+1}} \text{lc}(A_{k+1})^{n_k - n_{k+2}} R_X(A_{k+1}, A_{k+2})$$

4. Montrer que, pour f et g premiers entre eux, on a :

$$R_X(f, g) = (-1)^{\sigma} A_t^{m+n} \prod_{k=2}^{t-1} \text{lc}(Q_k)^{s_k}$$

où on a posé :

$$\begin{aligned}
n_k &= \sum_{i=k}^{t} d_i \text{ pour } 1 \leq k \leq t \\
\sigma &= \sum_{i=1}^{t-2} n_i n_{i+1} \\
s_k &= d_1 + 2\sum_{i=2}^{k-1} d_i + d_k \text{ pour } 2 \leq k \leq t-1
\end{aligned}$$

Corrigé.

Comme on a que $n_k = d_k + n_{k+1}$ On a $\deg(A_k) = \sum_{j=k}^{t} d_j$ pour $1 \leq k \leq t$.

On a $R_X(A,B) = (-1)^{\deg(A)\deg(B)}$ On applique la formule de Poisson en posant $f = B$, $g = A$, et $h = R$.

On applique dette formule à chaque étape de l'algorithme d'Euclide pour obtenir : pour $1 \leq k \leq t-2$:

$$R_X(A_k, A_{k+1}) = (-1)^{n_k n_{k+1}} lc(A_{k+1})^{n_k - n_{k+2}} R_X(A_{k+1}, A_{k+2})$$

On a maintenant :

$$\begin{aligned}
& R_X(f,g) \\
& = R_X(A_1, A_2) \\
& = (-1)^{n_1 n_2} \mathrm{lc}(A_2)^{n_1 - n_3} R_X(A_2, A_3) \\
& = (-1)^{n_1 n_2 + \cdots + n_k n_{k+1}} \mathrm{lc}(A_2)^{n_1 - n_3} \cdots \mathrm{lc}(A_{k+1})^{n_k - n_{k+1}} R_X(A_{k+1}, A_{k+2}) \\
& = (-1)^{n_1 n_2 + \cdots + n_{t-2} n_{t-1}} \mathrm{lc}(A_2)^{n_1 - n_3} \cdots \mathrm{lc}(A_{t-1})^{n_{t-2} - n_t} A_t^{n_{t-1}} \\
& = (-1)^{\sigma} \mathrm{lc}(A_2)^{d_1 + d_2} \cdots \mathrm{lc}(A_{k+1})^{d_k + d_{k+1}} \cdots \mathrm{lc}(A_{t-1})^{d_{t-2} + d_{t-1}} A_t^{d_{t-1}} \\
& = (-1)^{\sigma} \mathrm{lc}(Q_2)^{d_1 + d_2} \cdots \mathrm{lc}(Q_k)^{d_1 + 2d_2 + \cdots + 2d_{k-1} + d_k} \mathrm{lc}(A_{k+1})^{d_1 + 2d_2 + \cdots + 2d_k + d_{k+1}} \cdots \\
& \qquad \mathrm{lc}(A_{t-1})^{d_{t-2} + d_{t-1}} A_t^{d_{t-1}} \\
& = (-1)^{\sigma} \mathrm{lc}(Q_2)^{d_1 + d_2} \cdots \mathrm{lc}(Q_k)^{d_1 + 2d_2 + \cdots + 2d_{k-1} + d_k} \cdots \mathrm{lc}(Q_{t-2})^{d_1 + 2d_2 + \cdots + 2d_{t-3} + d_{t-2}} \\
& \qquad \mathrm{lc}(A_{t-1})^{d_1 + 2d_2 + \cdots + 2d_{t-2} + d_{t-1}} A_t^{d_{t-1}} \\
& = (-1)^{\sigma} \mathrm{lc}(Q_2)^{d_1 + d_2} \cdots \mathrm{lc}(Q_k)^{d_1 + 2d_2 + \cdots + 2d_{k-1} + d_k} \cdots \\
& \qquad \mathrm{lc}(Q_{t-1})^{d_1 + 2d_2 + \cdots + 2d_{t-2} + d_{t-1}} A_t^{d_1 + 2d_2 + \cdots + 2d_{t-1}}
\end{aligned}$$

Exercice 2.

Soient $f, g \in A[X]$ de même degré n où A est un anneau intègre;

1. Montrer que :

$$P^n_{X,Y}(f,g) = \frac{f(X)g(Y) - f(Y)g(X)}{X - Y} \in A[X,Y]$$

   est un polynôme tel que :

$$\mathrm{degpm}(P^n_{X,Y}(f,g)) = \max(\deg_X(P^n_{X,Y}(f,g)), \deg_Y(P^n_{X,Y}(f,g))) \leq n-1$$

   on posera

$$P^n_{X,Y}(f,g) = \sum_{i,j=0}^{n-1} c_{i,j} X^i Y^j$$

la matrice de Bezout est la matrice :

$$B_X^n(f,g) = (c_{n-i,n-j})_{1\le i,j\le n}$$

2. On pose

$$V(X) = \begin{pmatrix} X^{n-1}, & \cdots & ,X, & 1 \end{pmatrix} \in K[X]^n$$

Vérifier que dans $K[X,Y]$ on a :

$$P_{X,Y}^n(f,g) = V(X)\ B_X^n(f,g)\ {}^{\mathrm{t}}V(Y)$$

3. On considère la matrice *co-identité*

$$J_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \iddots & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Montrer que

$$\det(J_n) = (-1)^{\frac{n(n-1)}{2}} = (-1)^{[n/2]}$$

4. Montrer que :

$$S_X^{n,n}(f,g)\begin{pmatrix} 0 & J_n \\ -J_n & 0 \end{pmatrix} {}^{\mathrm{t}}S_X^{n,n}(f,g) = \begin{pmatrix} 0 & B_X^n(f,g) \\ -B_X^n(f,g) & 0 \end{pmatrix}$$

indication : on pourra multiplier les deux membres de cette égalité à gauche par $U(X)$ et à droite par $U(Y)$ avec

$$U(X) = \begin{pmatrix} X^{2n-1}, & \cdots & ,X, & 1 \end{pmatrix} = \big(X^n V(X), V(X)\big) \in K[X]^{2n}$$

5. En conclure que :

$$\det(B_X^n(f,g))^2 = R_X(f,g)^2$$

6. Montrer que :

$$B_X^n(X^n, X^n+1) = J_n$$

7. On considère les polynômes

$$\mathfrak{F} = \sum_{i=0}^{n} A_i X^i \qquad \mathfrak{G} = \sum_{j=0}^{n} B_j X^j$$

dont les coefficients sont des *indéterminées* sur $\mathbb{Z}$; vérifier que :

$$R_X(\mathfrak{F},\mathfrak{G}) = \epsilon \det(B_n(\mathfrak{F},\mathfrak{G})) \text{ avec } \epsilon \in \{-1,1\}$$

8. Montrer que :

$$\det(B_X^n(f,g)) = (-1)^{\frac{n(n-1)}{2}} R_X(f,g)$$

pour tout $f,g \in A[X]$.

Corrigé.

On remarque d'abord que $f(X)g(Y)-f(Y)g(X)$ est un polynôme de degré $2n$ divisible par $X-Y$ dans $K[X,Y]$ de sorte que $B_X^n(f,g)\in K[X,Y]$ est de degré $2n-1$. Posons :

$$U(X)=\begin{pmatrix}X^{2n-1}, & \cdots & ,X, & 1\end{pmatrix}$$

et

$$V(X)=\begin{pmatrix}X^{n-1}, & \cdots & ,X, & 1\end{pmatrix}$$

de sorte que :

$$U(X)=\big(X^nV(X),V(X)\big)$$

et

$$\frac{f(X)g(Y)-f(Y)g(X)}{X-Y}=V(X)B_X^n(f,g)^{\mathrm{t}}V(Y)$$

On a alors :

$$U(X)S_X^{n,n}(f,g)=(A(X),B(X))$$

avec

$$A(X)=(X^{n-i}f(X))_{1\leq i\leq n}\text{ et }B(X)=(X^{n-i}g(X))_{1\leq i\leq n}$$

En effet, pour $1\leq j\leq n$, la matrice de Sylvester $S_X^{n,n}(f,g)$ a pour colonne C_j (*resp.* C_{n+j}) les coefficients dans la base *canonique* $(X^{2n-i})_{1\leq i\leq 2n}$ du polynôme $X^{n-j}f(X)$ (*resp.* $X^{n-j}g(X)$) de sorte que le coefficient j (*resp.* $n+j$) de $U(X)S_X^{n,n}(f,g)$ est égal à $U(X).C_j=X^{n-j}f(X)$ (*resp.* $U(X).C_{n+j}=X^{n-j}g(X)$.

On a alors :

$$\begin{aligned}
&\left(U(X)S_{f,g}^{n,n}\right)\begin{pmatrix}0 & J_n\\ -J_n & 0\end{pmatrix}{}^{\mathrm{t}}\left(U(Y)S_{f,g}^{n,n}\right)\\
&\qquad=\big(A(X),B(X)\big)\begin{pmatrix}0 & J_n\\ -J_n & 0\end{pmatrix}\begin{pmatrix}{}^{\mathrm{t}}A(Y)\\ {}^{\mathrm{t}}B(Y)\end{pmatrix}\\
&\qquad=A(X)J_n{}^{\mathrm{t}}B(Y)-B(X)J_n{}^{\mathrm{t}}A(Y)\\
&\qquad=(X^{n-1}+X^{n-2}Y+\cdots+XY^{n-2}+Y^{n-1})(f(X)g(Y)-f(Y)g(X))\\
&\qquad=(X^n-Y^n)\frac{f(X)g(Y)-f(Y)g(X)}{X-Y}
\end{aligned}$$

On a par ailleurs :

$$\begin{aligned}
&U(X)\begin{pmatrix}0 & B_X^n(f,g)\\ -B_X^n(f,g) & 0\end{pmatrix}{}^{\mathrm{t}}U(Y)\\
&\qquad=\big(X^nV(X),V(X)\big)\begin{pmatrix}0 & B_X^n(f,g)\\ -B_X^n(f,g) & 0\end{pmatrix}\begin{pmatrix}Y^n\,{}^{\mathrm{t}}V(Y)\\ {}^{\mathrm{t}}V(Y)\end{pmatrix}\\
&\qquad=\big(-V(X)B_X^n(f,g),X^nV(X)B_X^n(f,g)\big)\begin{pmatrix}Y^n\,{}^{\mathrm{t}}V(Y)\\ {}^{\mathrm{t}}V(Y)\end{pmatrix}\\
&\qquad=-Y^n\,V(X)B_X^n(f,g)^{\mathrm{t}}V(Y)+X^nV(X)B_X^n(f,g)^{\mathrm{t}}V(Y)\\
&\qquad=(X^n-Y^n)P_{X,Y}^n(f,g)
\end{aligned}$$

Ainsi on a, *par identification des coefficients* :

$$S_{f,g}^{n,n}\begin{pmatrix}0 & J_n\\ -J_n & 0\end{pmatrix}{}^{\mathrm{t}}S_{f,g}^{n,n}=\begin{pmatrix}0 & B_X^n(f,g)\\ -B_X^n(f,g) & 0\end{pmatrix}$$

Il en résulte que, puisque $\det(J_n) = \pm 1$:

$$R_X^{n,n}(f,g)^2 = \det(B_X^n(f,g))^2$$

Considérons des *polynômes génériques* :

$$\mathfrak{F} = \sum_{i=0}^{n} A_i X^i \qquad \mathfrak{G} = \sum_{j=0}^{n} B_j X^j$$

On a donc :

$$R_X^{n,n}(\mathfrak{F},\mathfrak{G}) = \epsilon \det(B_X^n(\mathfrak{F},\mathfrak{G})) \text{ avec } \epsilon \in \{-1, 1\}$$

Par le *théorème de spécialisation* du résultant on a :

$$R_X^{n,n}(f,g) = \epsilon \det(B_X^n(f,g))$$

pour tout $f, g \in A[X]$ avec $\deg(f) = \deg(g) = n$.
Pour déterminer la valeur de ϵ on prend $f = X^n$ et $g = X^n + 1$; en utilisant l'expression du résultant en fonction des racines, on a $R_X(f,g) = 1$; par ailleurs on a :

$$\begin{aligned}
\frac{f(X)g(Y) - f(Y)g(X)}{X - Y} &= \frac{X^n(Y^n+1) - Y^n(X^n+1)}{X - Y} \\
&= \frac{X^n - Y^n}{X - Y} \\
&= X^{n-1} + X^{n-2}Y + \cdots + XY^{n-2} + Y^{n-1}
\end{aligned}$$

de sorte que

$$B_X^n(X^n, X^n+1) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} = J_n$$

mais on a :

$$\det(J_n) = (-1)^{\frac{n(n-1)}{2}} = (-1)^{[n/2]}$$