Université Ibn Khaldoun-Tiaret

Département des Mathématiques

Calcul Polynomial

Destinés aux étudiants de Master 2-AFA

par A.Larabi

0.1 Suite des restes de deux polynômes

Soit D un anneau intègre (sans diviseurs de zéros), commutatif et unitaire et $\mathbb{K}$ son corps de fractions, notons :
$\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$,
$\mathbb{K}[X]^*$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ non tous nuls.
Soit $A, B \in \mathbb{K}[X]$, $d = deg(A) \geq deg(B) \geq 0$.

Le quotient $Q(A,B)$ et le reste $Rem(A,B)$ sont les polynômes uniques de $\mathbb{K}[X]$ tels que :

$$A = Q(A,B).B + Rem(A,B) \tag{1}$$

avec $deg(Q(A,B)) = deg(A) - deg(B)$ et $deg(Rem(A,B)) < deg(B)$

Définition 0.1.1. *La suite des restes de la division euclidienne de deux polynômes A et B notée :*

$$R_d = R_d(A,B), R_{d-1} = R_{d-1}(A,B), ..., R_v = R_v(A,B)$$

est définie par :

$$R_d = A\ ;\ R_{d-1} = B$$
$$R_{d-2} = Rem(R_d, R_{d-1}), ..., R_{i-1} = Rem(R_{i+1}, R_i)$$
$$R_{v-1} = Rem(R_{v+1}, R_v) = 0$$

R_v est le dernier reste non nul.
La suite des quotients de A et B est la suite :

$$Q_{d-2} = Q(R_d, R_{d-1}), ..., Q_{v-1} = Q(R_{v+1}, R_v)$$

Notons que R_v est le pgcd de A et B, et si d_i est le degré de R_i alors $deg(Q_{i-1}) = d_{i+1} - d_i$ et $d_i < d_{i+1}$ pour $v \leq i \leq d-1$

Remarque 0.1.1. *L'algorithme d'Euclide étendu calcule les polynômes α_v et β_v dans $\mathbb{K}[X]$ tels que :*

$$\alpha_v.A + \beta_v.B = R_v \tag{2}$$

*Ces polynômes sont appelés **cofacteurs de Bézout** et cette equation est dite **égalité de Bézout**.*

Définition 0.1.2. *La suite des restes signés de A et B est définie par :*

$$F_d = A\ ;\ F_{d-1} = B$$
$$F_{d-2} = -Rem(F_d, F_{d-1}), .., F_{i-1} = -Rem(F_{i+1}, F_i), F_{v-1} = -Rem(F_{v+1}, F_v) = 0$$

*F_v est le dernier reste signé non nul. Cette suite est appelée aussi la suite de **Sturm généralisée**. Dans ce dernier cas si on prend $B = A'$ la dérivée de A on obtient la suite de **Sturm** classique.*

0.2 Sous-résultants classiques

Dans cette section nous définissons les sous-résultants classiques de deux polynômes et leurs propriétés.
L'algorithme d'Euclide pour deux polynômes A et B à coefficients dans un anneau intègre, commutatif et unitaire D ne génère pas forcément des restes à coefficients dans D mais dans son corps de fractions $\mathbb{K}$.
La suite de Sylvester-Habicht proportionnelle à celle des restes signés est stable algébriquement : les termes sont dans $D[X]$, contrairement aux termes de la suite des restes signés qui sont dans $\mathbb{K}[X]$.

Définition 0.2.1. *Pour $d \in \mathbb{N}^*$ on dit que (A, B) est un d-couple régulier si.*
$d = deg(A) > deg(B)$.
Soit (A, B) un d-couple régulier de $\mathbb{K}[X]$ et supposons que :

$$A(X) = a_d X^d + a_{d-1} X^{d-1} + ... + a_0 \tag{3}$$

$$B(X) = b_{d-1} X^{d-1} + b_{d-2} X^{d-2} + ... + b_0 \tag{4}$$

La j-ème matrice de Sylvester de A et B pour $j = 0, ..., d-1$, notée $Syl_j(A, B)$, est la matrice dont les lignes sont formées par les coefficients des polynômes :

$$AX^{d-2-j}, AX^{d-3-j}, ..., AX, A, B, BX, ..., BX^{d-2-j}, BX^{d-1-j} \tag{5}$$

écrits dans la base $(X^{2d-2-j}, X^{2d-3-j}, ..., X, 1)$

Ainsi $Syl_j(A, B)$ est de la forme :

$$Syl_j(A,B) = \underbrace{\begin{pmatrix} a_d & a_{d-1} & \dots & \dots & \dots & a_0 & \dots & \dots \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \dots & \dots & a_d & a_{d-1} & \dots & \dots & \dots & a_0 \\ \dots & \dots & \dots & b_{d-1} & b_{d-2} & \dots & \dots & b_0 \\ \dots & \dots & b_{d-1} & b_{d-2} & \dots & \dots & b_0 & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \dots \\ b_{d-1} & b_{d-2} & \dots & \dots & b_0 & \dots & \dots & \dots \end{pmatrix}}_{(2d-1-j \text{ colonnes})} (2d-2j-1 \text{ lignes}) \tag{6}$$

•C'est une matrice rectangulaire avec $(2d - 2j - 1)$ lignes et $(2d - 1 - j)$ colonnes.
Le cas $j = 0$ correspond à la matrice de **Sylvester** $(2d - 1)$.
Les $(d - j - 1)$ premières lignes sont associées aux polynômes $AX^{d-2-j}, AX^{d-3-j}, ..., AX, A$ et les $(d - j)$ dernières aux polynômes $B, BX, ..., BX^{d-2-j}, BX^{d-1-j}$.

•Nous désignons les lignes par leurs polynômes associés sous la forme AX^r et BX^s et les colonnes par leurs monômes sous la forme X^l.
Ainsi la première ligne de $Syl_j(A, B)$ est la ligne AX^{d-2-j} et la première colonne est la colonne X^{2d-2-j}.

• Si $deg(pgcd(A,B)) \geq 1$, il existe deux polynômes $U, V \in \mathbb{K}[X]^*$ tels que :

$$U.A + V.B = 0 \quad avec \quad deg(U) < deg(B) \quad et \quad \deg(V) < deg(A) \tag{7}$$

Soit $U = u_{d-2}X^{d-2} + \ldots + u_0$ et $V = v_{d-1}X^{d-1} + \ldots + v_0$, la relation de Bézout nous donne

$$U.A + V.B = (\sum_{r=0}^{d-2} u_r X^r).A + (\sum_{r=0}^{d-1} v_r X^r).B \tag{8}$$

$$= \sum_{r=0}^{d-2} u_r A.X^r + \sum_{r=0}^{d-1} v_r B.X^r \tag{9}$$

$$= (u_{d-2}, \ldots, u_0, v_0, \ldots, v_{d-1}). \begin{pmatrix} AX^{d-2} \\ \vdots \\ A \\ B \\ \vdots \\ BX^{d-1} \end{pmatrix} \tag{10}$$

or nous avons :

$$\begin{pmatrix} AX^{d-2} \\ \vdots \\ A \\ B \\ \vdots \\ BX^{d-1} \end{pmatrix} = Syl_0(A,B). \begin{pmatrix} X^{2d-2} \\ \vdots \\ \vdots \\ X \\ 1 \end{pmatrix} \tag{11}$$

donc si $det(Syl(A,B)) = 0$, il existe $(u_{d-2}, \ldots, u_0, v_0, \ldots, v_{d-1}) \in \mathbb{K}^{2d-1}$ non nul tel que :

$$(u_{d-2}, \ldots, u_0, v_0, \ldots, v_{d-1}).Syl(A,B) = (0, ..., 0) \tag{12}$$

Définition 0.2.2. *Le déterminant de la matrice de Sylvester, $Syl_0(A,B)$ est appelé résultant de A et B, noté $Res(A,B)$.*

Remarque 0.2.1.

$$deg(pgcd(A,B)) > 0 \Leftrightarrow Res(A,B) = 0 \tag{13}$$

• Pour $k \in \{0, ..., 2d-2-j\}$, soit $Syl_{j,k}(A,B)$ la matrice carrée d'ordre $(2d-1-2j)$ extraite de $Syl_j(A,B)$ et formée des premières $(2d-2-2j)$ colonnes et de la colonne X^k.

Définition 0.2.3. *La suite des* ***Sous-résultants*** $(S_j)_{d \geq j \geq 0}$ *de A et B est définie par :*

$$\begin{cases} S_d = A \\ S_j = \sum_{k=0}^{j} det(Syl_{j,k}(A,B))X^k \quad , pour \quad 0 \leq j \leq d-1 \end{cases} \tag{14}$$

On vérifie que $S_{d-1} = B$

Nous aurons besoin par la suite de plusieurs outils pour les démonstrations des théorèmes sur les sous-résultants, nous allons les énoncer :

Notons par $\mathcal{M}_{n,m}(\mathbb{K})$ l'ensemble des matrices $n \times m$ à coefficients dans $\mathbb{K}$.

Définition 0.2.4. *Soit $M \in \mathcal{M}_{n,m}(\mathbb{K})$ avec $m \geq n$ et Δ la matrice formée des $(n-1)$ premières colonnes de M.*
On définit une forme linéaire ψ sur $\mathbb{K}^n$ par :

Pour $\mathcal{X} \in \mathbb{K}^n$, $\psi(\mathcal{X}) = det(\Delta, \mathcal{X})$ où $(\Delta, \mathcal{X})$ est la matrice carrée d'ordre n formée des $(n-1)$ colonnes de Δ et de la colonne $\mathcal{X}$.
On note M_j la j-ème colonne de M.

On appelle ***Polynôme déterminantal*** *de M et on note $detPol(M)$ le polynôme :*

$$detPol(M) = \sum_{i=0}^{m-n} \alpha_i X^i \quad avec \quad \alpha_i = \psi(M_{m-i}) \tag{15}$$

Remarque 0.2.2. *:*
1. La matrice $Syl_j(A,B)$ a $(2d-j-1)$ colonnes et on montre que pour tout $j = 0, ..., d-1$:

$$S_j = \sum_{k=0}^{j} det(Syl_{j,k}(A,B)) = detPol(Syl_j(A,B)) \tag{16}$$

2. Si Δ est une matrice $n \times n$ et M une matrice $n \times m$ avec $m \geq n$ alors :

$$detPol(\Delta.M) = det(\Delta).detPol(M)$$

3. Soit $\Sigma_j = \Sigma_j(A,B)$ le bloc de dimension $(2d-1-2j) \times (2d-2-2j)$ constitué des colonnes relatives à $X^{2d-2-j}, ..., X^{j+1}$ de $Syl_j(A,B)$. La matrice Σ_j définit une forme linéaire $\sigma_j = \sigma_j(A,B)$ telle que

$$\sigma_j(\mathcal{X}) = det(\Sigma_j, \mathcal{X}) \quad pour\, tout \quad \mathcal{X} \in D^{2d-1-2j} \tag{17}$$

ainsi $det(Syl_{j,l}(A,B)) = \sigma_j(M_{2d-1-2j-l})$ et puisque $\sum_{l=j+1}^{2d-2-j} \sigma_j(M_{2d-1-2j-l})X^l = 0$ on a :

$$S_j = \sum_{l=0}^{j} \sigma_j(M_{2d-1-2j-l})X^l = \sum_{l=0}^{2d-2-j} \sigma_j(M_{2d-1-2j-l})X^l \tag{18}$$

$$S_j = \sum_{r=0}^{d-2-j} u_{j,r}.AX^r + \sum_{t=0}^{d-1-j} v_{j,t}BX^t \tag{19}$$

$$= (\sum_{r=0}^{d-2-j} u_{j,r}X^r).A + (\sum_{t=0}^{d-1-j} v_{j,t}X^t).B \tag{20}$$

$$= U_j.A + V_j.B \tag{21}$$

où les coefficients $u_{j,r} = u_{j,r}(A,B)$ et $v_{j,t} = v_{j,t}(A,B)$ des polynômes U_j et V_j, cofacteurs de Bézout, sont au signe près, les mineurs d'ordre maximal de Σ_j ou les coefficients de la forme linéaire σ_j.

Définition 0.2.5. *Soient A et B deux polynômes de $\mathbb{K}[X]^*$ avec $deg(A) \geq deg(B)$.*

*On définit le **reste gaussien** de A et B que l'on note $Gau(A,B)$ par :*

$$Gau(A,B) = (-\frac{Lc(B)}{Lc(A)})Rem(A,B) = (-\frac{Lc(B)}{Lc(A)}.A) + (\frac{Lc(B)}{Lc(A)}.Quo(A,B)).B \qquad (22)$$

où $Lc(A), Lc(B)$ sont les coefficients principaux de A et B (coefficient du terme de plus haut degré) et $Quo(A,B), Rem(A,B)$ le quotient et le reste de la division euclidienne de A par B.
*Le reste gaussien est appellé aussi **G-reste***

Remarque 0.2.3. *:*
$\forall a, b \in \mathbb{K}^* : Gau(aA, bB) = b.Gau(A,B)$

la suite $(G_i)_{d \geq i \geq 0}$ des G-restes est définie par :

$$\begin{cases} G_0 = A \\ G_1 = B \\ G_{i+1} = Gau(G_{i-1}, G_i), \quad i \geq 1 \end{cases} \qquad (23)$$

Théorème 0.2.4. *Soient (A,B) un d-couple régulier de $\mathbb{K}[X]^*$ et $(G_i)_{0 \leq i \leq d}$ la suite des restes gaussiens construite comme ci-dessus.*
Alors, pour tout $i = 0, ..., d$, il existe un polynôme $A_i \in \mathbb{K}[X]$ de degré $d_1 - d_i$ et un polynôme unitaire (de coefficient de tête égal à 1) $B_i \in \mathbb{K}[X]$ de degré $d_0 - d_i$ où $d_i = deg(R_i) = deg(G_i)$ tels que :

$$G_{i+1} = A_i.A + B_i.B \qquad (24)$$

Démonstration :
Les polynômes A_i et B_i sont construits par l'algorithme d'Euclide étendu.
Posons $G_0 = A$ et $G_1 = B$, nous avons :

$$G_2 = Gau(G_0, G_1) = -\frac{Lc(B)}{Lc(A)} Rem(A, B).$$

Soit $Q(A, B)$ le quotient de la division euclidienne de A par B,on a :
$Rem(A, B) = A - Q(A, B).B$ d'où :

$$\begin{aligned} G_2 &= [-\frac{Lc(B)}{Lc(A)}].A + [\frac{Lc(B)}{Lc(A)} Q(A, B)].B \\ &= A_1.A + B_1.B \end{aligned}$$

avec

$$deg(A_1) = d_1 - d_1 = 0 \text{ et } deg(B_1) = d_0 - d_1 = d - deg(R_1)$$

Supposons que :

$$\begin{cases} G_i = A_{i-1}.A + B_{i-1}.B \\ G_{i-1} = A_{i-2}.A + B_{i-2}.B \end{cases} \tag{25}$$

avec :

$$\begin{aligned} deg(A_{i-2}) = d_1 - deg(G_{i-2}), deg(B_{i-2}) = d_0 - deg(G_{i-2}) \\ deg(A_{i-1}) = d_1 - deg(G_{i-1}) \ , \ deg(B_{i-1}) = d_0 - deg(G_{i-1}) \end{aligned}$$

et cherchons G_{i+1} sous la forme $A_i.A + B_i.B$.
Nous avons :

$$\begin{aligned} G_{i+1} = Gau(G_{i-1}, G_i) &= -\frac{Lc(G_i)}{Lc(G_{i-1})} Rem(G_{i-1}, G_i) \\ &= -\frac{Lc(G_i)}{Lc(G_{i-1})} [G_{i-1} - Q(G_{i-1}, G_i).G_i] \end{aligned}$$

En remplaçant G_{i-1} et G_i par leurs expressions de (25) on trouve par identification :

$$A_i = -\frac{Lc(G_i)}{Lc(G_{i-1})} [A_{i-2} - Q(G_{i-1}, G_i).A_{i-1}]$$

$$B_i = -\frac{Lc(G_i)}{Lc(G_{i-1})} [B_{i-2} - Q(G_{i-1}, G_i).B_{i-1}]$$

avec

$$deg(A_i) = d_1 - deg(G_i) \text{ et } deg(B_i) = d_0 - deg(G_i)$$

de plus si B_{i-2} et B_{i-1} sont unitaires alors B_i l'est aussi (Exercice) $\square$.