

I. Polynômes univariés.

1 Généralités

On considère l'anneau $A[X]$ des polynômes à coefficients dans un anneau A (commutatif et unitaire). Si l'anneau A est *intègre*, l'anneau $A[X]$ est intègre et l'on a ¹ :

$$\deg(fg) = \deg(f) + \deg(g) \text{ pour tout } f, g \in A[X]$$

Toujours dans le cas A intègre, on dispose du *corps des fractions* $K = \text{Frac}(A)$ de A et $K(X)$ est le corps des fractions de $A[X]$.

On désigne par $A^\times$ le groupe (multiplicatif) des éléments *inversibles* de A ; deux éléments $x, y \in A$ sont *associés* ² s'il existe $u \in A^\times$ tel que $y = ux$; on obtient une relation d'équivalence sur A .

Un élément $p \in A$ est *premier* s'il vérifie le lemme d'Euclide ³ :

$$\text{pour tout } x, y \in A : p|xy \implies p|x \text{ ou } p|y$$

et un élément $p \in A$ est *irréductible* si :

$$\text{pour tout } a \in A : a|p \implies a \in A^\times \text{ ou } a \simeq p$$

Tout élément p premier est alors irréductible ; la réciproque est vérifiée lorsque A est *factoriel*. Si l'anneau A est *factoriel*, l'anneau $A[X]$ est factoriel. Dans ce cas, un polynôme $f \in A[X]$ est *primitif* si ses coefficients sont premiers entre eux. Tout polynôme non nul $f \in K[X]$ s'écrit de manière unique, aux éléments associés près, $f = \text{cont}(f)\text{pp}(f)$ avec $\text{cont}(f) \in K^*$ (*contenu* de f) et $\text{pp}(f) \in A[X]$ polynôme primitif (*partie primitive* de f). Etant donné $f \in K[X]$, on a $f \in A[X]$ si et seulement si $\text{cont}(f) \in A$.

On a de plus, pour $f, g \in K[X] \setminus \{0\}$:

1. $\text{cont}(fg) \simeq \text{cont}(f)\text{cont}(g)$
2. $\text{pp}(fg) \simeq \text{pp}(f)\text{pp}(g)$

Soit $f \in A[X]$ un polynôme primitif ; alors f est irréductible dans $A[X]$ si et seulement si f est irréductible dans $K[X]$ (lemme de Gauss). de sorte que les éléments irréductibles de $A[X]$ sont, d'une part les éléments irréductibles de A , d'autre part les polynômes primitifs de $A[X]$ irréductibles dans $K[X]$.

Un anneau A est *principal* s'il est intègre et si tout idéal de A est engendré par un élément ; alors A est factoriel et pour tout élément irréductible $p \in A$ l'idéal $\langle p \rangle$ est *maximal* ; en particulier l'anneau $A[X]$ est principal si et seulement si A est un *corps*.

Enfin un anneau A est *noethérien* si tout idéal de A possède un système générateur fini ⁴. Si l'anneau A est noethérien, l'anneau $A[X]$ est noethérien (théorème de la base finie de Hilbert).

Par ailleurs on dira qu'une structure algébrique est *effective* si l'on dispose :

1. d'une structure de données pour représenter les éléments
2. d'algorithmes pour effectuer les opérations et pour tester l'égalité

1. en général on a seulement $\deg(fg) \leq \deg(f) + \deg(g)$ pour tout $f, g \in A[X]$
 2. on notera $y \simeq x$ la relation d'association
 3. l'idéal $\langle p \rangle$ est premier i.e. $A/\langle p \rangle$ est intègre
 4. si A principal, A est évidemment noethérien

2 Algorithme d'Euclide

Soit K un corps commutatif ; on suppose que K est *effectif* ; alors l'anneau $K[X]$ est effectif et est *euclidien* (de manière effective aussi).

Algorithme 1 *Division euclidienne*

1. *entrée* : des polynômes non nuls $f, g \in K[X]$
2. *initialisations* : $q := 0, r := f$
3. *tant que* $r \neq 0$ *et* $\deg(r) \geq \deg(g)$ *boucle* :

$$\left\{ \begin{array}{l} (a) \ M := \frac{\text{lc}(r)}{\text{lc}(g)} X^{\deg(r) - \deg(g)} \\ (b) \ q := q + M \\ (c) \ r := r - Mg \end{array} \right\}$$
4. *sortie* : les polynômes $q, r \in K[X]$ que $f = gq + r$ avec $r = 0$ ou $\deg(r) < \deg(g)$

▽ Posons $m = \deg(f)$ et $n = \deg(g)$; l'algorithme de la division euclidienne comporte au plus $m - n + 1$ itérations (*terminaison*).

Notons q_i et r_i les quotients et restes partiels calculés à l'étape i ; on a alors :

$$\begin{aligned} M_i &= \frac{\text{lc}(r_i)}{\text{lc}(g)} X^{\deg(r_i) - \deg(g)} \\ q_{i+1} &= q_i + M_i \\ r_{i+1} &= r_i - M_i g \end{aligned}$$

Il en résulte que l'égalité $f = gq_i + r_i$ est un invariant de boucle (*correction*).

Pour tout polynôme non nul $h \in K[X]$, on pose :

$$\text{trn}(h) = h - \text{lc}(h) X^{\deg(h)}$$

de sorte que

$$\text{trn}(h) = 0 \text{ ou } \deg(\text{trn}(h)) < \deg(h)$$

et l'on a :

$$r_{i+1} \text{trn}(r_i) - M_i \text{trn}(g)$$

Ainsi une itération représente au plus $2n$ opérations dans le corps K et la division euclidienne comporte au plus $2n(m - n + 1)$ opérations dans le corps K est donc d'une *complexité* de l'ordre de $O(n(m - n))$. Δ

Pour tout entier $d \geq 0$, on désigne par $K[X]_{\leq d-1}$ le K -espace vectoriel de dimension d formé du polynôme nul et des polynômes de $K[X]$ de degré $\leq d - 1$. L'espace vectoriel $K[X]_{\leq d-1}$ possède la *base canonique* $(X^{d-1}, \dots, X, 1)$.

Soient $f = \sum_{i=0}^m a_i X^i \in K[X]$ et $g = \sum_{j=0}^n b_j X^j \in K[X]$ des polynômes à coefficients dans un corps commutatif K et à une indéterminée X , de degrés respectifs m et n ; l'application de *Bezout-Sylvester* est l'application K -linéaire :

$$\begin{aligned} \partial_{f,g}^{m,n} : K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} &\longrightarrow K[X]_{\leq m+n-1} \\ (u, v) &\longrightarrow u f + v g \end{aligned}$$

Lemme 1 *L'application de Bezout-Sylvester $\partial_{f,g}^{m,n}$ est bijective si et seulement si f et g sont premiers entre eux.*

▽ Soit $(u, v) \in \text{Ker}(\partial_{f,g}^{m,n})$; on a $uf + vg = 0$ de sorte que $f|vg$ donc $f|v$. Si on avait $v \neq 0$ on aurait $\deg(v) \geq m$ de sorte que $v = 0 = 0$. Ainsi $\partial_{f,g}^{m,n}$ est injective, donc un isomorphisme par égalité des dimensions.

Réciproquement si $\partial_{f,g}^{m,n}$ est bijective, on a $uf + vg = 1$ donc f et g sont premiers entre eux. Δ

Définition 1

Le déterminant $R_X(f, g) = \det(\partial_{f,g}^{m,n}) \in K$ de l'application $\partial_{f,g}^{m,n}$ (où $m = \deg(f)$ et $n = \deg(g)$) est le résultant des polynômes $f, g \in K[X]$.

En particulier on a $R_X(f, g) \neq 0$ si et seulement si f et g sont premiers entre eux.

Soient $f, g \in K[X]$ de degrés respectifs m et n ; on pose $\Delta = \text{pgcd}(f, g)$, $d = \deg(\Delta)$; l'application linéaire :

$$\begin{aligned} \partial_{f,g} : K[X]_{\leq n-d-1} \times K[X]_{\leq m-d-1} &\longrightarrow K[X]_{\leq m+n-2d-1} \\ (U, V) &\longrightarrow U \frac{f}{\delta} + V \frac{g}{\delta} \end{aligned}$$

est bijective. En particulier il existe des polynômes *uniques* $u \in K[X]_{\leq n-d-1}$ et $v \in K[X]_{\leq m-d-1}$ tels que $uf + vg = \Delta$ (*formule de Bezout*). L'*algorithme d'Euclide* permet de calculer *pgcd* Δ : Pour $f, g \in K[X]$, on définit des suites finies de polynômes *non nuls* : $f_0, \dots, f_t$ (*suite des restes*) et $q_1, \dots, q_t$ (*suite des quotients*) en posant $f_0 = f$ et $f_1 = g$ et pour chaque k , $1 \leq k \leq t$ on effectue la division euclidienne de f_{k-1} par f_k ; on a donc :

$$f_{k-1} = f_k q_k + r_{k+1} \text{ avec } r_{k+1} = 0 \text{ ou } \deg(r_{k+1}) < \deg(f_k) \text{ pour } 0 \leq k \leq t-1$$

Si $r_{k+1} = 0$ on pose $t = k$ et on s'arrête sinon on choisit $\mu_k \in K^*$; et on pose $f_{k+1} := \frac{1}{\mu_k} r_{k+1}$.

Les coefficients *non nuls* α , β et μ_k ($1 \leq k \leq t-1$) permettent d'introduire différentes variantes de l'algorithme :

Exemples :

1. L'algorithme d'Euclide *classique* s'obtient en prenant $\alpha = 1$, $\beta = 1$, $\lambda_k = \mu_k = 1$ et en utilisant la division euclidienne.
2. En prenant $\alpha = 1/\text{lc}(f)$, $\beta = 1/\text{lc}(g)$, $\lambda_k = 1$, $\mu_k = \text{lc}(\widetilde{f_{k+1}})$ et en utilisant la division euclidienne on obtient le *pgcd unitaire*.
3. Si $f, g \in A[X]$, en utilisant la division euclidienne et en prenant pour α (*resp.* β) le ppcm des dénominateurs des coefficients de f (*resp.* g), $\lambda_k = \text{lc}(\widetilde{f_{k+1}})^{\deg(f_{k-1}) - \deg(f_k) + 1}$, $\mu_k = 1$ (ou, ce qui revient au même, en utilisant la *pseudo-division* et en prenant $\lambda_k = 1$ et $\mu_k = 1$) on effectue les calculs dans $A[X]$.
4. Si $f, g \in A[X]$, en utilisant la division euclidienne et en prenant en prenant pour α (*resp.* β) le ppcm des dénominateurs des coefficients de f (*resp.* g), $\lambda_k = \text{lc}(\widetilde{f_{k+1}})^{\deg(f_{k-1}) - \deg(f_k) + 1}$, $\mu_k = \text{cont}(\widetilde{f_{k+1}})$ (ou, ce qui revient au même, en prenant la partie primitive du pseudo-reste avec $\lambda_k = 1$ et $\mu_k = 1$) on effectue les calculs dans $A[X]$ tout en modérant la *croissance des données intermédiaires*.

Algorithme 2 (Algorithme d'Euclide)

1. *entrée* : des polynômes $f, g \in K[X]$

2. *initialisations* : $f_0 := \alpha f$, $f_1 := \beta g$

3. *boucle* :

- $$\left\{ \begin{array}{l} (a) \ f_0 := q f_1 + r \text{ avec } r = 0 \text{ ou } \deg(r) < \deg(f_1) \\ (b) \text{ sortir quand } r = 0 \\ (c) \ f_0, f_1 := f_1, \frac{1}{\mu} r \text{ avec } \mu \in K^* \end{array} \right\}$$

4. *sortie* : le pgcd $\Delta = f_1$ de f et g

∇ Si l'on avait $f_i \neq 0$ pour tout $i \geq 1$, La suite $(\deg(f_k))_{k \geq 1}$ serait strictement décroissante ce qui n'est pas possible puisque $\mathbb{N}$ est un ensemble bien-ordonné (*terminaison*).

Si $f = qg + \mu r$ avec $\mu \in K^*$, on a $\text{pgcd}(f, g) = \text{pgcd}(g, r)$ de sorte que l'on a $\text{pgcd}(f, g) = \text{pgcd}(f_k, f_{k+1})$ pour $1 \leq k \leq t-1$ et finalement $\text{pgcd}(f, g) = \text{pgcd}(f_{t-1}, f_t) = f_t$. Ainsi f_t est un pgcd de f et de g (*correction*).

L'étape k comporte

$$2\deg(f_k)(\deg(f_{k-1}) - \deg(f_k) + 1)$$

opérations dans le corps K de sorte que le nombre d'opération est borné par :

$$\sum_{k=1}^t (2\deg(f_k)(\deg(f_{k-1}) - \deg(f_k) + 1)) \leq 2n(\deg(f_0) - \deg(f_t)) + 2nt = 2n(m-d+t) \leq 2n(m+t) \leq 4mn$$

de sorte que la *complexité* de l'algorithme d'Euclide est d'ordre $O(mn)$. Δ

L'*algorithme d'Euclide étendu* permet d'obtenir en plus les *coefficients de Bezout* u et v en définissant par récurrence les suites $u_0, \dots, u_t$ et $v_1, \dots, v_t$ par $u_0 = \alpha$, $u_1 = 0$, $v_0 = 0$, $v_1 = \beta$ et les relations : $u_{k+1} = \frac{1}{\mu_k}(u_{k-1} - q_k u_k)$ et $v_{k+1} = \frac{1}{\mu_k}(v_{k-1} - q_k v_k)$.

Proposition 1

On a :

1. $f_k = u_k f + v_k g$ ($k \geq 0$)
2. $u_k v_{k+1} - u_{k+1} v_k = \frac{(-1)^k}{\mu_1 \cdots \mu_k}$ ($k \geq 0$) En particulier, u_k et v_k sont premiers entre eux.
3. $\deg(u_k) = \deg(g) - \deg(f_{k-1})$ ($k \geq 2$)
4. $\deg(v_k) = \deg(f) - \deg(f_{k-1})$ ($k \geq 2$)

∇ Les égalités s'obtiennent par récurrence sur k en remarquant, pour les deux dernières, que $\deg(q_k) = \deg(f_{k-1}) - \deg(f_k)$.

On a $\Delta = f_t$, $u = u_t$ et $v = v_t$. On a par ailleurs :

$$\deg(f_t) < \cdots < \deg(f_k) < \deg(f_{k-1}) < \cdots < \deg(f_1)$$

de sorte que :

$$\begin{aligned} \deg(u_k) &= \deg(g) - \deg(f_{k-1}) < \deg(g) - \deg(f_t) \\ \deg(v_k) &= \deg(f) - \deg(f_{k-1}) < \deg(f) - \deg(f_t) \end{aligned}$$

Δ

Algorithme 3 (Algorithme d'Euclide étendu)

1. *entrée* : des polynômes $f, g \in K[X]$
2. *initialisations* : $f0 := f, f1 := g, u0 := \alpha, u1 := 0, v0 := 0, v1 := \beta$
3. *boucle* :

$$\left\{ \begin{array}{l} (a) \ f0 := q f1 + r \text{ avec } r = 0 \text{ ou } \deg(r) < \deg(f1) \\ (b) \text{ sortir quand } r = 0 \\ (c) \ f0, f1 := f1, \frac{1}{\mu} r \text{ avec } \mu \in K^\star \\ (d) \ u0, u1 := u1, \frac{1}{\mu} (u0 - q u1) \\ (e) \ v0, v1 := v1, \frac{1}{\mu} (v0 - q v1) \end{array} \right\}$$
4. *sortie* : le pgcd $\Delta = f1$ de f et g et les coefficients de Bezout $u = u1$ et $v = v1$ tels que $f u + g v = \Delta$ avec $u = 0$ ou $\deg(u) < \deg(\frac{g}{\Delta})$ et $v = 0$ ou $\deg(v) < \deg(\frac{f}{\Delta})$.

3 Le résultant

3.1 La matrice de Sylvester

Définition 2

Soient $f, g \in K[X]$ des polynômes non nuls de degrés respectifs m et n ; la matrice de Sylvester $S_X^{m,n}(f, g)$ est la matrice⁵ de l'application linéaire :

$$\begin{aligned} \partial_{f,g}^{m,n} : K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} &\longrightarrow K[X]_{\leq m+n-1} \\ (u, v) &\longrightarrow u f + v g \end{aligned}$$

dans les bases canoniques⁶ des espaces $K[X]_{\leq n-1} \oplus K[X]_{\leq m-1}$ et $K[X]_{\leq m+n-1}$.

Pour $1 \leq j \leq n$ (resp. $1 \leq i \leq m$), la matrice de Sylvester $S_X^{m,n}(f, g)$ a pour colonne C_j (resp. C_{n+i}) les coefficients du polynôme $X^{n-j} f(X)$ (resp. $X^{m-i} g(X)$) dans la base canonique $(X^{m+n-k})_{1 \leq k \leq m+n}$ du K -espace vectoriel de dimension $m+n$ des polynômes de degré $\leq m+n-1$; on a donc :

$$S_X^{m,n}(f, g) = \begin{pmatrix} a_m & 0 & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\ a_{m-1} & a_m & \vdots & & & b_{n-1} & b_n & & \vdots \\ \vdots & a_{m-1} & a_m & & & & b_{n-1} & & 0 \\ & \vdots & a_{m-1} & & 0 & \vdots & & & b_n \\ a_0 & & \vdots & & a_m & & \vdots & & b_{n-1} \\ 0 & a_0 & & \ddots & a_{m-1} & b_0 & & \ddots & \\ \vdots & 0 & a_0 & & \vdots & 0 & b_0 & & \vdots \\ & & 0 & & & \vdots & 0 & & \\ 0 & & & & a_0 & 0 & & & b_0 \end{pmatrix}$$

5. ou sa transposée

6. $((X^{n-1}, 0), \dots, (X, 0), (1, 0), (0, X^{m-1}), \dots, (0, X), (0, 1))$ est la base canonique de $K[X]_{\leq n-1} \oplus K[X]_{\leq m-1}$ et $(X^{m+n-1}, \dots, X, 1)$ est la base canonique de $K[X]_{\leq m+n-1}$

de sorte qu'en posant $S_X^{m,n}(f, g) = (S_{i,j})_{1 \leq i, j \leq m+n}$ on obtient :

$$\begin{aligned} & \star \text{ pour } 1 \leq j \leq n : \\ & \quad \begin{cases} S_{j+i,j} = a_{m-i} \text{ pour } 0 \leq i \leq m \\ S_{k,j} = 0 \text{ pour } k \notin [j, m+j] \end{cases} \\ & \star \text{ pour } 1 \leq i \leq m : \\ & \quad \begin{cases} S_{i+j,n+i} = b_{n-j} \text{ pour } 0 \leq j \leq n \\ S_{k,n+i} = 0 \text{ pour } k \notin [i, n+i] \end{cases} \end{aligned}$$

Le résultant

$$R_X(f, g) = \det(S_X^{m,n}(f, g))$$

des polynômes f et g est le déterminant de la matrice de Sylvester $S_X^{m,n}(f, g)$:

Corollaire 1

Soit A un anneau intègre de corps de fractions $K = \text{Frac}(A)$; si on a $f \in A$ et $g \in A$ on a $R_X(f, g) \in A$.

▽ La matrice $S_X^{m,n}(f, g)$ est à coefficients dans A et la formule de Leibniz montre que $R_X(f, g) = \det(S_X^{m,n}(f, g)) \in A$. Δ

Corollaire 2

Etant donnés des polynômes $f = \sum_{i=0}^m a_i X^i$ et $g = \sum_{j=0}^n b_j X^j$ de degrés m et n on a :

1. $R_X(f, g) = a_m^n$ si $m = 0$ (ie. f constant)
2. $R_X(\lambda f, \mu g) = \lambda^n \mu^m R_X(f, g)$ $\lambda, \mu \in K$
3. $R_X(g, f) = (-1)^{mn} R_X(f, g)$
4. $R_X(X - x, g) = g(x)$

▽ Pour 1. la matrice de Sylvester est de la forme :

$$S_X^{0,n}(f, g) = \begin{pmatrix} a_m & 0 & 0 & \cdots & 0 \\ 0 & a_m & \vdots & & \\ \vdots & 0 & a_m & & \vdots \\ & \vdots & 0 & \ddots & 0 \\ 0 & & \vdots & & a_m \end{pmatrix}$$

Pour 2. et 3. cela résulte de ce que le déterminant d'une matrice est une forme multilinéaire alternée par rapport aux colonnes de cette matrice. Pour 4. $R_X(X - x, g)$ est le déterminant de la matrice :

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & b_n \\ -x & 1 & \cdots & 0 & b_{n-1} \\ \vdots & -x & \ddots & \vdots & \vdots \\ 0 & \vdots & \ddots & 1 & b_1 \\ 0 & \cdots & \cdots & -x & b_0 \end{pmatrix}$$

En développant par rapport à la dernière colonne on obtient $\sum_{i=0}^n (-1)^{2n+2-i} b_i (-x)^i = g(x)$

Δ

Soit $f = \sum_{i=1}^m a_i X^i \in K[X]$ un polynôme de degré m ; on lui associe la K -algèbre

$$A = K[X]/\langle f \rangle$$

de rang m . Pour tout $g \in K[X]$ on considère :

$$\begin{aligned} m_g : A &\longrightarrow A \\ \bar{h} &\longrightarrow \bar{g}\bar{h} \end{aligned}$$

l'endomorphisme du K -espace vectoriel A induit par la multiplication par g .

Proposition 2 (formule de Poisson)

$$R_X(f, g) = a_m^n \det(m_g)$$

▽ voir l'exercice 2. de la fiche de TD 1 Δ

Corollaire 3 (multiplicativité) Soient $f, g, h \in K[X]$ des polynômes non nuls de degrés respectifs m, n, p ; on a :

$$R_X(f, gh) = R_X(f, g)R_X(f, h)$$

▽ D'après la formule de Poisson on a :

$$R_X(f, g) = a_m^n \det(m_g) \quad R_X(f, h) = a_m^p \det(m_h) \quad R_X(f, hg) = a_m^{n+p} \det(m_{gh})$$

or

$$\det(m_{gh}) = \det(m_g)\det(m_h)$$

Δ

Corollaire 4

On considère une K -extension Ω contenant les racines $x_1, \dots, x_m$ les racines de $f = \sum_{i=0}^m a_i X^i$ et les racines $y_1, \dots, y_n$ de $g = \sum_{j=0}^n b_j X^j$. On a alors :

$$R_X(f, g) = a_m^n b_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (x_i - y_j) = a_m^n \prod_{i=1}^m g(x_i) = (-1)^{mn} b_n^m \prod_{j=1}^n f(y_j)$$

▽ Les trois relations se déduisent l'une de l'autre puisque l'on a :

$$f = a_m \prod_{i=1}^m (X - x_i) \quad g = b_n \prod_{j=1}^n (X - y_j)$$

Le lemme de multiplicativité montre que :

$$R_X(f, g) = R_X(a_m \prod_{i=1}^m (X - x_i), g) = a_m^n \prod_{i=1}^m R_X((X - x_i), g) = a_m^n \prod_{i=1}^m g(x_i)$$

Δ

Corollaire 5

Considérons des polynômes non nuls $f, g \in K[X]$ de degrés respectifs m et n avec $m \leq n$; soit h le reste de la division euclidienne de g par f ; on a :

$$R_X(f, g) = \begin{cases} a_m^{n-r} R_X(f, h) & \text{si } h \neq 0 \text{ et } r = \deg(h) \\ 0 & \text{si } h = 0 \end{cases}$$

▽ On a $g = fq + h$ avec $h \in K[X]_{\leq m-1}$ de sorte que $m_g = m_h$. Si $h = 0$ on a $R_X(f, g) = 0$ Supposons maintenant $h \neq 0$; on a alors :

$$\begin{aligned} R_X(f, g) &= a_m^n \det(m_g) \\ &= a_m^n \det(m_h) \\ &= a_m^{n-r} a_m^r \det(m_h) \\ &= a_m^{n-r} R_X(f, h) \end{aligned}$$

Δ

3.2 Résultant et formule de Bezout

Proposition 3

Soit A un anneau factoriel de corps de fractions $K = \text{Frac}(A)$; on considère $f, g \in A[X]$ des polynômes premiers entre eux à coefficients dans A de degré respectifs m et n et $u \in K[X]_{\leq n-1}$ et $v \in K[X]_{\leq m-1}$ uniques tels que $u f + v g = R_X(f, g)$; on a alors $u, v \in A[X]$. En particulier on a $R_X(f, g) \in \langle f, g \rangle \cap A$.

▽ Soit $\widetilde{S_X^{m,n}}(f, g)$ la matrice transposée des cofacteurs (*comatrice*) de la matrice de Sylvester $S_X^{m,n}(f, g)$ de f et g . On a les formules de Cramer :

$$S_X^{m,n}(f, g) \widetilde{S_X^{m,n}}(f, g) = \widetilde{S_X^{m,n}}(f, g) S_X^{m,n}(f, g) = R_X(f, g) I$$

Puisque $S_X^{m,n}(f, g)$ est à coefficients dans A la *comatrice* $\widetilde{S_X^{m,n}}(f, g)$ est à coefficients dans A . Puisque f et g sont premiers entre eux dans $A[X]$ donc dans $K[X]$, l'application K -linéaire

$$\partial_{f,g}^{m,n} : K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} \longrightarrow K[X]_{\leq m+n-1}$$

est bijective de sorte qu'il existe $u \in K[X]_{\leq n-1}$ et $v \in K[X]_{\leq m-1}$ uniques tels que :

$$u f + v g = R_X(f, g)$$

ce qui s'écrit *matriciellement* :

$$S_X^{m,n}(f, g) \begin{pmatrix} u_{n-1} \\ \vdots \\ u_1 \\ u_0 \\ v_{m-1} \\ \vdots \\ v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ R_X(f, g) \end{pmatrix} = R_X(f, g) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

En appliquant la *comatrice* $\widetilde{S_X^{m,n}}(f, g)$ aux deux membres on obtient :

$$\begin{pmatrix} u_{n-1} \\ \vdots \\ u_1 \\ u_0 \\ v_{m-1} \\ \vdots \\ v_1 \\ v_0 \end{pmatrix} = \widetilde{S_X^{m,n}}(f, g) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Ainsi les polynômes u et v sont à coefficients dans A puisque la *comatrice* $\widetilde{S_X^{m,n}}(f, g)$ est à coefficients dans A . Δ

3.3 Spécialisation du résultant

Un morphisme d'anneaux $\phi : A \longrightarrow B$ se prolonge de manière unique en un morphisme $A[X] \longrightarrow B[X]$ (noté encore ϕ) tel que $\phi(X) = X$ autrement dit on a $\phi(\sum_{i=0}^m a_i X^i) = \sum_{i=0}^m \phi(a_i) X^i$.

Proposition 4 (spécialisation du résultant)

Soient $\phi : A \longrightarrow B$ un morphisme d'anneaux intègres, $f = \sum_{i=0}^m a_i X^i$ et $g = \sum_{j=0}^n b_j X^j$ des polynômes à coefficients dans A de degré (respectivement) m et n ; on alors :

$$\phi(R_X(f, g)) = \begin{cases} 0 & \text{si } \deg(\phi(f)) < \deg(f) \text{ et } \deg(\phi(g)) < \deg(g) \\ \phi(a_m)^k R_X(\phi(f), \phi(g)) & \text{si } \deg(\phi(f)) = \deg(f) \text{ et } \deg(\phi(g)) = \deg(g) - k \end{cases}$$

∇ On a :

$$\phi(R_X(f, g)) = \phi(\det(S_X^{m,n}(f, g))) = \det(\phi(S_X^{m,n}(f, g)))$$

avec :

$$\phi(S_X^{m,n}(f, g)) = \begin{pmatrix} \phi(a_m) & 0 & 0 & \cdots & 0 & \phi(b_n) & 0 & \cdots & 0 \\ \phi(a_{m-1}) & \phi(a_m) & \vdots & & & \phi(b_{n-1}) & \phi(b_n) & & \vdots \\ \vdots & \phi(a_{m-1}) & \phi(a_m) & & & & \phi(b_{n-1}) & & 0 \\ & \vdots & \phi(a_{m-1}) & & 0 & \vdots & & & \phi(b_n) \\ \phi(a_0) & & \vdots & & \phi(a_m) & & \vdots & & \phi(b_{n-1}) \\ 0 & \phi(a_0) & & \ddots & \phi(a_{m-1}) & \phi(b_0) & & \ddots & \\ \vdots & 0 & \phi(a_0) & & \vdots & 0 & \phi(b_0) & & \vdots \\ & & 0 & & \vdots & 0 & & & \\ 0 & & & \phi(a_0) & 0 & & & & \phi(b_0) \end{pmatrix}$$

Pour $\deg(\phi(f)) < m$ et $\deg(\phi(g)) < n$ ie. $\phi(a_m) = 0$ et $\phi(b_n) = 0$ la première ligne de la matrice $\phi(S_X^{m,n}(f, g))$ est nulle de sorte que $\phi(R_X(f, g)) = 0$.

Supposons que $\deg(\phi(f)) = m$ et $\deg(\phi(g)) = n - k$ ie. $\phi(a_m) \neq 0$ et $\phi(b_n) = \cdots = \phi(b_{n-k+1}) = 0$, $\phi(b_{n-k}) \neq 0$. Alors la matrice $\phi(S_X^{m,n}(f, g))$ a la décomposition en blocs :

$$\phi(S_X^{m,n}(f, g)) = \begin{pmatrix} T & 0 \\ \star & \phi(S_X^{m,n-k}(f, g)) \end{pmatrix}$$

où T est la matrice carrée d'ordre k , triangulaire :

$$\begin{pmatrix} \phi(a_m) & 0 & \cdots & 0 \\ \phi(a_{m-1}) & \phi(a_m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \cdots & \phi(a_m) \end{pmatrix}$$

Mais on a :

$$\phi(S_X^{m,n-k}(f, g)) = S_X^{m,n-k}(\phi(f), \phi(g))$$

de sorte que :

$$\phi(R_X(f, g)) = \phi(a_m)^k R_X(\phi(f), \phi(g))$$

△

3.4 Résultant et algorithme d'Euclide

Proposition 5

Soit K un corps commutatif; le résultant est l'unique application :

$$R_X : K[X] \setminus \{0\} \times K[X] \setminus \{0\} \longrightarrow K$$

vérifiant les conditions suivantes :

1. $R_X(a, g) = a^n$ pour $a \in K^*$, $g \in K[X] \setminus \{0\}$ de degré n .
2. $R_X(f, g) = (-1)^{mn} R_X(g, f)$ pour $f, g \in K[X] \setminus \{0\}$ de degrés respectifs m et n .
3. Pour $f, g \in K[X] \setminus \{0\}$ de degrés respectifs m et n avec f non constant et $m \leq n$, soit h le reste de la division euclidienne de g par f ; on a :

$$R_X(f, g) = \begin{cases} a_m^{n-r} R_X(f, h) & \text{si } h \neq 0 \text{ et } r = \deg(h) \\ 0 & \text{si } h = 0 \end{cases}$$

On a vu que le résultant $R_X(f, g)$ vérifie les propriétés précédentes.

Pour montrer l'unicité, supposons que l'on ait une application

$$\mathcal{R} : K[X] \setminus \{0\} \times K[X] \setminus \{0\} \longrightarrow K$$

vérifiant les trois propriétés ci-dessus.

On a évidemment $R_X(a, g) = \mathcal{R}(a, g)$ pour tout $a \in K^*$ et $g \in K[X] \setminus \{0\}$.

Supposons par hypothèse de récurrence que l'on a $R_X(f, g) = \mathcal{R}(f, g)$ pour tout $f, g \in K[X] \setminus \{0\}$ avec $\deg(f) < m$ et considérons f de degré m et g de degré n . Si $n < m$ on a :

$$\begin{aligned} R_X(f, g) &= (-1)^{mn} R_X(g, f) \\ &= (-1)^{mn} \mathcal{R}(g, f) \\ &= \mathcal{R}(f, g) \end{aligned}$$

Par contre si $m \leq n$ on effectue la division euclidienne $g = fQ + h$; si $h = 0$ on a évidemment $R_X(f, g) = \mathcal{R}(f, g) = 0$ et sinon :

$$\begin{aligned} R_X(f, g) &= a_m^r R_X(f, h) \\ &= (-1)^{mr} a_m^r R_X(h, f) \\ \mathcal{R}(f, g) &= a_m^r \mathcal{R}(f, h) \\ &= (-1)^{mr} a_m^r \mathcal{R}(h, f) \end{aligned}$$

avec $r = \deg(h) < m$ de sorte que $R_X(h, f) = \mathcal{R}(h, f)$ par l'hypothèse de récurrence et finalement $R_X(f, g) = \mathcal{R}(f, g)$. Δ

La caractérisation précédente conduit à un algorithme *sommaire* permettant de calculer un résultant par une variante de l'algorithme d'Euclide :

Algorithme 4 résultant

1. entrée : f, g polynômes en une indéterminée X
2. initialisations $F := f, G := g, R := 1$
3. boucle :
 $\{$
(a) si $\deg(F) > \deg(G)$ alors

- $$R := (-1)^{\deg(F)\deg(G)} R$$
- échanger F et G
- (b) si $\deg(F) = 0$ alors sortir $F^{\deg(G)} R$
- (c) calculer H le reste euclidien de G par F
- (d) si $H = 0$ alors sortir 0
- (e) $R := \text{lc}(F)^{\deg(G)-\deg(H)} R$
- (f) $G := H$
- }

4. sortie le résultant R

3.5 Le Discriminant

Soit K un corps ; on considère un polynôme $f \in K[X]$ de degré m et de coefficient dominant a_m et Ω une K -extension contenant les racines $x_1, \dots, x_m$ de f . On a le déterminant de Van der Monde :

$$V(x_1, \dots, x_m) = \det((x_i^{j-1})_{1 \leq i, j \leq m}) = \prod_{1 \leq i < j \leq m} (x_i - x_j)$$

On définit le *discriminant* de f (relativement à X) par :

$$\text{discrim}_X(f) = a_m^{2m-2} V(x_1, \dots, x_m)^2 \in \Omega$$

Corollaire 6

Soit $f \in K[X]$ un polynôme de degré m ; f est séparable⁷ si et seulement si $\text{discrim}_X(f) \neq 0$

▽ En effet le déterminant de Vandermonde $V(x_1, \dots, x_m)$ est non nul si et seulement si les x_i , $1 \leq i \leq m$ sont deux à deux distincts. △

Proposition 6

Soit $f \in K[X]$ un polynôme de degré m et de coefficient dominant a_m et tel que $f' \neq 0$, on a

$$\text{discrim}_X(f) = (-1)^{m(m-1)/2} a_m^{k-1} R_X(f, f') \text{ avec } k = m - 1 - \deg(f')$$

▽ Posons $d = \deg(f')$ de sorte que $k = m - 1 - d$.

On a

$$R_X(f, f') = a_m^d \prod_{i=1}^m f'(x_i)$$

Mais $f = a_m \prod_{i=1}^m (X - x_i)$ de sorte que

$$f' = a_m \sum_{i=1}^m (X - x_1) \cdots (X - x_{i-1})(X - x_{i+1}) \cdots (X - x_m)$$

On a donc :

$$f'(x_i) = a_m \prod_{i \neq j} (x_i - x_j)$$

7. ie. toutes les racines $x_1, \dots, x_m$ de f sont simples

d'où :

$$\begin{aligned}
R_X(f, f') &= a_m^d \prod_{i=1}^m a_m \prod_{i \neq j} (x_i - x_j) \\
&= a_m^{m+d} \prod_{1 \leq i \neq j \leq m} (x_i - x_j) \\
&= (-1)^{m(m-1)/2} a_m^{m+d} \prod_{1 \leq i < j \leq m} (x_i - x_j)^2 \\
&= (-1)^{m(m-1)/2} a_m^{m+d} V(x_1, \dots, x_m)^2
\end{aligned}$$

et finalement :

$$\begin{aligned}
a_m^{k-1} R_X(f, f') &= (-1)^{m(m-1)/2} a_m^{m+d+k-1} V(x_1, \dots, x_m)^2 \\
&= (-1)^{m(m-1)/2} a_m^{2m-2} V(x_1, \dots, x_m)^2 \\
&= (-1)^{m(m-1)/2} \text{discrim}_X(f)
\end{aligned}$$

Δ

Corollaire 7

Soient A un anneau intègre de corps des fractions $K = \text{Frac}(A)$; on a $\text{discrim}_X(f) \in A$ pour tout $f \in A[X]$.

▽ On a $\text{discrim}_X(f) = (-1)^{m(m-1)/2} a_m^{k-1} R_X(f, f')$ où $k = m - 1 - \deg(f')$. On a $R_X(f, f') \in A$ puisque $R_X(f, f')$ est le déterminant d'une matrice à coefficient dans A . De plus si $k \geq 1$ on a aussi $a_m^{k-1} \in A$ de sorte que $\text{discrim}_X(f) \in A$.

Supposons que $k = 0$ de sorte que la dérivée f' de f est de degré $m - 1$ le résultant $R_X(f, f') \in A$ est le déterminant de la matrice $S_X^{m, m-1}(f, f')$ dont la première ligne est de la forme

$$(a_m \quad 0 \quad \dots \quad 0 \quad ma_m \quad 0 \quad \dots \quad 0)$$

de sorte qu'en développant par rapport à cette ligne on voit que $R_X(f, f')$ est divisible par a_m . Dans ce cas aussi on a $\text{discrim}_X(f) \in A$. Δ

Corollaire 8

Soient A et B des anneaux intègres, $\phi : A \longrightarrow B$ un morphisme d'anneaux, $f = \sum_{i=0}^m a_i X^i \in A[X]$ tel que $\deg(f) = \deg(\phi(f))$; on a :

$$\phi(\text{discrim}_X(f)) = \text{discrim}_X(\phi(f))$$

▽ Notons que $\phi(f') = \phi(f)'$.

On pose $n = \deg(f')$ et $l = n - \deg(\phi(f'))$ de sorte que, par spécialisation du résultant :

$$\phi(R_X(f, f')) = \phi(a_m)^l R_X(\phi(X), \phi(f'))$$

On a finalement, compte tenu de ce que $k = m - 1 - n$:

$$\begin{aligned}
\phi(a_m) \phi(\text{discrim}_X(f)) &= (-1)^{m(m-1)/2} \phi(a_m)^k \phi(R_X(f, f')) \\
&= (-1)^{m(m-1)/2} \phi(a_m)^{k+l} R_X(\phi(X), \phi(f')) \\
&= (-1)^{m(m-1)/2} \phi(a_m)^{m-1-\deg(\phi(f'))} R_X(\phi(X), \phi(f')) \\
&= \phi(a_m) \text{discrim}_X(\phi(f))
\end{aligned}$$

Puisque $\phi(a_m) \neq 0$ et que B est intègre on a $\phi(\text{discrim}_X(f)) = \text{discrim}_X(\phi(f))$. Δ