1. Rappels et/ou Outils et/ou Compléments

Cette section est là pour rappeler des prérequis plus ou moins maitrisés avec un niveau de détail variable selon l'importance des résultats. Certains sont parfois redémontrés si cela permet d'introduire par exemple des éléments de preuve récurrents.

Dans toute la suite, les anneaux considérés sont par défaut commutatifs et unitaires tous les corps considérés par défaut commutatifs.

Assez peu de notions d'algèbre commutative seront utiles dans ce premier cours. Parmi elles, les notions d'anneau Euclidien, d'anneau Factoriel, corps des Fractions d'un anneau intègre, extension de corps.

1.1. Les structures utiles

Anneau (commutatif unitaire) : ensemble muni d'une addition lui donnant une structure de groupe abélien et d'une multiplication $\star$ qui est associative, distributive pour l'addition, commutative et possédant un élément neutre si l'anneau est unitaire.

Ideal : sous-groupe additif d'un anneau, stable par multiplication (à gauche et à droite dans notre cas) par un élément de l'anneau.

Anneau intègre : ne possède pas de diviseurs de 0.

Anneau Euclidien A : existence d'une « division Euclidienne » c'est à dire un stathme Euclidien ν , ou, autrement dit une application $\nu\colon A^\star \to \mathbb{N}$ tq $\forall a, b \in A^\star, \nu(b) \leqslant \nu(a\,b)$ et $\forall a \in A, b \in A^\star$, $\exists q, r$ tq $a = q\,b + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$.

Anneau Principal : idéal engendré par un seul élément

Anneau Factoriel : tout élément est produit fini d'irréductibles, et si $a = p_1 \ldots p_n = q_1 \ldots q_m$ alors $n = m$ et $p_i = q_{\sigma(i)}$

Rappel : Euclidien $\Rightarrow$ Principal $\Rightarrow$ Factoriel $\Rightarrow$ Intègre.

Corps des fractions d'un anneau intègre A : plus petit corps K contenant A . On peut le voir comme l'ensemble des couples $(a, b) \in A \times A^\star$ avec une multiplication $(a, b)\,(a', b') = (\mathrm{aa}', \mathrm{bb}')$, une addition $(a, b) + (a', b') = (a\,b' + a'\,b, b\,b')$ et une relation $(a, b) \sim (a', b')$ ssi $a\,b' = a'\,b$.

Corps algébriquement clos $\overline{K}$: tout non constant polynôme de $\overline{K}[X]$ s'écrit comme produit de polynômes de degré 1.

Clôture algébrique d'un corps K : plus petit corps algébriquement clos contenant K

$K[X]$ ou K est un corps : Euclidien donc principal donc factoriel.
$K[X_1, ..., X_n]$ ou K est un corps n'est pas principal donc pas Euclidien.
$A[X]$ ou A est Factoriel : Factoriel $\Rightarrow$ $A[X_1, ..., X_n]$ Factoriel.

Dans ce cours : $A = \mathbb{Z}, \mathbb{Q}[X], \mathbb{Q}[X_1, ..., X_n]$, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\frac{\mathbb{Z}}{p\,\mathbb{Z}}$ avec p premier et , $\mathbb{Q}(X_1, ..., X_n)$ le corps des fractions de $\mathbb{Q}[X_1, ..., X_n]$.

1.2. Déterminant d'une matrice, systèmes linéaires

Dans ce cours, beaucoup d'opérations se réduiront à des opérations simples d'algèbre linéaire, particulièrement la résolution de systèmes linéaires.

La définition est souvent oubliée .... mais est parfois utile :

DÉFINITION 1. *[Formule de Leibnitz] Soit* $M = (a_{i,j})_{i=1\ldots n}^{j=1\ldots n}$ *une matrice* $n \times n$ *à coefficients dans un anneau. Alors* $\det(M) = \sum_{\sigma \in \mathfrak{S}(n)} \epsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}$ *ou* $\mathfrak{S}(n)$ *est l'ensemble des permutations de* $\{1, ..., n\}$ *et* $\epsilon(\sigma)$ *la signature de* σ[1]

Majorer le déterminant est également un chose que l'on fait relativement souvent :

PROPOSITION 2. *Soit* M *une matrice* $n \times n$ *à coefficients réels. Désignons par* $C_1, \ldots, C_n$, *ses colonnes. Alors* $|\det(M)| \leqslant \|C_1\| \times .... \times \|C_n\|$ *ou* $\|.\|$ *est la norme euclidienne usuelle sur* $\mathbb{R}^n$.

Démonstration. On peut se restreindre au cas où $(C_1, ..., C_n)$ est une base de $\mathbb{R}^n$, car sinon $\det(M) = 0$. En appliquant le procédé d'orthogonalisation de Gram-Schmidt on construit une base orthogonale $(B_1, ..., B_n)$ avec $B_i = C_i + \sum_{j=1}^{i-1} \lambda_{i,j} C_j$. Soit B la matrice qui a pour colonnes les B_i. La matrice B est orthogonalement semblable à la matrice diagonale de coefficients diagonaux $\|B_1\|, ...\|B_n\|$. Par ailleurs $B = MT$ ou T est triangulaire supérieure avec uniquement des 1 sur la diagonale. Ainsi, $|\det(M)| = \|B_1\| \times .... \times \|B_n\|$ et, comme B_i est orthogonal à $\sum_{j=1}^{i-1} \lambda_{i,j} C_j$, alors $\|B_i\| \leqslant \|C_i\|$, ce qui conclut la démonstration. □

Une application directe de ce genre de borne est la majoration des numérateurs et dénominateurs des solutions d'un système linéaire à coefficients rationnels par exemple, en utilisant les formules de Cramer :

PROPOSITION 3. *[Formule de Cramer] Soit* $M = [a_{i,j}]$ *une matrice* $n \times n$ *à coefficients réels et* $V = [v_i]$ *un vecteur de dimension* n *à coefficients réels. Lorsque* $\det(M) \neq 0$, *le système linéaire* $MX = V$ *admet une unique solution* $X = [x_1, ..., x_n]^T$ *avec* $x_i = \frac{\det(M_i)}{\det(M)}$ *ou* M_i *est la matrice obtenue à partir de* M *en remplaçant la i-eme colonne de* M *par* V.

1.3. Algorithme d'Euclide et PGCD étendu

On suppose que $A[X]$ est un anneau Euclidien, et on se donne 2 polynômes $f, g \in A[X]$. On note $\deg_X(P)$ ou simplement $\deg(P)$ le degré de P en X et par $\mathrm{lc}_X(P)$ ou simplement $\mathrm{lc}(P)$ le coefficient du terme de plus haut degré de P en X (leading coefficient).

L'algorithme d'Euclide étendu appliqué à f et g est le calcul de la suite de triplets (t_l, s_l, r_l) tels que $r_0 = f$, $s_0 = 1$ $t_0 = 0$, $r_1 = g, s_1 = 0, t_1 = 1$ et vérifiant $s_i f + t_i g = r_i$ avec $\deg(r_{i+1}) < \deg(r_i), i \geqslant 1$.

Si elle existe, cette suite est finie à cause de la condition sur les degrés des r_i et on montre qu'elle se construit (donc existe) grace à l'opération de division Euclidienne :

Traditional Extended Euclidean Algorithm
- $r_0 = f$, $s_0 = 1$, $t_0 = 0$;
- $r_1 = g, s_1 = 0, t_1 = 1$:
- i:=1
- Tant que $r_i \neq 0$
  - $q_i, r_{i+1} :=$ Division(r_{i-1}, r_i)
  - $s_{i+1} := s_{i-1} - q_i s_i$
  - $t_{i+1} := t_{i-1} - q_i t_i$
  - i:=i+1
- l:=i-1
- RETURN$(l, (s_i, t_i, r_i)_{i=0\ldots l+1}, (q_i)_{i=1\ldots l})$

Si K est un corps, ou si on remplace simplement A par son corps des fractions, on peut définir "le" pgcd de 2 polynômes dans $K[X]$ en le supposant unitaire. Dans toute la suite, nous considèrerons la variante suivante ou les restes successifs sont tous unitaires :

1. On compte le nombre d'inversions, c'est à dire le nombre de couples (i, j) tels que $(i < j) \wedge (\sigma(i) > \sigma(j))$ la signature de σ est -1 si ce nombre est impair et 1 sinon.

(Normalized) **E**xtended **E**uclidean **A**lgorithm
$\rho_0 = \mathrm{lc}(f),\ \rho_1 = \mathrm{lc}(g)$
$r_0 = f/\rho_0,\ s_0 = 1/\rho_0,\ t_0 = 0;$
$r_1 = g/\rho_1, s_1 = 0, t_1 = 1/\rho_1$:
i:=1
Tant que $r_i \neq 0$
$q_i, r_{i+1} := \mathrm{Division}(r_{i-1}, r_i)$
$\rho_{i+1} := \mathrm{lc}(r_{i+1})$
$s_{i+1} := (s_{i-1} - q_i s_i)/\rho_{i+1}$
$t_{i+1} := (t_{i-1} - q_i t_i)/\rho_{i+1}$
i:=i+1
l:=i-1
RETURN(ρ_i,l, $(s_i, t_i, r_i)_{i=0\ldots l+1}, (q_i)_{i=1\ldots l}$)

Récapitulons les propriétés (plus ou moins) connues de cette suite

Lemme 4. *(Rappel)*

i. $\gcd(f,g) \sim \gcd(r_i, r_{i+1}) \sim r_l$

ii. $s_i f + t_i g = r_i$

iii. $\deg(s_i) = \deg(r_1) - \deg(r_{i-1})\ , \deg(t_i) = \deg(r_0) - \deg(r_{i-1})$

iv. $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$ *(En particulier s_i et t_i premiers entre eux)*

v. $\gcd(r_i, t_i) \sim \gcd(f, t_i)$

vi. $f = (-1)^i(t_{i+1} r_i - t_i r_{i+1})\ ,\ g = (-1)^i(s_{i+1} r_i - s_i r_{i+1})$

Etablissons 2 lemmes qui nous servirons par la suite :

Lemme 5. *Supposons que K soit un corps .*
$f, g, r, s, t \in K[X]$ avec $\deg(f) = n, r = s f + t g$ tq $\deg(r) + \deg(t) < n = \deg(f)$.
On suppose $\deg(r_j) \leqslant \deg(r) < \deg(r_{j-1})$. Alors, $\exists \alpha \in K[X]$ tq $r = \alpha r_j, s = \alpha s_j, t = \alpha t_j$.

Démonstration. On pose $\begin{pmatrix} s_j & t_j \\ s & t \end{pmatrix}\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_j \\ r \end{pmatrix}$. Supposons $s_j\, t \neq s\, t_j$. Alors $f = \frac{\det\begin{pmatrix} r_j & t_j \\ r & t \end{pmatrix}}{\det\begin{pmatrix} s_j & t_j \\ s & t \end{pmatrix}}$.
Mais $\deg(r_j\ t\ -\ t_j\ r) \leqslant \max\ (\deg(r_j)\ +\ \deg(t),\ \deg(r)\ +\ \deg(t_j)) \leqslant \max\ (\deg(r)\ +\ \deg(t),\ \deg(r) + n - \deg(r_{j-1})) < n$, ce qui est impossible.
Ainsi $s_j t = s\, t_j$ et comme s_j et t_j premiers entre eux alors t_j divise t, cad $\exists \alpha \in K[X]$ tq $\alpha t_j = t$ et donc $\alpha s_j t = s\, \alpha t_j = s\, \alpha t$, cad $\alpha s_j = s$ et finalement $\alpha r_j = \alpha(s_j f + t_j g) = s f + t g = r$. □

Lemme 6. *Un entier k tel que $0 \leqslant k \leqslant m < n$ n'apparait pas dans $(n_i = \deg(r_i))_{i=m\ldots l}$ si et seulement si $\exists (s,t)$ tq $t \neq 0, \deg(s) < m - k, \deg(t) < n - k, \deg(s f + t g) < k$.*

Démonstration. $\Rightarrow$ On choisit i, tq $2 \leqslant i \leqslant l+1$ et $n_i < k < n_{i+1}$ alors $s = s_i$ et $t = t_i$ conviennent et on a bien $\deg(s) = m - n_{i-1} < m - k$, $\deg(t) = n - n_i$ et $\deg(s f + t g) = \deg(r_i) = n_i < k$.

$\Leftarrow \exists i \in \mathbb{N}, \alpha \in K[X] \setminus \{0\}$ tq $\alpha s_i f + \alpha t_i g = \alpha r_i$ et $t = \alpha\, t_i, s = \alpha\, s_i, r = \alpha\, r_i$
Alors $n - n_{i-1} \leqslant \deg(\alpha) + n - n_{i-1} = \deg(\alpha\, t_i) = \deg(t) < n - k$ et $n_i \leqslant \deg(\alpha) + n_i = \deg(\alpha r_i) = \deg(r) < k$ et donc $n_{i-1} < k < n_i$ ce qui montre que k n'apparait pas dans la suite des restes. □

2. Sous-Resultants

Buts :

- Comprendre les problèmes de spécialisation de l'algorithme d'Euclide

- Elimination de variables (TD)
- Application : étude de courbes algébriques planes (TD)

Dans cette partie, A est un anneau factoriel et P_l désigne les polynômes de degré au plus l à coefficients dans K, le corps des fractions de A. Une famille de morphismes d'espaces vectoriels sur K pour f, g fixés dans $K[X]$ de degrés n, m:

$$\begin{array}{rccc} \varphi_k & : P_{m-k} \times P_{n-k} & \to & P_{n+m-2k} \\ & (s,t) & \to & (s\,f + t\,g) \text{ quo } X^k \end{array}$$

Commençons par un corrolaire ré-exprimant un résultat vu dans la section sur l'algorithme d'Euclide étendu :

PROPOSITION 7. $0 \leqslant k \leqslant m < n$

- *k apparait dans $(n_i = \deg(r_i))_{i=m\ldots s} \Leftrightarrow \varphi_k$ est un isomorphisme*
- *Si $k = n_i < n$ alors (s_i, t_i) est l'unique solution de $\varphi_k(s_i, t_i) = 1$ (restes normalisés)*

Démonstration.

- k n'apparait pas $\Leftrightarrow \exists (s,t) \neq (0,0), \varphi_k(s,t) = 0$ (thm précédent) $\Leftrightarrow \varphi_k$ pas injective
- Si $k = n_i$ alors par l'algorithme d'euclide étendu dans $K[X]$ donne $(s_i,\ t_i) \in K[X]$ tq $s_i\,P + t_i\,Q = r_i$ avec r_i unitaire de degré k, $\deg(s_i) = m - k, \deg(t_i) = n - k$. En particulier, $\varphi_k(s_i, t_i) = 1$. Comme φ_k est un isomorphisme d'après le premier point, (s_i, t_i) est même l'unique solution de $\varphi_k(s_i, t_i) = 1$. □

On Introduit :

$$S_k = \begin{pmatrix} f_n & 0 & \cdots & 0 & g_m & 0 & \cdots & \cdots & 0 \\ f_{n-1} & f_n & \ddots & \vdots & g_{m-1} & g_m & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & \ddots & \vdots \\ f_{n-m+k+1} & \cdots & \cdots & f_n & g_{k+1} & \cdots & \cdots & g_m & 0 \\ \vdots & & & \vdots & \vdots & & & & \ddots \\ f_{k+1} & \cdots & \cdots & f_m & g_{m-n+k+1} & \cdots & \cdots & \cdots & g_m \\ \vdots & & & \vdots & \vdots & & & & \vdots \\ \vdots & & & \vdots & \vdots & & & & \vdots \\ \underbrace{f_{2k-m+1}}_{m-k} & \cdots & \cdots & f_k & \underbrace{g_{2k-n+1}}_{n-k} & \cdots & \cdots & \cdots & g_k \end{pmatrix}$$

COROLLAIRE 8. $0 \leqslant k \leqslant m < n$

- *k apparait dans $(n_i = \deg(r_i))_{i=m\ldots l} \Leftrightarrow \det(S_k) \neq 0$*
- *Si $k = n_i < n$ et si $(y_0, \ldots, y_{m-k-1}, z_{n-k-1}, \ldots z_0)$ est l'unique solution de $S_k\,[y_0, \ldots, y_{m-k-1}, z_{n-k-1}, \ldots z_0]^T = [0, \ldots, 0, 1]^T$ alors :*
  - $s_{i=\sum_{0 \leqslant j < m-k} y_j X^j}$ *et* $t_{i=\sum_{0 \leqslant j < n-k} z_j X^j}$

DÉFINITION 9. *Soit A un anneau unitaire, K son corps des fractions et supposons que $f, g \in A[X]$.*
$\text{sres}_k = \det(S_k)$ *est le $k-$*ieme *coefficient sous-résultant principal associé à f et g.*
Si $\text{sres}_k \neq 0$ *alors* $\exists r_i \in K[X] \setminus \{0\}$ *dans la suite des restes normalisés dans $K[X]$ tel que* $\deg(r_i) = k$ *et* $\text{sres}_k\, r_i = \text{Sres}_k \in A[x]$.
Sres_k, *que l'on note éventuellement* $\text{Sres}_k(P, Q, X)$ *est alors le k-eme polynome sous-résultant associé à P, Q.*

DÉFINITION 10. *f, $g \in A[X]$ ou A est un anneau unitaire. Alors* $\text{sres}_0 = \text{Sres}_0 = \det(S_0)$ *est le Résultant de f et g. On remarque que S_0 est la transposée de la matrice de Sylvester* $\text{Syl}_X(P, Q)$.

THÉORÈME 11. *$\phi : A \to A'$ morphisme d'anneaux factoriels tel que $\phi(\text{lc}_X(f)) \neq 0$ et $\phi(\text{lc}_X(g)) \neq 0$. Alors $\phi(\text{Sres}_j(f, g, X)) = \text{Sres}_j(\phi(f), \phi(g), X)$*

Démonstration. Il suffit de remarquer que $\phi(\det(S_k(P,Q))) = \det(S_k(\phi(P),\phi(Q)))$, par exemple en utilisant la formule de Leibniz pour les déterminant et la définition d'un morphisme d'anneaux. La condition $\phi(\mathrm{lc}_X(f)) \neq 0$ et $\phi(\mathrm{lc}_X(g)) \neq 0$ ne sert qu'à s'assurer que les dimensions des matrices sont les mêmes. □

Exercice : Etant donnés f, $g \in A[X]$ ou A est un anneau factoriel. Monter que le polynôme sous-résultant non nul de plus petit degré est proportionnel au pgcd de f et g.