COURS 10

Pgcd, résultant, et approximants de Padé

Résumé

L'algorithme d'Euclide classique permet de calculer le pgcd et le pgcd étendu. Il est relié aux résultants qui permettent un calcul d'élimination. Les calculs efficaces de ces objets seront détaillés dans un cours ultérieur. Ils sont quasi-optimaux dans le cas univarié.

Les calculs de pgcd sont cruciaux pour la simplification des fractions, qu'il s'agisse de fractions d'entiers ou de fractions de polynômes. Les algorithmes efficaces de factorisation de polynômes reposent par ailleurs de manière essentielle sur le pgcd de polynômes. Comme pour la multiplication, les algorithmes efficaces de pgcd sont plus complexes dans le cas des entiers que dans le cas des polynômes à cause des retenues et nous ne détaillons que la version polynomiale. Dans les définitions et résultats de nature moins algorithmique, nous utilisons le cadre algébrique des anneaux euclidiens qui permet de traiter simultanément toutes les applications que nous avons en vue.

L'algorithme d'Euclide pour le calcul du pgcd est présenté en section 1. Dans le cas de polynômes de $\mathbb{K}[X]$, sa complexité est quadratique en nombre d'opérations dans le corps $\mathbb{K}$. Le résultant est également lié à l'algorithme d'Euclide, ses propriétés et son calcul sont présentés en section 2. En outre, une technique dite « des sous-résultants » permet de réduire l'explosion de la taille des coefficients intermédiaires dont souffre l'algorithme d'Euclide pour le pgcd dans $\mathbb{Q}[X]$. Le cours se termine en Section 3 sur un algorithme plus moderne, de complexité quasi-optimale, exploitant la multiplication rapide. Ces algorithmes, à base d'approximants de Padé, permettent aussi de calculer la *reconstruction rationnelle*, grâce à laquelle on peut retrouver une récurrence linéaire à coefficients constants d'ordre d à partir de $2d$ termes consécutifs d'une solution.

Dans ce cours, $\mathbb{A}$ désignera toujours un anneau intègre (commutatif et sans diviseurs de zéro) et unitaire.

1. Algorithme d'Euclide

1.1. Le pgcd. Des pgcd peuvent être définis dans tout anneau intègre $\mathbb{A}$: on appelle *plus grand diviseur commun* (pgcd) de A et B tout $G \in \mathbb{A}$ qui divise A et B et tel que tout diviseur de A et de B divise aussi G. Contrairement à l'usage, nous notons dans ce cours $\mathrm{pgcd}(A, B)$ tout pgcd de A et de B sans faire de choix de normalisation parmi les pgcd de A et de B.

L'algorithme d'Euclide présenté dans cette section permet le calcul du pgcd dans $\mathbb{Z}$ ou dans l'anneau $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps. Il repose sur l'existence d'une *division euclidienne* dans ces anneaux. Un anneau intègre $\mathbb{A}$ est appelé *anneau euclidien* s'il existe une fonction de taille $d : \mathbb{A} \to \mathbb{N} \cup \{-\infty\}$ telle que pour tout $a \in$

Euclide(A,B)
Entrée : A et B dans $\mathbb{A}$.
Sortie : Un pgcd de A et B.

1. $R_0 := A$; $R_1 := B$; $i := 1$.
2. Tant que R_i est non nul, faire :
   $R_{i+1} := R_{i-1} \bmod R_i$
   $i := i + 1$
3. Renvoyer R_{i-1}.

FIG. 1. L'algorithme d'Euclide

$\mathbb{A}$, $b \in \mathbb{A} \setminus \{0\}$, il existe q et r dans $\mathbb{A}$ avec

$$a = qb + r, \qquad d(r) < d(b).$$

En particulier, $d(0) < d(b)$ dès que b est non nul. Dans le cas des entiers, la valeur absolue fournit une telle fonction d, et le degré remplit ce rôle pour les polynômes. La notation $r := a \bmod b$ sert dans les deux cas à définir r à partir de a et de b. L'entier ou le polynôme r s'appelle *le reste*.

EXERCICE 1. Un élément d'un anneau est dit irréductible si les produits qui lui sont égaux font tous intervenir un élément inversible. Tout anneau euclidien est *factoriel* (c'est-à-dire que tout élément non nul y a une factorisation unique en irréductibles, à l'ordre près de la factorisation et à des multiplications près des facteurs par des inversibles de l'anneau). Le pgcd se lit aussi sur les factorisations. Si A et B se factorisent sous la forme

$$A = am_1^{k_1} \cdots m_s^{k_s}, \qquad B = bm_1^{\ell_1} \cdots m_s^{\ell_s},$$

où a et b sont inversibles dans $\mathbb{A}$, les m_i sont irréductibles et les k_i et ℓ_i sont des entiers positifs ou nuls, montrer qu'alors un pgcd de A et B est

$$G = m_1^{\min(k_1,\ell_1)} \cdots m_s^{\min(k_s,\ell_s)}.$$

Autrement dit, on « met » dans G les facteurs irréductibles communs de A et B, avec la plus grande multiplicité possible. La factorisation dans $\mathbb{Z}$ ou dans $\mathbb{K}[X]$ est plus coûteuse que le pgcd et cette propriété n'est donc pas utilisée pour le calcul du pgcd.

1.2. Calcul du pgcd. Étant donnés A, B dans un anneau euclidien $\mathbb{A}$, l'algorithme d'Euclide (Fig. 1) calcule une suite de restes successifs dont la taille décroît, jusqu'à atteindre le pgcd.

La terminaison provient de la décroissance stricte de la taille à chaque étape. La correction de cet algorithme se déduit de la relation

$$\operatorname{pgcd}(F, G) = \operatorname{pgcd}(H, G) \qquad \text{pour} \qquad H := F \bmod G,$$

dont la preuve est laissée en exercice. Par récurrence, il s'ensuit que $\operatorname{pgcd}(F, G) = \operatorname{pgcd}(R_i, R_{i+1})$ pour tout i. Si en outre R_{i+1} est nul, alors $\operatorname{pgcd}(R_i, R_{i+1}) = R_i$, ce qui prouve la correction.

EXEMPLE 1. Soient $A = X^4 - 13X^3 + 2X^2 - X - 1$ et $B = X^2 - X - 1$ dans $\mathbb{Q}[X]$. La suite des restes est :

$$\begin{aligned} R_0 &= X^4 - 13X^3 + 2X^2 - X - 1, \\ R_1 &= X^2 - X - 1, \\ R_2 &= -22X - 10, \\ R_3 &= -41/121, \\ R_4 &= 0, \end{aligned}$$

de sorte que $-41/121$ est un pgcd de A et B et donc 1 aussi.

PROPOSITION 1. *L'algorithme d'Euclide calcule un pgcd de A et B dans $\mathbb{K}[X]$ en $O(\deg A \deg B)$ opérations dans $\mathbb{K}$.*

DÉMONSTRATION. La correction a été prouvée dans le cas général. Pour l'étude de complexité, nous supposons d'abord que $\deg A \geq \deg B$. D'après le cours 3 (p. 1.1), le calcul de $P \bmod Q$ peut être effectué en $2 \deg Q(\deg P - \deg Q + 1)$ opérations de $\mathbb{K}$. Il s'ensuit que le coût de l'algorithme d'Euclide est borné par la somme des $2\deg(R_i)(\deg R_{i-1} - \deg R_i + 1)$, pour $i \geq 1$. Tous les $\deg(R_i)$ sont majorés par $\deg A$, de sorte que le coût est borné par $2 \deg A \sum_{i\geq 1}(\deg R_{i-1} - \deg R_i + 1) = 2 \deg A(\deg R_0 + \deg B) = O(\deg A \deg B)$.

Si le degré de B et supérieur à celui de A, la première étape ne coûte pas d'opération arithmétique, et la borne ci-dessus s'applique ensuite au reste du calcul. □

La borne de complexité quadratique reflète bien le comportement de l'algorithme : dans une exécution typique de l'algorithme, les quotients ont degré 1 à chaque itération, les degrés des restes successifs diminuent de 1 à chaque itération et leur calcul est linéaire ; le nombre de coefficients intermédiaires calculés est quadratique et ils sont calculés aussi efficacement qu'il est possible par un algorithme qui les calcule tous.

1.3. Pgcd étendu et inversion modulaire.

Relation de Bézout. Une relation de la forme $G = UA + VB$ qui donne le pgcd G de deux polynômes A et B avec deux cofacteurs polynomiaux U et V est appelée une *relation de Bézout*. L'algorithme d'Euclide étendu est une modification légère de l'algorithme d'Euclide qui calcule non seulement le pgcd, mais aussi une relation de Bézout particulière,

$$UA + VB = G, \quad \text{avec } d(UG) < d(B) \text{ et } d(VG) < d(A). \tag{1}$$

Une fois le pgcd G choisi, les cofacteurs U et V sont rendus uniques par la contrainte sur les degrés. Dans de nombreuses applications, c'est davantage de ces *cofacteurs* U et V que du pgcd lui-même dont on a besoin. On parle alors de calcul de pgcd *étendu*. Ce calcul intervient par exemple de manière importante dans les algorithmes de factorisation de polynômes dans $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$ par des techniques de type « Hensel » (cours 30), et dans le développement rapide des séries algébriques (cours 12).

Les calculs de pgcd étendu permettent d'effectuer des *inversions modulaires*. Lorsque A et B sont premiers entre eux ($G \in \mathbb{A}$), alors l'élément V est un inverse de B modulo A.

Exemple 2. La relation de Bézout pour $a+bX$ et $1+X^2$ s'écrit :

$$(a-bX)(a+bX)+b^2(1+X^2)=a^2+b^2.$$

L'inverse de $B=a+bX$ modulo $A=1+X^2$ vaut donc

$$V=\frac{a-bX}{a^2+b^2}.$$

Puisque le corps des complexes s'obtient par le quotient $\mathbb{R}[X]/(X^2+1)$, cette relation n'est autre que la formule d'inversion familière

$$\frac{1}{a+ib}=\frac{a-ib}{a^2+b^2}.$$

Si $A\in\mathbb{A}$ est irréductible, $\mathbb{A}/(A)$ est un corps et le calcul de la relation de Bézout permet d'y effectuer la division : si $B\neq 0 \mod A$ alors $N/B=NV \bmod A$.

Exemple 3. La « simplification » de la fraction rationnelle

$$r=\frac{\phi^4-\phi+1}{\phi^7-1}=\frac{25\phi-34}{169}$$

où ϕ est le « nombre d'or », défini par $A(\phi)=0$ pour $A(X)=X^2-X-1$, est obtenue par les trois calculs suivants :

- calcul du reste $U=13X+7$ par $U:=X^7-1 \bmod A$,
- détermination de la relation de Bézout

$$\frac{13X-20}{169}(13X+7)-A=1,$$

- calcul du reste $V=25X-34$ par $V:=(13X-20)(X^4-X+1) \bmod A$.

Plus généralement, dans le cas où $A\in\mathbb{K}[X]$ est un polynôme irréductible, ces calculs montrent que le corps $\mathbb{K}(\alpha)$ des fractions rationnelles en α racine de A est un espace vectoriel dont une base est $1,\alpha,\alpha^2,\dots,\alpha^{\deg A-1}$. Les algorithmes d'Euclide et d'Euclide étendu fournissent un moyen de calcul dans cette représentation. Il est ainsi possible de manipuler de manière exacte les racines d'un polynôme de degré arbitraire sans « résoudre ».

Exemple 4. Lorsque l'élément $A\in\mathbb{A}$ n'est pas irréductible, $\mathbb{A}/(A)$ n'est pas un corps. Cependant, les éléments inversibles peuvent y être inversés par le même calcul que ci-dessus. Lorsqu'un élément B non nul n'est pas inversible, la relation de Bézout se produit avec un G différent de 1. Il est alors possible de tirer parti de cette information (un facteur de A) en scindant le calcul d'une part sur G et d'autre part sur B/G.

Exemple 5. Le même calcul qu'à l'exemple 3 fonctionne sur des entiers :

$$r=\frac{25}{33}\equiv 5 \bmod 7$$

se déduit de

$$33 \bmod 7=5,\qquad 3\times 5-2\times 7=1,\qquad 3\times 25 \bmod 7=5.$$

Euclide étendu(A,B)

Entrée : A et B dans $\mathbb{A}$.
Sortie : Un pgcd de A et B et les cofacteurs U et V de l'identité de Bézout $UA + VB = G$.

1. $R_0 := A$; $U_0 := 1$; $V_0 := 0$; $R_1 := B$; $U_1 := 0$; $V_1 := 1$; $i := 1$.
2. Tant que R_i est non nul, faire :
   $R_{i+1} := QR_i + R_{i-1}$ la division euclidienne ;
   $U_{i+1} := U_{i-1} - QU_i$; $V_{i+1} := V_{i-1} - QV_i$;
   $i := i + 1$
3. Renvoyer $R_{i-1}, U_{i-1}, V_{i-1}$.

FIG. 2. L'algorithme d'Euclide étendu

Calcul des cofacteurs. L'idée-clé est de suivre pendant l'algorithme d'Euclide la décomposition de chacun des R_i sur A et B. Autrement dit, pour tout i, l'algorithme calcule des éléments U_i et V_i tels que

$$U_iA + V_iB = R_i,$$

dont les tailles sont bien contrôlées. Pour $i = 0$, il suffit de poser $U_0 = 1, V_0 = 0$, ce qui correspond à l'égalité

$$1 \cdot A + 0 \cdot B = A = R_0.$$

Pour $i = 1$, l'égalité

$$0 \cdot A + 1 \cdot B = B = R_1$$

est obtenue avec $U_1 = 0, V_1 = 1$. Ensuite, la division euclidienne

$$R_{i-1} = QR_i + R_{i+1}$$

donne la relation

$$R_{i+1} = R_{i-1} - QR_i = (U_{i-1} - QU_i)A + (V_{i-1} - QV_i)$$

qui pousse à définir U_{i+1} par $U_{i-1} - QU_i$ et V_{i+1} par $V_{i-1} - QV_i$, et à partir de laquelle une preuve par récurrence montre que les conditions de tailles de la relation de Bézout sont satisfaites.

L'algorithme est résumé en Figure 2. À nouveau, dans le cas des polynômes ou des entiers, la complexité est quadratique.

2. Résultant

2.1. Matrice de Sylvester. L'algorithme d'Euclide pour *deux* polynômes A, B à *une* variable est étroitement relié à la matrice de Sylvester. Si

$$A = a_mX^m + \cdots + a_0, \quad B = b_nX^n + \cdots + b_0,$$

appartiennent à $\mathbb{A}[X]$, cette matrice carrée s'écrit

$$\mathsf{Syl}(A,B) = \begin{pmatrix} a_m & a_{m-1} & \dots & a_0 & & \\ & a_m & a_{m-1} & \dots & a_0 & \\ & & \dots & \dots & & \\ & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & & \\ & b_n & b_{n-1} & \dots & b_0 & \\ & & \dots & \dots & & \\ & & b_n & b_{n-1} & \dots & b_0 \end{pmatrix}$$

avec les n premières lignes contenant les coefficients de A et les m suivantes contenant les coefficients de B.

La transposée de cette matrice représente l'application linéaire

$$(U,V) \mapsto AU + BV,$$

en se limitant aux paires (U,V) tels que $\deg U < \deg B$ et $\deg V < \deg A$, et en utilisant la base des monômes $1, X, \dots, X^{m+n-1}$ à l'arrivée. Les combinaisons linéaires des lignes de la matrice de Sylvester donnent donc les coefficients des polynômes qui peuvent être obtenus comme image. Au vu de la relation de Bézout (1), le pgcd de A et B peut être obtenu ainsi et il est caractérisé comme l'élément de plus petit degré qui peut l'être. Ceci permet de le lire sur une forme *échelonnée en ligne* de la matrice.

Definition 1. Une matrice est en forme *échelonnée en ligne* lorsque

1. les lignes nulles sont toutes en dessous des lignes non nulles,
2. le premier coefficient non nul de chaque ligne non nulle est à droite du premier coefficient non nul de la ligne précédente, les coefficients des lignes suivantes dans sa colonne étant nuls.

L'algorithme classique d'élimination de Gauss sans pivot sur les colonnes calcule une forme échelonnée en ligne d'une matrice, dont les lignes non nulles sont une base de l'espace vectoriel engendré par les lignes de la matrice de départ. En conclusion, nous avons obtenu une relation entre la matrice de Sylvester et le pgcd.

Proposition 2. *Soient A, B deux polynômes de $\mathbb{K}[X]$. Alors la forme échelonnée en ligne de la matrice de Sylvester $\mathsf{Syl}(A,B)$ contient sur sa dernière ligne non nulle les coefficients d'un pgcd de A et B. En outre, la dimension du noyau de cette matrice est le degré du pgcd.*

Exemple 6. Pour les polynômes $A = X^4 - X^3 - 7X^2 + 2X + 3$ et $B = X^3 - 4X^2 + 2X + 3$, la matrice de Sylvester et sa forme échelonnée en ligne sont :

$$\begin{pmatrix} 1 & -1 & -7 & 2 & 3 & 0 & 0 \\ 0 & 1 & -1 & -7 & 2 & 3 & 0 \\ 0 & 0 & 1 & -1 & -7 & 2 & 3 \\ 1 & -4 & 2 & 3 & 0 & 0 & 0 \\ 0 & 1 & -4 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & -4 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 & -4 & 2 & 3 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & -1 & -7 & 2 & 3 & 0 & 0 \\ 0 & 1 & -1 & -7 & 2 & 3 & 0 \\ 0 & 0 & 1 & -1 & -7 & 2 & 3 \\ 0 & 0 & 0 & -14 & 45 & -3 & -18 \\ 0 & 0 & 0 & 0 & -\frac{5}{7} & \frac{12}{7} & \frac{9}{7} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & -\frac{3}{10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

La dernière ligne non nulle donne le pgcd $X - 3$.

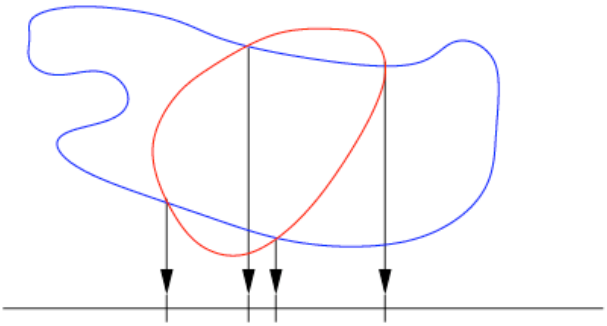

FIG. 3. Le résultant calcule des projections

DEFINITION 2. Le *résultant* de A et B est le déterminant de la matrice de Sylvester $\mathsf{Syl}(A, B)$. Il est noté $\mathrm{Res}(A, B)$ ou $\mathrm{Res}_X(A, B)$ si l'on veut insister sur l'élimination de la variable X.

Le résultant peut être vu comme une condition de cohérence pour le système formé par les deux polynômes A et B.

COROLLAIRE 1. *Soient A et B deux polynômes de $\mathbb{K}[X]$. Alors A et B sont premiers entre eux si et seulement si* $\mathrm{Res}(A, B) \neq 0$.

DÉMONSTRATION. Le déterminant d'une matrice carrée se lit sur la forme échelonnée en ligne en faisant le produit des éléments diagonaux. Il est non nul si et seulement si tous les éléments diagonaux le sont et dans ce cas un pgcd non nul est sur la dernière ligne. À l'inverse, s'il existe un pgcd G non nul, alors les polynômes $X^k G$ montrent l'existence de lignes avec un coefficient de tête non nul dans chaque colonne de la forme échelonnée. □

EXEMPLE 7. Le discriminant de A est par définition le résultant de A et sa dérivée A'. Il s'annule lorsque ces deux polynômes ont une racine commune dans une clôture algébrique de A, c'est-à-dire, en caractéristique nulle, lorsque A a une racine multiple.

EXERCICE 2. Calculer le discriminant de aX^2+bX+c en prenant le déterminant de la matrice de Sylvester.

2.2. Applications du résultant.

Calculs de projections. Algébriquement, la « résolution » d'un système polynomial se ramène souvent à une question d'*élimination*. Lorsqu'elle est possible, l'élimination successive des variables amène le système d'entrée sous une forme triangulaire. De proche en proche, la résolution d'un tel système se réduit alors à la manipulation de polynômes à une variable, pour lesquels compter, isoler, ... , les solutions est bien plus facile.

Géométriquement, l'élimination correspond à une projection. Cette section montre comment le résultant de deux polynômes permet de traiter ce genre de problèmes, pour les systèmes de deux équations en deux inconnues. Le schéma général est représenté en Figure 3. Cette opération est à la base d'une technique

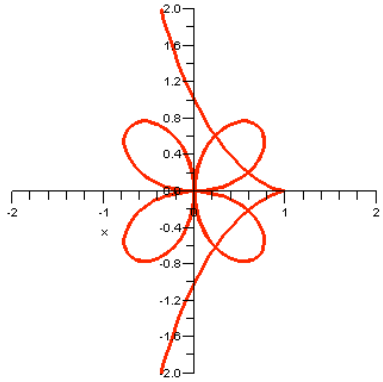

FIG. 4.

plus générale pour un nombre arbitraire d'équations et d'inconnues, la *résolution géométrique*, qui sera présentée au cours 20.

EXEMPLE 8. Les deux courbes de la Figure 4 ont pour équations

$$A = (X^2+Y^2)^3 - 4X^2Y^2 = 0, \qquad B = X^2(1+Y) - (1-Y)^3 = 0.$$

Ces deux polynômes sont irréductibles et leur pgcd qui vaut 1 ne renseigne pas sur leurs racines communes. Les résultants par rapport à X et Y donnent en revanche des polynômes qui s'annulent sur les coordonnées de ces points d'intersection :

$$\mathrm{Res}_X(A,B) = (4Y^7 + 60Y^6 - 152Y^5 + 164Y^4 - 95Y^3 + 35Y^2 - 9Y + 1)^2,$$
$$\mathrm{Res}_Y(A,B) = 16X^{14} + 6032X^{12} - 1624X^{10} + 4192X^8 - 815X^6 - 301X^4 - 9X^2 + 1.$$

Il n'y a que 4 points d'intersection visibles sur la figure, les 10 autres ont au moins une coordonnée qui n'est pas réelle. Le caractère bicarré du résultant en Y provient de la symétrie de la figure par rapport à l'axe des Y. C'est pour cette même raison que le premier résultant est un carré.

Le résultat général est le suivant.

PROPOSITION 3. *Soit $A = a_m Y^m + \cdots$ et $B = b_n Y^n + \cdots$ où les coefficients a_i et b_j sont dans $\mathbb{K}[X]$. Alors les racines du polynôme $\mathrm{Res}_Y(A,B) \in \mathbb{K}[X]$ sont d'une part les abscisses des solutions du système $A = B = 0$, d'autre part les racines communes de a_m et b_n.*

DÉMONSTRATION. Ce résultat est une conséquence immédiate du théorème 1 de la section 2.3 ci-dessous. □

Graphiquement, les racines « dégénérées » du second cas se traduisent par la présence d'asymptotes verticales.

EXEMPLE 9. Avec $A = X^2Y + X + 1$, $B = XY - 1$, on obtient $\mathrm{Res}_Y(A,B) = -X(2X+1)$ (asymptote en $X = 0$, « vraie » solution en $X = -\frac{1}{2}$). Les courbes correspondantes sont représentées en Figure 5.

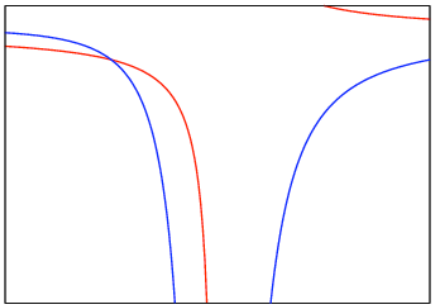

FIG. 5.

Une fois calculé le résultant donnant les coordonnées des abscisses des intersections des deux courbes, il est souhaitable d'obtenir les ordonnées correspondantes. Dans le cas simple où l'avant dernier reste de l'algorithme d'Euclide est de degré 1, il donne une telle paramétrisation.

EXEMPLE 10. Sur les deux polynômes A et B de l'exemple 8, vus comme polynômes dans $\mathbb{Q}(X)[Y]$, la suite des restes est

$$(X^4 - 13X^2 + 15)Y^2 - 4(X^2+2)(X^2+3)Y + (X^6 - 2X^4 - 8X^2 + 10),$$
$$(4X^8 - 344X^6 - 1243X^4 - 301X^2 - 21)Y + (84X^8 - 372X^6 + 169X^4 + 143X^2 + 15),$$
$$1.$$

Un calcul de pgcd du coefficient de Y dans l'avant dernier reste avec $\mathrm{Res}_Y(A,B)$ montre que ces deux polynômes sont premiers entre eux. Pour chaque racine X de $\mathrm{Res}_Y(A,B)$ il y a donc un unique point d'intersection aux deux courbes, d'ordonnée donnée par

$$Y = -\frac{84X^8 - 372X^6 + 169X^4 + 143X^2 + 15}{4X^8 - 344X^6 - 1243X^4 - 301X^2 - 21}.$$

En utilisant un calcul de pgcd étendu, ceci peut être récrit comme expliqué plus haut en un polynôme de degré au plus 13 en X.

Le même calcul sur A et B vus comme polynômes dans $\mathbb{Q}(Y)[X]$ donne B comme dernier reste avant le pgcd. Ceci correspond aux deux points ayant la même projection sur l'axe des Y.

Implicitation. Une autre application géométrique du résultant est l'*implicitation* de courbes du plan. Étant donnée une courbe paramétrée

$$X = A(T), \quad Y = B(T), \qquad A, B \in \mathbb{K}(T),$$

il s'agit de calculer un polynôme non trivial en X et Y qui s'annule sur la courbe. Il suffit pour cela de prendre le résultant en T du numérateur de $X - A(T)$ et $Y - B(T)$.

EXEMPLE 11. La courbe « en fleur » de la Figure 4 peut aussi être donnée sous la forme

$$X = \frac{4t(1-t^2)^2}{(1+t^2)^3}, \quad Y = \frac{8t^2(1-t^2)}{(1+t^2)^3}.$$

Il suffit d'effectuer le calcul du résultant

$$\mathrm{Res}_t((1+t^2)^3X - 4t(1-t^2)^2, (1+t^2)^3Y - 8t^2(1-t^2))$$

pour retrouver (à un facteur constant près) le polynôme A de l'exemple 8.

2.3. Propriétés. L'essentiel des propriétés du résultant est contenu dans le théorème suivant.

THÉORÈME 1. *Si les polynômes A et B de $\mathbb{A}[X]$ s'écrivent*

$$A = a(X-\alpha_1)\cdots(X-\alpha_m), \quad B = b(X-\beta_1)\cdots(X-\beta_n),$$

alors, le résultant de A et B vaut

$$\mathrm{Res}(A,B) = a^n b^m \prod_{i,j}(\alpha_i - \beta_j) = (-1)^{mn} b^m \prod_{1\le i\le n} A(\beta_i) = a^n \prod_{1\le i\le m} B(\alpha_i) = (-1)^{mn}\,\mathrm{Res}(B,A).$$

DÉMONSTRATION. Il suffit de prouver la première égalité. Les deux suivantes en sont des conséquences immédiates.

Le facteur $a^n b^m$ est une conséquence de la multilinéarité du déterminant. Nous considérons maintenant le cas où $a = b = 1$. Il est commode de considérer le cas générique où les α_i et β_j sont des indéterminées et où l'anneau $\mathbb{A}$ est $\mathbb{Z}[\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n]$. Si le résultat est vrai dans cet anneau, il l'est aussi pour des valeurs arbitraires des α_i et β_j. Le corollaire 1 dans $\mathbb{Q}(\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n)$ montre que le produit des $\alpha_i - \beta_j$ divise le résultant. Par ailleurs, le degré en α_i de chacune des n premières lignes de la matrice de Sylvester est 1 et ce degré est nul pour les m autres lignes. Ceci donne une borne n pour le degré en chaque α_i du résultant et de la même manière une borne m pour son degré en chaque β_j. Il s'ensuit que le résultant est égal au produit des $\alpha_i - \beta_j$ à un facteur constant près. Ce facteur est indépendant des α_i et β_j. En choisissant $\beta_1 = \cdots = \beta_n = 0$, c'est-à-dire $B = X^n$, et en développant le déterminant par rapport à ses m dernières lignes, on obtient que le résultant vaut $(-1)^{mn}A(0)^n$, ce qui donne le facteur 1 et conclut la preuve. □

COROLLAIRE 2 (Multiplicativité du résultant). *Pour tous polynômes A, B, C de $\mathbb{A}[X]$,* $\mathrm{Res}(AB,C) = \mathrm{Res}(A,C)\,\mathrm{Res}(B,C)$.

DÉMONSTRATION. L'anneau $\mathbb{A}$ est intègre, il possède donc un corps de fraction qui a lui-même une clôture algébrique dans laquelle les polynômes A, B et C peuvent s'écrire sous la forme utilisée dans le théorème précédent. L'identité sur les résultants (qui appartiennent à $\mathbb{A}$ par définition) est alors vérifiée en considérant les produits deux à deux de racines. □

Une dernière propriété utile du résultant est la suivante.

PROPOSITION 4. *Il existe U et V dans $\mathbb{A}[X]$ tels que le résultant s'écrive $S = UA + VB$.*

DÉMONSTRATION. En ajoutant à la dernière colonne de la matrice de Sylvester le produit des colonnes précédentes par des puissances adaptées de X, on fait apparaître dans la dernière colonne les polynômes A et B, sans avoir changé le déterminant. Le développement du déterminant par rapport à la dernière colonne permet alors de conclure. □

L'algorithme d'Euclide étendu montre que S (qui est un multiple par un élément du corps des fractions $\mathbb{K}$ de l'un des restes euclidiens « standards »), peut s'écrire comme une combinaison polynomiale de A et B, à coefficients dans $\mathbb{K}[X]$. Cette proposition montre que cette combinaison se fait « sans division », c'est-à-dire avec des coefficients dans $\mathbb{A}[X]$.

2.4. Calcul avec des nombres algébriques. L'idée que les polynômes sont des bonnes structures de données pour représenter leur racines amène à chercher des algorithmes pour effectuer les opérations de base sur ces racines, comme la somme ou le produit. Le résultant répond à cette attente.

PROPOSITION 5. *Soient $A = \prod_i (X - \alpha_i)$ et $B = \prod_j (X - \beta_j)$ des polynômes de $\mathbb{K}[X]$. Alors*

$$\begin{aligned}
\mathrm{Res}_X(A(X), B(T - X)) &= \prod_{i,j} (T - (\alpha_i + \beta_j)),\\
\mathrm{Res}_X(A(X), B(T + X)) &= \prod_{i,j} (T - (\beta_j - \alpha_i)),\\
\mathrm{Res}_X(A(X), X^{\deg B} B(T/X)) &= \prod_{i,j} (T - \alpha_i \beta_j),\\
\mathrm{Res}_X(A(X), T - B(X)) &= \prod_{i} (T - G(f_i)).
\end{aligned}$$

DÉMONSTRATION. C'est une application directe du Théorème 1. □

EXEMPLE 12. On sait que $\sqrt{2}$ est racine de $X^2 - 2$, tout comme $\sqrt{3}$ est racine de $X^2 - 3$. Un polynôme de degré minimal ayant pour racine $\sqrt{2} + \sqrt{3}$ est donné par

$$\mathrm{Res}_X(X^2 - 2, (T - X)^2 - 3) = T^4 - 10T^2 + 1.$$

Ces opérations ne distinguent pas les racines de A et B, les quatre racines du résultant sont donc $\pm\sqrt{2} \pm \sqrt{3}$.

Calcul du résultant bivarié. On dispose à l'heure actuelle d'un algorithme rapide (quasi-optimal) pour le calcul du résultant univarié. Le meilleur algorithme connu actuellement pour le calcul du résultant bivarié est une méthode d'évaluation-interpolation qui se ramène au résultant univarié. Cet algorithme n'est pas quasi-optimal. En revanche, pour les trois premières opérations de la Proposition 5, des algorithmes quasi-optimaux à base de multiplication rapide de séries existent, ils ont été présentés dans le cours 3.

2.5. ⋆ Sous-résultants ⋆.

La croissance des coefficients dans l'algorithme d'Euclide. Le nombre d'opérations dans le corps des coefficients n'est pas une mesure suffisante de la complexité des calculs lorsque les opérations elles-mêmes ont une complexité variable. C'est le cas pour le calcul de pgcd dans $\mathbb{Q}[X]$ et dans $\mathbb{K}(Y)[X]$. Dans ces corps de coefficients, on constate empiriquement les phénomènes suivants :

– l'algorithme d'Euclide amène à faire des divisions, et introduit des dénominateurs au cours du calcul ;

– la taille des coefficients croît rapidement ;
– ces coefficients peuvent souvent se « simplifier ».

EXEMPLE 13. L'exécution de l'algorithme d'Euclide sur

$$A = 115X^5 + 7X^4 + 117X^3 + 30X^2 + 87X + 44,$$
$$B = 91X^4 + 155X^3 + 3X^2 + 143X + 115.$$

produit les restes successifs suivants :

$$\frac{3601622}{8281}X^3 - \frac{1196501}{8281}X^2 + \frac{151912}{637}X + \frac{2340984}{8281}$$
$$\frac{189886027626841}{12971681030884}X^2 - \frac{57448278681703}{3242920257721}X - \frac{17501090665331}{3242920257721}$$
$$\frac{3748556212578804983806085060}{435414847094570987735 1001}X + \frac{1418333609151239693280148 92}{33493449776505460595007 7}.$$

En simplifiant ces restes par des multiplications par des constantes bien choisies, on obtient les restes :

$$3601622X^3 - 1196501X^2 + 1974856X + 2340984,$$
$$22930325761X^2 - 27749440252X - 8453612204,$$
$$288979986761465X + 142143002707719.$$

Il est souhaitable d'éviter le calcul sur les rationnels ou les fractions rationnelles pour lequel l'addition requiert des calculs de multiplications et éventuellement de pgcd. Une première idée consiste alors à éviter totalement les divisions en utilisant des *pseudo-restes*.

DEFINITION 3. Si A et B sont des polynômes de $\mathbb{A}[X]$ et b est le coefficient de tête de B, le *pseudo-reste* $\overline{R}$ de A et B est défini par

$$b^{\deg A - \deg B + 1} A = \overline{Q}B + \overline{R}.$$

Remplacer les calculs de restes de l'algorithme d'Euclide par des calculs de pseudo-restes évite d'introduire des dénominateurs. Cette idée seule n'est pas suffisante : les coefficients de ces pseudo-restes croissent trop.

EXEMPLE 14. Sur le même exemple, la modification de l'algorithme d'Euclide produit la suite de pseudo-restes

$$3601622X^3 - 1196501X^2 + 1974856X + 2340984,$$
$$189886027626841X^2 - 229793114726812X - 70004362661324,$$
$$257057096083899261191107914552182660X$$
$$+126440823512296156588839626542149756.$$

Une possibilité pour éviter cette croissance est de diviser ces polynômes par le pgcd de leurs coefficients à chaque étape. C'est ce que nous avons fait dans l'exemple ci-dessus. On parle alors de suite de pseudo-restes primitifs. Cependant, ces calculs de pgcd de coefficients sont trop coûteux.

L'algorithme des sous-résultants donné en Figure 6 est une modification de l'algorithme d'Euclide qui évite les divisions, tout en *prévoyant* des facteurs communs qui apparaissent dans les coefficients de la suite des pseudo-restes de sorte à limiter leur croissance. Ces pseudo-restes sont appelés des sous-résultants. Dans cet algorithme, on se contente de renvoyer le dernier sous-résultant non nul ; on conçoit

Sous-résultants(A,B)
Entrée : A et B dans $\mathbb{A}[X]$ avec $\deg B < \deg A$.
Sortie : Le dernier sous-résultant non nul.

1. $f = g = s = 1$
2. Tant que $\deg B > 0$
   (a) $d = \deg A - \deg B$
   (b) $R =$pseudoReste(A, B)
   (c) Si les degrés de A et B sont impairs, faire $s = -s$.
   (d) Faire $A := B$ et mettre dans B le quotient de la division de R par fg^d
   (e) Prendre $f :=$coefficientDominant(A)
   (f) Mettre à jour g en lui affectant le quotient de la division de f^d par g^{d-1}
3. $d = \deg A$;
4. Renvoyer le quotient de la division de sB^d par g^{d-1}.

FIG. 6.

aisément comment modifier l'algorithme pour obtenir *n'importe* quel sous-résultant (spécifié par des conditions de degré, par exemple).

EXEMPLE 15. Toujours sur les même polynômes, la suite des sous-résultants redonne les polynômes que nous avions déjà calculés par simplification :

$$3601622X^3 - 1196501X^2 + 1974856X + 2340984,$$
$$22930325761X^2 - 27749440252X - 8453612204,$$
$$288979986761465X + 142143002707719.$$

La suite des sous-résultant de cet exemple est donc primitive : les facteurs prédits par l'algorithme du sous-résultant ont suffi à éliminer tout facteur commun entre les coefficients des pseudo-restes.

Comme le résultant, les sous-résultants sont liés à la matrice de Sylvester et à l'algorithme d'Euclide. Une formule de Cramer sur une sous-matrice de la matrice de Sylvester donne le résultat suivant.

PROPOSITION 6. *Toutes les divisions effectuées au cours de l'algorithme des sous-résultants sont exactes.*

La preuve de ce résultat est technique et omise ici.

En corollaire, on remarque en outre qu'il est assez facile de déduire de ce résultat des estimations sur la « taille » des coefficients qui apparaissent au cours de l'algorithme. Un cas particulier intéressant est celui où $\mathbb{A}$ est l'anneau de polynômes $\mathbb{K}[Y]$. Alors, si A et B ont des degrés totaux m et n, tous les sous-résultants ont des degrés bornés par mn. Ces bornes permettent un calcul du résultant par évaluation-interpolation dès que l'on dispose d'un algorithme efficace dans le cas univarié.

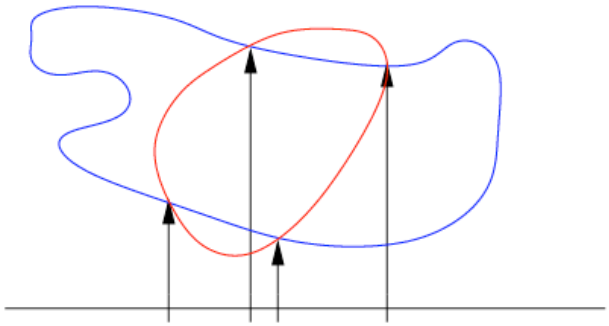

FIG. 7.

Calcul de la paramétrisation. Les sous-résultants permettent de finir la « résolution » des systèmes de deux polynômes bivariés. Pour simplifier, nous faisons l'hypothèse que pour tout x racine du résultant $R = \mathrm{Res}_Y(A, B)$, il n'y a qu'un seul y tel que $A(x, y) = B(x, y) = 0$. Dans ce cas, on peut montrer que le sous-résultant S_1 (de degré 1 en Y) est non nul ; écrivons-le sous la forme $S_1 = P_0(X)Y + Q_0(X)$. Comme pour le résultant, il existe des polynômes U et V dans $\mathbb{K}[X, Y]$ tels qu'on ait l'égalité

$$AU + BV = P_0(X)Y + Q_0(X).$$

On en déduit donc que toutes les solutions (x, y) du système $A = B = 0$ satisfont l'équation $P_0(x)y = Q_0$. Autrement dit, en écartant les solutions dégénérées où $P_0(x) = 0$, on obtient l'ordonnée des points solutions en évaluant la fraction rationnelle $-Q_0/P_0$ sur les racines du résultant R. Autrement dit, cette procédure permet de décrire les solutions du système sous la forme

$$\begin{cases} y = Q(x) \\ R(x) = 0 \end{cases}$$

Géométriquement, ce polynôme Q permet de retrouver y à partir de x, il permet donc d'effectuer l'opération symbolisée sur la Figure 7, la paramétrisation des solutions du système par les racines de R.

EXEMPLE 16. Sur les mêmes polynômes qu'à l'exemple 8, le sous-résultant redonne la paramétrisation calculée à partir de l'algorithme d'Euclide, mais en étant plus économe dans les opérations sur les coefficients.

3. Approximants de Padé-Hermite et algorithmes efficaces

3.1. Définitions.

DEFINITION 4. Un approximant de Padé de type (m, n) d'une série $S \in \mathbb{K}[[X]]$ est une fraction rationnelle $R \in \mathbb{K}(X)$ dont le numérateur a degré borné par m le dénominateur a degré borné par n et telle que

$$R - S = O(X^{m+n+1}).$$

DEFINITION 5. Un approximant de Padé-Hermite de type $m_1, \ldots, m_k$ d'un k-uplet de séries $S_1, \ldots, S_k$ de $\mathbb{K}(X)$ est un k-uplet de polynômes $p_1, \ldots, p_k$ de $\mathbb{K}[X]$ tels que $\deg p_i \leq m_i$, $i = 1, \ldots, k$ et

$$p_1 S_1 + \cdots + p_k S_k = O(X^{m_1+\cdots+m_k+k-1}).$$

Les approximants de Padé sont obtenus comme cas particulier des approximants de Padé-Hermite en prenant le couple de séries $(1, S)$.

3.2. Applications.

Reconstruction rationnelle. Si la série S provient du développement d'une fraction rationnelle P/Q, alors le calcul d'approximant de Padé à partir de suffisamment de termes de la série reconstruit cette fraction. En effet, si A/B est un approximant de type $(\deg P, \deg Q)$, l'identité

$$\frac{A}{B} = S + O(X^{\deg P+\deg Q+1}) = \frac{P}{Q} + O(X^{\deg P+\deg Q+1})$$

entraîne

$$AQ = BP + O(X^{\deg P+\deg Q+1}).$$

Le degré des polynômes intervenant dans cette égalité est borné par $\deg P + \deg Q$. Il s'ensuit que cette identité de séries est une identité de polynômes :

$$AQ = BP.$$

Les applications de cette propriété sont nombreuses : pour la résolution de systèmes différentiels à coefficients constants (cours 8), pour reconnaître une suite récurrente linéaire à partir de ses premiers termes, pour le calcul de polynômes minimaux de matrices creuses par l'algorithme de Wiedemann (cours 27), pour la résolution de systèmes linéaires à coefficients polynomiaux (cours 28), pour le décodage des codes BCH en théorie des codes, etc.

Pgcd. Si A et B sont des polynômes de $\mathbb{K}[X]$ de degrés m et n, il existe un approximant de Padé non nul de A/B type $(n-1, m-1)$ si et seulement si A et B ont un pgcd non trivial. Dans ce cas, l'élément de degré minimal de la base renvoyée par l'algorithme du Théorème 2 fournit deux polynômes U et V tels que

$$UA + VB = 0,$$

où l'égalité à 0 provient à nouveau de considérations de degré.

Il s'ensuit que

$$\frac{A}{B} = -\frac{V}{U}$$

et par conséquent le pgcd vaut $A/V = B/U$.

Pgcd étendu. Une fois trouvé le pgcd, l'identité de Bézout

$$UA + VB - G = 0$$

s'obtient par un approximant de Padé-Hermite de type $(n-1, m-1, 0)$ de (A, B, G), à nouveau dans la même complexité.

À l'inverse, il est possible de calculer des approximants de Padé à partir de l'algorithme d'Euclide étendu.

PROPOSITION 7. *Soit R_i la suite des restes associés à X^n et $\overline{F} = F \mod X^n$. Soit i le premier indice tel que $\deg R_i \leq m-1$, et A_i, B_i les cofacteurs correspondant :*

$$A_i X^n + B_i \overline{F} = R_i.$$

Il existe une solution au problème de Padé $(m, n-m)$ *si et seulement si* $\mathrm{pgcd}(R_i, B_i) = 1$. *Si c'est le cas, tous les approximants* $(m, n-m)$ *sont proportionnels au couple* (R_i, B_i).

3.3. Calcul. Le problème du calcul d'approximants de Padé-Hermite est un problème d'algèbre linéaire : les coefficients de $1, X, X^2, \ldots, X^{m_1+\cdots+m_k+k-2}$ fournissent un système linéaire (homogène) en les coefficients de $p_1, \ldots, p_k$ — c'est d'ailleurs cette réécriture qui sous-tend le choix de l'ordre de troncature : il y a autant d'équations que d'inconnues (à la constante d'homogénéité près : $p_1, \ldots, p_k$ ne peuvent être déterminés qu'à une constante près).

Davantage que de savoir si le problème a une solution, la question est donc plutôt ici de trouver cette solution rapidement : on veut faire mieux que la résolution brutale d'un système linéaire.

Il se trouve que l'on dispose d'un algorithme quasi-optimal, dont l'efficacité est utilisée dans ce cours comme la base de nombreux algorithmes efficaces. La constante dans le $O(\cdot)$ peut être améliorée dans le cas du pgcd et du pgcd étendu, mais il est plus simple pédagogiquement de se reposer sur une seule construction.

THÉORÈME 2. *Soit* $N = m_1 + \cdots + m_k + k - 1$. *Il est possible de calculer une base des approximants de Padé-Hermite sur* $\mathbb{K}[X]$ *en* $O(k^\omega \mathsf{M}(N))$ *opérations dans* $\mathbb{K}$.

L'algorithme repose sur un diviser pour régner assez subtil.

En corollaire, on obtient des algorithmes quasi-optimaux pour le calcul de pgcd et de pgcd étendus de polynômes.

Notes

Pour le résultant de deux polynômes (et les sous-résultants), on peut consulter [**7**, **1**, **2**] ou [**3**] pour une approche un peu plus complète. De nombreuses propriétés des résultants et de l'algorithme d'Euclide sont établies de manière élémentaire à l'aide des fonctions symétriques dans [**4**].

Le pgcd et le pgcd étendu peuvent aussi être définis dans un contexte non-commutatif. Ils sont alors utiles au calcul avec des opérateurs différentiels ou de récurrence. Cette généralisation sera présentée au cours 24.

Bibliographie

[1] Geddes (Keith O.), Czapor (Stephen R.), and Labahn (George). – *Algorithms for Computer Algebra*. – Kluwer Academic Publishers, 1992.

[2] Knuth (Donald E.). – *The Art of Computer Programming*. – Addison-Wesley Publishing Co., Reading, Mass., 1997, 3rd edition, *Computer Science and Information Processing*, vol. 2 : Seminumerical Algorithms, xiv+762p.

[3] Lang (Serge). – *Algebra*. – Springer-Verlag, New York, 2002, third edition, *Graduate Texts in Mathematics*, vol. 211, xvi+914p.

[4] Lascoux (Alain). – *Symmetric functions and combinatorial operators on polynomials*. – Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2003, *CBMS Regional Conference Series in Mathematics*, vol. 99, xii+268p.

[5] Pan (V. Y.) and Wang (X.). – Acceleration of Euclidean algorithm and extensions. In Mora (Teo) (editor), *ISSAC'2002*. pp. 207–213. – ACM, New York, 2002. Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, July 07–10, 2002, Université de Lille, France.

[6] Stehlé (D.) and Zimmermann (P.). – A binary recursive Gcd algorithm. In *ANTS-VI. Lecture Notes in Computer Science*, vol. 3076, pp. 411–425. – Springer, 2004.

[7] von zur Gathen (Joachim) and Gerhard (Jürgen). – *Modern computer algebra*. – Cambridge University Press, New York, 2003, 2nd edition, xiv+785p.

[8] Yap (Chee). – *Fundamental Problems in Algorithmic Algebra*. – Oxford University Press, 2000.