

LA RESULTANTE DE DEUX POLYNOMES

Alain LASCOUX

Résumé - Après avoir rétabli l'équation résultante de deux polynômes dans son sexe originel, nous montrons que la théorie des fonctions symétriques fournit sans calcul de nombreuses expressions déterminantales de la dite résultante, et plus généralement, du plus grand commun diviseur.

La résultante de deux polynômes a été l'objet de maintes recherches depuis le 18ème siècle, étant au coeur de la théorie de l'élimination. On la trouvait développée dans tous les livres d'algèbre du siècle dernier. De nos jours, sa part s'est malheureusement réduite à une expression déterminantale attribuée à Sylvester. Voilà sans doute qui explique la redécouverte périodique de certaines de ses propriétés [cf. Gerber, Householder]. Nous puiserons la majorité de nos références dans les cinq livres de [Muir] qui résument la majorité des formules déterminantales de la littérature (mathématique) jusqu'en 1920.

1. SYMETRIE -

La définition de la résultante de deux polynômes remonte à Euler et Bezout, si ce n'est plus tôt. Supposant les polynômes P et Q totalement factorisés, i.e. $P = \prod_{a \in A} (x-a)$ et $Q = \prod_{b \in B} (x-b)$, A et B étant les deux ensembles de racines, alors par définition

$$(1,1) \quad R(A,B) = \prod_{a \in A, b \in B} (a-b)$$

est la résultante et tout polynôme en les $a \in A$ et les $b \in B$ qui s'annule quand P et Q ont une racine commune est divisible par $R(A,B)$.

Bien entendu, on ne va pas chercher les racines des deux polynômes - problème dont [Ruffini], puis Galois ont montré la difficulté algébrique ; c'est la symétrie en les $a \in A$, ainsi qu'en les $b \in B$ qui fournit la méthode la plus directe d'évaluer la résultante. Nous avons donc besoin de quelques définitions relatives aux fonctions symétriques [Macdonald].

Soit M une matrice, k un entier positif, $I = (i_1, \dots, i_k) \in \mathbb{Z}^k$, $J \in \mathbb{Z}^k$. On note $M_{I,J}$ le mineur pris sur les lignes $i_1 + 1, \dots, i_k + k$ et les colonnes $j_1 + 1, \dots, j_k + k$ (on pose $M_{I,J} = 0$ si l'une de ces lignes ou colonnes n'existe pas ; pour $I = (0, \dots, 0) = 0^k = J$, on a le mineur "initial" pris sur les k premières lignes et k premières colonnes).

A toute série formelle $\sum_j \geq 0 z^j S_j$, on associe la matrice de ses coefficients

$$[S] = [S_{j-i}]_{i,j \geq 0}$$

avec $S_j = 0$ si $j < 0$, et les fonctions de Schur

$$(1.2) \quad S_{J/I} = [S]_{I,J}, \quad I, J \in \mathbb{Z}^k.$$

Dans le cas où $I = 0^k$, on écrit S_J .

Il faut noter que le produit des séries formelles ou l'inversion correspondent au produit des matrices, ou à l'inversion. La formule de Binet-Cauchy (cf. note) pour les mineurs d'un produit de matrices, ou la formule de Jacobi pour les mineurs de la matrice inverse donnent donc les fonctions de Schur pour le produit de deux séries ou l'inverse d'une série [Littlewood].

Etant donnés deux ensembles A, B d'indéterminées (nous dirons deux "alphabets"), les fonctions de Schur $S_{J/I}(A-B)$ sont les fonctions de Schur de la série :

$$(1.3) \quad \prod_{b \in B} (1 - zb) / \prod_{a \in A} (1 - za) = \sum z^j S_j(A-B)$$

Avec ces notations, les polynômes $\prod (x-a)$ et $\prod (x-b)$ s'écrivent respectivement $S_m(x-A)$ et $S_n(x-B)$, m et n étant les cardinaux de A et B .

On note $A+B$ l'union disjointe de deux alphabets. Les fonctions symétriques sont écrites en supposant toutes les indéterminées différentes, quitte à spécialiser ensuite.

La formule de Cauchy, dont on a fait le deuxième axiome des λ -anneaux, est l'expression de $\prod (a-b)$ (ou, de manière équivalente, de

$\Pi(1-ab)$, de $1/\Pi(1-ab)$) comme fonction symétrique en les $a \in A$, et les $b \in B$:

$$(1.4) \quad \Pi_{a \in A, b \in B} (a-b) = S_{n^m}^{(A-B)} \quad (\text{cf. note}).$$

Factorisant la série $\sum S_j(A-B)$ en $\sum S_j(A) \cdot \sum S_k(-B)$, on transforme comme suit la formule précédente :

$$(1.5) \quad \Pi(a-b) = \sum S_{n/I}^{(A)} \cdot S_I(-B),$$

somme sur toutes les partitions $I = 0 \leq i_1 \leq i_2 \leq \dots \leq i_m$.

Brioschi (1854 ; [Muir] II p.349) a donné l'expression (1.4) du résultant en définissant les $S_j(A-B)$ par :

$$(1.6) \quad S_{j+m-n}(A-B) = \sum_{a \in A} a^j Q(a)/P'(a).$$

2. METHODE D'EULER ET BEZOUT -

On doit aux mathématiciens sus-nommés un principe très puissant pour fournir des multiples du résultant : construire, pour un entier r quelconque, r polynômes de degré $\leq r-1$ qui s'annulent simultanément pour toute racine commune à $S_m(x-A)$ et $S_n(x-B)$. Alors le déterminant des coefficients de ces polynômes est un multiple du résultant, puisqu'il s'annule en même temps que lui (la matrice des coefficients admet le vecteur propre $1 \ C \dots C^{r-1}$ pour toute "racine commune" $C \in \{A \cap B\}$). On veille usuellement à ce que les r polynômes soient linéairement indépendants et tels que le déterminant de leurs coefficients soit de degré minimum (= mn) en A, B .

Soit par commodité $m=n$; Bezout note que pour $0 \leq j \leq n-1$, les n "équations dérivées"

$$(2.1) \quad P_j = S_j(x-A) \cdot S_n(x-B) - S_j(x-B) \cdot S_n(x-A)$$

sont des polynômes dont le degré ne dépasse pas $n-1$ et qui s'annulent pour toute racine commune dans $\{A \cap B\}$. La matrice des coefficients des P_j a été appelée "Bezoutien" par Sylvester ; (voir aussi [Jacobi], [Muir] I p.485 et [Muir] III p.343).

Le Bezoutien n'est pas identique à la matrice

$$[S_{n+j-i}(A-B)]_{1 \leq i, j \leq n}$$

il s'obtient à partir de cette dernière par multiplication à gauche

et à droite par la matrice triangulaire $[S_{j-i}(-A)]_{1 \leq i, j \leq n}$, le déterminant du Bezoutien est donc bien $R(A, B)$. Par exemple, pour $m = n = 3$, $R(A, B) = S_{333}(A-B)$ tandis que le Bezoutien est égal à

$$\begin{vmatrix} 1 & -A & S_2(-A) \\ 0 & 1 & -A \\ 0 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} S_3(A-B) & S_4(A-B) & S_5(A-B) \\ S_2(A-B) & S_3(A-B) & S_4(A-B) \\ S_1(A-B) & S_2(A-B) & S_3(A-B) \end{vmatrix} \cdot \begin{vmatrix} 1 & -A & S_2(-A) \\ 0 & 1 & -A \\ 0 & 0 & 1 \end{vmatrix}$$

$$= \begin{vmatrix} S_3(-B) - S_3(-A) & BS_3(-A) - AS_3(-B) & S_2(-A)S_3(-B) - S_2(-B)S_3(A) \\ S_2(-B) - S_2(-A) & S_3(-B) - S_3(-A) + BS_2(-A) - AS_2(-B) & BS_3(-A) - AS_3(-B) \\ A-B & S_2(-B) - S_2(-A) & S_3(-B) - S_3(-A) \end{vmatrix}$$

Sylvester préfère éliminer $1, x, \dots, x^{m+n-1}$ entre les polynômes $S_m(x-A)$, $S_{m+1}(x-A), \dots, S_{m+n-1}(x-A)$; $S_n(x-B), \dots, S_{m+n-1}(x-B)$ et obtient ainsi le déterminant d'ordre $m+n$ suivant :

$$(2.2) \quad \left| \begin{array}{ccc} S_0(-A) & \dots & S_{m+n-1}(-A) \\ \vdots & & \vdots \\ S_{-n+1}(-A) & \dots & S_m(-A) \\ \\ S_0(-B) & \dots & S_{m+n-1}(-B) \\ \vdots & & \vdots \\ S_{-m+1}(-B) & \dots & S_n(-B) \end{array} \right| \quad \left. \begin{array}{l} \left. \begin{array}{l} \vdots \\ \vdots \end{array} \right\} n \\ \left. \begin{array}{l} \vdots \\ \vdots \end{array} \right\} m \end{array} \right\}$$

(voir Jacobi (1835), [Muir] I p.214 ; Sylvester (1840), [Muir] I p.236 ; Richelot (1840), [Muir] I p.238 ; Cauchy (1840), [Muir] I p.242).

Il faut noter que, $S_{m+j}(x-A)$ étant égal à $x^j S_m(x-A)$ pour tout $j \geq 0$, ce déterminant s'obtient en prenant n lignes formées par les coefficients de $S_m(x-A)$, en décalant d'un cran, d'une ligne à l'autre, puis m lignes formées par les coefficients de $S_n(x-B)$.

Le développement du déterminant de Sylvester suivant ses n premières lignes donne une somme de produits de fonctions de Schur de $-A$ et de $-B$; si l'on revient à A , ce qui correspond au changement d'indice indiqué en note, on retrouvera très exactement l'expression (1.5) de la résultante. Par exemple, la résultante

$$\begin{aligned}
& \text{de } S_3(x-A) \text{ et } S_2(x-B) \text{ est égale à } S_{222}(A-B) = \\
& S_{222}(A) \cdot S_{000}(-B) + S_{122}(A) \cdot S_{001}(-B) + S_{112}(A) \cdot S_{011}(-B) \\
& + S_{022}(A) \cdot S_{002}(-B) + S_{012}(A) \cdot S_{012}(-B) + S_{111}(A) \cdot S_{111}(-B) \\
& + S_{002}(A) \cdot S_{022}(-B) + S_{011}(A) \cdot S_{112}(-B) + S_{001}(A) \cdot S_{122}(-B) \\
& + S_{000}(A) \cdot S_{222}(-B)
\end{aligned}$$

$$= \begin{vmatrix} 1 & -A & S_2(-A) & S_3(-A) & 0 \\ 0 & 1 & -A & S_2(-A) & S_3(-A) \\ 1 & -B & S_2(-B) & 0 & 0 \\ 0 & 1 & -B & S_2(-B) & 0 \\ 0 & 0 & 1 & -B & S_2(-B) \end{vmatrix}$$

3. LA RESULTANTE PAR DIVISION -

Le reste de la division d'un polynôme par un autre est divisible par le p.g.c.d. de ces deux polynômes. Au lieu de prendre, comme précédemment dans la méthode de Sylvester, les polynômes $S_m(x-A)$, $S_{m+1}(x-A)$, $S_{m+2}(x-A)$, ..., on peut se contenter de leurs restes par $S_n(x-B)$.

Voyons tout d'abord comment les fonctions de Schur interviennent dans la division.

Lemme 3.1. - Soient p un entier dans $\mathbb{Z}$, A et B deux alphabets, n le cardinal de B. Alors

$$S_p(x-A) - S_{p-n}(x-A+B) S_n(x-B) = \sum_0^{n-1} S_j(x-B) \cdot S_{p-j}(B-A).$$

En effet, $x-A = (x-B) + (B-A)$, et donc

$$S_p(x-A) = \sum_0^{\infty} S_j(x-B) \cdot S_{p-j}(B-A) = \sum_0^{n-1} + \sum_n^{\infty}.$$

Or, puisque B est de cardinal n,

$$h \geq 0 \Rightarrow S_{n+h}(x-B) = x^h S_n(x-B);$$

la sous somme $\sum_n^{\infty} S_j(x-B) \cdot S_{p-j}(B-A)$ est donc égale à

$$S_n(x-B) \sum_{h=0}^{\infty} x^h S_{p-n-h}(B-A) = S_n(x-B) S_{p-n}(x+B-A) \quad \square$$

Le membre de droite de 3.1 est donc le reste de la division de $S_p(x-A)$ par le polynôme $S_n(x-B)$.

En particulier, la matrice des coefficients des restes des polynômes $S_m(x-A), S_{m+1}(x-A), \dots, S_{m+n-1}(x-A)$ dans la base $S_0(x-B), \dots, S_{n-1}(x-B)$ est la matrice $S_{m,n}(B-A)$ déjà vue en 1.4.

Corollaire 3.2 - Pour tout $p \geq 0$, $x^p \equiv x^{n-1} S_k(B) - x^{n-2} S_{1k}(B) + x^{n-3} S_{11k}(B) - x^{n-4} S_{111k}(B) + \dots$ modulo le polynôme $S_n(x-B)$, avec $k = p-n+1$.

Le corollaire résulte de (3.1) pour un alphabet A vide ; on vérifie que la somme $\sum_{j=0}^{n-1} S_j(x-B) \cdot S_{p-j}(B) = \sum_{i,j} x^{n-1-i} S_{i+j+1-n}(-B) S_{p-j}(B)$ se transforme en ce qu'exige (3.2) moyennant l'identité (cf. note)

$$S_i(-B) S_k(B) + S_{i-1}(-B) S_{k+1}(B) + \dots + S_0(-B) S_{k+i}(B) = (-1)^i S_{1k}^{(i)}(B) \quad \square$$

Remarque : Si $0 \leq p \leq n-1$, un seul terme dans la somme (3.2) est non nul : c'est $(-1)^{n-1-p} x^p S_{1^{n-1-p}k}^{(n-1-p)}(B) = x^p S_{0^{n-p}}(B) = x^p$, comme il se doit.

Les restes d'autres ensembles de n polynômes peuvent donner des fonctions intéressantes. C'est le cas des $S_j^{(j)}(B-A-x) \cdot S_m(x-A)$, $0 \leq j \leq n-1$, comme le montre le lemme suivant (qui est équivalent, par linéarité, à 3.1).

Lemme 3.3 - Soient A et B deux alphabets de cardinaux respectifs

$$m, n, \text{ et } j \text{ un entier } \geq 0. \text{ Alors } S_{1j}^{(j)}(B-A-x) \cdot S_m(x-A) \equiv S_{1j_m}^{(j)}(B-A) + (x-B) S_{1j_{m-1}}^{(j)}(B-A) + S_2(x-B) S_{1j_{m-2}}^{(j)}(B-A) + \dots + S_{n-1}(x-B) S_{1j_{m-n}}^{(j)}(B-1) \text{ modulo } S_n(x-B).$$

Le déterminant des coefficients $S_{1j_{m-i}}^{(j)}(B-A)$, $0 \leq i, j \leq n-1$ des $n-1$ premiers restes est en fait égal à $(-1)^{\binom{n}{2}} S_m^{(n)}(B-A)$; plus généralement, toute fonction de Schur $S_{J/I}(B-A)$ peut s'exprimer comme un déterminant en les fonctions "équerrres" $S_{1\dots 1k}(B-A)$ [L & P].

On peut répéter la division et diviser $S_n(x-B)$ par le reste de la division de $S_m(x-A)$ par $S_n(x-B)$, et ainsi de suite ; les coefficients des restes successifs sont, comme plus haut, des fonctions de Schur (les "équerrres" $1 \dots 1$ k sont à remplacer par les partitions plus générales $1 \dots 1$ $k \dots k$, r fois k pour le r -ième reste). Cela donne la résultante comme un déterminant, de la taille que l'on désire, en fonctions de Schur. C'est à [Wronski] qu'il faut attribuer les relations entre fonctions de Schur nécessaires à la récurrence sur r .

4. RACINES COMMUNES -

Le résultant $R(A,B)$ est nul si le p.g.c.d de $S_m(x-A)$ et $S_n(x-B)$ est de degré ≥ 1 ; chacune des matrices que nous avons données dans les paragraphes précédents est alors de rang non maximal. On peut faire mieux que de constater la nullité du déterminant des dites matrices. Par exemple, le p.g.c.d s'exprime à l'aide des mineurs d'ordre approprié d'une quelconque des dites matrices. Les calculs reposent essentiellement sur le lemme élémentaire suivant.

Tout d'abord, étant donné un entier n , $J \in \mathbb{Z}^n$ et n couples d'alphabets $A_1, B_1, \dots, A_n, B_n$, on note $S_J(A_1-B_1, \dots, A_n-B_n)$ la fonction (que l'on dira encore de Schur)

$$|S_{j_k+k-h} (A_k-B_k)|_1 \leq h, k \leq n$$

Lemme 4.1. Soient $C_1, \dots, C_n$ des alphabets tels que $\text{card}(C_1) \leq n-1$, $\text{card}(C_2) \leq n-2, \dots, \text{card}(C_n) \leq 0$. Alors

$$S_J(A_1-B_1, \dots, A_n-B_n) = |S_{j_k+k-h} (A_k-B_k-C_h)|$$

i.e. on peut soustraire C_1 à la première ligne, C_2 à la deuxième, ... sans changer la valeur de la fonction de Schur.

En effet, pour tout entier p et tout alphabet C de cardinal r

$$S_p(A-B-C) = \sum_{j=0}^r S_{p-j}(A-B) S_j(-C).$$

La première ligne du déterminant S_J est donc modifiée par adjonction des suivantes puisque $\text{card}(C_1) \leq n-1$; il en est de même des

autres, la valeur du déterminant est inchangée. $\square$

Le lemme 4.1 permet de factoriser certaines fonctions de Schur ; cette factorisation est le point central de nombreux articles en théorie de l'élimination ; cependant, il ne semble pas que l'énoncé général en ait été breveté avant Berele et Regev, et c'est donc à ces auteurs, selon les recommandations de [Grothendieck] que nous attribuerons le lemme suivant ([Pomey] donne par exemple le cas $I = 0 \dots 0, J = 0 \dots 01 \dots 1$; [Giambelli (1908)] y ajoute le cas $J = 0 \dots 0 k$).

Lemme 4.2 : Soient p un entier positif, A, B deux alphabets de cardinaux respectifs $m, n, I \in \mathbb{N}^p, J \in \mathbb{N}^m$. Alors

$$S_{i_1 \dots i_p \ n+j_1 \dots n+j_m}^{(A-B)} = S_I^{(-B)} \cdot S_J^{(A)} \cdot R(A, B).$$

Notons en passant que le lemme 4.2 donne des invariants de la suite récurrente $\{S_j^{(A-B)}\}$ comme déterminants isobares ; c'est une autre approche de cette factorisation dont Euler connaissait des cas particuliers.

Soient A', B', C trois alphabets disjoints, de cardinaux respectifs $m-r, n-r, r$, $A = A' + C$, $B = B' + C$. L'ensemble des "racines communes" de $S_m(x-A)$ et $S_n(x-B)$ est $C = A \cap B$, i.e. le p.g.c.d des deux polynômes est $S_r(x-C)$.

Ecrivant $C = A - A'$, on peut développer le p.g.c.d :

$$S_r(x-C) = \sum_j S_{r-j}(x-A) \cdot S_j(A').$$

Les $S_j(A')$ nous sont données par le lemme 4.2, au facteur $R(A', B')$ près. En effet $S_{\square + 0 \dots 0j}^{(A-B)} = S_{\square + 0 \dots 0j}^{(A'-B')}$

$$= S_j(A') \cdot R(A', B') = S_j(A') \cdot S_{\square}^{(A'-B')}$$

$$= S_j(A') \cdot S_{\square}^{(A-B)}$$

en notant $\square$ et $\square + 0 \dots 0j$ les partitions

$$\underbrace{n-r, \dots, n-r}_{m-r \text{ fois}} \quad \text{et} \quad \underbrace{n-r, \dots, n-r}_{m-r-1 \text{ fois}}, n-r+j.$$

Toujours d'après 4.2,

$$0 \leq p < r \Rightarrow S_{(n-p)^{m-p}}(A-B) = S_{(n-p)^{r-p}}(-B') \cdot R(A', B') \cdot S_{(n-p)^{m-r}}(A')$$

est nul puisque $S_{n-p}(-B') = 0$, $n-p$ étant strictement supérieur au cardinal de B' ; comme réciproquement, pour un sous-alphabet de B , B' de cardinal $\leq n-r \Leftrightarrow S_n(-B) = S_{n-1}(-B) = \dots = S_{n-r+1}(-B) = 0$, on obtient finalement le lemme suivant.

Lemme 4.3 : Pour que le p.g.c.d des polynômes $S_m(x-A)$ et $S_n(x-B)$ soit de degré r , il faut et il suffit que les déterminants $S_{n^m}^{(A-B)}, \dots, S_{(n-r+1)^{m-r+1}}^{(A-B)}$ soient nuls et que $S_{\square}(A-B) \neq 0$, avec $\square = (n-r)^{m-r}$.

Dans ce cas, le p.g.c.d est, au facteur $S_{\square}(A-B)$ près, égal à

$$\sum_{j=0}^r S_{r-j}(x-A) \cdot S_{\square + 000j}(A-B).$$

La fonction $S_{\square + 000j}(A-B)$ est le mineur d'indice $(r^{m-r}, 0 \dots 0j)$ de la matrice $[S_{n-h+k}^{(A-B)}]_{1 \leq h, k \leq m}$, c'est-à-dire est un mineur de la première matrice qui nous a, en 1.4, donné la résultante; on n'éprouve pas plus de difficulté à identifier $S_{\square + 000j}(A-B)$ à un mineur des autres matrices dont le déterminant est la résultante. Prenons par exemple le déterminant de Sylvester (2.2) :

Lemme 4.4 : Soit r le degré du p.g.c.d de $S_m(x-A)$ et $S_n(x-B)$. Alors ce dit p.g.c.d est égal, à une constante près, au déterminant d'ordre $m+n-2r$

$$\begin{vmatrix} S_0(-A) & \dots & S_{m+n-2-2r}(-A) & S_{m+n-1-r}(x-A) \\ \vdots & & \vdots & \vdots \\ S_{-n+r+1}(-A) & \dots & S_{m-r-1}(-A) & S_m(x-A) \\ S_0(-B) & \dots & S_{m+n-2-2r}(-B) & S_{m+n-1-r}(x-B) \\ \vdots & & \vdots & \vdots \\ S_{-m+r+1}(-B) & \dots & S_{n-r-1}(-B) & S_n(x-B) \end{vmatrix}$$

Démonstration : on peut développer suivant les puissances de x et essayer de reconnaître les fonctions déjà rencontrées en (4.3). Il

est plus simple de constater que ce déterminant s'annule pour toute racine x commune aux deux polynômes de départ, puisqu'alors $A-x$ est un alphabet de card $m-1$ d'où $S_m(x-A) = S_{m+1}(x-A) = \dots = 0$ et similairement $S_n(x-B) = S_{n+1}(x-B) = \dots = 0$, i.e. la dernière colonne est nulle. En outre, le déterminant est un polynôme de degré $\leq r$, les puissances plus élevées de x s'éliminant en soustrayant à la dernière colonne x^0 fois la première + x^1 fois la seconde Enfin, on trouve comme coefficient de x^r la fonction non nulle $S_{\binom{n-r}{m-r}}^{m-r}(A-B) (= R(A', B'))$, en développant le déterminant suivant ses $\binom{n-r}{m-r}$ premières lignes comme on l'a fait, pour $r=0$, en 2.2. $\square$

Il y a de nombreuses manières de présenter les calculs de ce paragraphe ; bien des travaux du siècle dernier en théorie de l'élimination s'y rapportent. Le point de vue le plus instructif est sans doute celui d'Euler et Bezout, à savoir l'étude pour tout entier $p \geq 0$ de l'espace vectoriel V_p engendré par les polynômes $S_m(x-A), S_{m+1}(x-A), \dots, S_{m+p}(x-A); S_n(x-B), \dots, S_{n+p}(x-B)$ (en supposant $m \geq n$) ; cela revient à filtrer l'idéal engendré par $S_m(x-A)$ et $S_n(x-B)$; si $n-p > r = \text{degré du p.g.c.d.}$, alors $V_p = \mathbb{T}[x]f_p(x)$, où $f_p(x)$ est le $p+1$ -ième reste de la division de $S_m(x-A)$ par $S_n(x-B)$; f_{n-r-1} est le p.g.c.d. et $V_{n-r-1} = V_{n-r} = \dots = \text{Idéal engendré par } S_m(x-A) \text{ et } S_n(x-B)$.

Un historique tant soit peu complet est hors de portée de cet exposé ; voir l'index du cinquième volume de [Muir] et les pages 321-338 de [Pascal].

Voici toutefois quelques jalons :

[Jacobi] donne les restes et quotients successifs, ce qui revient à réduire la fraction rationnelle $S_m(x-A) / S_n(x-B)$ en fraction continue. La méthode de [Wronski] pour la séparation des racines d'un polynôme selon que leur module est supérieur à 1 ou non conduit aux mêmes calculs. L'expression des restes comme des déterminants du type 4.4 se trouve dans Sylvester (1840, [Muir] I p.238 ; [Muir] II p.340 ; oeuvres, I p.58 ; I p.429-586) , Faa de Bruno (1859, [Muir] III p.327). Abel et Liouville ont donné le p.g.c.d. lorsqu'il est de degré 1 ; [Brioschi] obtient le p.g.c.d. dans le cas général à l'aide des dérivées de $R(A,B)$ en tant que fonction des coefficients des deux polynômes. [Trudi] (1862, [Muir] III p.340) donne le lemme 4.4. [Pomey] (1888) exprime le dit p.g.c.d. à l'aide successivement des $S_j(A-B)$,

du Bezoutien et de la matrice de Sylvester ; dans [Weber] (p.188 et s) sont utilisées les équerres $S_{l,j,k}(A-B)$. [Giambelli (1908)] montre que l'on peut aussi employer un déterminant en les $S_i(A)$ et $S_j(B)$ (au lieu des $S_i(-A)$ et $S_j(-B)$ dans le déterminant de Sylvester).

5. AUTRES POINTS DE VUE -

Cayley (1853, Muir II p.138) donne une interprétation intéressante du Bezoutien : il considère la forme quadratique

$$Q(x,y) = [S_m(x-A) S_n(y-B) - S_m(y-A) S_n(x-B)] / (x-y) =$$

$$[1 \ x \dots x^{m-1}] [R_{ij}]_{1 \leq i,j \leq m} [1 \ y \dots y^{m-1}]^{\text{tr}}$$

supposant $m \geq n$. Cette forme quadratique s'annule quelque soit y si x est une racine commune des deux polynômes ; le déterminant de Q est donc nul quand la résultante l'est. En fait, $(x-y) Q(x,y)$ est égale au déterminant du produit de $\begin{bmatrix} 1 & x & \dots & x^m \\ 1 & y & \dots & y^m \end{bmatrix}$ par la

transposée $\begin{bmatrix} S_0(-A) & \dots & S_m(-A) \\ S_0(-B) & \dots & S_m(-B) \end{bmatrix}$; la formule de Binet-Cauchy

fournit alors que la matrice $[Q_{ij}]$ est le Bezoutien (voir aussi [Schendel]).

Plus généralement, étant donnés r polynômes $P_1, \dots, P_r$, on étudie la fonction symétrique en $x_1, \dots, x_r$:

$$|P_i(x_j)| / \prod_{i < j} (x_i - x_j) ;$$

voir en particulier l'application à la théorie des polynômes orthogonaux en [L & Shi]

La résultante est un déterminant de Hankel (i.e. une fonction de Schur "rectangle" S_n). Les identités vérifiées par ces déterminants servent en théorie^m des polynômes orthogonaux et de l'approximation de Padé [Brezinski] .

Une autre approche consiste à considérer le Bezoutien, en fixant un des deux polynômes, comme un morphisme de l'espace des polynômes

dans celui des matrices [Orzech].

Plus adapté aux méthodes informatiques est le calcul du Bezoutien de deux polynômes de degré n à l'aide de la valeur en $n + 1$ points de ces deux polynômes (Borchardt 1859, [Muir] II p. 147).

Le même Borchardt (1878, [Muir] III p. 161) donne aussi une expression non déterminantale de la résultante. Pour plus de deux polynômes, voir [Giambelli 1908].

6. APPROCHE GEOMETRIQUE -

On peut interpréter en termes géométriques la division d'un polynôme par un autre. En effet, soit B un fibré vectoriel de rang n sur une base quelconque Z , $IP(B) \rightarrow Z$ le projectif associé. L'anneau de Grothendieck de $IP(B)$ est le quotient de l'anneau de polynôme $K(Z)[x, x^{-1}]$ par l'idéal engendré par $S_n(x-B)$, x étant la classe du fibré vectoriel "tautologique" de rang 1, et $K(Z)$ l'anneau de Grothendieck de la base. On dispose d'un morphisme de $K(Z)$ -modules, (dit morphisme de Gysin) :

$$\Pi_{\star} : K(IP(B)) \rightarrow K(Z).$$

Le reste d'un polynôme $Q(x)$ quelconque s'écrit, à l'aide de ce morphisme :

$$Q(x) \equiv \sum_{k=0}^{n-1} x^{n-1-k} \Pi_{\star}(Q(x) \cdot S_k(x-B) \cdot x^{1-n})$$

(cf. [L & S1] pour la généralisation à la variété de drapeaux).

Le calcul de la résultante consiste à trouver un polynôme $Q(x)$ de degré $\leq n-1$ (unique à constante près) tel que $Q(x) \cdot S_m(x-A)$ soit congru à une constante différente de 0 modulo $S_n(x-B)$ (A est considéré comme la classe d'un fibré de rang m). On a déjà vu au paragraphe 4 que :

$$Q(x) = \begin{vmatrix} S_0(-A) & \dots & S_{m+n-2}(-A) & x^{n-1} \\ \vdots & & \vdots & \vdots \\ S_{1-n}(-A) & \dots & S_{m-1}(-A) & x^0 \\ S_0(-B) & \dots & S_{m+n-2}(-B) & 0 \\ \vdots & & \vdots & \vdots \\ S_{1-m}(-B) & & S_{n-1}(-B) & 0 \end{vmatrix}$$

et l'on peut retrouver, à l'aide du morphisme $\Pi_\star$ que $Q(x) \cdot S_m(x-A) \equiv R(A,B) \text{ modulo } S_n(x-B)$.

Pour respecter la symétrie en A et B , on peut faire appel à la grassmannienne $G_n(\mathbb{T}^{m+n}) = G$ que l'on plonge diagonalement dans $G \times G : \Delta \hookrightarrow G \times G$; sur G on dispose d'un module noyau tautologique de rang m , disons E , et d'un quotient F de rang n ; les classes de Chern de fibrés vectoriels dans l'anneau de cohomologie de $G \times G$ peuvent être considérés comme des polynômes : on pose $c(p_1^\star(E)) = \Pi_a \in A(1+a)$ et $c(p_2^\star(F)) = \Pi_b \in B(1+b)$, p_1 et p_2 étant les deux projections de $G \times G$ sur G . Alors la classe de la diagonale Δ dans l'anneau de cohomologie est la classe de Chern maximale $C_{mn}(p_1^\star(E) \otimes p_2^\star(F^V)) = \Pi(a-b) = R(A,B)$. Toutes les formules des paragraphes précédents se traduisent en termes géométriques; par exemple, le développement (1.5) exprime que la classe de Δ dans la cohomologie de $G \times G$ est égale à la somme de produits de cycles de Schubert d'indices complémentaires, les fonctions de Schur s'interprétant maintenant comme les cycles fondamentaux de la grassmannienne (cycles de Schubert); pour des groupes plus généraux que $GL(\mathbb{T}^n)$, ceci est le théorème de Chevalley.

On peut choisir comme [Giambelli] un point de départ plus algébrique : celui des idéaux de mineurs de matrices. On retrouve résultante, fonctions de Schur et grassmannienne !

7. UNE GENERALISATION -

Tout ce qui précède est l'étude de la fonction $R(A,B) = \Pi(a_i - b_j)$ pour deux ensembles $A = \{a_1, \dots, a_m\}$ et $B = \{b_1, \dots, b_n\}$. Supposons $m = n$. La moitié des termes dans la factorisation de la résultante :

$$R_{1/2}(A,B) = \Pi_{i+j \leq n} (a_i - b_j)$$

conduit aux mêmes types de propriétés que la résultante. Ainsi $R_{1/2}(A,B)$ se développe en une somme de produits de polynômes de Schubert [L & S 1], ce qui permet une interpolation de Newton à plusieurs variables [L & S 2]. L'interprétation géométrique fait appel aux variétés de drapeaux [L-S]; d'autres approches sont possibles, par exemple les tableaux (de Young) ou la classification des décompositions réduites dans le groupe symétrique. Ce qui sous-

entend tous ces points de vue, c'est l'action du groupe symétrique sur l'anneau des polynômes, l'algèbre libre, la variété de drapeaux.

NOTE -

La théorie des fonctions symétriques a été pendant longtemps essentiellement rattachée à celle des déterminants isobares ; l'interprétation en terme de caractères de groupe linéaire et symétrique n'est venue qu'avec les travaux de Frobenius, Young et Schur. Ces dites fonctions symétriques imposent un décalage dans les indices par rapport aux conventions prédominantes : si M est une matrice, et $I, J \in \mathbb{Z}^n$, alors $M_{I,J}$ est le mineur pris sur les lignes $i_1 + 1, \dots, i_n + n$ et colonnes $j_1, \dots, j_n + n$, ainsi que nous l'avons dit au premier paragraphe. A permutation de lignes (si toutes différentes) près, on peut supposer que I est une partition, i.e. une suite d'entiers croissante au sens large : $0 \leq i_1 \leq i_2 \leq \dots \leq i_n$. Le produit de matrices se définit par

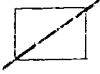
$$[MN]_{i,j} = \sum_h M_{i,h} \cdot N_{h,j}$$

la sommation est sur $h \in \mathbb{N}$, une fois étendue par des 0 les matrices en cause). Les mineurs de MN s'écrivent tout aussi simplement, à l'aide de la formule de Binet-Cauchy :

$$\forall n, \forall I, J \in \mathbb{Z}^n, [MN]_{I,J} = \sum_H M_{I,H} \cdot N_{H,J}$$

somme sur toutes les partitions H (bien entendu, il y a seulement un nombre fini de termes non nuls dans la somme si les matrices sont finies).

Si M est une matrice carrée (de déterminant égal à 1 pour simplifier), et si N est l'image de M^{-1} par rapport à

l'anti-diagonale , alors pour tout couple de partitions $I, J \in \mathbb{N}^n$,

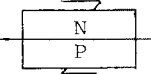
$$M_{I,J} = (-1)^{|J| - |I|} N_{I^-, J^-}$$

c'est la formule de Jacobi.

(I^- désigne la partition dite conjugée ou transposée de I , i.e. celle obtenue en transposant la représentation planaire de I ,

et $|I| = i_1 + i_2 + \dots$ est le poids de I , cf [Macdonald] p.2).

Enfin, le développement d'un déterminant suivant un sous-ensemble de lignes a été obtenu par Laplace ; supposons la matrice

M coupée en deux parties N, P  et les colonnes de N numérotées de gauche à droite, celles de P de droite à gauche.

Alors

$$\det(M) = \sum (-1)^{|J|} N_{0\dots 0, J} \cdot P_{0\dots 0, J^{\sim}}$$

somme sur toutes les partitions J (la notation $N_{0\dots 0, J}$ signifie que l'on prend le mineur sur toutes les lignes de N , et colonnes J).

Revenons aux fonctions de Schur. D'après la définition (1.3), la matrice $[S_{j-i}(A-B)]$ est le produit des matrices $[S_{j-i}(A)]$ et $[S_{j-i}(-B)]$, en d'autres termes,

$$S_j(A-B) = \sum S_{j-h}(A) \cdot S_h(-B).$$

On en déduit, par la formule de Binet-Cauchy,

$$S_{J/I}(A-B) = \sum S_{H/I}(A) \cdot S_{J/H}(-B)$$

somme sur toutes les partitions H .

Posant $B = A$ dans (1.3), on voit que $\sum S_j(A) \cdot \sum S_i(-A) = 1$, c'est-à-dire que les matrices $[S_{j-i}(A)]$ et $[S_{j-i}(-A)]$ sont inverses. D'après Jacobi on a donc, pour toute paire I, J de partitions,

$$S_{J/I}(A) = S_{J^{\sim}/I^{\sim}}(-A) ;$$

en particulier, pour tout entier k positif,

$$S_{1^k}(A) = (-1)^k S_k(-A)$$

La formule de Laplace permet enfin de développer, par lignes ou par colonnes, une fonction de Schur comme une somme de produits de fonctions de Schur. Par exemple, le développement suivant la dernière colonne s'écrit : pour tout $I \in \mathbb{Z}^n$, $j \in \mathbb{Z}$,

$$S_{Ij} = \sum_k (-1)^k S_{I/1k} \cdot S_{j+k}$$

(Ij désigne l'élément $(i_1, \dots, i_n, j)$ de $\mathbb{Z}^{n+1}$).

En particulier, pour une partition équerre ($n \geq 0$, $j \geq 1$),

$$S_{1n_j} = \sum_k (-1)^k S_{1n-k} \cdot S_{j+k}$$

identité que l'on peut aussi écrire : pour tout alphabet A ,

$$(-1)^n S_{1n_j}(A) = \sum_k S_{n-k}(-A) \cdot S_{j+k}(A).$$

BIBLIOGRAPHIE

- A. BERELE, A. REGEV - Hook Young diagrams, prepub.
 M. BEZOUT - Théorie générale des Equations algébriques, Paris 1779.
 C. BREZINSKI - Padé-type Approximants, Birk haüser 1980.
 F. BRIOSCHI - Théorie des déterminants, Paris 1856.
 Faa de BRUNO - Théorie de l'élimination, Thèse Paris 1856.
 H. GERBER - Am.M.M. 91 (1984) 644-646.
 Z. GIAMBELLI - Atti Torino 38 (1903) 551-572.
 Z. GIAMBELLI - Atti Torino 40 (1904) 1041-1062.
 Z. GIAMBELLI - Mem. R. Ist. Lomb. 20 (1904) 101-135.
 Z. GIAMBELLI - Rend. Palermo 25 (1908) 131-144.
 A. GROTHENDIECK - Récoltes et Semailles, IIème partie, Montpellier 1985.
 A.S. HOUSEHOLDER - The numerical treatment of a single non linear equation, Mc Graw Hill 1970.
 C.G. JACOBI - Crelle J.15 (1836) 101-124.
 [L - S] A. LASCoux - C.R. Acad. Sc. Paris 295 (1982) 393.
 [L & P] A. LASCoux & P. PRAGACZ - C.R. Acad. Sc. Paris 299 (1984) 955.
 [L & Shi] A. LASCoux & SHI He - C.R. Acad. Sc. Paris 300 (1985) 681.

- [L & S1] A. LASCoux & M.P. SCHÜTZENBERGER in Invariant Theory,
Springer L.N. 996.
- [L & S2] A. LASCoux & M.P. SCHÜTZENBERGER in Séminaire d'algèbre
M.P. Malliavin 1984-1985, Springer L.N. 1146.
- H. LAURENT - Nouv. Ann. M. (3)7 (1888) 60-65.
- D.E. LITTLEWOOD - The Theory of group characters, Oxford 1950.
- I.G. MACDONALD - Symmetric functions and Hall polynomials, Oxford
M. Mono 1979.
- T. MUIR - History of determinants, 5 volumes, Dover reprints 1960.
- G. ORZECCH - Lin. Mult. Alg. 16 (1984) 275-282.
- R. RUFFINI - Opere matematiche, reed. Palermo 1915.
- E. PASCAL - I determinanti, Hoepli 1923.
- E. POMEY - Nouv. Ann. M(3)7 (1888) 66-90 and 407-427.
- L. SCHENDEL - Zeit. 38 (1893) 84-94.
- J.J. SYLVESTER - Collected Work, Chelsea reprint.
- N. TRUDI - Teoria de determinanti, Napoli 1862.
- H. WEBER - Traité d'Algèbre supérieure, Paris 1989.
- H. WRONSKI - Philosophie de la TechnieAlgorithmique : Loi suprême
et universelle ; réforme des mathématique.Paris
1815-1817.