# MODULES DE CAUCHY, POLYNÔMES CARACTÉRISTIQUES ET RÉSOLVANTES

ANNICK VALIBOUZE*

10 Avril 1996

ABSTRACT. This paper gives a new and efficient algorithm to compute some characteristic polynomials using Cauchy modules. This algorithm is used for the computation of resolvents and multi-resolvents which are essential in Galois theory.

Cet article décrit un nouvel et efficace algorithme pour calculer certains polynômes caractéristiques en utilisant les modules de Cauchy. Cet algorithme est ensuite utilisé pour calculer des résolvantes et des multi-résolvantes, outils de base de la théorie des corps et donc aussi de la théorie de Galois effective.

Soit $\mathcal{R}$ un anneau commutatif unitaire et $x$ une variable. Dans tout cet article, $f$ est un polynôme de $\mathcal{R}[x]$, de degré $n$, dont la famille des racines dans une clôture algébrique de $\mathcal{R}$ est $\alpha = (\alpha_1, \ldots, \alpha_n)$. L'étude du polynôme $f$ peut se réaliser dans l'algèbre de décomposition universelle du polynôme $f$. La formule du calcul des polynômes caractéristiques d'endomorphismes dans cette algèbre quotient était jusqu'alors donnée avec un résultant $(n, n)$ (voir paragraphe 3). Le paragraphe 5 propose une nouvelle formule à partir des modules de Cauchy (voir paragraphe 4) et les résultants. Cette formule est simple, efficace et facile à mettre en œuvre. Aux paragraphes 6 et 10, elle est adaptée pour le calcul des résolvantes et des multi-résolvantes. La résolvante, introduite par Lagrange, est actuellement l'outil le plus efficace pour identifier les groupes de Galois de polynômes (voir [4] et [21] pour la correspondance entre les groupes et les résolvantes). Elle permet également de répondre dans certains cas au problème de Galois inverse (voir [21] et [8]). De manière générale, l'intérêt des résolvantes et des multi-résolvantes est dû à leurs facteurs irréductibles qui sont des polynômes minimaux d'éléments primitifs d'extensions algébriques (voir [10]).

*Pour simplifier les formules, nous supposerons que le polynôme $f$ est unitaire.*

---

* projet GALOIS du GDR de Calcul Formel MEDICIS; supportée par GAGE, le Centre de Calcul Formel de l'École Polytechnique

## 1. Notations

Pour tout polynôme $\Psi \in \mathcal{R}[x_1, \ldots, x_n]$, l'évaluation, $\Psi(\alpha_1, \ldots, \alpha_n)$, de $\Psi$ en les racines de $f$ (pour la numérotation choisie) est notée $\widetilde{\Psi}$.

L'action de $\mathfrak{S}_n$, le groupe symétrique de degré $n$, sur $\Psi$ est définie par $\tau.\Psi = \Psi(x_{\tau(1)}, \ldots, x_{\tau(n)})$ pour tout $\tau \in \mathfrak{S}_n$. Ainsi, l'orbite de $\Psi$ sous l'action de $\mathfrak{S}_n$ , notée $\mathfrak{S}_n.\Psi$, est donnée par :

$$\mathfrak{S}_n.\Psi = \{\tau.\Psi \mid \tau \in \mathfrak{S}_n\}$$

Pour $i = 1, \ldots, n$, notons $e_i$ la $i$-ième *fonction symétrique élémentaire* en $x_1, \ldots, x_n$ définie par :

$$e_i = \sum_{m \in \mathfrak{S}_n.(x_1 \cdots x_i)} m$$

Posons $e_0 = 1$ et $s_i = e_i - \tilde{e}_i$, pour $i = 1, \ldots, n$. Rappelons que $f(x) = x^n - \tilde{e}_1 x^{n-1} + \tilde{e}_2 x^{n-2} + \cdots + (-1)^n \tilde{e}_n$.

## 2. Polynôme caractéristique

L'action du groupe symétrique $\mathfrak{S}_n$ sur $\alpha$ est définie, pour tout $\sigma \in \mathfrak{S}_n$, par $\alpha_\sigma = (\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$.

Soit $V$ la variété $\{\alpha_\sigma \mid \sigma \in \mathfrak{S}_n\}$ et $\mathcal{I}$ l'idéal de cette variété. Cet idéal est appelé l'*idéal des relations symétriques entre les racines du polynôme* $f$. Cet idéal est l'ensemble des polynômes $r \in \mathcal{R}[x_1, \ldots, x_n]$ tels que $\widetilde{\tau.r} = 0$ pour tout $\tau \in \mathfrak{S}_n$. Il est bien connu que l'idéal $\mathcal{I}$ est engendré par les $n$ polynômes $s_1, s_2, \ldots, s_n$. Le paragraphe 4 présente d'autres générateurs : les modules de Cauchy.

Pour $j = 1, \ldots, n$, notons $\Theta_j$ la multiplication par $x_j$ dans $\mathcal{R}[x_1, \ldots, x_n]/\mathcal{I}$. C'est un endomorphisme du $\mathcal{R}$-espace vectoriel $\mathcal{R}[x_1, \ldots, x_n]/\mathcal{I}$.

**Théorème 2.1.** (Yokoyama-Noro-Takeshima) Le polynôme

$$\chi_\Psi(T) \quad = \quad \prod_{\sigma \in \mathfrak{S}_n} (T - \Psi(\alpha_\sigma)) = \prod_{\sigma \in \mathfrak{S}_n} (T - \widetilde{\sigma.\Psi})$$

est le polynôme caractéristique de l'endomorphisme $\Psi(\Theta_1, \ldots, \Theta_n)$ du $\mathcal{R}$-espace vectoriel $\mathcal{R}[x_1, \ldots, x_n]/\mathcal{I}$.

Dans le prochain paragraphe est présenté le calcul de ce polynôme caractéristique proposé par J.M. Arnaudiès. Dans le paragraphe 5 sera présentée une nouvelle méthode de calcul.

## 3. Formule de Poisson-Perron

Notons $x_{n+1}$ une indéterminée supplémentaire. Pour $\Psi \in \mathcal{R}[x_1, \ldots, x_n]$ de degré $d > 0$, l'homogénéisé de $\Psi$, noté $\Psi^*$, est donné par :

$$\Psi^* = x_{n+1}^d \Psi(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}) \qquad .$$

En particulier, $s_i^* = e_i - \tilde{e}_i x_{n+1}^i$.

Nous notons $\mathrm{Res}(g_1, \ldots, g_n)$ le résultant de $n$ polynômes $g_1, \ldots, g_n$ homogènes non constants à $n$ variables.

**Théorème 3.1.** (Arnaudiès) Soit $\Psi \in \mathcal{R}[x_1, \ldots, x_n]$. Alors

$$\chi_\Psi(T) \quad = \quad \mathrm{Res}(s_1^*, \ldots, s_n^*, T x_{n+1}^d - \Psi^*) \qquad .$$

Ce théorème démontré dans [3] se déduit de la formule de Poisson-Perron (voir [2], p. 243).

## 4. Modules de Cauchy

Les résultats de ce paragraphe proviennent de l'article [14].

**4.1. Définition.** Les $n$ fonctions définies par récurrence dans $\mathcal{R}[x]$ :

$$\begin{aligned} f_1(x) &= f(x) \qquad \text{et pour } k = 2, \ldots, n \\ f_k(x) &= f_k(x_1, \ldots, x_{k-1}, x) = \frac{f_{k-1}(x_1, \ldots, x_{k-2}, x) - f_{k-1}(x_1, \ldots, x_{k-1})}{x - x_{k-1}} \end{aligned}$$

sont les *fonctions interpolaires* introduites par Ampère (voir [1]). Rappelons ce théorème (voir [7]) :

**Théorème 4.1.** (Cauchy) Soit $F(x_1, \ldots, x_n)$ un polynôme à coefficients dans $\mathcal{R}$ et symétrique en les variables $x_1, \ldots, x_n$. Pour éliminer $x_n, \ldots, x_1$ dans le polynôme $F$, il suffit de diviser successivement $F$ par les divers termes de la suite $f_n(x_n), \ldots f_2(x_2)$, $f_1(x_1)$, en considérant chaque $f_i$ comme une fonction de $x_i$. Le dernier reste obtenu sera indépendant de $x_1, \ldots, x_n$ et donnera la valeur $F(\alpha_1, \ldots, \alpha_n)$ en fonction des coefficients de $f$.

**Théorème 4.2.** (Machì-Valibouze) Soient $f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)$ les polynômes associés à $f \in \mathcal{R}[x]$ obtenus à partir des fonctions interpolaires. Ces $n$ polynômes, appelés *modules de Cauchy*, forment une base standard réduite de l'idéal $\mathcal{I}$ pour l'ordre lexicographique.

Soient $r$ un entier positif et $s$ un entier compris entre 1 et $n$. Notons $h_r(x_1, \ldots, x_s)$ la $r$-ième *fonction symétrique complète*, c'est-à-dire la somme des monômes de degré total $r$ en $x_1, \ldots, x_s$, avec $h_0(x_1, \ldots, x_s) = 1$.

**Théorème 4.3.** (Machì-Valibouze) Soit le polynôme $f(x) = x^n - \tilde{e_1} x^{n-1} + \tilde{e_2} x^{n-2} + \cdots + (-1)^n \tilde{e_n}$ à coefficients dans $\mathcal{R}$. Alors, pour $0 \leq r < n$, le $(r+1)$-ième module de Cauchy associé à $f$ est donné par :

$$(1) \quad f_{r+1}(x_1, x_2, \ldots, x_r, x_{r+1}) = \sum_{i=0}^{n-r} (-1)^i \tilde{e_i} h_{n-r-i}(x_1, x_2, \ldots, x_r, x_{r+1}) \qquad .$$

En particulier $f_1(x_1) = f(x_1)$ et $f_n(x_1, \ldots, x_n) = e_1 - \tilde{e_1}$.

*Remarque* 1. A. Cauchy donna la formule jusqu'à $n = 4$. Une démonstration simple proposée par A. Lascoux peut-être faite à l'aide des différences divisées (voir [12]).

## 5. Modules de Cauchy et polynôme caractéristique

Soient $u$ et $v$ deux polynômes de $\mathcal{R}[x]$, avec $u(x) = a^m \prod_{i=1}^{m}(x-\beta_i)$ où $\beta_1, \ldots, \beta_m$ appartiennent à une clôture algébrique de $\mathcal{R}$. Le résultant en $x$ des deux polynômes $u$ et $v$, noté $\mathrm{Res}_x(u,v)$, peut s'exprimer ainsi :

$$\mathrm{Res}_x(u,v) = a^{\deg(v)} \prod_{i=1}^{m} v(\beta_i) \qquad . \tag{2}$$

**Théorème 5.1.** Soit $f$ un polynôme unitaire de $\mathcal{R}[x]$ et $f_1, \ldots, f_n$ les modules de Cauchy associés à $f$ (voir le paragraphe 4). Prenons $\Psi \in \mathcal{R}[x_1, \ldots, x_n]$ et définissons la suite finie $R_0, R_1, \ldots, R_{n-1}$ par récurrence :

$$\begin{aligned} R_0(T, x_1, \ldots, x_{n-1}) &= \mathrm{Res}_{x_n}(f_n(x_1, \ldots, x_n), T - \Psi(x_1, \ldots, x_n)) \\ R_i(T, x_1, \ldots, x_{n-(i+1)}) &= \mathrm{Res}_{x_{n-i}}(f_{n-i}(x_1, \ldots, x_{n-i}), R_{i-1}(T, x_1, \ldots, x_{n-i})), \end{aligned} \tag{3}$$

pour $i = 1, \ldots, n-1$. Alors le polynôme caractéristique est donné par

$$\chi_\Psi(T) = R_{n-1}(T) \qquad . \tag{4}$$

*Preuve.* Nous montrons le théorème par récurrence sur $n$, le degré du polynôme $f$. Pour $n = 1$, puisque $f = (x - \alpha_1)$ est unitaire nous avons bien

$$Res_{x_1}(f(x_1), T - \Psi(x_1)) = (T - \Psi(\alpha_1)) = \chi_\Psi(T) \qquad .$$

Montrons-le également pour $n = 2$. Nous avons $f_2(x_1, x_2) = x_1 + x_2 - \tilde{e_1}$ et donc $R_0(T, x_1) = \mathrm{Res}_{x_2}(f_2(x_1, x_2), T - \Psi(x_1, x_2)) = T - \Psi(x_1, \tilde{e_1} - x_1))$. D'où

$$\begin{aligned} R_1(T) &= Res_{x_1}(f(x_1), T - \Psi(x_1, \tilde{e_1} - x_1)) \\ &= (T - \Psi(\alpha_1, \tilde{e_1} - \alpha_1))(T - \Psi(\alpha_2, \tilde{e_1} - \alpha_2)) \\ &= (T - \Psi(\alpha_1, \alpha_2))(T - \Psi(\alpha_2, \alpha_1)) \\ &= \chi_\Psi(T) \qquad . \end{aligned}$$

Supposons désormais que le théorème soit vrai jusqu'à $n-1$ dans tout anneau commutatif unitaire, donc en particulier dans $\mathcal{R}[x_1]$. Ainsi, en posant pour tout $x_1$, $F(x) = f_2(x_1, x)$ et en notant $F_1(x_2), F_2(x_2, x_3), \ldots F_{n-1}(x_2, \ldots, x_n)$ les modules de Cauchy associés à $F$, nous avons $F_{j-1}(x_2, \ldots, x_j) = f_j(x_1, \ldots, x_j)$ pour $j = 2, \ldots, n$. Notons $\beta_2(x_1), \ldots, \beta_n(x_1)$ les $n-1$ racines de $F(x)$ dans une clôture algébrique de $\mathcal{R}[x_1]$. Par hypothèse de récurrence et puisque $F(x)$ est unitaire, nous avons

$$R_{n-2}(T, x_1) = \prod_{\tau \in \mathfrak{S}_{n-1}} (T - \Psi(x_1, \beta_{\tau(2)}(x_1), \ldots, \beta_{\tau(n)}(x_1))) \qquad ,$$

et donc

$$R_{n-1}(T) = \prod_{i=1}^{n} \prod_{\tau \in \mathfrak{S}_{n-1}} (T - \Psi(\alpha_i, \beta_{\tau(2)}(\alpha_i), \ldots, \beta_{\tau(n)}(\alpha_i))) \qquad . \tag{5}$$

Or, pour $i = 1, \ldots, n$, pour $j = 2, \ldots, n$ et pour $\tau \in \mathfrak{S}_{n-1}$, nous savons que $\beta_{\tau(j)}(\alpha_i)$ est une racine de $F(x) = f_2(\alpha_i, x) = \frac{f(\alpha_i) - f(x)}{\alpha_i - x}$ et est donc une racine de $f$ distincte de $\alpha_i$. Ainsi, les $n!$ $n$-uplets $(\alpha_i, \beta_{i_2}(\alpha_i), \dots, \beta_{i_n}(\alpha_i))$ sur lesquels s'évalue $\Psi$ dans le produit (5) sont les $n!$ $n$-uplets $(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ où $\sigma$ parcourt $\mathfrak{S}_n$. Ceci achève la démonstration. $\square$

*Remarque* 2. Si $f$ est unitaire, alors il est facile de voir que $f_i(x_1, \dots, x_i)$ est également unitaire en $x_i$ pour $i = 1, \dots, n$. Dans le cas où $f$ n'est pas unitaire, et où $a$ est son coefficient dominant, il est toujours possible de poser $g(x) = a^{n-1} f(x/a)$ qui, lui, est un polynôme unitaire. Si l'on désire garder $f$, il faut alors introduire le coefficient dominant de $f$ ainsi que ceux des modules de Cauchy $f_2, \dots, f_n$ dans le calcul des résultants successifs.

## 6. Polynômes caractéristiques et résolvantes

Nous allons étudier le lien entre les polynômes caractéristiques et les résolvantes. La résolvante a été introduite par Lagrange pour étudier a priori les polynômes d'une variable (voir [10]). Elle est un outil important de la théorie de Galois algébrique puisqu'elle permet de calculer des polynômes minimaux d'éléments primitifs d'extensions algébriques.

Soit $\Psi \in \mathcal{R}[x_1, \dots, x_n]$. Notons $H$ le groupe constitué des permutations de $\mathfrak{S}_n$ qui laissent le polynôme $\Psi$ invariant. C'est-à-dire

$$H = \{\tau \in \mathfrak{S}_n \mid \tau.\Psi = \Psi\} \qquad .$$

On dit alors que $\Psi$ est un *invariant primitif de $H$ relatif à $\mathfrak{S}_n$*. Par exemple, si $\Psi = x_1 + x_2$, alors $H = \mathfrak{S}_2 \times \mathfrak{S}_{n-2}$.

Alors, *la résolvante de $f$ par $\Psi$*, notée $\mathcal{L}_{\Psi,f}$, est définie comme suit :

$$\mathcal{L}_{\Psi,f}(T) = \prod_{\Theta \in \mathfrak{S}_n . \Psi} (T - \tilde{\Theta}) \qquad . \tag{6}$$

Soit $\mathcal{T}$ une transversale gauche de $\mathfrak{S}_n$ modulo $H$. Pour tout $\tau \in \mathcal{T}$ et pour tout $h \in H$, on a $\tau.\Psi = \tau h.\Psi$ et si $\sigma \in \mathcal{T}$ avec $\sigma \neq \tau$, alors $\sigma.\Psi \neq \tau.\Psi$. Donc, nous avons les deux identités suivantes (voir [4]) :

$$\begin{aligned} \mathcal{L}_{\Psi,f}(T) &= \prod_{\tau \in \mathcal{T}} (T - \Psi(\alpha_{\tau(1)}, \dots, \alpha_{\tau(n)}) \qquad \text{et} \\ \chi_\Psi(T) &= \mathcal{L}_{\Psi,f}^{|H|}(T) \qquad . \end{aligned} \tag{7}$$

Voici, traduit en terme de résultants, une méthode proposée par Lagrange pour calculer des résolvantes (voir [10]) :

Soit $U_0(T, x_1, \dots, x_{n-1}) = Res_{x_n}(f(x_n), T - \Psi(x_1, \dots, x_n))$ et, par récurrence sur $k = 1, \dots, n-1$, $U_k(T, x_1, \dots, x_{n-k-1}) = Res_{x_{n-k}}(f(x_{n-k}), U_{k-1}(T, x_1, \dots, x_{n-k}))$. Alors, d'après (2) et puisque $f$ est unitaire :

$$U_{n-1}(T) = \prod_{i_1=1}^{n} \prod_{i_2=1}^{n} \cdots \prod_{i_n=1}^{n} (T - \Psi(\alpha_{i_1}, \dots, \alpha_{i_n})) \qquad . \tag{8}$$

Nous voyons que dans cette formule ne sont pas exclues les égalités deux à deux, trois à trois, ... , $n$ à $n$ des indices apparaissant dans les produits et que, par conséquent, $U_{n-1}$ comporte des facteurs parasites déjà signalés par Lagrange. Ce sont ces facteurs parasites qu'évite la suite $R_{n-1}$, obtenue à partir des modules de Cauchy (voir le Théorème 5.1). Par exemple, si $\Psi = x_1 + 2x_2$ et n=2, alors

$$U_1(T) = (T - 3\alpha_1)(T - 3\alpha_2)\,\mathcal{L}_{\Psi,f} \qquad \text{et} \qquad R_1(T) = \mathcal{L}_{\Psi,f} \qquad .$$

Lagrange signalait également des puissances parasites provenant des symétries de la fonction $\Psi$, que nous retrouvons dans la formule (7). Il est possible de neutraliser des symétries dans le cas où l'arité de $\Psi$ est différente de $n$ (voir le paragraphe 7). Dans les autres cas, il est possible d'en éliminer en cours de calcul (voir paragraphe 8).

Toutes ces constatations sur les symétries furent faites en parallèle par Frédéric Lehobey qui calcule des résolvantes avec une méthode duale de celle présentée ici. Cette méthode est abordée dans [13].

## 7. Arité et symétries

Soit $\Psi \in \mathcal{R}[x_1, \dots, x_n]$. Si $m$ est le plus petit entier $j$ tel qu'il existe $j$ entiers distincts $i_1, \dots, i_j$ tels que $\Psi \in \mathcal{R}[x_{i_1}, \dots, x_{i_j}]$, alors $\Psi$ est dit d'*arité* $m$.

Soit donc $\Psi \in \mathcal{R}[x_1, \dots, x_n]$ d'arité $m$. Par injection canonique, il est possible de supposer (en renumérotant les variables) que $\Psi \in \mathcal{R}[x_1, \dots, x_m]$. Le sous-groupe $H$ de $\mathfrak{S}_n$ laissant $\Psi$ invariant est nécessairement de la forme $K \times \mathfrak{S}_{n-m}$, où $K$ est un sous-groupe de $\mathfrak{S}_m$.

Dans ce cas, la méthode de Lagrange consiste à modifier la suite finie $(U_j)$ en posant $U_{n-m} = Res_{x_m}(f(x_m), T - \Psi(x_1, \dots, x_m))$ et en conservant la récurrence jusqu'à $U_{n-1}$.

Pour la méthode utilisant les modules de Cauchy, nous modifions, de même, la suite finie $(R_j)$ comme suit (pour $j \in [1, m]$) :

$$V_{n-(m+1)}(T, x_1, \dots, x_m) \quad = \quad T - \Psi(x_1, \dots, x_m), \tag{9}$$

$$V_{n-j}(T, x_1, \dots, x_{j-1}) \quad = \quad \mathrm{Res}_{x_j}(f_j(x_1, \dots, x_j), V_{n-j-1}(T, x_1, \dots, x_j)). \tag{10}$$

Il en découle naturellement l'identité suivante :

$$R_{n-j} = V_{n-j}^{(n-m)!} \qquad , \tag{11}$$

pour $j = m{+}1, \dots, 1$. Pour le voir, il suffit de constater que c'est vrai pour $j = m{+}1$ et d'utiliser l'identité $\mathrm{Res}_x(g(x), h(x)k(x)) = \mathrm{Res}_x(g(x), h(x))\mathrm{Res}_x(g(x), k(x))$, pour tous polynômes $g, h, k$.

Nous en déduisons les deux identités suivantes :

$$\chi_\Psi(T) = V_{n-1}(T)^{(n-m)!} \qquad \text{et} \tag{12}$$

$$V_{n-1}(T) = \mathcal{L}_{\Psi,f}(T)^{|K|} \qquad . \tag{13}$$

*Remarque* 3. L'arité est également utilisée pour accélérer les calculs de résolvantes dans la méthode basée sur les polynômes symétriques (voir [20]).

## 8. Éliminations successives de symétries

Dans la pratique, le calcul de $\mathcal{L}_{\Psi,f}(T)$ ne se réalise pas sans éliminer au fur et à mesure les puissances parasites dues aux symétries du polynôme $\Psi$ (voir (13)) . Nous allons illustrer ceci à travers deux exemples :

*Exemple* 1. Choisissons $\Psi = x_1 + x_2 + x_3$ un invariant primitif de $K = \mathfrak{S}_3$ relatif à $\mathfrak{S}_3$. Nous avons

$$V_{n-2}(T, x_1) = \mathrm{Res}_{x_2}(f_2(x_1, x_2), Res_{x_3}(f_3(x_1, x_2, x_3), T - (x_1 + x_2 + x_3))) \quad .$$

Il est alors possible d'éliminer des symétries à ce niveau puisque :

$$\begin{aligned} V_{n-2}(T, x_1) &= \prod_{i=2}^{n-1} \prod_{j \in I(i)} (T - (x_1 + \beta_i(x_1) + \beta_j(x_1))) \\ &= \prod_{i=2}^{n} \prod_{2 \leq j < i} (T - (x_1 + \beta_i(x_1) + \beta_j(x_1)))^2 = W_{n-2}(T, x_1)^2 \quad . \end{aligned}$$

où $I(i) = \{j \in [2, n] \mid j \neq i\}$ et $\beta_2(x_1), \ldots, \beta_n(x_1)$ sont les racines de $f_2(x_1, x)$. Posons $W_{n-1}(T) = \mathrm{Res}_{x_1}(f_1(x_1), W_{n-2}(T, x_1))$, alors

$$W_{n-1}(T) = \prod_{r=1}^{n} \prod_{i=2}^{n} \prod_{2 \leq j < i} (T - (\alpha_r + \beta_i(\alpha_r) + \beta_j(\alpha_r))) \quad .$$

Ainsi, comme pour $r = 1, \ldots, n$, le facteur $(T - (\alpha_r + \alpha_i + \alpha_j))$ est obtenu 3 fois avec $(T - (\alpha_r + \beta_i(\alpha_r) + \beta_j(\alpha_r))$, $(T - (\alpha_i + \beta_r(\alpha_i) + \beta_j(\alpha_i))$ et $(T - (\alpha_j + \beta_i(\alpha_j) + \beta_r(\alpha_j))$, il vient :

$$W_{n-1}(T) = \mathcal{L}_{\Psi,f}(T)^3 \quad . \tag{14}$$

Avec la formule (13), nous constatons que nous obtenons la résolvante cherchée à la puissance 3 à la place de la puissance $6 = |K|$.

*Exemple* 2. Si $\Psi = 2x_1 + x_2 + x_3$, alors de même, nous calculons $W_{n-2}(T, x_1)$, tel que $V_{n-2}(T, x_1) = W_{n-2}(T, x_1)^2$ et nous avons finalement :

$$\mathcal{L}_{\Psi,f}(T) = \mathrm{Res}_{x_1}(f_1(x_1), W_{n-2}(T, x_1)) \quad .$$

Cet exemple permet de voir qu'il est préférable d'éliminer d'abord les symétries. Nous constatons que nous obtenons la résolvante au lieu de son carré donné par la formule (13).

## 9. Autres améliorations et autres méthodes

L'interpolation permet de remplacer la variable $T$ par un entier et le théorème des restes chinois permet de réaliser les calculs modulairement (voir [16]).

D'autres méthodes permettent de calculer les résolvantes. Certaines sont basées sur des séries génératrices (voir [6]) ou sur des manipulations de polynômes symétriques (voir [11] et [18]). Les résultants permettent également de calculer très rapidement certaines résolvantes (voir [5]). K.Girstmair propose l'interpolation sur les variables $x_1, \ldots, x_n$ (voir [9]). Une méthode ancienne utilise les invariants (voir, par exemple, [17]).

## 10. Généralisation aux multi-résolvantes

Soient $f = (f^{(1)}, \ldots, f^{(p)})$ un $p$-uplet de polynômes de $\mathcal{R}[x]$ de degrés respectifs $d_1, \ldots, d_p$ et posons $d = d_1 + \cdots + d_p$. Donnons-nous $x_1, \ldots, x_d$ des indéterminées.

Pour tout $\Theta \in \mathcal{R}[x_1, \ldots, x_d]$, nous noterons $\tilde{\Theta}$ une évaluation de $\Theta$ telle que, pour $i \in [1, p]$, les $d_i$ variables $x_{d_1+\cdots+d_{i-1}+1}, \ldots, x_{d_1+\cdots+d_i}$ s'évaluent en les $d_i$ racines du polynôme $f^{(i)}$ et ce pour un choix d'évaluation quelconque fixé une fois pour toutes.

Fixons $\Psi \in \mathcal{R}[x_1, \ldots, x_d]$. Soit $\mathcal{S} = \mathfrak{S}_{d_1} \times \cdots \times \mathfrak{S}_{d_p}$, comme pour le cas $d = 1$, nous notons $\mathcal{S}.\Psi$ l'orbite de $\Psi$ sous l'action de $\mathcal{S}$ en faisant agir chaque $\mathfrak{S}_{d_i}$ sur les $d_i$ variables $x_{d_1+\cdots+d_{i-1}+1}, \ldots, x_{d_1+\cdots+d_i}$ de $\Psi$.

*Exemple* 3. Prenons $d_1 = 2$ et $d_2 = 3$ et notons $y_1 = x_3, y_2 = x_4$ et $y_3 = x_5$ pour faciliter la lisibilité. Pour $\Psi = x_1y_1 + x_2y_2^3$, nous avons

$$\begin{aligned}\mathcal{S}.\Psi \quad = \quad & \{x_1y_1 + x_2y_2^3\,, x_1y_2 + x_2y_1^3\,, x_1y_1 + x_2y_3^3\,, x_1y_3 + x_2y_1^3\,, x_1y_2 + x_2y_3^3\,,\\ & x_1y_3 + x_2y_2^3\,, x_2y_1 + x_1y_2^3\,, x_2y_2 + x_1y_1^3\,, x_2y_1 + x_1y_3^3\,, x_2y_3 + x_1y_1^3\,,\\ & x_2y_2 + x_1y_3^3\,, x_2y_3 + x_1y_2^3\} \qquad .\end{aligned}$$

Pour tout entier $i > 0$, notons $Id_i$ le sous-groupe identité de $\mathfrak{S}_i$. Le cardinal de l'orbite $\mathcal{S}.\Psi$ est $2 \times 6 = 12$, puisque le stabilisateur de $\Psi$ dans $\mathcal{S} = \mathfrak{S}_2 \times \mathfrak{S}_3$ est $Id_2 \times Id_3$ et que $Id_i$ est d'indice $i!$ dans $\mathfrak{S}_i$.

*Exemple* 4. Pour $\Theta = x_1y_1 + 4y_2 + 4y_3$, nous avons

$$\begin{aligned}\mathcal{S}.\Theta \quad = \quad & \{x_1y_1 + 4y_2 + 4y_3\,, x_1y_2 + 4y_1 + 4y_3, x_1y_3 + 4y_2 + 4y_1\,,\\ & x_2y_1 + 4y_2 + 4y_3\,, x_2y_2 + 4y_1 + 4y_3\,, x_2y_3 + 4y_2 + 4y_1\} \qquad .\end{aligned}$$

Le cardinal de cette orbite est $2 \times 3 = 6$, puisque le stabilisateur de $\Theta$ dans $\mathcal{S}$ est $Id_2 \times (\mathfrak{S}_1 \times \mathfrak{S}_2)$. L'indice de $\mathfrak{S}_1 \times \mathfrak{S}_2$ dans $\mathfrak{S}_3$ est 3.

La *multi-résolvante* de $f$ par $\Psi$ est le polynôme :

$$\mathcal{L}_{\Psi,f}(y) = \prod_{\Theta \in \mathcal{S}.\Psi} (y - \tilde{\Theta}) \qquad .$$

Pour calculer une multi-résolvante, il suffit d'utiliser les algorithmes de calcul des résolvantes conçus pour des invariants avec des coefficients non numériques (i.e. l'anneau $R$ n'est pas nécessairement l'anneau des entiers $\mathbb{Z}$ ou le corps $\mathbb{Q}$). En ce cas l'invariant $\Psi$ est considéré successivement comme un polynôme en $x_1, \ldots, x_{d_1}$, puis en $x_{d_1+1},\ldots,x_{d_1+d_2},\ldots$ puis enfin en $x_{d_1+\cdots+d_{p-1}+1},\ldots,x_d$ et il s'agit de calculer une résolvante à chaque étape. Cela se réalise aisément lorsque la résolvante se calcule avec des polynômes symétriques (voir [18]). Voyons sur des exemples comment ce calcul est réalisé avec la méthode proposée dans cet article :

*Exemple* 5. Reprenons les exemples 3 et 4. Nous considérons d'abord $\Psi = x_1y_1 + x_2y_2^3$ comme un polynôme en $x_1, x_2$. Posons $f^{(1)} = f$ et $f^{(2)} = g$. Notons $f_i$ les modules de Cauchy de $f$ et $g_i$ ceux de $g$. Soient

$$V_{n-2}(T, x_1, y_1, y_2) = Res_{x_2}(f_2(x_1, x_2), T - (x_1y_1 + x_2y_2^3)) \text{ et}$$

$$V_{n-1}(T, y_1, y_2) = Res_{x_1}(f(x_1), V_{n-2}(T, x_1)) \qquad .$$

Puis

$$V'_{n-2}(T, y_1) = Res_{y_2}(g_2(x_1, x_2), V_{n-1}(T, y_1, y_2)) \qquad et$$

$$V'_{n-1}(T) = Res_{y_1}(g(x_1), V'_{n-2}(T, y_1)) \qquad .$$

Comme il n'y a pas de symétrie, nous avons directement :

$$\mathcal{L}_{\Psi,(f,g)} = V'_{n-1} \qquad .$$

Faisons de même avec $\Theta = x_1y_1 + 4y_2 + 4y_3$. $V_{n-1}(T) = Res_{x_1}(f(x_1), T - (x_1y_1 + 4y_2 + 4y_3))$, puis

$$V'_{n-3}(T, y_1, y_2) = Res_{y_3}(g_3(x_1, x_2, x_3), V_{n-1}(T, y_1, y_2, y_3)),$$

$$V'_{n-2}(T, y_1) = Res_{y_2}(g_2(x_1, x_2), V'_{n-3}(T, y_1, y_2)) = W_{n-2}(T, y_1)^2$$

et enfin $V'_{n-1}(T) = Res_{y_1}(g(x_1), W_{n-2}(T, y_1))$. La seule symétrie étant retirée en cours de calcul, nous avons donc

$$\mathcal{L}_{\Theta,(f,g)} = V'_{n-1} \qquad .$$

## 11. Programmation en MACSYMA

Le module `SYM` de `MACSYMA` (voir [19] et [15]) est une extension de `MACSYMA` qui manipule des polynômes symétriques et calcule des résolvantes. Les fonctions ci-dessous seront désormais incorporées dans `SYM`.

**11.1. Calcul des modules de Cauchy.** Soit `fs_complete(degre,arite,vars)` la fonction de `SYM` qui calcule la `degre`-ième fonction complète sur les `arite` premières variables contenues dans la liste `vars`.

La fonction `cauchy_modules(f,x,vars)` calcule en `MACSYMA` les $m$=`length(vars)` premiers module de Cauchy $f_1(x_1),\ldots,f_m(x_1,\ldots,x_m)$ où les variables $x_1,\ldots,x_m$ sont les éléments de la liste `vars`.

```
cauchy_modules(f,x,vars):=
   block([degref,modules,coeffs],
         degref:hipow(f,x),
         if not(coeff(f,x,degref)=1) then f:f/coeff(f,x,degref),
         coeffs:makelist(coeff(f,x,i),i,0,degref),
         modules:[ev(f,x=first(vars))],
         For r:1 thru length(vars)-1 do
            modules:cons(sum(coeffs[j+1]*fs_complete(j-r,r+1,vars),
                              j,r,degref),
                         modules),
         modules)$
```

Vérifions que l'on retrouve bien les formules données par Cauchy en degré 4 :

```
(C40) cauchy_modules(x^4+a3*x^3+a2*x^2+a1*x+a0,x,[x1,x2,x3,x4]);
                                   2                                   2
(D40) [X4 + X3 + X2 + X1 + A3, X3  + A3 (X3 + X2 + X1) + X2 X3 + X1 X3 + X2

            2         3         2             2         2
 + X1 X2 + X1  + A2, X2  + A3 (X2  + X1 X2 + X1 ) + X1 X2  + A2 (X2 + X1)

     2        3          4        3         2
 + X1  X2 + X1  + A1, X1  + A3 X1  + A2 X1  + A1 X1 + A0]

(C41) fs_complete(3,2,[x1,x2,x3]);
                             3        2     2       3
(D41)                      X2  + X1 X2  + X1  X2 + X1
```

**11.2. Calcul des résolvantes.** Afin de simplifier la présentation nous donnons un programme dans lequel les symétries ne sont pas éliminées en cours de calcul. La variable `invariant` représente l'invariant $\Psi$ d'arité $m$. Les $m$ variables dont dépend $\Psi$ sont données dans la liste `vars`. La fonction `resolvante` calcule $\mathcal{L}_{\Psi,f}(y)^{|H|}$, où $H$ est le stabilisateur de $\Psi$ dans $\mathfrak{S}_m$.

```
resolvante(f,x,invariant,vars,y):=
      resolvante2(cauchy_modules(f,x,vars),
                  reverse(vars),
                  y-invariant)$

resolvante2(modules,rvars,sol):=
     if length(modules)=0 then sol
        else resolvante2(rest(modules),
                         rest(rvars),
                         resultant(first(modules),
                                   sol,
                                   first(rvars)))$
```

## 12. Comparaisons de temps

L'extension `SYM` de `MACSYMA` comporte différentes fonctions permettant de calculer des résolvantes. La plupart s'appuient sur des formules permettant d'appliquer le théorème fondamental des polynômes symétriques (voir [18]).

Notons $\delta_k$, le déterminant de Vandermond : $\delta_k = \prod_{1\leq i<j\leq i}(x_i - x_j)$. Un invariant $\Psi \in k[x_1, \ldots, x_n]$ est dit *linéaire* s'il s'exprime comme une combinaison linéaire de $x_1, \ldots, x_n$, il est dit *monomial*, s'il s'exprime comme un monôme en $x_1, x_2 \ldots, x_n$.

Les comparaisons réalisées entre la méthode avec les modules de Cauchy, proposée ici, et celle fondée sur les polynômes symétriques permettent de conclure que la méthode avec les modules de Cauchy est moins efficace avec des invariants monomiaux et qu'elle est plus efficace avec les invariants linéaires ou avec les invariants $\delta_i$ (sauf dans le cas où $i = n - 1$ avec $n =$deg$(f)$). Par exemple, pour les invariants linéaires ne comportant aucune symétrie, le gain est d'au moins un facteur 20.

## References


1. Ampère, M. 1826. Fonctions interpolaires. *Annales de M.Gergonne*
2. J.-M. Arnaudiès **Elimination** Thèse de l'Université P. Sabatier de Toulouse, 1989, à paraître dans Adv. in Math.
3. J.-M. Arnaudiès *Théorème de Bézout, Formule de Poisson-Perron et Courbes Rationnelles Planes Génériques*, Rapport interne LITP **92-24**, 1992
4. J.-M. Arnaudiès, A. Valibouze *Résolvantes de Lagrange*, Conférence MEGA'96 (Eindhoven June'96) (Rapport LITP 93.61 )
5. J.-M. Arnaudiès, A. Valibouze *Partial Computation for special Resolvents* proposed to Math. Comp.
6. Casperson, D., McKay, J.: *Symmetric functions, m-sets, and Galois groups* Math. Comp., 1994
7. Cauchy, A. *Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée.* Oeuvre Volume **5** p.473 extrait 108.
8. I. Gil-Delessalle, A. Valibouze, (1996), *Galois inverse problem for some subgroups of degree 12*, proposé à MEGA'96
9. Girstmair, *On the Computation of Résolvents and Galois groups* Manuscripta Mathematica **43** , 1983, P.289-307
10. Lagrange, J.L., *Réflexions sur la résolution algébrique des équations*, **Mémoires de l'Académie de Berlin**, 205-421, (**Oeuvres de Lagrange**, tome IV, 205-421)
11. Lagrange, J.L., *Traité de la résolution des équations numériques : Notes sur la théorie des équations algébriques*, Oeuvres de Lagrange , Tome VIII, 133-367
12. A. Lascoux, P.Pragaz (1988) *S-function series*, J. Phys.A : Math. Gen. bf 21, 4105-4114.
13. F. Lehobey(1994), *Algorithmique Methods and Practical Issues in the Computation of Galois Group of Polynomials*, Mémoire de DEA, Univ. Rennes.
14. A. Machì, A. Valibouze, (1991), *L'idéal des relations symétriques et l'idéal des relations* prépublication
15. Maxima DOE maintenu par William Schelter
16. Leonard Soicher, *The computation of the Galois groups*, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).

17. E.H. Berwick , (1929) *On Soluble Sextic equations* Proc. London Math. Soc. (2) **29**, 1-28.
18. A. Valibouze, (1988), *Manipulations de fonctions symétriques*, Thèse de l'Université Paris VI.
19. Valibouze A. (1993) **Extension `SYM` de `MACSYMA`, manuel de l'utilisateur**
20. A. Valibouze (1992) *Sur l'arité des fonctions*, European Journal of Combinatorics, 1993, **14**, 359-372
21. A. Valibouze, (1995) *Computation of the Galois group of the Resolvent Factors for the Direct and Inverse Galois Problems*, Conference AAECC'95, (Paris, Juillet 1995), LNCS **948**

L.I.T.P., Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05
*E-mail address*: avb@medicis.polytechnique.fr