Calcul de résolvantes avec les modules de Cauchy

Nicolas Rennert et Annick Valibouze

TABLE DES MATIÈRES

Les auteurs remercient le projet GALOIS du GDR de Calcul Formel MEDICIS.

Cet article décrit un algorithme nouveau et efficace pour calculer des polynômes caractéristiques d'endomorphismes dans un algèbre quotient en utilisant les modules de Cauchy. Cet algorithme est ensuite utilisé pour calculer des résolvantes et des multi-résolvantes absolues, outils de base de la théorie des corps et donc aussi de la théorie de Galois constructive.

We give a new and efficient algorithm to compute some characteristic polynomials using Cauchy modules. This algorithm is used for the computation of absolute resolvents and multi-resolvents which are essential tools in constructive Galois theory.

1. INTRODUCTION

La résolvante est l'outil de base de la théorie de Galois effective dont le calcul à la main s'avère vite impossible. Ainsi, chercher à diminuer le temps consacré à son calcul améliore celui du calcul du groupe de Galois d'un polynôme. Historiquement les premiers à réaliser de tels calculs à l'aide de l'outil informatique, furent R. P. Stauduhar [1973] et K. Girstmair [1983] utilisant pour le premier une méthode basée sur des calculs numériques. Bien que le résultat ne soit pas certifié, cette méthode s'avère être la plus rapide dans le cas général. Le logiciel GALP [Eichenlaub et Olivier 1996] basée sur la librairie PARI/GP, utilise ces techniques pour déterminer le groupe de Galois de polynômes.

Les méthodes algébriques ont en revanche l'avantage d'être exactes. Parmi elles, les méthodes basées sur les fonctions symétriques s'avèrent efficaces pour des invariants particuliers ; voir [Valibouze 1989]. Cet article s'intéresse aux algorithmes qui calculent des résolvantes pour un invariant quelconque et qui sont basés sur l'opération de résultant.

Le résultant est un outil particulièrement puissant pour manipuler algébriquement les racines de polynômes qui depuis Lagrange a servi pour le calcul de la résolvante ; voir [Lagrange 1770]. Le premier qui

1058-6458/1999 $0.50 per page

sur machine a utilisé le résultant pour le calcul de résolvantes (absolues) est L. H. Soicher [1984] pour des invariants linéaires.

Jusqu'à présent les méthodes basées sur le résultant pour calculer la résolvante (absolue) se heurtaient à deux défauts : apparition de facteurs et de puissances "parasites" qui augmentent considérablement la taille des polynômes nécessaires et réduisent donc l'efficacité. Cet article présente un algorithme simple et rapide (voir théorème 4.7) qui calcule, sans formation de facteurs parasites, le polynôme caractéristique d'un endomorphisme multiplicatif associé à un invariant quelconque donné. Le polynôme caractéristique est une puissance de la résolvante pour ce même invariant. Ainsi le problème des facteurs "parasites" est résolu, reste encore celui de la puissance "parasite". L'algorithme proposé utilise essentiellement le résultant et les modules de Cauchy qui forment une base de Gröbner réduite de l'idéal des relations symétriques (pour l'ordre lexicographique). Si les calculs du théorème 4.7 sont réalisés modulo l'idéal des relations symétriques alors la puissances à laquelle nous obtenons la résolvante est réduite et les calculs intermédiaires accélérés. Si les calculs modulaires n'aboutissent pas à la résolvantes mais à une puissance strictement positive (ce qui est prévisible *a priori* alors nous utilisons alors le résultat de F. Lehobey [1997] pour éliminer ces puissances en cours de calcul (ce travail fait référence aux résultats de article). Ainsi le problème de la puissance parasite est également résolu (voir algo 6.10).

Dans le paragraphe 7 l'algorithme de calcul des résolvantes est naturellement généralisé au cas des multi-résolvantes — c'est-à-dire les résolvantes relatives à un produit de groupes symétriques. Les derniers paragraphes sont consacrés à l'implantation de cette méthode, la comparaison avec d'autres algorithmes algébriques ainsi que des améliorations.

2. NOTATIONS ET DÉFINITIONS

- $\mathcal{K}$ désigne un corps de caractéristique 0 ;
- x est une variable indéterminée sur $\mathcal{K}$;
- f est un polynôme unitaire de $\mathcal{K}[x]$ de degré n ;
- $x_1, \ldots, x_n$ sont des variables indéterminées sur $\mathcal{K}$;
- $\mathcal{K}[x_1, \ldots, x_n]$ désigne l'anneau des polynômes en les variables $x_1, \ldots, x_n$ et à coefficients dans $\mathcal{K}$;
- $\mathcal{K}(x_1, \ldots, x_n)$ désigne le corps des fractions de $\mathcal{K}[x_1, \ldots, x_n]$;
- Ψ est un polynôme appartenant à $\mathcal{K}[x_1, \ldots, x_n]$;
- $\alpha = (\alpha_1, \ldots, \alpha_n)$ est une liste (ordonnée) formée des n racines du polynôme f dans une clôture algébrique $\hat{\mathcal{K}}$ de $\mathcal{K}$;
- $\Psi(\alpha) = \Psi(\alpha_1, \ldots, \alpha_n)$;
- $\mathfrak{S}_n$ désigne le groupe symétrique de degré n.

Definition 2.1. Le polynôme Ψ est dit d'*arité* m si m est le plus petit entier j tel qu'il existe j entiers distincts $i_1, \ldots, i_j$ vérifiant $\Psi \in \mathcal{K}[x_{i_1}, \ldots, x_{i_j}]$.

Definition 2.2. Si $\Psi(\alpha) = 0$ alors Ψ est appelée une *α-relation.*

Definition 2.3. L'action du groupe symétrique $\mathfrak{S}_n$ sur Ψ est définie par :

$$\tau.\Psi = \Psi(x_{\tau(1)}, \ldots, x_{\tau(n)}) \text{ pour tout } \tau \in \mathfrak{S}_n.$$

Definition 2.4. L'action du groupe symétrique $\mathfrak{S}_n$ sur $\hat{\mathcal{K}}^n$ est définie, pour tout $\sigma \in \mathfrak{S}_n$ et tout

$$\beta = (\beta_1, \ldots, \beta_n) \in \hat{\mathcal{K}}^n,$$

par $\beta_\sigma = (\beta_{\sigma(1)}, \beta_{\sigma(2)}, \ldots, \beta_{\sigma(n)})$.

Definition 2.5. *L'orbite de Ψ sous l'action d'un sous-groupe L de $\mathfrak{S}_n$*, notée $L.\Psi$, est définie par :

$$L.\Psi = \{\tau.\Psi \mid \tau \in L\}$$

Definition 2.6. Soient L et H deux sous-groupes de $\mathfrak{S}_n$ tels que L contienne H. Le polynôme Ψ est dit *L-primitif H-invariant* si H est le stabilisateur de Ψ dans L :

$$H = \mathrm{Stab}_L(\Psi) = \{\tau \in L \mid \tau.\Psi = \Psi\}.$$

Lorsque $L = \mathfrak{S}_n$, l'invariant Ψ est dit également *H-invariant primitif.*

Exemple 2.7. Soit $H = \mathfrak{S}_2 \times \mathfrak{S}_{n-2}$. Le polynôme $\Psi = x_1 + x_2$ est un $\mathfrak{S}_n$-primitif H-invariant.

Definition 2.8. Soient deux sous-groupes L et H du groupe symétrique $\mathfrak{S}_n$ tels que L contienne H. On appelera l'ensemble $\{\tau_1, \ldots, \tau_e\}$ une *transversale à gauche de L* mod H si $\tau_1 H, \ldots, \tau_e H$ sont les différentes classes à gauches de L mod H.

Definition 2.9. Pour $i = 0, \ldots, n$, la i-ième *fonction symétrique élémentaire en $x_1, \ldots, x_n$*, notée e_i, est définie par $e_0 = 1$ et

$$e_i = \sum_{m \in \mathfrak{S}_n.(x_1 \cdots x_i)} m \quad \text{pour } i \geq 1.$$

Remarque 2.10. Rappelons que

$$f(x) = x^n - e_1(\alpha)x^{n-1} + e_2(\alpha)x^{n-2} + \cdots + (-1)^n e_n(\alpha).$$

Definition 2.11. Les n *fonctions interpolaires* introduites par Ampère [1826] vérifient :

$$f_i \in \mathcal{K}[x_{i+1}, \ldots, x_n][x] \qquad \text{et} \qquad \deg_x(f_i) = i$$

et sont définies par $f_n(x) = f(x)$ et

$$f_i(x) = f_i(x, x_{i+1}, \ldots, x_n) = \frac{f_{i+1}(x) - f_{i+1}(x_{i+1})}{x - x_{i+1}}$$

pour $n - 1 \geq i \geq 1$.

Definition 2.12. Les polynômes $f_1(x_1)$, $f_2(x_2)$, $\ldots$, $f_n(x_n)$ sont appelés les *modules de Cauchy* associés au polynôme f.

Definition 2.13. Soit L un sous-groupe du groupe symétrique $\mathfrak{S}_n$. L'idéal

$$I_\alpha^L = \{r \in \mathcal{K}[x_1, \ldots, x_n] \mid (\forall \sigma \in L)\ (\sigma.r)(\alpha) = 0\}$$

est un idéal radical appelé *idéal des α-relations invariantes par L.*

Definition 2.14. L'idéal $I_\alpha^{\mathfrak{S}_n}$, noté $\mathcal{I}$, est connu sous le nom d'*idéal des relations symétriques entre les racines du polynôme f.*

Definition 2.15. Soit I_n le groupe identité dans $\mathfrak{S}_n$. L'idéal $I_\alpha^{I_n}$, noté I_α, est connu sous le nom d'*idéal des α-relations.*

Remarque 2.16. Le quotient $\mathcal{K}[x_1, \ldots, x_n]/\mathcal{I}$ est appelé *algèbre de décomposition universelle.*

Definition 2.17. Le sous-groupe G_α du groupe symétrique $\mathfrak{S}_n$ défini par

$$G_\alpha = \{\sigma \in \mathfrak{S}_n \mid (\forall r \in \mathcal{I}_\alpha)\ (\sigma.r)(\alpha) = 0\}$$

est connu abusivement sous le nom de *groupe de Galois de f*. On le nommera groupe de Galois de α.

Notation 2.18. Soit I un idéal de $\mathcal{K}[x_1, \ldots, x_n]$. Pour $\Theta \in \mathcal{K}[x_1, \ldots, x_n]$ notons $\hat{\Theta}$ la multiplication par la classe de Θ dans l'anneau quotient $\mathcal{K}[x_1, \ldots, x_n]/I$. C'est un endomorphisme du $\mathcal{K}$-espace vectoriel

$$\mathcal{K}[x_1, \ldots, x_n]/I.$$

Le polynôme caractéristique de l'endomorphisme $\hat{\Theta}$ sera noté $\chi_{\Theta,I}$. Si $I = \mathcal{I}$ alors il sera noté simplement χ_Θ.

Definition 2.19. Soit L un sous-groupe du groupe symétrique $\mathfrak{S}_n$ tel que L contienne le groupe de Galois G_α du polynôme f. La *L-relative résolvante de f par Ψ* (associée à la numérotation α), notée $\mathcal{L}_{\Psi,L,\alpha}$, est le polynôme de $\mathcal{K}[T]$ défini comme suit :

$$\mathcal{L}_{\Psi,L,\alpha}(T) = \prod_{\Theta \in L.\Psi} (T - \Theta(\alpha)).$$

Si $L = \mathfrak{S}_n$, la résolvante est notée $\mathcal{L}_{\Psi,f}$ et appelée *résolvante (absolue) de f par Ψ.*

Comme le groupe L contient le groupe de Galois G_α et que le corps $\mathcal{K}$ est parfait, par la théorie de Galois, la résolvante appartient bien au corps $\mathcal{K}[T]$.

3. POLYNÔMES CARACTÉRISTIQUES ET RÉSOLVANTES

Dans ce paragraphe, le polynôme f est supposé séparable (ses racines sont distinctes deux à deux) et L désigne un sous-groupe de $\mathfrak{S}_n$ qui contient le groupe de Galois G_α.

Proposition 3.1. *La variété de l'idéal I_α^L dans une clôture algébriques de $\mathcal{K}$, notée $V(I_\alpha^L)$, est l'orbite de la liste α sous l'action du groupe L :*

$$V(I_\alpha^L) = \{\alpha_\sigma \mid \sigma \in L\}.$$

Comme le polynôme f est séparable, le cardinal de cette variété est celui du groupe L.

Démonstration. La preuve est simple. Voir [Valibouze 1999]. □

Pour un idéal I radical, le théorème de Stickelberger donne cette expression explicite du polynôme caractéristique de l'endomorphisme $\hat{\Psi}$ associé à un idéal I (voir notation 2.18) :

$$\chi_{\Psi,I}(T) = \prod_{\beta \in V(I)} (T - \Psi(\beta)).$$

Comme l'idéal I_α^L est radical et que le polynôme f est séparable, il vient :

$$\chi_{\Psi,I_\alpha^L}(T) = \prod_{\sigma \in L} (T - (\sigma.\Psi)(\alpha)).$$

En particulier pour $I = \mathcal{I}$, l'idéal des relations symétriques, on a :

$$\chi_\Psi(T) = \prod_{\sigma \in \mathfrak{S}_n} (T - (\sigma.\Psi)(\alpha)). \tag{3–1}$$

Soient H un sous-groupe du groupe L et $\mathcal{T}$ une transversale à gauche de L mod H. Si Ψ est un L-primitif H-invariant nous avons l'identité suivante bien connue :

$$\mathcal{L}_{\Psi,L,\alpha}(T) = \prod_{\tau\in\mathcal{T}} (T - (\tau.\Psi)(\alpha)).$$

En effet, pour tout $\tau \in \mathcal{T}$ et pour tout $h \in H$, on a $\tau.\Psi = \tau h.\Psi$. De plus si $\sigma \in \mathcal{T}$ avec $\sigma \neq \tau$, alors $\sigma.\Psi \neq \tau.\Psi$.

Et nous obtenons (voir [Arnaudiès et Valibouze 1997] pour $L = \mathfrak{S}_n$) :

$$\chi_{\Psi,I^L_\alpha} = (\mathcal{L}_{\Psi,L,\alpha})^{\operatorname{card}(H)} \tag{3–2}$$

où il apparaît que le polynôme caractéristique s'exprime comme une puissance de la résolvante absolue.

Dans le prochain paragraphe nous verrons comment se calcule le polynôme caractéristique χ_Ψ lié à l'algèbre de décomposition universelle, puis dans les suivants nous chercherons à calculer la résolvante absolue à partir de la trame de l'algorithme de calcul du polynôme caractéristique.

4. CALCUL DU POLYNÔME CARACTÉRISTIQUE DANS L'ALGÈBRE DE DÉCOMPOSITION UNIVERSELLE

Ce paragraphe énonce la formule de J. M. Arnaudiès et l'algorithme de J. L. Lagrange puis il termine par un nouvel algorithme inspiré de celui de Lagrange.

Rappel 4.1. Soient u et v deux polynômes de $\mathcal{K}[x]$, avec $u(x) = a\prod_{i=1}^m (x - \beta_i)$ où $\beta_1, \dots, \beta_m$ appartiennent à une clôture algébrique de $\mathcal{K}$. Le résultant en x des deux polynômes u et v, noté $\operatorname{Res}_x(u, v)$, peut s'exprimer ainsi :

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

4A. La méthode d'Arnaudiès

la méthode proposée dans [Arnaudiès 1992] est basée sur le résultant à n variables.

Notons x_{n+1} une indéterminée supplémentaire et d le degré total de Ψ en $x_1, \dots, x_n$. L'homogénéisé de Ψ, noté Ψ^*, est donné par :

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

Notons $\operatorname{Res}(g_1, \dots, g_n)$ le résultant de n polynômes $g_1, \dots, g_n$ homogènes non constants à n variables.

Théorème 4.2 (Arnaudiès). *Posons $s_i = e_i - e_i(\alpha)$ pour $i = 1, \dots, n$. Alors le polynôme caractéristique est donné par :*

$$\chi_\Psi(T) = \operatorname{Res}(s_1^*, \dots, s_n^*, Tx_{n+1}^d - \Psi^*).$$

Ce théorème démontré dans [Arnaudiès 1992] se déduit de la formule de Poisson–Perron : voir [Arnaudiès 1989, p. 243]. Le calcul de résultant à n variables s'avère très coûteux, cette méthode n'est donc pas utilisable en pratique.

4B. La méthode de Lagrange

Ce paragraphe traduit en terme de résultants, la méthode que J. L. Lagrange [1770] proposait pour calculer la résolvante absolue $\mathcal{L}_{\Psi,f}$ et qui calcule le polynôme caractéristique.

Soit $(U_i)_{0\le i\le n}$ la suite finie définie inductivement par $U_0(T, x_1, \dots, x_n) = T - \Psi(x_1, \dots, x_n)$ et

$$U_i(T, x_{i+1}, \dots, x_n) = \operatorname{Res}_{x_i}(f(x_i, \dots, x_n), U_{i-1}(T, x_i, \dots, x_n))$$

pour $1 \le i \le n$. Alors, d'après le rappel 4.1 et puisque f est unitaire :

$$U_n(T) = \prod_{i_n=1}^n \prod_{i_{n-1}=1}^n \cdots \prod_{i_1=1}^n (T - \Psi(\alpha_{i_1}, \dots, \alpha_{i_n})).$$

Les facteurs sur $\mathcal{K}$ du polynôme $U_n(T)$ sont

- le polynôme caractéristique χ_Ψ ;
- des facteurs dits *parasites* provenant des égalités deux à deux, trois à trois, $\dots, n$ à n des indices apparaissant dans les produits. Effectivement les nombres algébriques tels $\Psi(\alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n)$, $\Psi(\alpha_1, \alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n)$, $\dots$, $\Psi(\alpha_1, \alpha_1, \dots, \alpha_1)$ sont racines de $U_n(T)$ et ne sont pas racines du polynôme caractéristique.

Ces facteurs parasites étaient déjà signalés par J. L. Lagrange. Ce sont des polynômes caractéristiques associés à des invariants d'*arité* strictement inférieure à celle de l'invariant Ψ. Par décroissance stricte de l'arité, il est donc toujours possible de déduire le polynôme caractéristique χ_Ψ à partir du polynôme U_n. Donnons un exemple explicite :

Exemple 4.3. Choisissons l'invariant $\Psi = x_1 + 2x_2$ et $n = 2$. Alors

$$U_2(T) = \chi_\Psi \cdot \chi_{3x_1}$$

où $\chi_{3x_1} = \mathrm{Res}_x(f(x), T - 3x)$. De plus $\mathcal{L}_{\Psi,f} = \chi_\Psi$ puisque Ψ est un I_2-invariant primitif.

La méthode proposée au paragraphe 4C évite la formation des facteurs parasites et calcule donc directement le polynôme caractéristique. Lagrange, qui cherchait à calculer la résolvante, signalait également la puissance parasite provenant des symétries de l'invariant Ψ et que nous retrouvons dans la formule (3–2). Il est possible de diminuer la puissance en cours de calcul (voir le paragraphe 6 consacré au calcul de la résolvante).

4C. Méthode des modules de Cauchy

Notons $f_1, \ldots, f_n$ les modules de Cauchy associés au polynôme f (voir définition 2.12).

Definition 4.4. Soient r un entier positif et s un entier compris entre 1 et n. La r-ième *fonction symétrique complète*, notée $h_r(x_1, \ldots, x_s)$, est la somme des monômes de degré total r en $x_1, \ldots, x_s$, avec $h_0(x_1, \ldots, x_s) = 1$.

Le théorème suivant permet de les calculer efficacement il se démontre facilement.

Théorème 4.5 (Machì–Valibouze). *Soit le polynôme*

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

à coefficients dans $\mathcal{K}$. *Posons* $a_0 = 1$. *Alors, pour* $1 \le r \le n$, *le* r*-ième module de Cauchy associé à* f *est donné par*:

$$f_r(x_r) = \sum_{i=0}^{r} h_i(x_r, \ldots, x_n) a_{r-i}.$$

En particulier $f_n(x_n) = \sum_{i=0}^{n} h_i(x_n) a_{n-i} = f(x_n)$ *et* $f_1(x_1) = h_1(x_1, \ldots, x_n) + a_1$.

Remarque 4.6. 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 [Lascoux et Pragacz 1988].

Le théorème suivant donne une méthode explicite du calcul du polynôme caractéristique :

Théorème 4.7. *Soit la suite finie* $R_0, R_1, \ldots, R_n$ *définie inductivement par* $R_0(T, x_1, \ldots, x_n) = T - \Psi$ *et*

$$R_i(T, x_{i+1}, \ldots, x_n) = \mathrm{Res}_{x_i}(f_i(x_i), R_{i-1}(T, x_i, \ldots, x_n))$$

pour $1 \le i \le n$. *Alors le polynôme caractéristique est donné par*

$$\chi_\Psi(T) = R_n(T).$$

Démonstration. Nous montrons le théorème par récurrence sur n, le degré du polynôme f.

Pour $n = 1$, $f = (x - \alpha_1)$, comme le polynôme f est unitaire nous avons bien :

$$\mathrm{Res}_{x_1}(f(x_1), T - \Psi(x_1)) = (T - \Psi(\alpha_1)) = \chi_\Psi(T).$$

Montrons-le également pour $n = 2$. Nous avons

$$f_2(x_1, x_2) = x_1 + x_2 - e_1(\alpha)$$

et donc

$$\begin{aligned} R_1(T, x_1) &= \mathrm{Res}_{x_1}(f_1(x_1, x_2), T - \Psi(x_1, x_2)) \\ &= T - \Psi(x_2, e_1(\alpha) - x_2)). \end{aligned}$$

D'où

$$\begin{aligned} R_2(T) &= \mathrm{Res}_{x_2}(f(x_2),\, T - \Psi(x_2, e_1(\alpha) - x_2)) \\ &= (T - \Psi(\alpha_1,\, e_1(\alpha) - \alpha_1)) \\ &\quad \times (T - \Psi(\alpha_2,\, e_1(\alpha) - \alpha_2)) \\ &= (T - \Psi(\alpha_1, \alpha_2))(T - \Psi(\alpha_2, \alpha_1)) \\ &= \chi_\Psi(T) \quad \text{d'après la formule (3–1).} \end{aligned}$$

Supposons désormais que le théorème soit vrai jusqu'à $n - 1$ dans tout anneau commutatif unitaire, donc en particulier dans $\mathcal{K}[x_n]$. Ainsi, en posant, $F(x) = f_{n-1}(x, x_n) = f_{n-1}(x)$ et en notant $F_{n-1}(x_{n-1})$, $F_{n-2}(x_{n-2}, x_{n-1})$, …, $F_1(x_1, \ldots, x_{n-1})$ les modules de Cauchy associés à F, nous avons $F_j(x_j, \ldots, x_{n-1}) = f_j(x_j, \ldots, x_n)$ pour $j = 1$, …, $n-1$. Notons $\beta_1(x_n)$, …, $\beta_{n-1}(x_n)$ les $n-1$ racines de $F(x)$ dans une clôture algébrique de $\mathcal{K}[x_n]$. Par hypothèse de récurrence et puisque $F(x)$ est unitaire, nous avons

$$R_{n-1}(T, x_n) = \prod_{\tau \in \mathfrak{S}_{n-1}} \left(T - \Psi(\beta_{\tau(1)}(x_n), \ldots, \beta_{\tau(n-1)}(x_n), x_n)\right),$$

et donc

$$R_n(T) = \prod_{i=1}^{n} \prod_{\tau\in\mathfrak{S}_{n-1}} (T - \Psi(\beta_{\tau(1)}(\alpha_i), \dots, \beta_{\tau(n-1)}(\alpha_i), \alpha_i)). \tag{4–1}$$

Or, pour $i = 1, \dots, n$, pour $j = 1, \dots, n-1$ et pour $\tau \in \mathfrak{S}_{n-1}$, nous savons que $\beta_{\tau(j)}(\alpha_i)$ est une racine de

$$F(x) = f_2(x, \alpha_i) = \frac{f(\alpha_i) - f(x)}{\alpha_i - x}$$

et est donc une racine de f distincte de α_i. Ainsi, les $n!$ n-uplets $(\beta_{\tau(1)}(\alpha_i), \dots, \beta_{\tau(n-1)}(\alpha_i), \alpha_i)$ sur lesquels s'évalue l'invariant Ψ dans le produit (4–1) sont les $n!$ n-uplets $(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ où σ parcourt $\mathfrak{S}_n$. Ceci achève la démonstration. □

Remarque 4.8. Comme le polynôme f est supposé unitaire, alors chaque module de Cauchy $f_i(x_1, \dots, x_i)$ 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 suffit de poser $g(x) = a^{n-1} f(x/a)$ qui, lui, est un polynôme unitaire. Pour garder le polynôme f, il faut alors introduire le coefficient dominant de $f = f_n$ ainsi que ceux des modules de Cauchy $f_1, \dots, f_{n-1}$ dans les calculs des résultants successifs.

5. RÉDUCTIONS AVEC DES BASES DE GRÖBNER

5A. Bases de Gröbner

L'idéal $\mathcal{I}$ est engendré par les n polynômes

$$e_1 - e_1(\alpha),\ \dots,\ e_n - e_n(\alpha).$$

Mais ces polynômes n'en forment pas une base de Gröbner ; voir [Becker et Weispfenning 1993].

Rappelons le théorème historique de Cauchy dans lequel il énonce comment les utiliser pour évaluer les polynômes symétriques :

Théorème [Cauchy 1882]. *Soit $F(x_1, \dots, x_n)$ un polynôme à coefficients dans $\mathcal{K}$ et symétrique en les variables $x_1, \dots, x_n$. Pour éliminer $x_n, \dots, x_1$ dans le polynôme F, il suffit de diviser successivement F par les divers termes de la suite $f_1(x_1)$, …, $f_{n-1}(x_{n-1})$, $f_n(x_n)$, en considérant chaque f_i comme une fonction de x_i. Le dernier reste obtenu sera indépendant de $x_1, \dots, x_n$ et donnera la valeur $F(\alpha_1, \dots, \alpha_n)$ en fonction des coefficients de f.*

Autrement dit, lorsque le polynôme f est séparable, les modules de Cauchy de f forment une base de Gröbner réduite de l'idéal $\mathcal{I}$ des relations symétriques. Pour évaluer un polynôme symétrique il suffit de le *réduire* modulo l'idéal $\mathcal{I}$.

Notation 5.1. Pour $i \in [1, n]$, la notation $\mathcal{I}_i$ désigne l'idéal engendré dans $\mathcal{K}[x_i, \dots, x_n]$ par les modules de Cauchy $f_i, \dots, f_n$.

Il est bien connu qu'alors les polynômes $f_i, \dots, f_n$ forment une base de Gröbner réduite pour l'ordre lexicographique de l'idéal $\mathcal{I}_i$ [Becker et Weispfenning 1993]. Ainsi, en considérant $\mathcal{K}[x_i, \dots, x_n]$ comme un sous-anneau de $\mathcal{K}[x_1, \dots, x_n]$:

$$\begin{aligned}\mathcal{I}_i &= \mathcal{I} \cap \mathcal{K}[x_i, \dots, x_n] \\ &= \{P \in \mathcal{K}[x_i, \dots, x_n] \mid (\forall\sigma \in \mathfrak{S}_n)\ (\sigma.P)(\alpha) = 0\}.\end{aligned}$$

En particulier $\mathcal{I}_1 = \mathcal{I}$.

Le théorème de Cauchy se généralise facilement ainsi:

Théorème 5.2. *Supposons que le polynôme f soit réductible sur $\mathcal{K}$: $f = gh$ où $g, h \in \mathcal{K}[x]$ avec $deg(g) = m$ et $deg(h) = p = n - m$. Choisissons la numérotation des racines du polynôme f de telle sorte que $\alpha_1, \dots, \alpha_m$ soient les m racines du polynôme g. Notons $g_1, \dots, g_m$ les modules de Cauchy du polynôme g et $h_1, \dots, h_p$ ceux du polynôme h. Alors les n polynômes $g_1, \dots, g_m, h_1, \dots, h_p$ forment une base de Gröbner réduite de l'idéal $I_\alpha^{\mathfrak{S}_m \times \mathfrak{S}_p}$.*

Démonstration. D'après [Valibouze 1999], l'idéal $I_\alpha^{\mathfrak{S}_m \times \mathfrak{S}_p}$ est engendré dans $\mathcal{K}[x_1, \dots, x_n]$ par l'idéal dans $\mathcal{K}[x_1, \dots, x_m]$ des relations symétriques entre les racines du polynôme g et l'idéal dans

$$\mathcal{K}[x_{m+1}, \dots, x_n]$$

des relations symétriques entre les racines du polynôme h :

$$\mathcal{I}_\alpha^{\mathfrak{S}_m \times \mathfrak{S}_p} = \mathcal{I}^{\mathfrak{S}_m}_{(\alpha_1, \dots, \alpha_m)} + \mathcal{I}^{\mathfrak{S}_p}_{(\alpha_{m+1}, \dots, \alpha_n)}.$$ □

5B. Réduction modulo un idéal triangulaire

Definition 5.3. Un ensemble T de n polynômes de $\mathcal{K}[x_1, \dots, x_n]$ est dit *triangulaire* de $\mathcal{K}[x_1, \dots, x_n]$ si $T = \{p_1(x_1), \dots, p_n(x_1, \dots, x_n)\}$ où chaque polynôme p_i est unitaire en x_i avec degré$(p_i, x_i) > 0$.

Definition 5.4. Un idéal $\mathcal{J}$ est dit *triangulaire* s'il est engendré par un ensemble triangulaire.

Exemple 5.5. L'idéal $\mathcal{I}$ est un idéal triangulaire, ainsi que l'idéal $I_\alpha^{\mathfrak{S}_m \times \mathfrak{S}_p}$ défini au théorème 5.2.

Soit maintenant $\mathcal{J}$ un idéal triangulaire, engendré par l'ensemble triangulaire :

$$\{p_1(x_1), p_2(x_1, x_2), \ldots, p_n(x_1, \ldots, x_n)\}.$$

Réduire le polynôme Θ de $\mathcal{K}[x_1, \ldots, x_n]$ par l'idéal $\mathcal{J}$ revient a réaliser successivement des divisions euclidiennes par chaque polynôme p_j considéré comme un polynôme en x_j, pour $j \in [1, n]$. Le reste de cette division appartiendra au quotient $\mathcal{K}[x_1, \ldots, x_n]/\mathcal{J}$.

Notation 5.6. Pour $\Theta \in \mathcal{K}[x_i, \ldots, x_n][T]$ le résultat de cette réduction sera noté $\Theta \bmod \mathcal{J}$.

Algorithme 5.7 (Réduction).

entrées : $\Theta \in \mathcal{K}[x_1, \ldots, x_n][T]$
  $p_1, \ldots, p_n$: une base triangulaire de $\mathcal{J}$
sortie : $\Theta \bmod \mathcal{J}$

resultat $\leftarrow \Theta$
pour $j \in [1, .., n]$ **répète**
  resultat $\leftarrow$ *Reste*(*resultat*, p_j, x_j)
renvoie *resultat*

Où *Reste*(p, q, x_k) est le reste de la division euclidienne de p par q, considérés comme des polynômes de $\mathcal{K}[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n, T][x_k]$.

6. CALCUL DE LA RÉSOLVANTE ABSOLUE

La formule (3–2) montre que le polynôme caractéristique est une puissance de la résolvante. Cette partie est donc consacrée à l'élimination de cette puissance. Le paragraphe 6A rappelle les résultats de F. Lehobey sur ce point et le paragraphe 6D montre comment certaines puissances sont éliminées lorsque les calculs sont réalisés dans l'algèbre de décomposition universelle.

Les modules de Cauchy du polynôme f sont notés $f_1, \ldots, f_n$.

6A. Méthode de Lehobey

Dans la pratique, le calcul de la résolvante $\mathcal{L}_{\Psi,f}(T)$ ne se réalise pas sans réduire la puissance parasite due aux symétries de l'invariant Ψ à chaque étape de l'algorithme 6.3 (voir (3–2)). La formation de cette puissance est illustrée au travers de l'exemple suivant :

Exemple 6.1. Fixons $n = 3$ et choisissons $\Psi = 2x_3 + x_1 + x_2$ un $\mathfrak{S}_3$-primitif H-invariant où $H = \mathfrak{S}_2 \times \mathfrak{S}_1$. D'après la définition de la suite $(R_j)_j$ du théorème 4.7, il vient :

$$R_{n-1}(T, x_3) = \operatorname{Res}_{x_2}(f_2(x_2, x_3), \operatorname{Res}_{x_1}(f_1(x_1, x_2, x_3), T - \Psi)).$$

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

$$R_2(T, x_3) = (T - (2x_3 + \beta_1(x_3) + \beta_2(x_3)))^2,$$

où $\beta_1(x_3)$ et $\beta_2(x_3)$ sont les racines de $f_2(x)$ dans $\mathcal{K}[x_3][x]$. En posant $V_2(T, x_3)^2 = R_2(T, x_3)$, nous avons finalement :

$$\mathcal{L}_{\Psi,f}(T) = \operatorname{Res}_{x_3}(f_3(x_3), V_2(T, x_3)).$$

Nous constatons que nous obtenons la résolvante au lieu de son carré donné par la formule (3–2). Cet exemple montre également qu'il est préférable d'éliminer d'abord les symétries.

L'exemple 6.1 suppose connu le polynôme V_2 qui se calcule par la méthode de F. Lehobey [1997]. Cette méthode s'appuie sur le théorème 6.2 et aboutit à l'algorithme 6.3 exposés ci-après.

Le théorème 6.2 explicite le degré de chaque puissance superflue qui apparaît après un calcul de résultant.

Théorème 6.2 (Lehobey). *Soient A un anneau intègre de caractéristique nulle, $f \in A[x]$ un polynôme unitaire, de degré n ; H_n un sous-groupe de $\mathfrak{S}_n$; $\Psi \in A[x_1, \ldots, x_n]$ un H_n-invariant primitif ; $f_1, \ldots, f_n$, les n modules de Cauchy de f et $H_i = \operatorname{Stab}_{\mathfrak{S}_i}(\Psi)$, pour $1 \le i \le n-1$, les $n-1$ stabilisateurs sur $\mathfrak{S}_i$ de Ψ considéré comme un élément de*

$$A[x_{i+1}, \ldots, x_n][x_1, \ldots, x_i].$$

Soit l'entier m_i défini par :

$$m_i = \frac{\operatorname{card} H_i}{\operatorname{card} H_{i-1}} \quad \textit{pour } 1 \le i \le n,$$

avec $\operatorname{card} H_0 = 1$. Alors la suite finie $V_0, \ldots, V_n$ définie récursivement par $V_0(T, x_1, \ldots, x_n) = T - \Psi$ et

$$V_i(T, x_{i+1}, \ldots, x_n) = (\operatorname{Res}_{x_i}(f_i(x_i), V_{i-1}(T, x_i, \ldots, x_n)))^{1/m_i}$$

calcule la résolvante de f par Ψ :

$$\mathcal{L}_{\Psi,f}(x) = V_n(x).$$

6B. La racine r-ième

L'algorithme de calcul de la résolvante (6.3) ainsi que les algorithmes qui en découlent, font appel à la fonction *racine*() définie de la façon suivante :

Soient A un anneau commutatif de caractéristique nulle quelconque, m un entier positif et p un polynôme de $\mathcal{K}[x_1, \ldots, x_m]$ unitaire en x_i, pour $i \in [1 \ldots m]$; alors pour tout $k \in \mathbb{N}$ la fonction

$$racine(p^k, k, x_i)$$

retourne le polynôme p. Cette fonction est basée sur le travail de P. Henrici [1956].

6C. L'algorithme de calcul de la résolvante

Algorithme 6.3 (Résolvante).

entrées : f : un polynôme de $\mathcal{K}[x]$
 Ψ : un polynôme de $\mathcal{K}[x_1, \ldots, x_n]$ H-invariant primitif
 puissancesParasites : une liste d'entiers contenant les degrés des puissances parasites
sortie : la résolvante de f par Ψ

resultat $\leftarrow T - \Psi$
pour *cm* **dans** *modulesDeCauchy*$(f, [x_1, \ldots, x_n])$
 v **dans** $[x_1, \ldots, x_n]$
 pp **dans** *puissancesParasites*
 répète *resultat* $\leftarrow$
 racine(*resultant*(*cm*, *resultat*, v), *pp*, T)
renvoie *resultat*

Où :

- la fonction *modulesDeCauchy*$(f, [x_1, \ldots, x_n])$ renvoie la liste $[f_1(x_1), \ldots, f_n(x_n)]$ des modules de Cauchy de f;
- *racine*(f, n, y) calcule la racine n-ième de f comme polynôme en y (voir section 6B);
- la liste des puissances parasites *puissancesParasites* est fonction de l'invariant. Elle peut être calculée en utilisant des stabilisateurs (voir théorème 6.2) avec le logiciel GAP [Schönert et al. 1995] ou par la factorisation des calculs intermédiaires.

Démonstration. Cet algorithme découle des théorèmes 4.7 et 6.2. □

Exemple 6.4. Prenons le polynôme

$$f = x^6 - 243x^2 + 729$$

et l'invariant $\Psi = x_5x_6 + x_3x_4 + x_1x_2$. Le temps nécessaire au calcul du polynôme caractéristique puis à celui de la résolvante à partir de la formule (3–2) est de 1 heure et 40 minutes. Avec l'algorithme 6.3 le temps nécessaire au calcul de la résolvante n'est plus que de 1 seconde.

6D. Calculs modulo l'idéal des relations symétriques

L'un des inconvénients de l'algorithme 6.3 est la croissance des degrés en les variables $x_1, \ldots, x_n$ dans les calculs intermédiaires du polynôme *resultat*. Nous étudions donc le moyen de contrôler cette croissance par réductions utilisant des divisions euclidiennes. Nous constaterons que la méthode employée aboutit parfois à l'élimination de plusieurs variables lors d'un même pas de boucle. L'élimination prématurée des variables par réduction n'occasionne donc aucune puissance superflue. Une réduction est alors équivalente à autant de pas de l'algorithme 6.3 que de variables éliminées prématurément par réduction.

Réduction de polynômes. Soit $i \in [1, n]$. Puisque f_i, $\ldots$, f_n est une base de Gröbner réduite de l'idéal $\mathcal{I}_i$ de dimension zéro (voir notation 5.1), l'anneau quotient $\mathcal{K}[x_i, \ldots, x_n]/\mathcal{I}_i$ est engendré en tant que $\mathcal{K}$-module par les monômes m tels que, pour $j \in [i, n]$, degré$(m, x_j) < j = \deg_{x_j}(f_j(x_j))$ (voir définition 2.12). Autrement dit :

$$\mathcal{K}[x_i, \ldots, x_n]/\mathcal{I}_i \simeq \bigoplus_{0 \le b_j < j} \mathcal{K}.x_i^{b_i} \ldots x_n^{bn}.$$

Ainsi les degrés en x_j $(0 < j \le n)$ des polynômes de l'algorithme 6.3 peuvent être contrôlés pour ne pas dépasser $j - 1$.

Notation 6.5. Soit I un idéal quelconque. La notation

$$\textbf{expression} \bmod I,$$

qui désigne le résultat de la réduction de **expression** modulo l'idéal I, sous-entend que tous les calculs d'**expression** sont effectués modulo l'idéal I.

Élimination automatique des puissances superflues. Commençons par des exemples qui illustrent comment, après une réduction, des variables peuvent être éliminées prématurément évitant ainsi, d'une part, des calculs de résultants et, d'autre part, l'apparition de puissances superflues.

Exemple 6.6. L'arité de l'invariant est importante, ce que l'on peut voir de la façon suivante : Prenons un polynôme f de degré 4. Supposons que $\Psi = x_4+2x_3$ où 2 est donc l'arité de Ψ (voir définition 2.1). Soit $S_0 = (T-\Psi) \bmod \mathcal{I} = T-(x_4+2x_3)$, puis $S_1 = \mathrm{Res}_{x_3}(f_3(x_3,x_4),S_0) = T^3+(2-x_4)T^2+T(3x_4^2)+5x_4^3+6x_4^2 = S_1 \bmod \mathcal{I}_4$. Alors

$$\begin{aligned}S_2 &= \mathrm{Res}_{x_4}(f_4(x_4),S_1)\\ &= T^{12}+9T^{11}+33t^{10}+63T^9+40T^8\\ &\quad -120T^7-346T^6-336T^5+2348T^4\\ &\quad +7332T^3+7416T^2+3888T+5864\\ &= \mathcal{L}_{\Psi,f}.\end{aligned}$$

Le calcul de la résolvante s'est alors réalisé en évitant deux résultants et par conséquent sans l'apparition de puissances superflues induites par ces résultants. De manière générale, si $m \leq 1$ et $\Psi \in \mathcal{K}[x_m,\ldots,x_n]$ est un $\mathfrak{S}_{n-m}$-primitif K-invariant alors le calcul de la résolvante se réalise sans les m premiers résultants définissant la suite $(R_j)_j$ du théorème 4.7. Ces premiers résultants sont nécessaires au calcul du polynôme caractéristique mais parfaitement inutiles à celui de la résolvante. De plus, ils introduisent une puissance superflue égale à $m!$. En effet, si la suite $(R_j)_j$ du théorème 4.7 est modifiée en ignorant les m premiers termes et en posant

$$R_{m+1} = T-\Psi(x_m,\ldots,x_n),$$

alors

$$\chi_\Psi = R_n^{m!} \quad \text{et} \quad R_n = (\mathcal{L}_{\Psi,f})^{\mathrm{card}(K)}.$$

Exemple 6.7. Prenons $f = x^4+x^3+2$ et choisissons $\Psi = x_3x_4+x_1x_2$ un $\mathcal{D}_4$-invariant primitif (où $\mathcal{D}_4$ est le groupe diédral). Le calcul du polynôme

$$S_0 = (T-\Psi) \bmod \mathcal{I}_1$$

aboutit à $S_0 = x_3^2+(-2\,x_4-1)\,x_3-x_4^2-x_4+T$. Les variables x_1 et x_2 sont éliminées sans un calcul de résultant. Le calcul du polynôme

$$S_1 = \mathrm{Res}_{x_3}(f_3(x_3),S_0) \bmod \mathcal{I}_4$$

aboutit à $S_1 = T^3-8\,T-2$. Comme le degré du polynôme S_1 est égal à celui de la résolvante $\mathcal{L}_{\Psi,f}$, le théorème 6.8 nous assure que ces polynômes sont égaux.

Théorème 6.8. *Posons $I_{n+1} = (0)$ et définissons la suites finie d'entiers $(k_i)_{0\leq i\leq j}$ ($k_i \in [0,n]$) et la suite finie de polynômes $(S_i)_{0\leq i\leq j}$ de la manière suivante :*

- *l'entier naturel $n-k_i+1$ est l'arité du polynôme S_i qui appartient à $\mathcal{K}[T][x_{k_i},\ldots,x_n]$;*
- *l'entier j est le plus petit entier i tel que $k_i = n+1$ ($i.e$ l'arité de S_i est nulle) ;*
- *Au départ :*

$$S_0(T,x_{k_0},\ldots,x_n) = T-\Psi \bmod \mathcal{I}_1$$

et pour $i \in [0,j[$

$$S_{i+1}(T,x_{k_{(i+1)}},\ldots,x_n) =$$
$$\mathrm{Res}_{x_{k_i}}(f_{k_i}(x_{k_i}),S_i(T,x_{k_i},\ldots,x_n))^{1/m_{k_i}} \bmod \mathcal{I}_{k_i+1},$$

où l'entier m_{k_i} est celui défini au théorème 6.2.

Alors le dernier terme de la suite est une puissance de la résolvante cherchée :

$$S_j(T)^m = \mathcal{L}_{\Psi,f}(T) \quad \text{pour } m > 0. \tag{6–1}$$

Démonstration. La démonstration se déroule en trois étapes. La première montre que l'on peut remplacer chaque V_i de la suite $(V_i)_i$ définie au théorème 6.2 par $V_i \bmod \mathcal{I}_{i+1}$. La seconde montre que l'on peut réaliser tous les calculs de la suite $(V_i)_i$ modulo les idéaux $\mathcal{I}_j$ ($j \in [1,n]$) et la troisième étape montre comment éviter des calculs en tenant compte des variables éliminées prématurément.

Soit $W = V_i \bmod \mathcal{I}_{i+1}$, c'est à dire, d'après l'algorithme 6.10, $V_i = \sum_{j=i+1}^n \$f_j(x_j)+W$ où \$ désigne un polynôme quelconque (en l'occurrence un quotient d'une division euclidienne par $f_j(x_j)$). Alors dans les résultants successifs définissant $V_{i+1},\ldots,V_n$, le polynôme V_i peut-être remplacé par le polynôme W sans que le polynôme V_n soit modifié, puisque ces résultants sont réalisés avec les polynômes $f_{i+1}(x_{i+1})$, $\ldots$, $f_n(x_n)$.

Maintenant posons $P = \mathrm{Res}_{x_i}(f_i(x_i),V_{i-1}) = V_i^{m_i}$ et $S = P \bmod \mathcal{I}_{i+1}$, c'est à dire, d'après l'algorithme 6.10, $P = \sum_{j=i+1}^n \$f_j(x_j)+S$. Alors $S = W^{m_i} \bmod \mathcal{I}_{i+1}$. Ainsi, en remplaçant V_i par $S^{1/m_i} \bmod \mathcal{I}_{i+1}$ dans la suite $(V_j)_j$, le résultat $V_n = \mathcal{L}_{\Psi,f}$ n'est pas modifié.

Tenons compte maintenant des variables de W. Supposons que le polynôme V_i soit remplacé par W dans la suite $(V_j)_j$. Nous avons donc

$$V_{i+1}^{m_{i+1}} = \mathrm{Res}_{x_{i+1}}(f_{i+1}(x_{i+1}),W).$$

Si W ne dépend pas de x_{i+1}, alors $V_{i+1}^{m_{i+1}} = W^{i+1}$. Ainsi, si V_{i+1} est remplacé par W dans la suite $(V_j)_j$, alors $V_n = \mathcal{L}_{\Psi,f}^{i+1/m_{i+1}}$. □

Remarque 6.9. Dans l'équation (6–1), l'entier m sera égal à 1 si les résultants évités par élimination prématurée des variables (voir la dernière partie de la démonstration) correspondent à des symétries de l'invariant Ψ et non pas au fait que l'invariant Ψ n'est pas séparable. Par exemple, si Ψ est un H-invariant primitif, où H est un sous-groupe propre de $\mathfrak{S}_n$, et que $\Psi - \Psi(\alpha) \in \mathcal{I}$, alors $i_0 = 0$, $S_{i_0} = T - \Psi(\alpha) \in \mathcal{K}[T]$ et $\mathcal{L}_{\Psi,f} = S_{i_0}^{[\mathfrak{S}_n:H]}$. L'identification du groupe de Galois du polynôme f se réalise avec les facteurs simples des résolvantes. Donc, en pratique, dès que le programme détecte que le saut de plusieurs résultants n'aboutira pas au calcul exact de la résolvante (i.e. $m = 1$), il sera stoppé pour choisir un autre invariant du même groupe ou pour transformer le polynôme f. Cette détection se fait avec les degrés des modules de Cauchy et les entiers m_i de Lehobey dès que le calcul d'un résultant est évité.

Algorithme 6.10 (Calcul de la résolvante avec réductions).

entrées : f : un polynôme de $\mathcal{K}[x]$,
  Ψ : un polynôme de $\mathcal{K}[x_1,\dots,x_n]$ H-invariant primitif
  puissancesParasites : une liste d'entiers contenant les degrés des puissances parasites
sortie : la H-résolvante de f par Ψ

varutiles ← *variables*(Ψ)
cm ← *modulesDeCauchy*(f, *varutiles*)
resultat ← $T - \Psi$
tant que *arite*(*resultat*) $\neq 1$ **répète**
  v ← *mainVariable*(*resultat*)
  k ← *position*(v, *varutiles*)
  pp ← *puissancesParasites*[k]
  resultat ←
    resultant(*cm*[k], *resultat*, v)$^{1/pp}$ mod $\mathcal{I}_{k+1}$
renvoie *resultat*

Où :

- la fonction *arite*(P) renvoie l'arité de P,
- la fonction *position*(v, lv) renvoie la position de v dans la liste lv,
- la fonction *mainVariable*(P) renvoie la variable principale de P,
- la notation $l[k]$ désigne le k-ième élément de la liste l,
- la fonction *variables*(P) renvoie la liste des variables de P,
- la fonction *modulesDeCauchy*($f,[x_1,\dots,x_n]$) renvoie la liste $[f_1(x_1),\dots,f_n(x_n)]$ des modules de Cauchy de f,
- l'idéal $\mathcal{I}_{k+1}$ est défini notation 5.1,
- la notation P mod $\mathcal{I}_{k+1}$ est décrite en notation 6.5,
- le calcul de $P^{\frac{1}{k}}$ mod $\mathcal{I}$ est réalisé à l'aide de la fonction *racine*(p,k,v) décrite au paragraphe 6B.
- La liste des puissances parasites *puissancesParasites* est fonction de l'invariant. Elle peut être calculée en utilisant des stabilisateurs (voir théorème 6.2) avec le logiciel GAP [Schönert et al. 1995] ou par la factorisation des calculs intermédiaires.

7. GÉNÉRALISATION AUX MULTI-RÉSOLVANTES

Soient $F = (f^{(1)},\dots,f^{(p)})$ un p-uplet de polynômes de $\mathcal{K}[x]$ de degrés respectifs $d_1,\dots,d_p$ et $d = d_1+\dots+d_p$. Donnons-nous $x_1,\dots,x_d$ des indéterminées. Soit Ω_F la liste des racines des polynômes de F, ordonnées ainsi : $\Omega_F = (\Omega^{(1)},\dots,\Omega^{(p)})$ où $\Omega^{(i)}$ est une liste quelconque des racines du polynôme $f^{(i)}$ pour $i \in [1,p]$.

Fixons $\Psi \in \mathcal{K}[x_1,\dots,x_d]$ et posons $\mathcal{S} = \mathfrak{S}_{d_1} \times \dots \times \mathfrak{S}_{d_p}$.

Definition 7.1. *La multi-résolvante absolue* de F par Ψ, notée $\mathcal{L}_{\Psi,F}$, est la résolvante relative $\mathcal{L}_{\Psi,\mathcal{S},\Omega_F}$. La multi-résolvante de F est donc le polynôme

$$\mathcal{L}_{\Psi,F} = \prod_{\Theta \in \mathcal{S}.\Psi} (y - \Theta(\Omega_F))$$

Pour calculer une multi-résolvante, il suffit d'utiliser les algorithmes de calcul des résolvantes conçus pour des invariants avec des coefficients non numériques. Dans la pratique, le corps $\mathcal{K}$ peut être remplacé par un anneau intègre de caractéristique nulle (voir théorème 6.2). En ce cas l'invariant Ψ est considéré successivement comme un polynôme en $(x_1,\dots,x_{d_1})$, puis en $(x_{d_1+1},\dots,x_{d_1+d_2})$, …, puis enfin en $(x_{d_1+\cdots+d_{p-1}+1},\ldots,x_d)$. L'algorithme de calcul d'une multi-résolvante est donc le suivant.

Algorithme 7.2 (Multi-résolvante absolue).

entrées : $F=[f^{(1)},\ldots,f^{(p)}]$: une liste de polynômes de $\mathcal{K}[x]$
 Ψ : un polynôme de $\mathcal{K}[x_1,\ldots,x_n]$ qui est H-invariant primitif
 lpp : la liste des degrés des puissances parasites
 lvar : la liste des variables $x_1,\ldots,x_n$
sortie : la multi-résolvante de F par Ψ

resultat $\leftarrow T-\Psi$
cm $\leftarrow$ [ ]
toutesVariables $\leftarrow$ *variables*(Ψ)
pour $i\in[1\,..\,p]$ **répète**
 $f\leftarrow F[i]$
 varutiles $\leftarrow$ *variablesDuBloc*(Ψ, *lvar*, i, F)
 cm $\leftarrow$ *cons*(*modulesDeCauchy*(f, *varutiles*), *cm*)
resultat $\leftarrow$ *resultat* mod $\langle cm\rangle$
tant que *arite*(*resultat*) $\neq 1$ **répète**
 $v\leftarrow$ *mainVariable*(*resultat*)
 $k\leftarrow$ *position*(v, *toutesVariables*)
 $pp\leftarrow lpp[k]$
 resultat $\leftarrow$
 $resultant(cm[k], resultat, v)^{1/pp}$ mod $\langle cm[k{+}1..n]\rangle$
renvoie *resultat*

Où:

- *variablesDuBloc*(Ψ, *lvar*, i, F) renvoie les variables du polynôme Ψ associées au polynôme $F[i]$,
- la fonction *arite*(P) renvoie l'arité du polynôme P,
- la fonction *position*(v, lv) renvoie la position de l'élément v dans la liste lv,
- la fonction *mainVariable*(P) renvoie la variable principale du polynôme P,
- la notation $l[k]$ désigne le k-ième élément de la liste l,
- la notation $l[k\,..\,j]$ désigne les éléments k, $k+1$, $\ldots$, j de la liste l,
- la fonction *cons*(e, l) renvoie la liste composée de l'élément e et de la liste l,
- la fonction *variables*(P) renvoie la liste des variables du polynôme P,
- la fonction *modulesDeCauchy*(f, $[x_1,\ldots,x_n]$) renvoie la liste $[f_1(x_1),\ldots,f_n(x_n)]$ des modules de Cauchy du polynôme f,
- la notation $\langle cm\rangle$ désigne l'idéal engendré par les polynômes de cm,
- l'expression P mod $\mathcal{I}$ qui désigne la réduction du polynôme P modulo l'idéal $\mathcal{I}$ est décrite en notation 6.5,
- le calcul de $P^{1/k}$ mod $\mathcal{I}$ est réalisé à l'aide de la fonction *racine*(p, k, v) décrite au paragraphe 6B.

Voyons sur un exemple comment ce calcul est réalisé avec la méthode proposée dans cet article :

Exemple 7.3. Prenons les polynômes $f=x^2+5x-89$ et $g=x^2-9x-23$ et l'invariant $\Psi=x_1x_3+x_2x_4^3$. Soient $f_1(x_1,x_2)=x_2+x_1-9$ et $f_2(x_1)=x_1^2-9x_1-23$, les modules de Cauchy associés au polynôme f. Soient $g_1(x_3,x_4)=x_4+x_3+5$ et $g_2(x_3)=x_3^2+5x_3-89$, les modules de Cauchy associés au polynôme g. Nous avons la liste $cm=[g_1,g_2,f_1,f_2]$. Calculons la suite $(R_i)_i$ correspondant à la suite des valeurs prises par la variable *resultat* de l'algorithme 7.2.

$$\begin{aligned}R_0&=T-\Psi \bmod \langle cm\rangle\\&=(-115x_1+1026)x_3-1015x_1+T+9135,\\R_1&=\mathrm{resultant}_{x_3}(R_0,g_2) \bmod \langle f_1,f_2\rangle\\&=T^2+(-1455T+6343920)x_1\\&\qquad+T+13140T-73902264,\\R_2&=\mathrm{resultant}_{x_1}(R_1,f_2)\\&=T^4+13185T^3-138809523T^2\\&\qquad+200429193960T+316431786384576.\end{aligned}$$

Alors $R_2=\mathcal{L}_{\Psi,(f,g)}$.

8. IMPLANTATION

Le système de calcul formel Axiom [Jenks et Sutor 1992] a été choisi pour l'implantation des différents algorithmes. Ce choix est motivé par la grande modularité d'Axiom, parfaitement adaptée aux mathématiques. L'implantation se veut aussi générale que possible. Ainsi le choix du domaine de polynômes est laissé libre à l'utilisateur des différents programmes.

8A. L'organisation générale

La figure 1 décrit l'organisation des différents *paquets* (*packages*), *domaines* (*domains*) et *catégories* (*categories*).

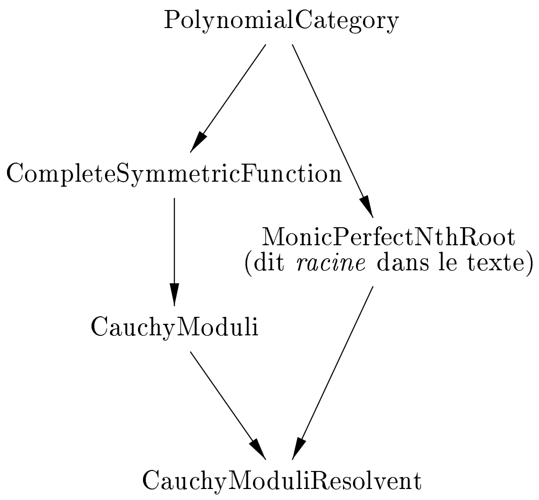

FIGURE 1. Organisation du logiciel.

8B. Un exemple commenté

Voici comment en Axiom obtenir la résolvante $\mathcal{L}_{\Theta,f}$ comme polynôme en la variable y, où $f = x^5 + 4x^4 - 17x^3 - x^2 + x + 1$ et $\Theta = x_4x_5^2 + x_3x_4^2 + x_2x_3^2 + x_5x_1^2 + x_1x_2^2$.

Définition des domaines utilisés. La variable `R` représente l'anneau de base (dans ce cas $\mathbb{Z}$) :

```
R:=Integer
```

La variable `POL` représente l'anneau de polynôme `R`$[x]$ (ici $\mathbb{Z}[x]$). La variable `x` est définie comme le polynôme x :

```
POL:=UnivariatePolynomial(x,R)
x:POL:=x
```

Le choix de la représentation des polynômes de `R`$[x_1, \dots, x_n, y]$ est relativement vaste. Des tests ont montré que les performances varient de façon significative selon l'implantation choisie. La représentation récursive des polynômes est particulièrement adaptée aux algorithmes 6.3 et 6.10. La variable `OVL` désigne le domaine des variables de l'anneau de polynôme `R`$[x_1, \dots, x_n, y]$. La variable `DP` désigne l'anneau de polynômes `R`$[x_1, \dots, x_6, y]$:

```
lv:=[x6,x5,x4,x3,x2,x1,y]
OVL:= OrderedVariableList(lv)
DP:=SparseMultivariatePolynomial(R,OVL)
```

Les variables `x1`, ..., `x6` représentent les polynômes $x_1,\dots,x_6$ de `DP` :

```
x1:=monomial(1$DP,variable(x1)$(OVL)::(OVL),1)$DP;
x2:=monomial(1$DP,variable(x2)$(OVL)::(OVL),1)$DP;
x3:=monomial(1$DP,variable(x3)$(OVL)::(OVL),1)$DP;
x4:=monomial(1$DP,variable(x4)$(OVL)::(OVL),1)$DP;
x5:=monomial(1$DP,variable(x5)$(OVL)::(OVL),1)$DP;
x6:=monomial(1$DP,variable(x6)$(OVL)::(OVL),1)$DP;
```

Instanciation du paquet principal. La variable `DRES` représente une instance du paquet `CauchyModuliResolvent` paramétré par les types définis précédemment. La signature du paquet `CauchyModuliResolvent` est la suivante :

```
CauchyModuliResolvent(R,E,OV,P,X,Y): Public == Private where
R  : EuclideanDomain              (correspond à l'anneau de base)
OV : OrderedSet                   (correspond au domaine des exposants du domaine de polynômes)
E  : OrderedAbelianMonoidSup      (correspond au domaine des variables du domaine de polynômes)
P  : PolynomialCategory(R,E,OV)   (correspond au domaine de polynômes multivariés)
X  : Symbol                       (correspond à la variable x du polynôme de départ)
Y  : OV                           (correspond à la variable de la résolvante)
```

```
DRES:=CauchyModuliResolvent(R,IndexedExponents(OVL),OVL,DP,'x,'y::OVL)
```

Utilisation du paquet. La variable `thetaG1` représente l'invariant Θ ; la variable `f` représente le polynôme f ; la variable `lpp` représente la liste des puissances parasites (voir théorème 6.2).

```
thetaG1:=x4*x5^2+x3*x4^2+x2*x3^2+x5*x1^2+x1*x2^2
f:=x^5+4*x^4-17*x^3-x^2+x+1
lpp:=[1,1,1,1,1,5]
```

La résolvante de f par thetaG1 s'obtient par la commande suivante :

```
r1:=resolvent(f,thetaG1,lpp)$DRES
```

Le résultat est le suivant :

```
thetaG1:=x4*x5^2+x3*x4^2+x2*x3^2+x5*x1^2+x1*x2^2
               2     2          2        2        2
   (106)  x4 x5  + x1 x5 + x3 x4  + x2 x3  + x1 x2
Type: SparseMultivariatePolynomial(Integer,OrderedVariableList [x6,x5,x4,x3,x2,x1,y])
                                       Time: 0.05 (IN) + 0.02 (OT) = 0.07 sec

f:=x^5+4*x^4-17*x^3-x^2+x+1
           5     4      3    2
   (107)  x  + 4x  - 17x  - x  + x + 1
                                        Type: UnivariatePolynomial(x,Integer)
                                                   Time: 0.03 (IN) = 0.03 sec

r1:=resolvent(f,thetaG1,[1,1,1,1,1,5])$DRES

   (108)
      24       23         22           21             20               19
     y   - 390y   + 31765y   + 4780444y   - 647704873y   - 29613862040y
                     18                   17                     16
     + 4952685405792y   + 162526229247165y   - 19020045312189109y
                          15                        14
     - 789049792414412487y   + 28429669450472325254y
                              13                           12
     + 2033502682726556521322y   + 20740342899934941360904y
                                 11                              10
     - 1053157069581828323779746y   - 32557903559648254823580435y
                                   9                                 8
     - 104470564098416503608748049y + 10468326081468786710315799331y
                                      7                                  6
     + 194777917508064488992955129653y + 141850166083564860766030651571y
                                        5                                     4
     - 40049172378844668175673051246282y - 535229018893816475452407292822548y
                                         3
     - 678630031684626941978361684969815y
                                           2
     + 54559355718963585052978366769531424y
     + 618019689068720129370987442816431340y
     + 2646070054199041746352956015103736544

Type: SparseMultivariatePolynomial(Integer,OrderedVariableList [x6,x5,x4,x3,x2,x1,y])
             Time: 0.02 (IN) + 27.36 (EV) + 0.07 (OT) + 9.32 (GC) = 36.76 sec
```

9. TEMPS DE CALCULS ET COMPARAISONS AVEC SYM

Nous comparons maintenant les différents algorithmes de l'article et le logiciel SYM [Valibouze 1989] qui intègre différents algorithmes de calcul de résolvantes dont un algorithme général basé sur le calcul des fonctions puissances des racines de la résolvante. Lorsque la forme de l'invariant induit des formules closes de ces fonctions puissances, le logiciel SYM offre des algorithmes spécialisés. SYM est une extension du système de calcul formel *Maxima* [Maxima $\geq$ 1999].

Les temps donnés correspondent aux temps "machine" donnés par les différents logiciels. Ils ont été mesurés sur un Pentium Pro à 200 Mhz doté de 512 Mo de mémoire vive.

L	H	L-primitif H-invariant
$\mathfrak{S}_6$	T_1	$x_5x_6^2+x_4x_5^2+x_3x_4^2+x_2x_3^2+x_6x_1^2+x_1x_2^2$
$\mathfrak{S}_6$	T_2	$(x_5x_6+x_3x_4+x_1x_2)+2(x_4x_6+x_3x_5+x_2x_6+x_2x_4+x_1x_5+x_1x_3)+3(x_4x_5+x_2x_3+x_1x_6)$
$\mathfrak{S}_6$	T_3	$(x_5x_6+x_4x_5+x_3x_4+x_2x_3+x_1x_6+x_1x_2)$
$\mathfrak{S}_6$	T_4	$(x_6x_5^2+x_4x_6^2+x_5x_4^2+x_3x_5^2+x_4x_3^2+x_6x_2^2+x_2x_4^2+x_3x_2^2+x_1x_6^2+x_5x_1^2+x_1x_3^2+x_2x_1^2)+2(x_3x_5x_6+x_2x_4x_5+x_2x_3x_6+x_1x_4x_6+x_1x_3x_4+x_1x_2x_5)+3(x_3x_6^2+x_6x_3^2+x_2x_5^2+x_5x_2^2+x_1x_4^2+x_4x_1^2)+4(x_3x_4x_6+x_2x_5x_6+x_2x_3x_5+x_1x_4x_5+x_1x_3x_6+x_1x_2x_4)+5(x_3x_4x_5+x_2x_4x_6+x_1x_5x_6+x_1x_2x_3)$
$\mathfrak{S}_6$	T_5	$x_4x_6^2+x_3x_5^2+x_6x_2^2+x_2x_4^2+x_5x_1^2+x_1x_3^2$
$\mathfrak{S}_6$	T_6	$x_3x_5x_6+x_2x_4x_5+x_2x_3x_6+x_1x_4x_6+x_1x_3x_4+x_1x_2x_5$
$\mathfrak{S}_6$	T_{12}	$x_3x_5x_6+x_3x_4x_6+x_2x_5x_6+x_2x_4x_5+x_2x_3x_4+x_1x_4x_6+x_1x_4x_5+x_1x_3x_5+x_1x_2x_6+x_1x_2x_3$
$\mathfrak{S}_6$	T_{14}	$x_3x_5x_4x_6(x_3x_5+x_4x_6)+x_2x_4x_5x_6(x_2x_4+x_5x_6)+x_4x_5x_1x_6(x_4x_5+x_1x_6)+x_2x_5x_3x_6(x_2x_5+x_3x_6)+x_1x_3x_5x_6(x_1x_3+x_5x_6)+x_2x_6x_1x_5(x_2x_6+x_1x_5)+x_3x_4x_2x_6(x_3x_4+x_2x_6)+x_1x_4x_3x_6(x_1x_4+x_3x_6)+x_1x_2x_4x_6(x_1x_2+x_4x_6)+x_2x_3x_1x_6(x_2x_3+x_1x_6)+x_2x_3x_4x_5(x_2x_3+x_4x_5)+x_3x_4x_1x_5(x_3x_4+x_1x_5)+x_1x_4x_2x_5(x_1x_4+x_2x_5)+x_1x_2x_3x_5(x_1x_2+x_3x_5)+x_1x_3x_2x_4(x_1x_3+x_2x_4)$
$\mathfrak{S}_6$	$\mathfrak{S}_2\times\mathfrak{S}_2\times\mathfrak{S}_2$	$x_1x_2-x_3x_4$
$\mathfrak{S}_8$	T_4	$x_7x_8+x_3x_6+x_2x_5+x_1x_4+2(x_6x_8+x_3x_5+x_2x_4+x_1x_7)$
$\mathfrak{S}_8$	T_{47}	$x_1x_2x_3x_4+x_5x_6x_7x_8$
$\mathfrak{S}_9$	T_{14}	$(x_4x_6x_7x_9+x_4x_5x_6x_8+x_3x_5x_8x_9+x_3x_5x_6x_7+x_3x_4x_7x_8+x_2x_7x_8x_9+x_2x_5x_6x_9+x_2x_4x_5x_7+x_2x_3x_6x_8+x_2x_3x_4x_9+x_1x_6x_8x_9+x_1x_5x_7x_8+x_1x_4x_5x_9+x_1x_3x_7x_9+x_1x_3x_4x_6+x_1x_2x_6x_7+x_1x_2x_4x_8+x_1x_2x_3x_5)+2(x_4x_5x_7x_8+x_4x_5x_6x_9+x_3x_7x_8x_9+x_3x_5x_6x_8+x_3x_4x_6x_7+x_2x_6x_8x_9+x_2x_5x_6x_7+x_2x_4x_7x_9+x_2x_3x_5x_9+x_2x_3x_4x_8+x_1x_6x_7x_9+x_1x_5x_8x_9+x_1x_4x_6x_8+x_1x_3x_5x_7+x_1x_3x_4x_9+x_1x_2x_7x_8+x_1x_2x_4x_5+x_1x_2x_3x_6)$
$\mathfrak{S}_9$	T_{10}	$x_6x_7x_8x_9+x_5x_6x_7x_8+x_4x_5x_8x_9+x_4x_5x_6x_7+x_3x_5x_7x_9+x_3x_4x_8x_9+x_3x_4x_7x_8+x_3x_4x_5x_6+x_2x_5x_7x_9+x_2x_4x_7x_9+x_2x_4x_6x_9+x_2x_4x_6x_8+x_2x_3x_7x_8+x_2x_3x_6x_7+x_2x_3x_4x_5+x_1x_7x_8x_9+x_1x_5x_6x_9+x_1x_4x_6x_8+x_1x_4x_5x_9+x_1x_3x_6x_8+x_1x_3x_5x_8+x_1x_3x_5x_7+x_1x_2x_8x_9+x_1x_2x_6x_7+x_1x_2x_5x_6+x_1x_2x_3x_9+x_1x_2x_3x_4$
$\mathfrak{S}_r$	$A_r\times\mathfrak{S}_r$	$\prod_{1\leq i<j\leq r}(x_i-x_j)$

TABLEAU 1. Polynômes invariants utilisés dans les calculs des résolvantes et multi-résolvantes. Pour un degré donné n, la notation T_i désigne les sous-groupes transitifs de $\mathfrak{S}_n$ décrits dans [Butler et McKay 1983].

Le tableau 1 donne les polynômes invariants que nous avons utilisés dans les calculs des résolvantes et multi-résolvantes. Les invariants ont été calculés par le programme Primitive Invariants [Abdeljaouad 1999].

Calcul de résolvante absolue: algorithmes généraux. Pour $f = x^6 - 243x^2 + 729$, les temps sont :

Groupe	Algo. 6.10	Algo. 6.3	SYM
T_1	$41'$	$\star$	$\star$
T_2	$41'$	$\star$	$\star$
T_3	$57'$	$\star$	$\star$
T_4	1h20′	$\star$	$\star$
T_5	1h30′	6h	$\star$
T_6	2h	$\star$	$\star$
T_{12}	2h	5h55′	7h7′
T_{14}	$11'$	6h	$\star$
$\mathfrak{S}_2 \times \mathfrak{S}_2 \times \mathfrak{S}_2$	$3'10''$	$3'30''$	$6'8''$

$\star$: calcul non terminé.

Calcul de résolvante absolue: algorithmes spécialisés. On prend maintenant le cas des invariants de faible arité. Fixons $f = x^7 + 8x^6 - 5x^4 - 18x^2 + x - 1$. Les temps sont :

Groupe	Algo. 6.10	Algo. 6.3	SYM
$x_1x_2 - x_3x_4$	$3'10''$		$2,5''$
$x_1 + 2x_2 + 3x_3$	$171''$	$128''$	2h23′
$x_1x_2^2x_3^3$	$18'26''$	$48'$	$16'16''$
$x_1x_2x_3$	$200''$	$250''$	$2,5''$

Calculs de multi-résolvantes absolues. Fixons
$$F = (f^{(1)}, f^{(2)}, f^{(3)}, f^{(4)})$$
où :
$$\begin{aligned} f^{(1)} &= x^3 + 6095519139889209290x^2 \\ &\quad + 1488819284363725564 8x \\ &\quad + 3495901233607471790 \end{aligned}$$
$$\begin{aligned} f^{(2)} &= x^3 + 17595319154460550344x^2 \\ &\quad + 11186788950436463054x \\ &\quad + 11049608948604938510 \end{aligned}$$
$$f^{(3)} = x + 8358981594339387494$$
$$f^{(4)} = x + 4843668258729955558$$
Les temps mesurés sont les suivants :

Groupes	Algorithme 7.2	SYM
$A_4 \times \mathfrak{S}_4$	$0,27''$	15h20′
T_{47}	$0,06''$	$\star$
T_4	$5,46''$	$\star$

$\star$: temps de calcul supérieur à 2 jours.

Fixons maintenant $P = (p^{(1)}, p^{(2)}, p^{(3)}, p^{(4)})$ où :
$$p^{(1)} = x^4 + 119x^3 + 442x^2 + x - 1$$
$$\begin{aligned} p^{(2)} &= x^3 + 17595319154460550344x^2 \\ &\quad + 11186788950436463054x \\ &\quad + 11049608948604938510 \end{aligned}$$
$$p^{(3)} = x + 8358981594339387494$$
$$p^{(4)} = x + 4843668258729955558$$

Groupes	Algorithme 7.2
T_{14}	$0,05''$
T_{10}	1h28′

10. CONCLUSIONS

Cet article a montré comment éviter les deux principaux défauts des méthodes de calcul de résolvantes basées sur le résultant (facteurs parasites et puissances superflues). L'algorithme auquel nous avons abouti (algorithme 6.10) a permis de calculer des résolvantes qui n'étaient pas calculables par d'autres méthodes (par exemple : la résolvante de T_1 en degré 6). Les algorithmes spécialisés implantés dans SYM peuvent être beaucoup plus rapides (cas des résolvantes produits, symétriques) mais ce n'est pas toujours le cas (résolvantes linéaires, résolvantes monomiales). Pour les invariants de grande arité, les temps de calcul restent élevés et au delà du degré 7, de nombreux exemples n'aboutissent pas. En revanche, l'algorithme de multi-résolvante (algorithme 7.2) est très efficace.

DISPONIBILITÉ ELECTRONIQUE

Les rapports internes et techniques sont disponibles sur le serveur http://www.lip6.fr/reports/ .

BIBLIOGRAPHIE

[Abdeljaouad 1999] I. Abdeljaouad, "Calculs d'invariants primitifs de groupes finis", *Theor. Inform. Appl.* **33**:1 (1999), 59–77.

[Ampère 1826] A.-M. Ampère, *Fonctions interpolaires*, Annales de M.Gergonne, 1826.

[Arnaudiès 1989] J.-M. Arnaudiès, *Elimination*, Ph.D. thesis, Universit Paul Sabatier de Toulouse, 1989. à paraître dans *Adv. in Math.*

[Arnaudiès 1992] J.-M. Arnaudiès, "Théorème de Bézout, formule de Poisson-Perron et courbes rationnelles planes génériques", Technical Report 92-24, LITP, 1992.

[Arnaudiès et Valibouze 1997] J.-M. Arnaudiès et A. Valibouze, "Lagrange resolvents", *J. Pure Appl. Algebra* **117/118** (1997), 23–40.

[Becker et Weispfenning 1993] T. Becker et V. Weispfenning, *Gröbner bases: A computational approach to commutative algebra*, Springer, New York, 1993. In cooperation with Heinz Kredel.

[Butler et McKay 1983] G. Butler et J. McKay, "The transitive groups of degree up to eleven", *Comm. Algebra* **11**:8 (1983), 863–911.

[Cauchy 1882] A. L. Cauchy, "Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée", pp. 473 Gauthier-Villars, Paris, 1882.

[Eichenlaub et Olivier 1996] Y. Eichenlaub et M. Olivier, "GALP: un programme pour calculer des groupes de Galois", Technical report, 1996. Voir http://www.math.u-bordeaux.fr/A2X/Logiciels.html.

[Girstmair 1983] K. Girstmair, "On the computation of resolvents and Galois groups", *Manuscripta Math.* **43**:2-3 (1983), 289–307.

[Henrici 1956] P. Henrici, "Automatic computations with power series", *J. Assoc. Comput. Mach.* **3** (1956), 10–15.

[Jenks et Sutor 1992] R. D. Jenks et R. S. Sutor, *AXIOM, The scientific computation system*, Numerical Algorithms Group Ltd., Oxford, 1992.

[Lagrange 1770] J.-L. de Lagrange, "Réflexions sur la résolution algébrique des équations", (1770). Reprinted as pp. 205–421, v. 4, in *Œuvres de Lagrange*, edited by J.-A. Serret, Paris, Gauthier-Villars.

[Lascoux et Pragacz 1988] A. Lascoux et P. Pragacz, "*S*-function series", *J. Phys. A Math. Gen.* **21**:22 (1988), 4105–4114.

[Lehobey 1997] F. Lehobey, "Resolvent computations by resultants without extraneous powers", dans *ISSAC 97: Proceedings*, édité par W. Küchlin, ACM Press, New York, 1997.

[Maxima $\geq$ 1999] Maxima, "MAXIMA", Voir http://www.ma.utexas.edu/maxima.html. Common Lisp implementation of Macsyma, maintained by William Schelter.

[Schönert et al. 1995] M. Schönert et al., *GAP: Groups, algorithms, and programming*, 5e éd., Lehrstuhl D für Mathematik, RWTH Aachen, 1995. Voir http://www-gap.dcs.st-and.ac.uk/~gap.

[Soicher 1984] L. H. Soicher, "An algorithm for computing Galois groups", pp. 291–296 dans *Computational group theory* (Durham, 1982), édité par M. D. Atkinson, Academic Press, London, 1984.

[Stauduhar 1973] R. P. Stauduhar, "The determination of Galois groups", *Math. Comp.* **27** (1973), 981–996.

[Valibouze 1989] A. Valibouze, "SYM, Symbolic computation with symmetric polynomials: an extension to MACSYMA", pp. 308–320 dans *Computers and mathematics* (Cambridge, MA, 1989), édité par Kaltofen, Erich and Watt, Stephen M., Springer, New York, 1989.

[Valibouze 1999] A. Valibouze, "Etude des relations algébriques entre les racines d'un polynôme d'une variable", *Bull. Belgian Math. Soc.* **6**:4 (1999), 507–535.

Nicolas Rennert, LIP6, case 167, Université Paris VI, 4 place Jussieu, 75252 Paris Cedex 05, France (Nicolas.Rennert@lip6.fr)

Annick Valibouze, LIP6, case 167, Université Paris VI, 4 place Jussieu, 75252 Paris Cedex 05, France (avb@medicis.polytechnique.fr, Annick.Valibouze@lip6.fr)