Algebraic certification of numerical algorithms computing Lagrange resolvents

Ines Abdeljaoued-Tej, Faiçal Bouazizi, Annick Valibouze

▶ **To cite this version:**

Ines Abdeljaoued-Tej, Faiçal Bouazizi, Annick Valibouze. Algebraic certification of numerical algorithms computing Lagrange resolvents. Journal of Algebra and Its Applications, 2018, 17 (1), pp.1850007. 10.1142/S021949881850007X . hal-00483257

HAL Id: hal-00483257

https://hal.science/hal-00483257v1

Submitted on 13 May 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CERTIFICATION ALGÉBRIQUE POUR LE CALCUL DE LA RÉSOLVANTE DE LAGRANGE

INES ABDELJAOUED-TEJ, FAÏÇAL BOUAZIZI, ANNICK VALIBOUZE

Résumé
Nous présentons deux algorithmes de calcul de la résolvante de Lagrange d'un polynôme d'une variable. Le premier est algébrique et s'inspire de celui de Lagrange ne fonctionnant que pour les résolvantes absolues car basé sur l'effectivité du théorème fondamental des fonctions symétriques. Nous devons donc généraliser l'effectivité de ce théorème à tout sur-groupe du groupe de Galois du polynôme. Le deuxième algorithme est numérique avec certification algébrique. Il calcule simultanément le polynôme minimal de l'endomorphisme multiplicatif.

Abstract
In this article, we introduce two new methods to calculate Lagrange resolvents. The first one, based on Lagrange's algorithm, enables to calculate algebraically the resolvent and the second one is numeric with algebraic certification.

Introduction

Le théorème fondamental des fonctions symétriques possède diverses formes effectives (voir, par exemple, [9],[8],[13]). Le système de calcul formel Maxima possède un bibliothèque importante sur le sujet (voir "Symmetries" dans [11]). La méthode due à Cauchy consiste à réduire un polynôme symétrique modulo l'idéal des relations symétriques $\mathfrak{S}$ engendré par l'ensemble triangulaire formé par les modules de Cauchy ([4]). Le théorème de Galois quant à lui n'est pas formulé sous une forme constructive mais il généralise le théorème fondamental des fonctions symétriques. Il s'énonce non rigoureusement ainsi : *Toute expression polynomiale sur un corps k en les racines d'un polynôme d'une variable à coefficients dans k appartient à k si et seulement si elle est invariante par le groupe de Galois.* Son calcul efficace est l'enjeu de la théorie de Galois effective : étant donné un polynôme f de $k[x]$, calculer son groupe de Galois G sur k ainsi que l'idéal $\mathfrak{M}$ de ses relations. Cet idéal maximal $\mathfrak{M}$ contient l'idéal des relations symétriques. Pour que le calcul de $\mathfrak{M}$ soit efficace, il est nécessaire de calculer simultanément le groupe de Galois et donc des résolvantes ([14]). La résolvante offre un double avantage. Elle exclut des groupes

Date: 13 mai 2010.

Keywords : Résolvante de Lagrange, polynôme minimal, groupe de Galois, Idéal galoisien , idéal triangulaire.

et fournit des éléments primitifs d'idéaux galoisiens, ces idéaux intermédiaires entre $\mathfrak{S}$ et $\mathfrak{M}$. La résolvante est donc un outil fondamental de la théorie de Galois.

Lorsque la résolvante est absolue, ses coefficients sont symétriques en les racines du polynôme f et le théorème fondamental des fonctions symétriques s'applique. C'est ainsi que Lagrange proposa deux algorithmes pour son calcul. Le premier utilise la technique d'élimination ; c'est-à-dire le résultant sans le nommer puisqu'il n'existait pas encore en tant qu'objet mathématique ([6]). Le second fait appel aux fonctions puissances des racines de la résolvante, le calcul direct des coefficients étant trop coûteux ([7], page 237). La fonction `resolvante` de `Maxima` implante cet algorithme (avec le drapeau `resolvante :general`). Un algorithme portant sur les idéaux triangulaires et utilisant le résultant a été élaboré pour les résolvantes absolues ou non ([2]).

Nous présentons deux nouveaux algorithmes : le paragraphe 2 est consacré à la méthode algébrique faisant appel aux fonctions puissances des racines de la résolvante et le paragraphe 3 à la certification algébrique de la méthode numérique lorsque les coefficients de f appartiennent à $\mathbb{Z}$.

L'algorithme algébrique nécessite une généralisation de l'effectivité du théorème fondamental des fonctions symétriques. Nous nous inspirons de la méthode de Cauchy afin d' "évaluer" les polynômes multivariés en les racines de f à l'aide d'un idéal galoisien quelconque (voir paragraphe 2.1). L'implantation dans le système de Calcul Formel `Sage` décrit l'algorithme (voir paragraphe 2.3). Afin de bien mesurer de l'efficacité de notre algorithme, les comparaisons de temps établies au paragraphe 2.4 ne tiennent pas comptent des optimisations proposées au paragraphe 2.5. Dans ce paragraphe, nous constaterons que l'algorithme se parallélise naturellement et que nous pouvons lui appliquer une méthode efficace de calcul de produit dans un anneau quotienté par un idéal triangulaire ([3]). Il présente l'autre avantage de pouvoir détecter des facteurs linéaires de la résolvante tout en accélérant son calcul.

1. Rappels

Dans tout cet article, f est un polynôme d'une variable de degré n, à coefficients dans un corps parfait k, $\underline{\alpha} = (\alpha_1, ..., \alpha_n)$ est un n-uplet formé des n racines de f supposées distinctes (avec $n > 0$). Le corps $k(\underline{\alpha}) = k[\underline{\alpha}]$ des racines du polynôme f est le corps de décomposition de f. Nous fixons $x_1, \ldots, x_n$ des variables algébriquement indépendantes, $k[x_1, \ldots, x_n]$ est l'anneau des polynômes en ces variables et à coefficients dans k ; $k(x_1, \ldots, x_n)$ est son corps des fractions. Nous notons S_n, le groupe symétrique de degré n.
Tous les rappels non cités de ce paragraphe sont issus de [14].

1.1. **Actions du groupe.**

Nous fixons L un sous-groupe du groupe symétrique S_n et H un sous-groupe de L. L'action du groupe symétrique S_n sur le corps $k(x_1, ..., x_n)$ est définie par :

$$\begin{array}{lll} S_n \times k(x_1, ..., x_n) \to k(x_1, ..., x_n) & & \\ (\sigma, \quad P) & \longrightarrow & \sigma.P(x_1, ..., x_n) = P(x_{\sigma(1)}, ..., x_{\sigma(n)}) \end{array}$$

Définition 1.1. *L'orbite* $L.P$ de P sous l'action de L est définie par :

$$L.P = \{\sigma.P \mid \sigma \in L\}.$$

Définition 1.2. Le stabilisateur $\mathrm{Stab}_L(P)$d'un polynôme P de $k[x_1, ..., x_n]$ dans L est défini par :

$$\mathrm{Stab}_L(P) = \{\sigma \in L \mid P = \sigma.P\}$$

et stabilisateur de H dans le groupe L est défini par :

$$\mathrm{Stab}_L(H) = \{\sigma \in L \mid \forall\, r \in H \;\; r = \sigma.r\}.$$

Définition 1.3. Un polynôme P de $k[x_1, ..., x_n]$ est appelé *un invariant de* L (ou un L-invariant) si

$$L.P = \{P\}.$$

Il appelé un *H-invariant L-primitif* si

$$H = \mathrm{Stab}_L(P) = \{\sigma \in L \mid \sigma.P = P\}.$$

Lorsque $L = S_n$, le polynôme P est dit *H-invariant primitif.*

Exemples 1.4.
- Le déterminant de Vandermonde $\delta_n = \prod_{1\leq i<j\leq n}(x_i - x_j)$ est un *A_n-invariant S_n-primitif* où A_n est le sous-groupe alterné du groupe symétrique S_n.
- Soit $\mathfrak{D}_4$ le sous-groupe diédral du groupe symétrique S_4. Alors le polynôme $x_1x_2 + x_3x_4$ est un *$\mathfrak{D}_4$-invariant S_4-primitif.*
- Les polynômes $x_1 + 2x_2 + ... + (n-1)x_{n-1}$ et $x_1x_2^2...x_{n-1}^{n-1}$ sont des *I_n-invariants S_n-primitifs*, où I_n est le sous-groupe identité de S_n.

1.2. **Polynômes symétriques.**

Un polynôme s de $k[x_1, ..., x_n]$ est dit *symétrique* (en $x_1, x_2, ..., x_n$) si $s = \sigma.s$ pour toute permutation $\sigma \in S_n$. Deux bases importantes de l'anneau $k[x_1, ..., x_n]^{S_n}$ des polynômes symétriques sont rappelées ci-dessous :

- les *fonctions symétriques élémentaires* en $x_1, ..., x_n$, notées $e_0, e_1, e_2, ..., e_n, ...$ et définies par $e_0 = 1, e_r = 0$ si $r > n$, et pour $r \in [\![1, n]\!]$

$$e_r = \sum_{m \in S_n.(x_1x_2...x_r)} m \;;$$

- les *fonctions puissances* (encore appelées fonctions de Newton), en $x_1, ..., x_n$, notées $p_0, p_1, p_2, ..., p_n, ...$, et données par

$$p_r = \sum_{i=1}^{n} x_i^r \;.$$

Les *formules de Girard-Newton* ([5]) forment un système triangulaire permettant de passer d'une base à une autre : pour tout entier $r > 0$

$$p_re_0 - p_{r-1}e_1 + \cdots + (-1)^{r-1}p_1e_{r-1} + (-1)^r r.e_r = 0.$$

Posons $a_i = (-1)^i e_i(\underline{\alpha})$. Alors le polynôme f s'exprime sous la forme

$$f = x_n + a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_n$$

et les relations de Girard-Newton nous donnent :

$$p_r(\underline{\alpha}) + p_{r-1}(\underline{\alpha})a_1 + \cdots + p_1(\underline{\alpha})a_{r-1} + r a_r = 0.$$

Le *théorème fondamental des fonctions symétriques* nous dit que tout polynôme symétrique à coefficients dans un anneau s'exprime comme un polynôme en les fonctions symétriques élémentaires et à coefficients dans cet anneau. Ainsi, tout polynôme symétrique en les racines d'un polynôme s'exprime en ses coefficients et également, par les formules de Girard-Newton, en les fonctions puissances de ses racines.

1.3. **Idéaux Triangulaires.**

Définition 1.5. Un ensemble T est dit *triangulaire* si

$$T = \{f_1(x_1), ..., f_n(x_1, ..., x_n)\}$$

où chaque f_i est un polynôme unitaire en tant que polynôme en x_i avec $\deg(f_i, x_i) > 0$. Cet ensemble triangulaire T est dit *séparable* si chaque polynôme f_i vérifie la condition

$$\forall \beta = (\beta_1, ..., \beta_{i-1}) \in \widehat{k}^{i-1} \ \ tel\ que\ \ f_1(\beta_1) = f_2(\beta_1, \beta_2) \cdots f_{i-1}(\beta_1, ..., \beta_{i-1}) = 0$$

le polynôme à une variable $f_i(\beta_1, ..., \beta_{i-1}, x_i)$ n'admet pas de racine multiple.

Exemple 1.6.
Pour $n = 8$ l'ensemble T suivant est triangulaire séparable.

$$\begin{aligned} T \ = \{ \ & f_1 = x_1^8 + 9x_1^6 + 23x_1^4 + 14x_1^2 + 1, \\ & f_2 = x_2 + x_1, \\ & f_3 = x_3^3 + (x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1)x_3^2 \\ & \qquad\qquad + (x_1^6 + 9x_1^4 + 21x_1^2 + 6)x_3 + x_1^7 + 9x_1^5 + 23x_1^3 + 14x_1, \\ & f_4 = x_4^2 + (x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1)(x_4 + x_3) + x_3 x_4 + x_3^2 + x_1^6 + 9x_1^4 + 21x_1^2 + 6, \\ & f_5 = x_5 + x_4 + x_3 + x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1, \\ & f_6 = x_6 + x_3, \\ & f_7 = x_7 + x_4, \\ & f_8 = x_8 + x_5 \ \} \end{aligned}$$

En effet : les polynômes f_2,f_5,f_6,f_7 et f_8 satisfont la condition puisqu'ils sont respectivement linéaires en x_2, x_5, x_6, x_7 et x_8 ; le polynôme f_1 est irréductible sur un corps parfait k donc séparable ; le polynôme $f_3(\alpha_1, x)$ est un facteur de $f_1(x)$ sur $k(\alpha_1)$ ce qui entraîne sa séparabilité ; et enfin $f_4(x_1, x_3, x_4) = \frac{1}{x_3 - x_4}(f_3(x_1, x_3) - f_3(x_1, x_4))$, d'où sa séparabilité.

Définition 1.7. Les *modules de Cauchy* de f sont les polynômes $f_1, ..., f_n$ de $k[x_1, ..., x_n]$ définis inductivement comme suit :

- $f_1(x_1) = f(x_1)$,
- pour $i = 2, ..., n$:

$$f_i(x_i) = \frac{f_{i-1}(x_1, x_2, \ldots, x_{i-2}, x_{i-1}) - f_{i-1}(x_1, x_2, \ldots, x_{i-1}, x_i)}{x_{i-1} - x_i}$$

Les modules de Cauchy forment un ensemble triangulaire séparable.

Définition 1.8. Un idéal I est dit *triangulaire* s'il est engendré par un ensemble triangulaire séparable.

Soit I un idéal triangulaire engendré par l'ensemble triangulaire suivant :

$$\{f_1(x_1), f_2(x_1, x_2), ..., f_n(x_1, ..., x_n)\}.$$

Réduire le polynôme P de $K[x_1, ..., x_n]$ par l'idéal I revient à réaliser successivement des divisions euclidiennes par chaque polynôme f_i considéré comme un polynôme en x_i, pour $i \in [\![1, n]\!]$. Le reste de cette division est une forme normale de P dans l'anneau quotient $k[x_1, ..., x_n]/I$.
Le résultat de cette réduction sera noté P mod I.

Algorithme : `ReductionTriangulaire(P,I)`
entrées : `P` $\in k[x_1, ..., x_n]$ `et` $f_1, ..., f_n$`, une base triangulaire de I`
Sortie : `P mod I`
`P mod I`$\longleftarrow$ `P`
`Pour` $i \in [\![1, n]\!]$ `Faire P mod I` $\longleftarrow$ `Reste(P mod I,` f_i`,` x_i`)`
`Retourner P mod I`

où `Reste(p, q, x)` est le reste de la division euclidienne de `p` par `q` considérés comme polynômes en `x`.

L'idéal des relations symétriques $\mathfrak{S}$ est triangulaire et engendré par les modules de Cauchy ([10]). Cauchy proposa une forme effective du théorème fondamental des fonctions symétriques que nous exprimons sous la forme suivante :

Théorème 1.9. *(Cauchy,* [4]*) Soit s un polynôme symétrique de $k[x_1, \ldots, x_n]$. Alors $s(\underline{\alpha})$ est la sortie de l'algorithme* `ReductionTriangulaire`*$(s, \mathfrak{S})$.*

1.4. Idéal des $\underline{\alpha}$-relations et groupe de Galois.

Définition 1.10. Un polynôme $P \in k[x_1, ..., x_n]$ est appelé une *$\underline{\alpha}$-relation* si

$$P(\underline{\alpha}) = 0.$$

Définition 1.11. L'idéal $\mathfrak{M}$ de $k[x_1, ..., x_n]$ défini par

$$\mathfrak{M} = \{R \in k[x_1, ..., x_n] \mid R(\underline{\alpha}) = 0\}$$

est appelé *l'idéal des $\underline{\alpha}$-relations.*

Définition 1.12. Le *groupe de Galois* $G_{\underline{\alpha}}$ de $\underline{\alpha}$ sur k est le stabilisateur de $\mathfrak{M}$ dans S_n :

$$G_{\underline{\alpha}} = \{\sigma \in S_n \mid (\forall R \in \mathfrak{M}) \ \sigma.R \in \mathfrak{M}\}.$$

Théorème 1.13. *(Galois) Soit $P \in k[x_1, \ldots, x_n]$. Nous avons $\sigma.P(\underline{\alpha}) = P(\underline{\alpha})$ pour tout $\sigma \in G_{\underline{\alpha}}$ si et seulement si $P(\underline{\alpha}) \in k$.*

Définition 1.14. Soit L un sous-ensemble de S_n. L'idéal

$$I^L_{\underline{\alpha}} = \{R \in k[x_1, ..., x_n] \mid (\forall \sigma \in L) \ \sigma.R(\underline{\alpha}) = 0\}$$

est appelé *l'idéal des $\underline{\alpha}$-relations invariantes par L*. Un tel idéal est appelé un *idéal galoisien de f (sur k)*

Remarque 1.
- L'idéal des $\underline{\alpha}$-relations $\mathfrak{M}$ est l'idéal des $\underline{\alpha}$-relations invariantes par I_n, le sous-groupe identité de S_n.
- L'idéal $\mathfrak{S} = I^{S_n}_{\underline{\alpha}}$ est l'*idéal des relations symétriques* entre les racines de f.

Définition 1.15. Soit I un idéal galoisien de f (sur k). L'*injecteur* de I dans $\mathfrak{M}$ est donné par :

$$\mathrm{Inj}(I, \mathfrak{M}) = \{\sigma \in S_n \mid (\forall R \in I) \ R(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}) = 0\}.$$

Exemple 1.16. $\mathrm{Inj}(\mathfrak{S}, \mathfrak{M}) = S_n$ et $\mathrm{Inj}(\mathfrak{M}, \mathfrak{M}) = G_{\underline{\alpha}}$.

Nous avons les identités suivantes :

$$\mathrm{Card}(V(I)) = \mathrm{Card}(\mathrm{Inj}(I, \mathfrak{M})) = \dim_k k[x_1, \ldots, x_n]/I \tag{1}$$

où $V(I)$ est la variété algébrique de I, l'ensemble de ses zéros.

Lorsque l'injecteur de I dans $\mathfrak{M}$ est un groupe, l'idéal I est dit *pur*. Un idéal galoisien I inclus dans $\mathfrak{M}$ est pur si et seulement son injecteur dans lui-même (on a $\mathrm{Inj}(I, I) = \mathrm{Stab}_{S_n}(I)$) contient le groupe de Galois $G_{\underline{\alpha}}$; ce qui est équivalent à

$$\mathrm{Inj}(I, I) = \mathrm{Inj}(I, \mathfrak{M}) \ ;$$

ce qui, d'après (1), est encore équivalent à

$$\mathrm{Card}(\mathrm{Inj}(I, I)) = \dim k[x_1, \ldots, x_n]/I \quad .$$

Dans [2], les auteurs montrent qu'un idéal galoisien pur est triangulaire. Par exemple, les idéaux $\mathfrak{S}$ et $\mathfrak{M}$ sont purs. Les idéaux galoisiens considérés sont pour la plupart purs ou bien on se ramène à ce cas par des permutations de ses relations ([15]). Dans ce cas, la réduction modulo l'idéal revient à réaliser n divisions euclidiennes avec ses générateurs (voir paragraphe 1.3).

1.5. **Polynômes Caractéristiques, Minimaux et Résolvantes.**

Nous considérons $I \subset \mathfrak{M}$, un idéal galoisien d'injecteur L dans $\mathfrak{M}$, H un groupe inclus dans L et P un H-invariant L-primitif.

Soit $\widehat{P}$ l'endomorphisme multiplicatif de $k[x_1, ..., x_n]/I$ induit par P :

$$\begin{array}{rccc} \widehat{P}: & k[x_1,...,x_n]/I & \to & k[x_1,...,x_n]/I \\ & \Theta & \longmapsto & \Theta.P \end{array}$$

Le *polynôme caractéristique* de $\widehat{P}$ est le polynôme de $k[x]$ degré $\mathrm{Card}(L)$ donné par

$$\chi_{\widehat{P},\mathfrak{S}} = \prod_{\sigma \in L} (x - \sigma.P(\underline{\alpha})). \tag{2}$$

Ce résultat se déduit aisément de l'identité (1) et du théorème de Stickelberger exprimant le polynôme caractéristique de tels endomorphismes multiplicatifs pour les idéaux de variété finie non nécessairement radicaux. Nous pouvons également affirmer que $\chi_{\widehat{P},\mathfrak{S}} \in k[x]$ par le théorème de Galois puisque l'injecteur L contient le groupe de Galois.

Lorsque le corps k est parfait, le *polynôme minimal* de l'endomorphisme $\widehat{P}$ est la forme sans facteur carré sur k du polynôme caractéristique (voir Théorème 3.1) :

$$\mathrm{Min}_{\widehat{P},I} = \prod_{\psi \in \{Q(\underline{\alpha}) \mid Q \in L.P\}} (x - \psi).$$

La *résolvante L-relative* de $\underline{\alpha}$ par P est, par définition, le polynôme

$$R_{P,I} = \prod_{Q \in L.P} (x - Q(\underline{\alpha})). \tag{3}$$

Elle appartient à $k[x]$ puisque ses coefficients sont invariants par L et que L contient le groupe de Galois $G_{\underline{\alpha}}$. Lorsque la résolvante est sans facteur carré, elle s'identifie au polynôme minimal. Nous avons l'identité

$$\chi_{\widehat{P},\mathfrak{S}} = R_{P,I}^{\mathrm{Card}(H)} \quad . \tag{4}$$

Lorsque $L = S_n$, la résolvante ne dépendant pas de la numérotation des racines de f, elle est dite absolue et appelée *résolvante de f par P*.

Exemple 1.17.
Fixons $n = 3$, $f = (x - x_1)(x - x_2)(x - x_3)$ et prenons $P = x_1x_2^2$. Alors

$$R_{P,\mathfrak{S}}(x) = (x - x_1x_2^2)(x - x_1x_3^2)(x - x_2x_1^2)(x - x_2x_3^2)(x - x_3x_1^2)(x - x_3x_2^2) \quad .$$

1.6. **Hypothèses générales.**

Jusqu'à la fin de l'article, nous supposons que I est un idéal galoisien pour lequel nous disposons d'une base de Gröbner réduite permettant d'effectuer la réduction modulo I. Nous désignons par L l'injecteur de I dans un idéal maximal $\mathfrak{M}$ contenant I et nous fixons un groupe H inclus dans L ainsi qu'un polynôme P de $k[x_1, ..., x_n]$ H-invariant L-primitif.

2. Algorithme algébrique

Comme nous l'avons rappelé dans l'introduction, lorsqu'un polynôme est symétrique, il existe de nombreuses méthodes pour l'évaluer en les racines de f. Dans notre cas, nous cherchons à évaluer en
Min_Salpha des polynômes invariants par un sur-groupe L du groupe de Galois $G_{\underline{\alpha}}$ sans que le groupe $G_{\underline{\alpha}}$ soit déterminé. Ensuite, nous en déduirons un algorithme pour le calcul de la résolvante $R_{P,I}$.

2.1. **Evaluation en $\underline{\alpha}$ d'un polynôme invariant par L.**

Lorsque $L = S_n$, pour l'évaluation en $\underline{\alpha}$, nous disposons du théorème fondamental des fonctions symétriques (voir paragraphe 1.2) et lorsque $L = G_{\underline{\alpha}}$, nous disposons du théorème 1.13 de Galois. Nous réunissons ici ces deux théorèmes en un seul sous une forme effective (il n'est pas nécessaire que I soit pur).

Théorème 2.1. *Soit I un idéal galoisien de f contenu dans l'idéal $\mathfrak{M}$ des $\underline{\alpha}$-relations et L l'injecteur de I dans $\mathfrak{M}$. Soit $R \in k[x_1, ..., x_n]$ tel que $\sigma.R = R$ pour tout $\sigma \in L$. Alors $R(\underline{\alpha})$ appartient au corps k des coefficients de f et*

$$R - R(\underline{\alpha}) \in I.$$

Autrement dit, $R(\underline{\alpha})$ s'obtient comme la réduction de R modulo I.

Démonstration. Puisque L est l'injecteur de I dans $\mathfrak{M}$, le groupe de Galois $G_{\underline{\alpha}}$ est inclus dans L. Posons $\lambda = R(\underline{\alpha})$. Puisque le polynôme R est invariant par L, il l'est par $G_{\underline{\alpha}}$. Par conséquent, d'après le théorème 1.13, $\lambda \in k$ et $R - \lambda \in k[x_1, \ldots, x_n]$. Pour tout $\sigma \in L$, nous avons

$$\sigma.(R - \lambda)(\underline{\alpha}) \ = \sigma.R(\underline{\alpha}) \ - \lambda \ = R(\underline{\alpha}) - \lambda = 0 \quad ,$$

puisque R est invariant par L. Donc, par définition des idéaux galoisiens, $R - R(\underline{\alpha}) \in I$. D'où le résultat. □

2.2. **Le principe du calcul.**

En vertu du théorème 2.1, nous pouvons faire émerger un algorithme pour trouver la résolvante $R_{P,I}$. Il est inspiré de celui de Lagrange restreint à la résolvante absolue ([7], page 237). Sa méthode consiste à calculer les fonctions puissances des racines de la résolvante absolue (i.e. $L = S_n$ et $I = \mathfrak{S}$) en s'appuyant sur l'effectivité du

théorème fondamental des fonctions symétriques puis d'en déduire les coefficients de la résolvante avec les relations de Girard-Newton. C'est donc le calcul des fonctions puissances de la résolvante qui nécessite une étude généralisée au cas où I est quelconque.

Tout d'abord, le lemme bien connu suivant nous fournit un moyen de calculer sans répétition inutile l'orbite $L.P$ de P sous l'action de L :

Lemme 2.2. *Soit d l'indice de H dans L. Alors l'orbite $L.P$ est formée des d polynômes distincts $\tau.P$ où τ parcourt une transversale à gauche de L mod H.*

Fixons $i \in [\![1, d]\!]$. D'après la définition (3) de la résolvante $R_{P,I}$, la i-ème fonction puissance de ses est donnée par :

$$p_i(R_{P,I}) \ = \ \sum_{Q \in L.P} Q^i(\underline{\alpha}) \quad .$$

Le polynôme $p_i(R_{P,I})$ est l'évaluation en $\underline{\alpha}$ du polynôme

$$p_i(L.P) \ = \ \sum_{Q \in L.P} Q^i \quad .$$

Vérifions avec le lemme suivant que $p_i(L.P)$ est invariant par L :

Lemme 2.3. *Soient $L.P = \{P_1, \ldots, P_d\}$ et s un polynôme symétrique de $k[x_1, ..., x_d]$. Alors le polynôme $s(P_1, \ldots, P_d)$ est invariant par L.*

Démonstration. Pour tout $\sigma \in L$

$$\sigma.s(P_1, \ldots, P_d) = s(\sigma.P_1, \ldots, \sigma.P_d) = s(P_{\tau(1)}, \ldots, P_{\tau(d)})$$

où $\tau \in S_d$ puisque $\sigma \in L$ et que $\{P_1, \ldots, P_d\}$ est l'orbite de P sous l'action de L. Comme s est un polynôme symétrique, le lemme est prouvé. □

Dans notre cas, $s(L.P) = \sum_{Q \in L.P} Q^i = p_i(L.P)$ avec $s = p_i(x_1, \ldots, x_d)$. Par conséquent, le lemme 2.3 s'applique, le polynôme $p_i(L.P)$ est invariant par L et son évaluation $p_i(R_{P,I})$ en les racines de f s'obtient en lui appliquant le théorème 2.1 :

$$p_i(R_{P,I}) \ = \ \sum_{Q \in L.P} Q^i \mod I.$$

Comme il s'agit trouver la valeur dans k de $p_1(R_{P,I}), \ldots, p_d(R_{P,I})$ où d, l'indice de H dans L, est le degré de la résolvante, notre algorithme évite développer chaque polynôme $\sum_{Q \in L.P} Q^i$ pour le réduire ensuite modulo I. Nous expliquons ci-après le processus choisi.

Posons $\overline{R} = R \mod I$, pour tout $R \in k[x_1, \ldots, x_n]$, et $p_i = p_i(R_{P,I})$.

Nous calculons les $\overline{Q}$, $Q \in L.P$, que nous conservons dans une listes `lp` et nous construisons la liste `lpp=(1,...,1)` de longueur d. A la i-ième étape, $1 \leq i \leq d$, nous supposons avoir conservé dans `lpp` les calculs des $\overline{Q^{i-1}}$, $Q \in L.P$, de l'étape

précédente ainsi que la liste `lp` de la première étape. La fonction puissance p_i est alors calculée ainsi :

(1) $p_i := 0$

(2) Parcourir simultanément les listes `lp` et `lpp` afin de remplacer chaque polynôme $u = \overline{Q^{i-1}}$ de `lpp` par $\overline{u * \overline{Q}}$ où $\overline{Q}$ est l'élément extrait de `lp`.

(3) Pour chaque polynôme (réduit) u de `lpp` Faire $p_i := \overline{p_i + u}$.

2.3. **L' algorithme.**

Toutes les fonctions de cet algorithme sont décrites sous le langage du logiciel du calcul formel `Sage`.

Fonction `ResolvanteAlgebrique`.
Entrées :
- `n` le degré du polynôme f de la variable `x`
- `I` un idéal galoisien donné avec sa base de Gröbner réduite
- `L` l'injecteur de `I` dans un idéal maximal contenant `I`
- `H` un groupe inclus dans `L`
- `P` un `H`-invariant `L`-primitif
- `d` est l'indice de `H` dans `L`

Sortie : La résolvante en x `L`-relative de $\underline{\alpha}$ par `P` pour tout $\underline{\alpha} \in V(\mathtt{I})$.

```
def ResolvanteAlgebrique(P,L,H,I,n,d,x):
     d=gap.Index(L,H)
     lp=Orbite(P,L,H,n)
     lp=[s.mod(I) for s in lp]
     lpp=[1 for i in range(d)]
     pui=[d]
     for i in range(d):
         for j in range(d):
             lpp[j]=(lp[j]*lpp[j]).mod(I)
         pui= pui + [somme_mod(lpp,I)]
     Resolvante=pui2polynome(d,[s for s in pui],x)
     return Resolvante
```

où :
- La fonction `somme_mod(lpp,I)` renvoie la somme des réductions modulo I des éléments de la liste `lpp`.
- La fonction `Orbite(P,L,H,n)` calcule l'orbite du polynôme `P` un `H`-invariant `L`-primitif sous l'action de `L` :

```
def Orbite(P,L,H,n)
    from sage.groups.perm_gps.permgroup import from_gap_list
    Sn=SymmetricGroup(n)
    rc= gap.RightCosets(L,H)
    rc=gap.List(rc,'i->Representative(i)')
```

```
    LTransv=[s for s in rc]
    Orbite=[P * si for si in from_gap_list(Sn,"%s" % LTransv)]
    return Orbite
```

- La fonction `pui2polynome(p,x)` calcule un polynôme de degré d d'une variable `x` à partir des $d+1$ fonctions puissances $p_0 = d, p_1, \ldots, p_d$ de ses racines rangées dans la liste `p` :

```
def pui2polynome(p,x):
  a=[p[0]]
  pol=x^a
  for i in range(1,d+1):
      ai=p[i]+sum(p[j]*a[i-j] for j in range(1,i))
      a=a+[-1/i*ai]
      pol=pol+a[i]*x^(d-i)
  return pol
```

Exemple 2.4.
Prenons comme exemple le polynôme $f = x^6 + 2$. Soit son idéal galoisien I défini par

$$\begin{aligned}
I \;=\; \langle & f_1 = 24x_6 + x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + 6x_3^3x_2x_1^3 + 5x_3^3x_1^4 + 8x_3^2x_2^3x_1^2 + 4x_3^2x_2^2x_1^3 \\
& \quad +8x_3^2x_2x_1^4 + 6x_3x_2^3x_1^3 + 8x_3x_2^2x_1^4 - 4x_3x_2x_1^5 + 12x_3 + 5x_2^3x_1^4 + 12x_2 + 14x_1, \\
& f_2 = 24x_5 - 5x_3^3x_2^4 - 7x_3^3x_2^3x_1 - 16x_3^3x_2^2x_1^2 - 7x_3^3x_2x_1^3 - 5x_3^3x_1^4 - 8x_3^2x_2^4x_1 \\
& \quad -12x_3^2x_2^3x_1^2 - 12x_3^2x_2^2x_1^3 - 8x_3^2x_2x_1^4 - 12x_3x_2^4x_1^2 - 16x_3x_2^3x_1^3 - 12x_3x_2^2x_1^4 \\
& \quad +8x_3 - 5x_2^4x_1^3 - 5x_2^3x_1^4 - 2x_2 - 2x_1, \\
& f_3 = 24x_4 + 5x_3^3x_2^4 + 6x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + x_3^3x_2x_1^3 + 8x_3^2x_2^4x_1 + 4x_3^2x_2^3x_1^2 + \\
& \quad 8x_3^2x_2^2x_1^3 + 12x_3x_2^4x_1^2 + 10x_3x_2^3x_1^3 + 4x_3x_2^2x_1^4 + 4x_3x_2x_1^5 + 4x_3 + 5x_2^4x_1^3 + 14x_2 + 12x_1, \\
& f_4 = x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 \\
& \quad +x_3x_2^3 + x_3x_2^2x_1 + x_3x_2x_1^2 + x_3x_1^3 + x_2^4 + x_2^3x_1 + x_2^2x_1^2 + x_2x_1^3 + x_1^4, \\
& f_5 = x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5, \\
& f_6 = x_1^6 + 2\rangle
\end{aligned}$$

possédant pour injecteur le groupe
$L_1 = \langle (1,3)(2,4), (1,3,4)(2,5,6), (2,3)(4,5), (3,5)(4,6), (3,4,5,6)\rangle$ d'ordre 128. Soit H_1 le sous-groupe du groupe L_1 d'indice 10 dans L_1 défini par :

$$H_1 = \langle (1,2)(3,4)(5,6), (1,3,5)(2,4,6), (3,5)(4,6)\rangle.$$

En utilisant le paquetage `PrimitiveInvariant` de `GAP` ([1]), nous calculons le H_1-invariant L_1-primitif

$$P = x_3x_6 + x_1x_6 + x_4x_5 + x_2x_5 + x_1x_4 + x_2x_3.$$

La résolvante $R_{P,I} = x^{10}+2x^7-4x^4-8x$ est calculée avec la fonction `ResolvanteAlgebrique`.

2.4. **Temps et comparaisons avec d'autres méthodes.**

Nous allons comparer notre algorithme avec deux autres. Le premier, que nous appelons `Algo2`, est celui décrit dans [2] basé sur les résultants et qui calcule le polynôme caractéristique (i.e. une puissance de la résolvante). Nous disposons de son implantation en `Maxima` avec la version 2 de sa bibliothèque "Symmetries" (non distribuée). Le second, que nous appelons `Algo3`, est la méthode naturelle provenant de la définition du polynôme minimal de $\widehat{P}$. Nous calculons sous `Maple` la matrice de l'endomorphisme $\widehat{P}$ avec la fonction `MultiplicationMatrix` puis $\mathrm{Min}_{\widehat{P},I}$ avec la fonction `MinimalPolynomial`. Notre fonction `ResolvanteAlgebrique`, en `Sage`, est désignée par `Algo1`.

Le tableau ci-après présente les temps d'exécution CPU en secondes avec $k = \mathbb{Q}$, $n = \deg(f)$, $c = \mathrm{Card}(L)$, $d = \deg(R_{P,I})$, D, le degré total de l'invariant P, N son nombre de monômes et r son arité.

n	c	(D,N,r)	d	`Algo1`	`Algo2`	`Algo3`
4	4!	$(6,12,4)$	2	0.18	0.6	2.96
5	5!	$(4,25,5)$	12	2.63	9.04	8.14
5	5!	$(4,20,5)$	24	15.94	19.58	766.27
5	5!	$(3,6,5)$	60	88.09	96.60	2361.34
6	6!	$(6,30,6)$	6	2.52	170.1	318
6	128	$(2,6,6)$	10	7.97	11.43	18.50
6	6!	$(2,12,6)$	15	2.60	3.57	860.92
6	6!	$(7,45,6)$	20	4.22	12079.5	571.97
6	6!	$(3,18,6)$	30	120	876.22	4212.70
6	6!	$(2,8,6)$	45	118.15	214.05	1577.51
8	128	$(6,32,8)$	2	8.15	11.92	14.92
8	1152	$(2,8,8)$	9	17.56	337.42	994.84
9	9!	$(1,8,9)$	9	5.16	67.45	867.84

Remarque 2. L'algorithme `Algo1` est basé sur les réductions modulo I, `Algo2` calcule un polynôme caractéristique de degré la dimension sur k de $R = k[x_1, \ldots, x_n]/I$ et `Algo3` produit une matrice carrée de dimension $\dim_k(R)^2$. Donc, dans notre tableau, la valeur de l'ordre c de l'injecteur L de l'idéal I est essentielle car c'est aussi la dimension de R sur k.

Commentaires
Nous constatons qu'`Algo3` est le plus lent et que, de plus, il ne nous dit rien sur les multiplicités des racines de la résolvante lorsque celle-ci n'est pas séparable. Pour les déterminer, il faut trouver le polynôme caractéristique dans un temps plus long que celui nécessaire à celui du polynôme minimal puis en calculer une racine c/d-ième (voir (4)). Cette méthode n'offre donc aucun intérêt en terme d'efficacité. Lorsque les coefficients de f sont numériques, il est alors envisageable de calculer numériquement les valeurs propres de la matrice puis d'utiliser la certification algébrique

afin que cette méthode soit praticable. Mais dans ce cas, la méthode numérique de Stauduhar est plus efficace (voir paragraphe 3).

Nous constatons également qu'`Algo2` est presque toujours plus lent qu'`Algo1`. C'est ce que Lagrange remarquait déjà dans son mémoire [7] en écrivant page 240 : *"... mais, comme on ne voit pas de cette manière de quel degré devrait être cette équation finale en x, qu'on pourrait même parvenir à une équation en x d'un degré plus haut qu'elle ne devrait être, ce qui est l'inconvénient ordinaire des méthodes d'élimination, nous avons cru devoir montrer comment on peut trouver cette équation a priori et s'assurer du degré précis auquel elle doit monter."* Ce que Lagrange exprimait et que nous traduisons ici, c'est que les méthodes d'élimination introduisent des puissances parasites et que, de plus, ces puissances lui sont inconnues ; alors qu'avec les fonctions puissances, il trouve directement la résolvante. Nous savons désormais que cette puissance est l'ordre du stabilisateur de l'invariant P puisqu'il calculait le polynôme caractéristique $\chi_{\widehat{P},\mathfrak{S}}$ de degré $n!$.

Remarque 3. Notons que l'algorithme `Algo2` est largement plus efficace que celui proposé par Lagrange. En effet, la méthode de Lagrange qui est restreinte aux résolvantes absolues (i.e. $L = S_n$) consiste à éliminer les variables $x_n, \ldots, x_1$ du polynôme $x - P$ avec les polynômes $f(x_n), \ldots, f(x_1)$; il trouve un polynôme g de degré n^n dont $\chi_{\widehat{P},\mathfrak{S}}$ est un facteur. Ensuite, le diviseur cherché $\chi_{\widehat{P},\mathfrak{S}}$ de g est extrait après division de g par ses "facteurs parasites", calculés également par des éliminations. Avec `Algo2`, l'élimination se réalise avec les modules de Cauchy (ici $L = S_n$) de degrés respectifs n,$n-1, \ldots, 1$ en $x_n, \ldots, x_1$ et le polynôme $\chi_{\widehat{P},\mathfrak{S}}$ de degré $n!$ en est le résultat.

Pour cette comparaison qui prouve l'efficacité de notre fonction `ResolvanteAlgebrique`, nous n'avons pas eu à introduire les optimisations proposées paragraphes suivant.

2.5. **Optimisations et parallélisation de l'algorithme Résolvante.**

Parallélisation
Supposons que $L.P = \{P_1, \ldots, P_d\}$. Notre algorithme `ResolvanteAlgebrique` est parallélisable de la façon suivante :

Etape 1 En parallèle, pour $j = 0, ..., d$, calculer la liste l_j des $\overline{P_j^i}$, $i = 1, \ldots, d$:
(1) $l_j = [P_j \mod I]$
(2) Pour $i = 1, \ldots, d$ $\quad l_j = l_j + [\, l_j[1] * l_j[j-1] \mod I\,]$.

Etape 2 En parallèle, pour $i = 0, ..., d$, calculer la i-ième fonction puissance p_i avec la fonction `somme_mod(ll,I)` où `ll` est la liste formée des i-ièmes éléments de chaque liste l_j, $j = 1, \ldots, d$.

Méthode efficace pour le produit dans $k[x_1, \ldots, x_n]/I$
Lorsque l'idéal I est triangulaire, notre algorithme peut être grandement amélioré en optimisant la partie consacrée à la multiplication des polynômes modulo I.

En effet, nous pouvons intégrer la méthode décrite dans [3] basée sur des techniques d'évaluation et d'interpolation. Cette optimisation est applicable à la fonction `ResolvanteAlgebrique` et aussi à l'étape 1 de la version parallèle.

Détection de racines dans k
Nous pouvons alléger les calculs lorsqu'il existe $Q \in L.P$ tel que $\lambda = Q \mod I$ appartient à k. Si $I = \mathfrak{M}$, d'après le théorème de Galois et le théorème 2.1, la résolvante possède une racine $Q(\underline{\alpha})$ dans k si et seulement si $Q \mod \mathfrak{M}$ appartient à k. Pour I quelconque, la résolvante peut posséder une racine dans k sans qu'aucun polynôme Q de $L.P$ ne se réduise dans k modulo I. En revanche, la réciproque est vraie comme l'exprime le lemme suivant :

Lemme 2.5. *Soit $Q \in L.P$ et $\overline{Q} = Q \mod I$. Si $\overline{Q} \in k$ alors $x - \overline{Q}$ est un facteur sur k de la résolvante $R_{P,I}$ et, pour tout $i \geq 0$,*

$$p_i(L.P\backslash\{Q\}) \mod I \quad ,$$

est la i-ème fonction puissance s_i des racines de $\frac{R_{P,I}}{x-\overline{Q}}$.

Démonstration. Nous avons toujours $Q(\underline{\alpha}) = Q \mod \mathfrak{M}$. Supposons que $\lambda = Q \mod I$ appartienne à k. Alors $Q(\underline{\alpha}) = Q \mod I$ puisque $I \subset \mathfrak{M}$ et qu'alors $Q(\underline{\alpha}) = Q \mod \mathfrak{M} = \lambda$. Donc $x - \lambda$ est un facteur de la résolvante $R_{P,I}$. Nous avons $s_0 = d - 1$ et pour $i \geq 1$

$$p_i(L.P\backslash\{Q\}) \mod I = (p_i(L.P) - \lambda^i) \mod I = (p_i(L.P) \mod I) - \lambda^i = s_i.$$

□

Lorsque $\lambda \in k$, le polynôme Q est retiré de l'orbite $L.P$. Il s'agit de calculer $s_0 =$, $s_1, \ldots, s_{d-1}$, les d premières fonctions puissances des racines du polynôme $\frac{R_{P,I}}{x-\lambda}$. Ceci est possible, daprès le lemme 2.5, puisque $s_0 = d - 1$ et que pour $i = 1, \ldots, d - 1$

$$s_i = p \mod I$$

où $p = p_i(L.P\backslash\{Q\})$. Ainsi, bien que le polynôme p ne soit pas invariant par L et que le théorème 2.1 ne s'applique pas, comme $p - s_i$ est une $\underline{\alpha}$-relation invariante par L, nous obtenons s_i comme la réduction de p modulo I.

3. Algorithme numérique certifié

Dans toute cette partie, le polynôme f est supposé à coefficients dans $\mathbb{Z}$.

3.1. La méthode numérique.

La méthode employée par Stauduhar ([12]) consiste à calculer

$$\tilde{\underline{\alpha}},$$

un n-uplet constitué d'approximations numériques des racines de f puis un d-uplet $\underline{\tilde{\beta}} = (\tilde{\beta}_1, \ldots, \tilde{\beta}_d)$ formé des évaluations de l'invariant P en les d permutations de $\tilde{\underline{\alpha}}$ par une transversale à gauche de $L \mod H$ (voir lemme 2.2). Pour $i = 1, \ldots, d$,

notons e_i l'entier le plus proche de $e_i(\tilde{\underline{\beta}})$, la i-ème fonction symétrique élémentaire de $\tilde{\beta}_1, \ldots, \tilde{\beta}_d$. Le polynôme

$$\widetilde{R} = x^d - e_1 x^{d-1} + \cdots + (-1)^d e_d$$

est candidat à être la résolvante $R_{P,I}$.

3.2. **Certification algébrique.**

Pour que $\widetilde{R}$ soit la résolvante $R_{P,I}$, il est nécessaire que la marge d'erreur de calcul sur les coefficients de la résolvante soit strictement inférieure à $1/2$. Afin de parer à cette difficulté numérique, nous proposons une certification algébrique basée sur le théorème suivant :

Théorème 3.1. *Soit $\widehat{P}$ l'endomorphisme multiplicatif de $k[x_1, \ldots, x_n]/I$ induit par $P \in k[x_1, \ldots, x_n]$. Alors*

$$\mathrm{Min}_{\widehat{P},I}(P) = 0 \mod I$$

et $\mathrm{Min}_{\widehat{P},I}$ est le polynôme de plus bas degré de $k[x]$ satisfaisant cette propriété. Lorsque k est parfait, $\mathrm{Min}_{\widehat{P},I}$ est la forme sans facteur carré du polynôme caractéristique.

Démonstration. La première partie est évidente puisque l'identité $h(P) = 0 \mod I$ est équivalente au fait que $h(\widehat{P})$ soit l'endomorphisme nul de $k[x_1, \ldots, x_n]/I$. On conclut avec la définition du polynôme minimal d'un endomorphisme.
D'après l'identité (2) exprimant le polynôme caractéristique, sa forme sans facteur carré est le polynôme

$$S = \prod_{\psi \in \{\Psi(\underline{\alpha}) \mid \Psi \in L.P\}} (x - \psi).$$

Lorsque k est parfait, S appartient à $k[x]$. Comme pour tout $\tau \in L$, $(\tau.S(P))(\underline{\alpha}) = S(\tau.P(\underline{\alpha})) = 0$, le polynôme $S(P)$ de $k[x_1, \ldots, x_n]$ appartient à I et S est donc un multiple du polynôme minimal de $\widehat{P}$. Comme $\mathrm{Min}_{\widehat{P},I}(P) \in I$, par définition des idéaux galoisiens, pour tout $\tau \in L$ nous avons $\mathrm{Min}_{\widehat{P},I}(\tau.P(\underline{\alpha})) = (\tau.\mathrm{Min}_{\widehat{P},I}(P))(\underline{\alpha}) = 0$. Par conséquent, puisque toute les racines de $\mathrm{Min}_{\widehat{P},I}$ sont des racines de S qui est sans racine multiple, le polynôme S divise $\mathrm{Min}_{\widehat{P},I}$; ces deux polynômes sont donc égaux. □

Ainsi, un polynôme h de $k[x]$ satisfait $h(P) = 0 \mod I$ si et seulement si h est un multiple du polynôme minimal de $\widehat{P}$.

Nous proposons de détecter lors du calcul les racines multiples de $\widetilde{R}$. Ainsi une approximation $\widetilde{M}(x) \in \mathbb{Z}[x]$ de $\mathrm{Min}_{\widehat{P},I}(x)$ est calculée. Si $\widetilde{M}(P) \in I$ alors $\mathrm{Min}_{\widehat{P},I}$ est un facteur du polynôme sans facteur carré $\widetilde{M}$. Le théorème évident suivant exprime le cas dans lequel $\widetilde{M}$ possède des facteurs "parasites" :

Théorème 3.2. *Supposons que* $\widetilde{M}(P) \in I$. *Alors le polynôme* $\widetilde{M}$ *et son facteur* $\mathrm{Min}_{\widehat{P},I}$ *sont distincts si et seulement si il existe un polynôme* g *de* $\mathbb{Z}[x]$ *tel que*

$$g^2 = \prod_i^m (x - \beta_i)$$

divise la résolvante $R_{P,I}$ *et que les approximations* $\tilde{\beta}_1, \ldots, \tilde{\beta}_m$ *de ses racines sont deux-à-deux distinctes.*
Si tel est le cas alors

$$\prod_i^m (x - \tilde{\beta}_i) = \tilde{g}.g$$

avec $\tilde{g} \in \mathbb{Z}[x]$ *et tel que* $\tilde{g}.\mathrm{Min}_{\widehat{P},I}$ *est un facteur de* $\widetilde{M}$.

Ce que ce théorème exprime c'est que si les approximations numériques aboutissent à considérer comme distinctes des racines identiques de la résolvante, et ce pour toutes les racines d'un facteur g sur $\mathbb{Z}$ de la résolvante, alors ce facteur double n'est pas détecté et $\tilde{g} \neq g$ apparaît comme un facteur parasite dans $\widetilde{M}$. Ce cas est donc très peu probable. Néanmoins, il est toujours possible de certifier le résultat en cherchant sur $\mathbb{Z}$ un facteur h de $\widetilde{M}$ et de degré minimum tel que $h(P) \in I$. Dans ce cas, on est assuré que $h = \mathrm{Min}_{\widehat{P},I}$.

La certification algébrique nécessite d'évaluer $\widetilde{M}$ en l'invariant P pour le réduire modulo I. Pour ne pas être brutale, cette évaluation doit être réalisée en calculant inductivement $P \mod I, P^2 \mod I, \ldots, P^s \mod I$, avec $s = deg(\widetilde{M})$, simultanément au calcul de $\widetilde{M}(P)$. C'est donc le shéma d'évaluation de Horner qui est adapté à la situation. Pour le décrire dans notre contexte, supposons que $\widetilde{M} = x^s + a_{s-1}x^{s-1} + \cdots + a_0$. Alors $\widetilde{M}(P) \mod I$ est la valeur de u suite au calcul suivant :

`u=1 et v=P` $\mod I$
`Pour i=s-1 à 0 Faire u= u*v+`$a_i \mod I$

3.3. **Exemple.**

Nous choisissons volontairement un exemple très simple afin d'illustrer la certification algébrique. Soit $f(x) = x^4 - 4x + 1$ de racines approchées

$$\tilde{\alpha_1} = 0.25099 + 0.E - 38 \times i,$$

$$\tilde{\alpha_2} = 1.49335 + 0.E - 38 \times i,$$

$$\tilde{\alpha_3} = -0.87217 - 1.38103 \times i,$$

$$\tilde{\alpha_4} = \overline{\tilde{\alpha_3}}$$

et $\mathfrak{S}$ son idéal des relations symétriques engendré par les modules de Cauchy de f :

$$\begin{aligned}
&x_1^4 - 4x_1 + 1,\\
&x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3 - 4,\\
&x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2,\\
&x_4 + x_3 + x_2 + x_1.
\end{aligned}$$

Nous avons $L = S_5$, le groupe symmétrique de degré 5, et nous prenons le groupe alterné pour H. La transversale à gauche de L mod H est formée par les deux permutations $\sigma_1 = Id_4$ et $\sigma_2 = (3, 4)$. Le H-invariant L-primitif que nous choisissons est le polynôme

$$\begin{aligned}
P = x_4^3x_3^2x_2 + x_4x_3^3x_2^2 + x_4^2x_3x_2^3 + x_4^2x_3^3x_1\\
+x_4^3x_2^2x_1 + x_3^2x_2^3x_1 + x_4^3x_3x_1^2 + x_3^3x_2x_1^2 + x_4x_2^3x_1^2\\
+x_4x_3^2x_1^3 + x_4^2x_2x_1^3 + x_3x_2^2x_1^3 \quad .
\end{aligned}$$

Notons $\tilde{\beta}_1$ et $\tilde{\beta}_2$ les deux approximations des racines de la résolvante obtenues comme suit :

$$\tilde{\beta}_1 \;=\; \sigma_1.P(\underline{\tilde{\alpha}}) \;=\; P(\underline{\tilde{\alpha}}) \;=\; -24.000 + 40.792 \times i$$

et $\tilde{\beta}_2 = \sigma_2.P(\underline{\tilde{\alpha}}) \;=\; -24.000 - 40.792 \times i$, le conjugué de $\tilde{\beta}_1$. Il n'y a pas de racine multiple à exclure. Notons a la partie réelle de $\tilde{\beta}_1$ et b sa partie imaginaire. Alors

$$\widetilde{M} \;=\; (x - \tilde{\beta}_1)(x - \tilde{\beta}_2) = x^2 - 2ax + a^2 + b^2 = x^2 + 48x + 2240 \quad .$$

Le résultat de la réduction de $\widetilde{M}(P)$ modulo l'idéal I étant nul et $\widetilde{M}(P)$ ne pouvant être réductible sur $\mathbb{Z}$, en vertu de notre certification, nous affirmons que

$$R_{P,I} = Min_{\widehat{P},I} \;=\; \widetilde{M}(P) = x^2 + 48x + 2240 \quad .$$

Conclusion

Afin d'élaborer nos algorithmes, nous avons exploité les propriétés des idéaux galoisiens. Dans le cas de l'algorithme algébrique, nous avons généralisé le théorème fondamental des fonctions symétriques et dans le cas numérique, nous certifions avec l'appartenance à un idéal. Les comparaisons de temps montrent l'efficacité de notre algorithme algébrique `ResolvanteAlgebrique`. Les propositions présentées pour son optimisation apporteront des gains importants. Nous travaillons à une implantation en `Sage` de la version parallèle incluant les résultats de [3].

Références

[1] Ines Abdeljaouad. Calculs d'invariants primitifs de groupes finis. *Theor. Inform. Appl.*, 33(1) :59–77, 1999. (`http://www-gap.mcs.st-and.ac.uk/Gap3/Contrib3/contrib.html`).

[2] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6) :635–651, 2000.

[3] A. Bostan, M. Chowdhury, J. Van der Hoeven, and É. Schost. Homotopy methods for multiplication modulo triangular sets, 2009. Technical Report http ://arxiv.org/abs/0901.3657v1, Arxiv. To appear in JSC.

[4] A. Cauchy. Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée. *Oeuvres*, **5** :473 Extrait 108, 1840.

[5] Girard. Invention nouvelle en algèbre. *Amsterdam*, 1629.

[6] J.-L. Lagrange. Réflexions sur la résolution algébrique des équations. *Prussian Academy*, 1770.

[7] J.-L. Lagrange. *Oeuvres, Tome VIII, Notes sur la théorie des équations algébriques, Note X.* Publiées sous les auspices du ministère de l'instruction publique, 1808.

[8] A. Lascoux and M.P. Schützenberger. Formulaire raisonné de fonctions symétriques. Publication interne L.A. 248, Laboratoire LITP, Université Paris 7, France, 1985.

[9] I.G. Macdonald. *Symmetric Functions and Hall Polynomials, second ed.* Oxford : Clarendon Press. ISBN 0-19-850450-0 (paperback, 1998), 1995.

[10] N. Rennert and A. Valibouze. Calcul de résolvantes avec les modules de Cauchy. *Experiment. Math.*, 8(4) :351–366, 1999.

[11] W. Schelter. *Manuel de Maxima*, 2001. `(http://maxima.sourceforge.net)`.

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

[13] A. Valibouze. Théorie de Galois constructive, 1994. HDR, Université Pierre et Marie Curie (UPMC-Paris 6), France.

[14] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4) :507–535, 1999. (Version longue du rapport LIP6 1997/014).

[15] A. Valibouze. Classes doubles, idéaux de Galois et résolvantes. *Rev. Roum. de Math. Pures et Appl.*, 52 no 1, 2007.

Ines Abdeljaoued-Tej, ESSAI, 6 rue des metiers, La Charguia 2, 2036 Ariana, Tunisia, Email : i.tej@gnet.tn

Faiçal Bouazizi, Département de Mathématiques, Faculté des Sciences de Sfax, 3000 Sfax, Tunisia & LIP6, Université Pierre et Marie Curie, 4, place Jussieu, F-75252 Paris Cedex 05, France, Email : faical.bouazizi@lip6.fr

Annick Valibouze, LIP6 and LSTA, Université Pierre et Marie Curie, 4, place Jussieu, F-75252 Paris Cedex 05, France, Email : annick.valibouze@upmc.fr