THÉORIE DE GALOIS CONSTRUCTIVE

ANNICK VALIBOUZE *

Cet article présente la correspondance entre les groupes finis et les résolvantes de Lagrange et montre comment elle est utilisée pour les problèmes de Galois directe et inverse.

Introduction

Soit k un corps de caractéristique 0. Nous considérons un polynôme f, sans facteur multiple, de degré n et à coefficients dans k. L'étude des racines du polynôme f se réalise à travers l'idéal I des relations algébriques entre ces racines. Le calcul effectif de cet idéal est algorithmiquement possible mais extrêmement coûteux. Il est en fait presque toujours irréalisable (voir [30] et [1]). En revanche, cet idéal permet d'exhiber des outils pour obtenir des informations sur les racines du polynôme f. En particulier, l'ensemble des permutations pour lesquelles ces relations restent invariantes est un groupe fini défini par Évariste Galois en l'identifiant à l'ensemble des permutations qui échangent les racines d'un facteur irréductible simple sur k de la *résolvante de Galois* de f (voir le paragraphe 1.2). Ce groupe fini est noté $\mathrm{Gal}_k(f)$ et appelé **groupe de Galois du polynôme f sur k**. Le groupe de Galois de f sur k est isomorphe au groupe des k-automorphismes du corps de décomposition de f.

Tous les sous-corps du corps de décomposition du polynôme f s'obtiennent à partir de tous les sous-groupes de $\mathrm{Gal}_k(f)$, et réciproquement. Cette correspondance entre des groupes et des corps s'appelle la **correspondance Galoisienne**. La correspondance de Lagrange entre des corps et des *résolvantes* (définies au paragraphe 1.2) est à la base de la correspondance Galoisienne. Cette présentation définit ce que sont les résolvantes et décrit la correspondance entre les résolvantes et les groupes. Cette correspondance utilise la correspondance Galoisienne et s'appuie sur le théorème de conservation de l'élément primitif (voir le paragraphe 3).

La correspondance entre les groupes et les résolvantes permet d'obtenir tous les algorithmes pour déterminer le groupe de Galois d'un polynôme avec des résolvantes et donc d'en extraire le meilleur. Pour un implantation efficace, il est nécessaire de coupler cet algorithme avec des techniques modulaires (voir [23], [18] ou [31]).

Cette nouvelle correspondance offre également des réponses partielles très simples au **problème de Galois inverse** : *étant donné un groupe fini, chercher s'il existe un polynôme dont il soit le groupe de Galois.* (voir paragraphe 2.2).

La recherche effective du groupe de Galois d'un polynôme nécessite des calculs de résolvantes. Les différentes méthodes ne seront pas abordées ici (voir par exemples [5], [7], [12], [19], [20],[26], [27], [28], [32], [35],...). En `Macsyma`, les résolvantes se calculent avec l'extension `SYM` (voir [22] et [29]).

---

*projet Galois supporté par le GDR de Calcul Formel MEDICIS; Centre de Calcul Formel de l'École Polytechnique

Dans toute la suite, nous nous donnons un ensemble d'indéterminées $x_1, \ldots, x_n$. Le groupe symétrique de degré n est noté $\mathfrak{S}_n$. Nous nous donnons également L, un sous-groupe quelconque de $\mathfrak{S}_n$, et H, un sous-groupe quelconque de L. Nous fixons $\mathcal{T} = \{\tau_1, \ldots, \tau_e\}$, une transversale gauche de L mod H (i.e. $L/H = \{\tau_1 H, \ldots, \tau_e H\}$).

1. Résolvantes

Dans son mémoire *Réflexions sur la résolution algébrique des équations*, Lagrange trace un historique fort intéressant (voir [19]). Pour les degrés 3 et 4, il présente les méthodes employées pour résoudre les équations, en essayant de les comparer. Puis, pour chaque méthode, il s'emploie à montrer qu'un même outil, qu'il appelle *résolvante*, est utilisé ; Lagrange écrit sur son travail : *Cet examen aura un double avantage ; d'un côté il servira à répandre une plus grande lumière sur les résolutions connues du troisième et du quatrième degré ; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des degrés supérieurs, en leur fournissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles.* Lagrange disait vrai. Après lui, l'étude des équations ne pourra plus, comme auparavant, être menée à coups d'astuces.

1.1. Actions de groupes et invariants. Le groupe symétrique $\mathfrak{S}_n$ agit naturellement sur le corps des fractions $k(x_1, \ldots, x_n)$: soient $\sigma \in \mathfrak{S}_n$ et $P \in k(x_1, \ldots, x_n)$ alors $\sigma.P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Soit E un sous-ensemble de $\mathfrak{S}_n$, l'**orbite de P sous l'action de** E, notée $E.P$ est $\{\tau.P \mid \tau \in E\}$. Pour tout sous-groupe G de $\mathfrak{S}_n$ agissant sur un corps K, le sous-corps de K constitué par les éléments de K invariants par G est noté K^G.

Un polynôme Θ de $k[x_1, \ldots, x_n]$ est un **invariant primitif de H relativement à** L si $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$. Si $L = \mathfrak{S}_n$ on dit que Θ est un **invariant primitif du groupe H**. Tout sous-groupe de L possède un invariant primitif (en réalité plusieurs) relativement à L et tout polynôme de $k(x_1, \ldots, x_n)^L$ est un invariant primitif d'un sous-groupe de L relativement à L. Un polynôme $\Theta \in k[x_1, \ldots, x_n]$ est un invariant primitif de H relativement à L si et seulement si Θ est un élément primitif du corps $k(x_1, \ldots, x_n)^H$ sur le corps $k(x_1, \ldots, x_n)^L$. Si tel est le cas, alors l'orbite $L.\Theta$ est constituée des e fonctions distinctes $\tau_1.\Theta, \ldots, \tau_e.\Theta$.

La recherche des invariants primitifs est souvent intuitive, (voir [5], [13], [8], [25] et d'autres). Il existe néanmoins une méthode automatique de recherche d'un invariant primitif, optimale du point de vue du degré des monômes apparaissant dans son expression (voir [14]).

Exemple 1. Le polynôme x_1x_2 est un invariant primitif de $\mathfrak{S}_2 \times \mathfrak{S}_{n-2}$, le déterminant de Vandermonde $\delta_n = \prod_{1 \le i < j \le n}(x_i - x_j)$ est un invariant primitif du groupe alterné $\mathfrak{A}_n$, le polynôme $x_1x_2^2x_3^3$ est un invariant primitif du sous-groupe identité dans $\mathfrak{S}_4$ et le polynôme $b_4 = x_1x_2 + x_3x_4$ est un invariant primitif du groupe diédral $\mathcal{D}_4$ dans $\mathfrak{S}_4$.

1.2. La résolvante. Soit Θ un invariant primitif de H relativement à L. La **résolvante (générique) par Θ relative à** L, notée $\mathcal{L}_\Theta^L$, est le polynôme minimal de

Θ sur $k(x_1,\dots,x_n)^L$. Elle est formellement donnée par

$$\mathcal{L}^L_\Theta(x) = \prod_{\Psi\in L.\Theta}(x-\Psi) = \prod_{i=1}^{e}(x-\tau_i.\Theta) \qquad . \tag{1}$$

Une telle résolvante est une **H-résolvante relative à L.**

Si $\Psi \in k(x_1,\dots,x_n)$, une évaluation quelconque de Ψ en les n racines du polynôme f est notée $\tilde{\Psi}$. Cette évaluation en les racines de f est à manipuler avec prudence ; en effet, si τ est une permutation de $\mathfrak{S}_n$, l'égalité $\widetilde{\tau\Psi} = \tau\tilde{\Psi}$ n'est certaine que si $\tau \in \mathrm{Gal}_k(f)$.

la résolvante de f par Θ relative à L, est le polynôme $\mathcal{L}^L_{\Theta,f} = \widetilde{\mathcal{L}^L_\Theta}$. Si Θ est un invariant primitif du groupe identité Id_n dans $\mathfrak{S}_n$, la résolvante $\mathcal{L}_{\Theta,f}$ est une **résolvante de Galois de f** si tous ses facteurs sont simples.

Si $\mathrm{Gal}_k(f)$ est inclus dans le groupe L, les coefficients de la résolvante $\mathcal{L}^L_{\Theta,f}$ appartiennent au corps k puisque, étant invariants par L, ils le sont aussi par $\mathrm{Gal}_k(f)$. Lorsque $L = \mathfrak{S}_n$, la résolvante $\mathcal{L}^L_{\Theta,f}$ est notée $\mathcal{L}_{\Theta,f}$ et appelée **résolvante de f par Θ**. Ses coefficients sont des polynômes symétriques en les racines de f.

Pour tout τ dans L, $\tau.\Theta$ est un invariant primitif du conjugué $H^\tau = \tau H \tau^{-1}$ de H dans L et la H^τ-résolvante $\mathcal{L}^L_{\tau.\Theta,f}$ est identique à la H-résolvante $\mathcal{L}^L_{\Theta,f}$.

Exemple 2. Fixons $n = 3$ et prenons $\Theta = x_1x_2^2$, alors

$$\mathcal{L}_\Theta(x) = (x-x_1x_2^2)(x-x_1x_3^2)(x-x_2x_1^2)(x-x_2x_3^2)(x-x_3x_1^2)(x-x_3x_2^2) \qquad .$$

1.3. Partition d'un polynôme. À un polynôme à coefficients dans k et sans racine multiple, on associe une partition qui consiste en la suite finie d'entiers $(i_1,\dots,i_q)$ (avec $i_1 \geq \dots \geq i_q$), des différents degrés des facteurs du polynôme qui sont irréductibles sur k. Cette suite d'entiers est appelée la **partition du polynôme**. Un invariant pour lequel la résolvante associée est sans facteur multiple est dit **f-séparable**.

Exemple 3. La partition du polynôme $(x^5+x^2+1)(x^3+3)(x^3+x+1)(x^2+x+1)(x+5)$ est $(5,3,3,2,1)$, notée également sous la forme exponentielle $(5,3^2,2,1)$.

2. Matrices des partitions et des groupes

Dans ce qui suit, sauf indication contraire, nous supposerons que les invariants considérés sont f-séparables. Nous supposons, de plus, que $\mathrm{Gal}_k(f)$ est un sous-groupe de L.

2.1. Matrice des partitions. La partition d'une H-résolvante de f relative à L ne dépend que de L de H et de $\mathrm{Gal}_k(f)$, on la note $[\mathrm{Gal}_k(f),H]_L$. (On note $[\mathrm{Gal}_k(f),H]$ lorsque $L = \mathfrak{S}_n$.) Le groupe de Galois de f est défini à une conjugaison près (i.e. à une permutation près de ses racines) et une H-résolvante ne dépend que de la classe de conjugaison de H dans L (voir paragraphe précédent). Donc une partition $[G,H]_L$ ne dépend que des classes de conjugaison dans L des sous-groupes G et H de L.

L'idée de construire, a priori, une matrice carrée $\mathcal{A}_L = ([G,H]_L)_{G,H}$ est assez naturelle et possible (voir [2]). La matrice $\mathcal{A}_L$ est appelée **matrice des partitions relative à L.** Le groupe G est appelé le **groupe candidat** (i.e. candidat à être le groupe de Galois) et le groupe H est appelé le **groupe test** (i.e. à tester f avec une H-résolvante pour connaître son groupe de Galois).

Deux formules simples permettent de **calculer la partition** $[G, H]_L$: cette partition est égale à la séquence (ordonnée comme une partition) des cardinaux des orbites de G sur les classes à gauche de L mod H ; cette partition s'obtient également à partir des indices $[G : G \cap H^\tau]_L$ où τ parcourt la transversale $\mathcal{T}$ (voir le paragraphe 3.2 dans [2]).

Le système GAP (voir [16]) a été utilisé pour le calcul des matrices $\mathcal{A}_{\mathfrak{S}_4}, \ldots, \mathcal{A}_{\mathfrak{S}_8}$. Les matrices $\mathcal{A}_{\mathfrak{S}_9}, \mathcal{A}_{\mathfrak{S}_{10}}$ et $\mathcal{A}_{\mathfrak{S}_{11}}$ sont partiellement calculées (voir [3], [17] et[33]). Ces matrices et sous-matrices sont tabulées sous forme de listes et sont exploitables dans un programme.

2.2. Matrice des groupes. De même que pour la partition d'une résolvante, **le groupe de Galois d'un facteur simple d'une H-résolvante du polynôme f relative à L ne dépend que du groupe L, du groupe test H et du groupe de Galois de f** (voir [34]). Chercher à identifier, a priori, ces groupes de Galois est une idée que l'on peut trouver dans l'article d'E.H. Berwick sur le degré 6. A. Colin a également travaillé sur les différents groupes apparaissant lors de l'étude d'une résolvante (voir [11]).

L'information la plus fine concerne les facteurs irréductibles simples. La restriction aux facteurs irréductibles simples des résolvantes relatives à L induit une matrice $\mathcal{B}_L$, appelée **matrice des groupes relative à** L. La matrice $\mathcal{B}_L$ inclut les informations de la matrice $\mathcal{A}_L$.

Les groupes de Galois des facteurs simples des résolvantes sont des groupes pour lesquels le problème de Galois inverse peut être envisagé ; en effet, si le groupe de Galois G d'un facteur h de degré m d'une résolvante est connu, avec sa représentation dans $\mathfrak{S}_m$, le calcul de h donne un polynôme dont le groupe de Galois est G. Cette méthode utilisée avec $m = 12$ a permis de calculer un trentaine de polynômes (voir [17]).

Les groupes de Galois des facteurs simples d'une résolvante d'un polynôme de groupe de Galois G s'obtiennent également avec un algorithme permettant d'identifier G et un polynôme connu dont le groupe de Galois est G. C'est un intérêt que présente le problème de Galois inverse par rapport au problème direct.

Une légère modification du programme GAP qui calcule la matrice $\mathcal{A}_L$ permet de calculer, a priori, les groupes de Galois des facteurs simples des résolvantes.

3. Matrices et résolvantes

Le lien entre les partitions des résolvantes et les matrices $\mathcal{A}_L$ et $\mathcal{B}_L$ se réalise avec le **Théorème de conservation de l'élément primitif** (voir [2] Théorème 6.6 et [34]) : **Soit Θ un invariant primitif de H relativement à L tel que $\tilde{\Theta}$ soit une racine simple de la résolvante $\mathcal{L}^L_{\Theta,f}$. Alors, $\tilde{\Theta}$ est un élément primitif du corps $k(\alpha_1, \ldots, \alpha_n)^{G \cap H}$ sur le corps $k(\alpha_1, \ldots, \alpha_n)^{G \cap L} = k$, où $G = \mathsf{Gal}_k(f)$.**

L'idée de ce théorème est de comprendre ce qui se passe lors de la spécialisation de la résolvante $\mathcal{L}^L_\Theta$ en les racines $\alpha_1, \ldots, \alpha_n$ de f.

Remarque 1. Avec le Théorème de conservation de l'élément primitif les résultats bien connus suivants deviennent évidents : les facteurs irréductibles de la résolvante de Galois d'un polynôme sont tous de degré égal à l'ordre du groupe de Galois de ce polynôme ($H = Id_n$) ; $G = \mathrm{Gal}_k(f)$ est inclus dans un des conjugués d'un groupe test H si et seulement si il existe une H-résolvante de f qui ait un facteur linéaire simple ($G \cap H^\tau = H^\tau$); en particulier, $\mathrm{Gal}_k(f)$ est pair si et seulement si le discriminant de f est un carré ($H = \mathfrak{A}_n$ et $\Theta = \delta_n$).

4. Identification de groupe de Galois

Jusqu'en 1993, deux orientations ont été envisagées : une première, intuitive, n'utilise que des sous-matrices de $\mathcal{A}_{\mathfrak{S}_n}$ avec des résolvantes absolues et l'autre utilise des résolvantes relatives sans exploiter les matrices $\mathcal{A}_L$. Les deux premiers paragraphes aborderont ces méthodes et le troisième décrira celle qui utilise les matrices $\mathcal{A}_L$ et $\mathcal{B}_L$.

4.1. Méthode intuitive utilisant $\mathcal{A}_{\mathfrak{S}_n}$. Si une sous-matrice de $\mathcal{A}_{\mathfrak{S}_n}$, obtenue en retirant des groupes tests, a ses lignes distinctes, alors il est possible de déterminer le groupe de Galois du polynôme f avec les groupes tests restants. C'est le choix de ces groupes tests, de leur invariants primitifs et des méthodes employées pour calculer les résolvantes qui a déterminé les avancées dans la recherche du groupe de Galois d'un polynôme.

Si le choix des groupes tests est intuitif, les lignes de la sous-matrice de $\mathcal{A}_{\mathfrak{S}_n}$, induite par ce choix, ne sont donc pas nécessairement distinctes. De plus, dans la littérature, le polynôme f est toujours supposé irréductible. La première étude complète est due à E.H. Berwick en degré 6 (voir [5]). Il conserve comme groupes tests les sous-groupes maximaux de $\mathfrak{S}_6$. S'inspirant des travaux d'E.H. Berwick, en 1931 H.O. Foulkes établit une sous-matrice des partitions $\mathcal{A}_{\mathfrak{S}_7}$ avec 3 groupes tests (voir [13]). Les sept lignes de sa sous-matrice étant toutes distinctes, les trois groupes tests suffisent à identifier le groupe de Galois de tout polynôme irréductible de degré 7. Pour utiliser la méthode de H.O. Foulkes, il est nécessaire de calculer des résolvantes de degré 30 (associée à $PSL(2,7) = G_{168}$) et 120. Personne, à ce jour, n'a su calculer une G_{168}-résolvante. H.O. Foulkes utilise la même méthode que E.H. Berwick pour calculer sa sous-matrice de $\mathcal{A}_{\mathfrak{S}_7}$: *faire agir le groupe candidat G sur les conjugués dans $\mathfrak{S}_n$ d'un invariant primitif du groupe test H puis calculer le nombre d'éléments dans chaque orbite.* En 1981, L.E. Soicher et McKay ont choisi des groupes tests pour lesquels les résolvantes et les partitions sont facilement calculables sur machines, c'est-à-dire des groupes, non transitifs, du type $H_m = \mathfrak{S}_m \times \mathfrak{S}_{n-m}$ ou bien $K_m = \mathrm{Id}_m \times \mathfrak{S}_{n-m}$ (voir [26] ou [25]). Les résolvantes associées aux invariants primitifs $x_1 \cdots x_m$ et $x_1^{a_1} \cdots x_m^{a_m}$ de H_m et K_m, respectivement, se calculent très rapidement (voir [32] et [7]). Les sous-matrices de partitions publiées par L.E. Soicher ont été calculées par G. Butler en étudiant l'action du groupe candidat sur les m-ensembles pour les groupes tests H_m et sur les m-séquences pour les groupes tests K_m. Avec ces sous-matrices, le groupe de Galois d'un polynôme irréductible de degré inférieur ou égal à 7 s'identifie rapidement. C'est cette méthode qui est implantée dans `MAPLE` (voir [21]). En 1981, G. Butler and J. McKay (voir [6]) publient la liste des sous-groupes transitifs de $\mathfrak{S}_n$ ($n \leq 11$) permettant à J. McKay et E.Regener de publier des sous-matrices des matrices $\mathcal{A}_{\mathfrak{S}_n}$ ($n \leq 11$) pour les groupes tests du type H_m et K_m et des groupes candidats transitifs (voir [24]). Mais ces groupes tests ne suffisent pas en degré 8, 9, 10 et 11 (i.e. les lignes de ces sous-matrices ne sont pas distinctes).

4.2. Méthodes des résolvantes relatives. L'utilisation des résolvantes relatives à un sous-groupe strict L de $\mathfrak{S}_n$ a été initiée par R.P. Stauduhar (voir [28]). Sa méthode, reprise plus tard par Y. Eichenlaub et M. Olivier (voir [10]), consiste à tester l'inclusion du groupe de Galois dans des sous-groupes de $\mathfrak{S}_n$. En effet, si $\mathrm{Gal}_k(f)$ est un sous-groupe de L et si la résolvante $\mathcal{L}^L_{\Theta,f}$ a un facteur linéaire simple $(x - \widetilde{\tau.\Theta})$ sur k, alors le groupe de Galois de f est un sous-groupe du conjugué H^τ de H (voir Remarque 1). L'algorithme de Stauduhar démarre en testant l'inclusion de $\mathrm{Gal}_k(f)$ dans chaque sous-groupe maximal de $\mathfrak{S}_n$ (au départ les résolvantes sont donc absolues) puis descend dans le graphe des sous-groupes en réordonnant les racines de f en fonction du conjugué dans lequel le groupe de Galois de f est inclus. L'algorithme s'arrête sur L tel que, pour tout sous-groupe maximal H de L, aucune H-résolvante n'a de facteur linéaire simple. À ce stade $\mathrm{Gal}_k(f) = L$. La méthode de calcul des résolvantes, proposés par Stauduhar, est numérique. Il existe un algorithme de recherche de groupe de Galois entièrement algébrique s'inspirant de la méthode de Stauduhar (voir [12]).

4.3. Utilisation de la matrice $\mathcal{B}_L$.

Cas $L = \mathfrak{S}_n$. Les lignes de la matrice carrée des partitions $\mathcal{A}_{\mathfrak{S}_n}$ sont distinctes deux à deux (voir [2] Théorème 3.1). Ce qui signifie qu'il est toujours possible de trouver le groupe de Galois d'un polynôme séparable, non nécessairement irréductible, avec les partitions des résolvantes absolues.

Comme la matrice $\mathcal{B}_{\mathfrak{S}_n}$ contient toutes les informations de la matrice $\mathcal{A}_{\mathfrak{S}_n}$, ses lignes sont également distinctes. Cette matrice livre toutes les possibilités d'utilisation de résolvantes absolues, il devient possible d'élaborer le "meilleur" algorithme permettant d'identifier le groupe de Galois d'un polynôme de degré n, par l'unique étude des résolvantes absolues.

L'utilisation de la matrice $\mathcal{B}_{\mathfrak{S}_n}$ permet parfois de départager les groupes candidats plus rapidement qu'avec uniquement les partitions des résolvantes absolues (voir l'Exemple 4) et elle permet de départager des groupes candidats alors la sous-matrice de $\mathcal{A}_{\mathfrak{S}_n}$ calculée sur machine ne suffit pas (voir l'Exemple 5) ;

Les temps nécessaire au calcul des résolvantes et à leur factorisation conditionnent les critères de sélection et d'ordonnancement des groupes tests. Ces critères sont donc l'indice d'un groupe test H dans $\mathfrak{S}_n$ et la rapidité de calcul d'une H-résolvante. Par exemple, le premier groupe test est toujours $H = \mathfrak{S}_1 \times \mathfrak{S}_{n-1}$ dont une résolvante associée est le polynôme f lui-même, qu'il suffit de factoriser. A priori, le second groupe test est le groupe alterné avec δ_n comme invariant primitif (voir Remarque 1).

Exemple 4. Avec seulement les partitions des résolvantes absolues, il est coûteux de départager trois sous-groupes T_{25}, T_{36} et T_{48} de $\mathfrak{S}_8$. Soit H le sous-groupe de $\mathfrak{S}_8$ d'indice 35 dont $x_1x_2x_3x_4x_5^2x_6^2x_7^2x_8^2$ est un invariant primitif. Si f a T_{25}, T_{36} ou T_{48} comme groupe de Galois, alors il existe une H-résolvante de f qui ait un facteur simple de degré 7. Le groupe de Galois de ce facteur est différent selon que celui de f est T_{25}, T_{36} ou T_{48}. La détermination de ces groupes est alors très rapide (voir [34]).

Exemple 5. Dans la sous-matrice de $\mathcal{A}_{\mathfrak{S}_{10}}$ calculée avec `GAP`, les lignes de deux groupes candidats T_{38} et T_{39} sont identiques (i.e. on ne sait pas les départager avec des partitions). Mais les lignes de T_{38} et T_{39} sont distinctes dans la sous-matrice de $\mathcal{B}_{\mathfrak{S}_{10}}$. Il est donc possible de les départager (voir [34]).

Cas général. Lorsque $L \neq \mathfrak{S}_n$, La matrice des groupes $\mathcal{B}_L$ permet d'exploiter toute la factorisation de la résolvante $\mathcal{L}^L_{\Theta,f}$ pour déterminer le groupe de Galois de f, plutôt que de se contenter seulement des facteurs linéaires. La distinction habituellement faite entre la recherche par les résolvantes relatives et celle par les résolvantes absolues n'a donc pas lieu d'être. La méthode générale consiste à calculer et à factoriser d'abord des résolvantes absolues rapides à obtenir puis, à chaque étape, à évaluer la complexité effective des différents calculs possibles de résolvantes (absolues ou relatives) pour déterminer la plus intéressante à calculer et à factoriser. Restreinte à la matrice $\mathcal{A}_L$, cette méthode appelée *la chasse aux résolvantes relatives* est préconisée dans [2] page 29.

Remarque 2. La parité du groupe de Galois d'un facteur est aussi une information intéressante, même quand le degré du facteur est supérieur à celui de f.

5. Résolvantes non séparables

Dans ce qui précède, il est supposé que les invariants sont f-séparables, ce qui est loin de refléter la réalité. Mais, **pour tout sous-groupe H de $\mathfrak{S}_n$, il existe une H-résolvante f-séparable** (voir [2] Théorème 4.5). Il existe également des résolvantes séparables pour tout f ; par exemple la résolvante de Cayley est séparable pour tout polynôme irréductible (voir [2] Théorème 10.9).

Soit Θ un invariant non f-séparable. Une méthode est de remplacer f par une résolvante de Tschirnhaus, avec $H = \mathfrak{S}_1 \times \mathfrak{S}_{n-1}$ et $\Theta \in k[x_1]$. Si la résolvante $\mathcal{L}_{\Theta,f}$ est sans facteur multiple, alors son groupe de Galois est celui f. Une autre est de transformer l'invariant primitif non f-séparable (voir [12]). Ces méthodes présentent l'inconvénient d'accroître les coefficients. Elle peuvent parfois être évitées avec le Théorème des multiplicités (voir [2] Théorème 10.6 et Remarque 14).

6. Factorisation des résolvantes

Il n'est pas toujours nécessaire de factoriser toute une résolvante. Par exemple, la matrice $\mathcal{A}_{\mathfrak{S}_6}$ fait apparaître que H_{12}, le sous-groupe pair d'ordre 36 dans $\mathfrak{S}_6$ départage les groupes D_6 et Z_6 (le groupe diédral et le groupe cyclique, respectivement) avec comme partitions $[D_6, H_{12}] = (2, 6, 12)$ et $[Z_6, H_{12}] = (2, 6^3)$ (voir [3]). Il suffit donc de ne factoriser qu'un facteur de degré 12, pour départager les deux groupes. Dans ce cas c'est possible, puisque l'invariant $\delta_6 b_6$ de H_{12} permet d'obtenir le facteur de degré 12 de la résolvante associée $\mathcal{L}_{\delta_6 b_6,f}$ à partir du facteur de degré 6 de la résolvante $\mathcal{L}_{b_6,f}$ (à supposer que f ait D_6 ou Z_6 comme groupe de Galois) (voir [3]). Dans d'autres cas, ce sont les facteurs irréductibles de petits degrés de la résolvante qui permettent de départager les groupes. C. J. Williamson réalise des factorisations partielles pour calculer le groupe de Galois d'un polynôme de degré 24 (voir [9]).

Une implantation est réalisée dans le système de calcul formel `AXIOM` et des optimisations sont en cours (voir [4] et [20]).

References

1. Hirokazu Anai, Masayuki Noro and Kazuhiro Yokoyama *Computation of the splitting field and the Galois groups of polynomials* présentation orale à MEGA94
2. J.M.Arnaudiès , A. Valibouze, (1993) *Résolvantes de Lagrange*, Rapport interne LITP 93.61
3. J.M.Arnaudiès , A. Valibouze, (1994) *Groupes de Galois de polynômes en degré 4 à 11*, Rapports internes LITP 94.25, 94.30, 94.48, 94.49, 94.50
4. `AXIOM` *The Scientific Computation System* Richard Jenks and Robert Sutor,Springer-Verlag 1992,ISBN 0-387-97855-0
5. E.H. Berwick , (1929) *On Soluble Sextic equations* Proc. London Math. Soc. (2) **29**, 1-28.
6. G. Butler and J. McKay, (1983), *The transitive groups of degree up to 11*, Comm. Algebra **11**, 863-911.
7. D. Casperson, J. McKay (1994) *Symmetric functions, m-sets, and Galois groups* à paraître dans Math. Comp.
8. A. Cayley, (1861), *On a new auxiliary equation in the theory of equation of the fifth order*, Philosophical Transactions of the Royal Society of London, **CLL**
9. C. J. Williamson (1994) *On Algebraic Construction Of Tri-Diagonal Matrices*, Submitted to Proceedings of CNTA-4 (Canadian Number Theory Association)
10. Henri Cohen **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics **138**, Springer Verlag, 1993
11. A. Colin *Théorie de Galois effective et implantation en AXIOM* Mémoire de DEA
12. A. Colin *Formal Computation of Galois groups using relative resolvent polynomials* AAECC'95 (Paris, Juillet 1995), LNCS **948**.
13. H.O. Foulkes, (1931), *The résolvents of an equation of seventh degree*, Quart. J. Math. Oxford Ser. (2), 9-19.
14. K. Girstmair *On invariant Polynomials and Their Application in Field Theory* Maths of Comp., vol. 48, no 178, 1987 (781-797)
15. Galois, E., **Oeuvres Mathématiques**, publiées sous les auspices de la SMF, Gauthier-Villars, 1897
16. G.A.P. `Groups, Algorithms and Programming` Martin Schönert and others, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, **93**, gap@samson.math.rwth-aachen.de
17. I. Gil-Delessalle, A. Valibouze, (1996), *Galois inverse problem for some subgroups of degree 12*, proposé à MEGA'96
18. J.C. Lagarios et A.M. Odlyzko *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields (L-functions and Galois Theory), A. Frölich, ed., Academic Press, 1977, pp. 409-464
19. Lagrange, J.L., *Reflexions sur la résolution algébrique des équations*, **Mémoires de l'Académie de Berlin**, 205-421, (**Oeuvres de Lagrange**, tome IV, 205-421)
20. F. Lehobey *Algorithmiques Méthods and Practical Issues in the Computation of Galois Groupe of Polynomials*, Mémoire de DEA option algorithmique, Algèbre et Géométrie, Université de Rennes I, (1994)
21. `MAPLE` 3 volumes : *Maple V - Maple Language Reference Manual, Maple V - Maple Library Reference Manual, Maple V - First Leaves: A Tutorial Introduction to Maple*, Springer-Verlag
22. `MAXIMA` Maxima DOE maintenu par William Schelter
23. J. McKay, (1979), *Some remarks on computing Galois groups*, SIAM J. Comput. **8**, 344-347.
24. J. McKay et E.Regener, (1985), *Actions of permutation groups on r-sets* Communications in Algebra, 13(3), 619-630

25. J. McKay and L. Soicher, (1985), *Computing Galois Groups over the rationals*, Journal of number theory **20**, 273-281.
26. L. Soicher, *The computation of the Galois groups*, Thèse du departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).
27. L. Soicher, An Algorithm for Computing Galois Groups, Computational Group Theory, 1984 Academic Press, London, 291-296
28. R.P. Stauduhar, (1973), *The determination of Galois groups*, Math. Comp. **27**, 981-996.
29. **Extension SYM de MACSYMA, manuel de l'utilisateur**, Valibouze A.
30. N. Tchebotarev **Grundzüge des Galois'shen Theorie** P. Noordhoff, 1950
31. B.L. Van des Waerden, **Modern Algebra**, Vol. 1, Ungar, New York, 1953.
32. A. Valibouze, (1988), *Manipulations de fonctions symétriques*, Thèse de l'Université Paris VI.
33. A. Valibouze, (1994) **Mémoire d'habilitation à diriger les recherche**, Université Paris 6, Dec. 1994.
34. A. Valibouze, (1995) *Computation of the Galois group of the Resolvent Factors for the Direct and Inverse Galois Problems*, Conference AAECC'95, (Paris, Juillet 1995), LNCS **948**
35. A. Valibouze, (1995) *Modules de Cauchy, polynômes caractéristiques et résolvantes*, Rapport interne LITP 95-62.

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