Dépendances Algébriques des Zéros de Polynômes et Groupes de Galois

Annick Valibouze

Version Auteur 8 avril 2004
Identique à sa parution :
Bull. Math. Soc. Sc. Math. Roumanie Tome 48(96) No. 1, 2005,

DÉPENDANCES ALGÉBRIQUES DES ZÉROS DE POLYNÔMES ET GROUPES DE GALOIS

ANNICK VALIBOUZE

Laboratoire LIP6
Université Pierre et Marie Curie, 4 place Jussieu 75252 Paris Cedex 05, France
e-mail : Annick.Valibouze@lip6.fr

Résumé

Cet article généralise des résultats sur les idéaux de Galois, les matrices de partitions et les résolvantes relatives pour pouvoir calculer plus efficacement des corps de décomposition de polynômes d'une variable simultanément à leur groupe de Galois.

Abstract

This paper generalizes some properties about Galois ideals, partitions matrices and relative resolvents in order to compute more efficiently splitting fields.

1. Introduction

Dans tout cet article, k désigne un corps parfait et $x_1, \ldots, x_n$ sont des variables algébriquement indépendantes sur k. Nous fixons un polynôme f d'une variable sur k et de degré n en cette variable. Les racines du polynôme f sont supposées deux-à-deux distinctes. Nous notons $\hat{k}$ une clôture algébrique de k.

Nous nous intéressons au calcul simultané du groupe de Galois $\mathrm{Gal}_k(f)$ du polynôme f sur k et de son corps de décomposition K (i.e. le corps des racines du polynôme f). Nous verrons que le groupe de Galois est obtenu avec son action sur les racines du polynôme f sans avoir à imposer que ses coefficients soient des entiers (voir ci-dessous la méthode de Stauduhar) ou qu'il soit irréductible.

Les algorithmes de détermination de groupes de Galois disposent d'une classification des groupes transitifs jusqu'au degré 31 (voir [20]). Deux approches sont généralement utilisées : la méthode, dite de Stauduhar (voir [25]) et la méthode des résolvantes absolues initiée par Berwick puis poursuivie par Foulkes et plus récemment par McKay et Butler, McKay et Soicher, puis Mattman et McKay (voir [10], [11], [16], [21] et [22]). Ces auteurs supposent toujours le polynôme f irréductible. La méthode consiste à construire a priori une sous-matrice $\mathcal{P}$ de la *matrice des partitions* relative au groupe symétrique S_n de degré n (voir [6] ou Paragraphe 8 de

Date: 8 avril 2004.
AMS Subject Classification 2000 : 12F10 12Y05 11Y40.
Keywords : Galois group, Galois ideal, splitting field, partitions matrices, resolvents.

cet article) de telle sorte que les lignes de $\mathcal{P}$ soient deux-à-deux distinctes. Il s'agit ensuite de comparer les degrés des facteurs irréductibles **simples** des résolvantes absolues de f avec les éléments de la matrice $\mathcal{P}$ afin d'en éliminer successivement toutes les lignes sauf une, celle associée au groupe de Galois de f. Il existe des implantations de cette méthode en GAP et en Maple (voir [22] et [21]). L'inconvénient majeur de cette méthode est l'accroissement important des degrés des résolvantes, et ce, dès le degré 11. De plus, le groupe de Galois n'est pas décrit avec son action sur les racines. Les algorithmes de calcul de résolvantes absolues sont basés sur le théorème fondamendal des fonctions symétriques (voir [12] et [28] en plus des citations précédentes).

La méthode de Stauduhar, évoquée plus haut, suppose le polynôme f irréductible et à coefficients entiers. Le groupe de Galois est supposé être un sous-groupe d'un groupe M (au départ, M est le groupe symétrique S_n de degré n). Le coeur de la méthode consiste à choisir un sous-groupe maximal H du groupe M et à calculer une H-résolvante M-relative (polynôme de degré l'indice de H dans M). Si cette résolvante possède un facteur linéaire **simple** alors son groupe de Galois (pour un certain ordre des racines) est inclus dans le groupe H. En descendant ainsi dans l'arbre des sous-groupes de S_n, l'algorithme s'arrête sur le groupe de Galois. La décroissance des degrés des résolvantes au cours de l'algorithme est un de ses avantages, l'autre étant que le groupe de Galois est déterminé avec son action sur les racines. La difficulté de mise en œuvre de cette méthode est le calcul des résolvantes relatives. En effet, dès la deuxième étape, le théorème fondamental des fonctions symétriques ne s'applique plus. Stauduhar propose d'utiliser des approximations numériques des racines (le polynôme f doit appartenir à l'anneau $\mathbb{Z}[x]$). Une implantation de cette méthode a été réalisée dans le logiciel Pari (voir [15]). Cette méthode pose des problèmes de précision. Yokoyama a proposé l'utilisation d'approximations p-adiques. Il a implanté sa méthode jusqu'en degré 8 dans le système de calcul formel Asir (voir [30]). Dans [19], Geissler et Klüners utilisent le calcul de sous-corps ou des résolvantes absolues (lorsque le groupe de Galois est imprimitif) pour calculer le groupe de Galois par la méthode de Stauduhar avec des approximations p-adiques. Ils ont implanté leur approche jusqu'en degré 15 dans le système de calcul formel Kant. Enfin, Colin (voir [14]) a proposé une version algébrique de la méthode de Stauduhar en développant une méthode décrite dans [5] pour le calcul des résolvantes relatives. Cette version algébrique trouve ses limites lorsque le degré n s'élève ($n > 6$).

Chacune des deux méthodes (des résolvantes absolues et de Stauduhar) présente des inconvénients. En fait, elles sont des cas particuliers d'une méthode générale, celle des matrices des partitions (évoquées plus haut) utilisable avec les résolvantes aussi bien absolues que relatives (et sans supposer le polynôme f irréductible). C'est cette méthode que nous décrivons maintenant. Supposons le groupe de Galois de f inclus (pour un certain ordre des racines) dans un groupe M ($M = S_n$ au départ) et considérons la matrice $\mathcal{P}_M$ des partitions relatives à M construite a priori et indépendamment du polynôme f (ses éléments sont des listes d'entiers). Les colonnes et les lignes sont associées à des sous-groupes de M ; ceux des colonnes sont

les groupes tests et ceux des lignes sont les groupes candidats (à être le groupe de Galois). Pour un groupe test H, la liste des degrés des facteurs irréductibles **simples** (sur k) d'une H-résolvante M-relative R est comparée à chaque élément de $\mathcal{P}_M$ dans la colonne associée à H. Lorsque les listes diffèrent, la ligne correspondante est éliminée de la matrice (elle n'est pas associée au groupe de Galois). En particulier, si la résolvante possède un facteur linéaire simple, seules les lignes associées à des sous-groupes de H sont (éventuellement) conservées (i.e. la méthode de Stauduhar est automatiquement appliquée). Lorsque M est un sous-groupe d'un groupe M', la résolvante R est un facteur d'une H-résolvante M'-relative. Lorsque les degrés des résolvantes M-relatives deviennent trop élévés, si le groupe G engendré par les groupes candidats (i.e. ceux associés aux lignes conservées dans $\mathcal{P}_M$) est distinct de M, G remplace M dans l'algorithme. S'il ne reste qu'une seule ligne de la matrice $\mathcal{P}_M$ alors elle est associée au groupe de Galois et l'algorithme s'achève (c'est toujours possible car les lignes de $\mathcal{P}_M$ sont deux-à-deux distinctes). Si $M = S_n$ tout au long du calcul, c'est la méthode des résolvantes absolues qui est appliquée. Le problème reste celui du calcul des résolvantes relatives à coefficients dans un corps parfait quelconque. Nous évoquerons plus loin une méthode entièrement algébrique et qui supporte l'élévation des degrés.

Intéressons-nous maintenant au calcul du corps de décomposition K du polynôme f. Il est calculable avec le polynôme minimal m d'un élément k-primitif γ de K à travers l'isomorphisme suivant :

$$K \simeq k(\gamma) \simeq k[x]/ < m > \qquad .$$

Le calcul direct du polynôme m passe par celui d'une résolvante dite de *Galois*. Cette résolvante est un polynôme de degré $n!$ dont le polynôme m est un facteur (voir [18] ou [29]). Qui plus est, le polynôme m ayant l'ordre du groupe de Galois pour degré, lorsque cet ordre est élevé, les calculs dans $k[x]/ < m >$ sont difficilement praticables. Il n'est donc pas envisageable d'utiliser cette méthode lorsque le degré n est élevé.

Les idéaux de Galois étudiés dans [27] offrent plusieurs avantages :
- éviter le calcul de la résolvante de Galois pour le calcul du corps K,
- calculer algébriquement des résolvantes relatives,
- les calculs dans le corps K sont plus aisés qu'avec le polynôme minimal m,
- les calculs sont combinables avec d'autres méthodes, comme celle de factorisation dans les extensions algébriques (voir [4]),
- le groupe de Galois est déterminé avec son action sur les racines du polynôme f.

Un *idéal de Galois de f (sur k)* est un idéal radical de l'anneau de polynômes $k[x_1, x_2, \ldots, x_n]$ dont chaque zéro dans $\hat{k}^n$ est un n-uplet formé des n racines distinctes du polynôme f. L'intersection de tous les idéaux de Galois du polynôme f sur k est un idéal de Galois $\mathcal{S}$ appelé *idéal des relations symétriques*. Un idéal de Galois peut être également défini comme un idéal de l'algèbre universelle $k[x_1, x_2, \ldots, x_n]/\mathcal{S}$. Cette façon d'étudier les idéaux de Galois complique leur présentation et ne correspond pas directement à la réalité algorithmique puisqu'il s'agit d'obtenir des ensembles triangulaires de $k[x_1, x_2, \ldots, x_n]$ engendrant ces idéaux.

Fixons un idéal maximal $\mathcal{M}$ qui soit un idéal de Galois de f sur le corps k. Alors nous avons l'isomorphisme :

$$K \simeq k[x_1, x_2, \ldots, x_n]/\mathcal{M}$$

et le groupe de décomposition de l'idéal $\mathcal{M}$ (i.e. l'ensemble des permutations laissant $\mathcal{M}$ globalement invariant) est le groupe de Galois de f décrit avec son action sur ses racines. L'idéal $\mathcal{M}$ est un idéal triangulaire (i.e. engendré par un ensemble triangulaire séparable de n polynômes). Le cardinal du groupe de Galois est le produit des degrés des polynômes (i.e. de leurs "monômes initiaux") engendrant $\mathcal{M}$. C'est ce qui rend plus aisés les calculs dans le corps K qu'avec le polynôme minimal m. Le groupe de décomposition de $\mathcal{M}$ est calculable par les méthodes décrites dans [4] et dans [3] (cette dernière est applicable à tout idéal triangulaire). Le calcul simultané du corps K et du groupe de Galois consiste donc à obtenir un ensemble triangulaire de générateurs de l'idéal $\mathcal{M}$.

Dans [5], Arnaudiès et l'auteur obtiennent l'idéal $\mathcal{M}$ en rajoutant une certaine relation R à l'idéal des relations symétriques. L'inconvénient est que sans information sur le groupe de Galois, le calcul de la relation R nécessite celui du polynôme minimal m. Si le groupe de Galois est connu, alors cette relation peut émaner du calcul d'une résolvante absolue de degré l'indice du groupe de Galois dans le groupe symétrique (qui peut être encore trop élevé). En supposant cette relation calculée, le calcul de l'ensemble triangulaire engendrant $\mathcal{M}$ est bien souvent trop important. L'idée est donc de calculer l'idéal $\mathcal{M}$ de proche en proche pour casser la complexité de son calcul direct. C'est ce qui est décrit ci-après.

Donnons auparavant quelques informations nécessaires à la compréhention. À chaque idéal de Galois I contenu dans $\mathcal{M}$ est associé une partie de S_n, son injecteur L dans $\mathcal{M}$ (voir Paragraphe 2). Cet injecteur n'est pas nécessairement un groupe mais il contient toujours le groupe de décomposition de $\mathcal{M}$ (i.e. "le groupe de Galois"). Si l'injecteur L est un groupe, il s'identifie au groupe de décomposition de l'idéal I (c'est le cas lorsque $I = \mathcal{M}$ ou $I = \mathcal{S}$, d'injecteur S_n).

En étendant la définition des résolvantes L-relatives au cas où L n'est pas un groupe, si l'idéal I est engendré par un ensemble triangulaire alors les facteurs de toute résolvante L-relative sont calculables (voir [9]). Si le degré de la résolvante est connu (comme dans le cas où L est un groupe), ses facteurs simples sont identifiables. L'idéal $\mathcal{S}$ est engendré par l'ensemble triangulaire formé des modules de Cauchy du polynôme f (voir [13]).

Dans [27], l'algorithme `GaloisIdéal` combine des calculs de résolvantes relatives (et par conséquent le calcul du groupe de Galois) avec le calcul de l'idéal $\mathcal{M}$. Il construit une chaîne ascendante d'idéaux de Galois :

$$I_1 \subset I_2 \subset \cdots \subset I_l = \mathcal{M} \tag{1}$$

à partir d'un idéal de Galois I_1 donné par ses générateurs et son injecteur dans $\mathcal{M}$. Il est toujours possible de prendre pour I_1 l'idéal $\mathcal{S}$ des relations symétriques.

Pour chaque idéal I_j de la chaîne (1), il s'agit de pouvoir calculer un ensemble triangulaire T_j l'engendrant et son injecteur L_j dans $\mathcal{M}$ connaissant T_{j-1} et L_{j-1}.

Faute de résultats généraux, l'algorithme `GaloisIdéal` suppose que l'injecteur L_1 est un groupe. On est donc placé dans le cas classique de la détermination du groupe de Galois avec des résolvantes L_1-relatives décrit plus haut. La matrice des partitions relative à L_1 est utilisée pour éliminer des groupes candidats à être le groupe de Galois. Dès que le calcul devient avantageux, il faut remplacer le groupe L_1 par un sous-groupe L_2 de L_1 contenant le groupe de Galois et calculer un ensemble de générateurs de l'idéal triangulaire I_2 (en utilisant un facteur irréductible d'une résolvante L_1-relative). Et ainsi de suite jusqu'à l'idéal $\mathcal{M}$.

La complexité du calcul de l'idéal I_{j+1} dépend fortement du cardinal de l'injecteur L_j de l'idéal I_j (degrés des résolvantes L_j-relatives et calcul d'un ensemble triangulaire T_{j+1} à partir de l'ensemble T_j dont le produit des degrés initiaux est le cardinal de L_j). Ceci reste vrai lorsque L_j n'est pas un groupe. Or, il existe de nombreux exemples où sont construits efficacement des idéaux de Galois triangulaires dont les injecteurs ne sont pas des groupes (voir Exemple 1.1, Paragraphe 10 et [24]). Parfois les injecteurs sont de cardinaux très inférieurs à $n!$, celui de l'injecteur de l'idéal des relations symétriques. Pour calculer l'idéal $\mathcal{M}$ à partir d'un idéal de Galois I, donné par un ensemble triangulaire de générateurs T et un injecteur, il existe trois solutions :
- calculer la décomposition de l'idéal I en idéaux premiers (ici maximaux) qui seront tous conjugués (souvent impraticable car trop générale)
- factoriser des polynômes déduits de T dans des extensions algébriques déduites également de T (impraticable lorsque l'ordre du groupe de Galois est élevé, voir [4])
- utiliser un algorithme `GaloisIdéal` *étendu* applicable à tous les idéaux de Galois.

Les résultats généraux présentés dans cet article permettent d'étendre l'algorithme `GaloisIdéal` aux idéaux de Galois dont les injecteurs ne sont pas des groupes. Pour se convaincre de l'intérêt et de l'efficacité de cet algorithme étendu, il suffit de se reporter à l'article [24] où sont étudiés tous les cas des polynômes en degrés 8 (non 2-transitifs).

Remarque 1. Pour ne calculer que des relations linéaires en la variable principale d'un générateur de l'idéal $\mathcal{M}$, la méthode proposée dans [23] applique une formule généralisée d'interpolation de Lagrange à des évaluations numériques des racines. Cette méthode est en particulier applicable à l'exemple du polynôme f_{12} (voir ci-dessous) pour lequel il ne restera qu'une telle relation linéaire à calculer.

Exemple 1.1. Pour tout cet article, nous fixons le polynôme

$$f_{12}(x) = x^8 + 9x^6 + 23x^4 + 14x^2 + 1$$

irréductible sur $\mathbb{Q}$ calculé par Mattman, McKay et Smith. Nous allons calculer un idéal de Galois J_{12} de f_{12} (et un injecteur L_{12} de J_{12}) qui est l'intersection de 2 idéaux maximaux alors que l'idéal des relations symétriques est l'intersection de 1680 idéaux maximaux (voir Exemple 2.1). L'injecteur L_{12} n'étant pas un groupe, l'algorithme `GaloisIdéal` ne s'applique pas à l'idéal J_{12} sans sa généralisation. Cet exemple est choisit volontairement simple pour illustrer les différents résultats.

Cet article se décompose ainsi : le paragraphe 2 définit les idéaux de Galois, leurs injecteurs, le groupe de Galois et rappelle des résultats de [27] utiles pour la suite de l'article ; le paragraphe 3 est un rappel sur les idéaux triangulaires et contient un théorème qui donne une condition suffisante pour qu'un idéal triangulaire soit un idéal de Galois ; le paragraphe 4 liste les résultats à obtenir pour pouvoir étendre l'algorithme `GaloisIdéal`. Les paragraphes suivants fournissent les résultats théoriques listés au paragraphe 4. Le paragraphe 5 fixe des notations et hypothèses générales pour la suite de l'article. Le paragraphe 6 comporte un théorème sur la décomposition de la variété d'un idéal de Galois et de son injecteur. Le paragraphe 7 est dédié au calcul du degré des résolvantes relatives afin d'identifier les facteurs simples. Le paragraphe 8 généralise les matrices des groupes et des partitions (voir [6] et [26]). Au paragraphe 9, nous verrons comment calculer les générateurs d'un idéal de Galois incluant un idéal de Galois dont les générateurs sont connus (i.e. il sera alors possible de calculer I_j à partir de I_{j-1} lorsque l'injecteur L_{j-1} n'est pas un groupe). Au paragraphe 10, est traité un exemple venant compléter celui du polynôme f_{12}.

2. Rappels

Cette partie reprend les résultats de l'article [27] que nous ne redémontrons pas.

Nous posons $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ un n-uplet des racines distinctes du polynôme f dans une clôture algébrique $\hat{k}$ de k. Le corps de décomposition K de f est donc $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Nous utiliserons l'action naturelle du groupe symétrique S_n sur l'anneau des polynômes $k[x_1, \ldots, x_n]$ et sur les n-uplets en posant, pour tout $\sigma \in S_n$, $P \in k[x_1, \ldots, x_n]$ et tout n-uplet $e = (e_1, \ldots, e_n)$:

$$\sigma.P = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \quad \text{et} \quad \sigma.e = (e_{\sigma(1)}, \ldots, e_{\sigma(n)}).$$

Nous étendons naturellement cette action aux ensembles de polynômes et à l'action d'un sous-ensemble de S_n sur un n-uplet.

Notons $\mathcal{M}$ l'*idéal des $\underline{\alpha}$-relations* défini par :

$$\mathcal{M} = \{R \in k[x_1, \ldots, x_n] \mid R(\alpha_1, \ldots, \alpha_n) = 0\}\ .$$

Cet idéal est maximal puisqu'il est le noyau du morphisme surjectif d'évaluation qui à P dans $k[x_1, \ldots, x_n]$ associe $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ dans K.

Le *groupe de Galois de $\underline{\alpha}$ sur k*, noté $\mathrm{Gal}_k(\underline{\alpha})$, est défini par :

$$\mathrm{Gal}_k(\underline{\alpha}) = \{\sigma \in S_n \mid (\forall R \in \mathcal{M})\ \ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\}\ .$$

Pour une partie H du groupe symétrique S_n, l'idéal $Id(H.\underline{\alpha})$ des polynômes de $k[x_1,\ldots,x_n]$ s'annulant sur la variété

$$H.\underline{\alpha} = \{(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}) \mid \sigma \in H\}$$

de $\hat{k}^n$ est appelé un *idéal de Galois de f (sur k)*.

L'idéal $Id(S_n.\underline{\alpha})$ est appelé l'*idéal des relations symétriques* (entre les racines du polynôme f). L'idéal des $\underline{\alpha}$-relations $\mathcal{M}$ est l'idéal $Id(\underline{\alpha})$ ($= Id(\{\underline{\alpha}\})$).

Fixons un idéal de Galois J de f tel que le n-uplet $\underline{\alpha}$ annule les polynômes de J.

L'*injecteur* $\mathrm{Inj}(J,\mathcal{M})$ *de J dans $\mathcal{M}$* est l'ensemble des permutations σ de S_n telles que $\sigma.J \subset \mathcal{M}$. Cet injecteur sera aussi appelé l'*injecteur de J relatif à $\underline{\alpha}$* et noté $\mathrm{Inj}(J,\underline{\alpha})$. (Cette définition reste valable lorsque $\underline{\alpha}$ n'annule pas l'idéal J.)

L'injecteur $\mathrm{Inj}(J,\underline{\alpha})$ est l'union des parties H de S_n telles que $J = Id(H.\underline{\alpha})$. L'idéal J est entièrement déterminé par $\underline{\alpha}$ et $\mathrm{Inj}(J,\underline{\alpha})$. Ainsi J pourra être appelé l'*$\underline{\alpha}$-idéal de Galois d'injecteur* $\mathrm{Inj}(J,\underline{\alpha})$ (relatif à $\underline{\alpha}$).

Un injecteur n'est pas nécessairement un groupe (voir Exemple 2.1). Une condition nécessaire et suffisante pour que $\mathrm{Inj}(J,\underline{\alpha})$ soit un groupe est qu'il existe un sous-groupe H de S_n tel que $J = Id(H.\underline{\alpha})$ et que $\mathrm{Gal}_k(\underline{\alpha})$ soit un sous-groupe de H. Dans ce cas, l'idéal J ne possède qu'un injecteur, le groupe H, que nous appelons l'*injecteur de l'idéal J* et que nous notons $\mathrm{Inj}(J)$.

Remarque 2. L'injecteur de l'idéal des relations symétriques est le groupe symétrique S_n et celui de l'idéal $\mathcal{M}$ des $\underline{\alpha}$-relations est le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$. En particulier, nous avons $\mathcal{M} = Id(\mathrm{Gal}_k(\underline{\alpha}).\underline{\alpha})$.

Pour toute partie H de S_n telle que $J = Id(H.\underline{\alpha})$, nous avons l'identité suivante :

$$\mathrm{Inj}(J,\underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})H \quad (= \{gh \mid g \in \mathrm{Gal}_k(\underline{\alpha}) \text{ et } h \in H\}) \tag{2}$$

qui, appliquée à $H = \mathrm{Inj}(J,\underline{\alpha})$, induit l'inclusion :

$$\mathrm{Gal}_k(\underline{\alpha}) \subset \mathrm{Inj}(J,\underline{\alpha})\ . \tag{3}$$

La variété $V(J) = \{\underline{\beta} \in \hat{k}^n \mid (\forall R \in J)\ R(\underline{\beta}) = 0\}$ de l'idéal J s'exprime sous la forme :

$$V(J) = \{(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}) \mid \sigma \in \mathrm{Inj}(J,\underline{\alpha})\} = \mathrm{Inj}(J,\underline{\alpha}).\underline{\alpha}\ . \tag{4}$$

Si l'idéal J est inclus dans un idéal de Galois I de f (sur k) alors :

$$\mathrm{Inj}(I,\underline{\alpha}) \subset \mathrm{Inj}(J,\underline{\alpha})\ . \tag{5}$$

Pour tout ensemble $\mathcal{G}$ de parties de S_n, nous avons l'identité :

$$Id((\cup_{H\in\mathcal{G}}H).\underline{\alpha}) = \bigcap_{H\in\mathcal{G}} Id(H.\underline{\alpha})\ . \tag{6}$$

Exemple 2.1. Considérons G_{12} le sous-groupe de S_8 d'ordre 24 et engendré par les permutations $(1,3,2,6)(4,5,7,8)$ et $(1,3,7)(2,6,4)$. Soit $\alpha\in\hat{\mathbb{Q}}$ tel que $f_{12}(\alpha)=0$. Dans $\mathbb{Q}(\alpha)$, le polynôme f_{12} se factorise en 2 facteurs linéaires et 2 facteurs de degrés 3. En appliquant les résultats de [24] à cette factorisation, nous savons que G_{12} est, à un isomorphisme près, le groupe de Galois du polynôme f_{12} sur $\mathbb{Q}$ et nous construisons l'ensemble triangulaire séparable :

$$\begin{aligned}
T_{12} \ = \{\ & g_1 = x_1^8 + 9x_1^6 + 23x_1^4 + 14x_1^2 + 1,\\
& g_2 = x_2 + x_1,\\
& g_3 = x_3^3 + (x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1)x_3^2\\
& \qquad\qquad +(x_1^6 + 9x_1^4 + 21x_1^2 + 6)x_3 + x_1^7 + 9x_1^5 + 23x_1^3 + 14x_1,\\
& g_4 = x_4^2 + (x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1)(x_4 + x_3) + x_3x_4 + x_3^2 + x_1^6 + 9x_1^4 + 21x_1^2 + 6,\\
& g_5 = x_5 + x_4 + x_3 + x_1^7 + 8x_1^5 + 16x_1^3 + 3x_1,\\
& g_6 = x_6 + x_3,\\
& g_7 = x_7 + x_4,\\
& g_8 = x_8 + x_5\ \}
\end{aligned}$$

engendrant un idéal de Galois que nous notons J_{12} et dont l'un des injecteurs est la partie L_{12} de S_8 donnée par :

$$L_{12} = G_{12} + G_{12}\sigma\ ,$$

où $\sigma=(3,4)(6,7)$. D'après l'identité (6), l'idéal J_{12} est l'intersection de deux idéaux maximaux dont l'un, noté $\mathcal{M}_{12}$, possède le groupe G_{12} pour injecteur et l'autre le groupe $\sigma^{-1}G_{12}\sigma$.

Soit $\underline{\alpha}=(\alpha_1,\ldots,\alpha_8)\in\hat{\mathbb{Q}}^8$ annulant les polynômes de T_{12}. Nous avons :

$$\mathbb{Q}[x_1,\ldots,x_8]/\mathcal{M}_{12}\simeq\mathbb{Q}(\underline{\alpha})\quad\text{et}\quad\mathbb{Q}(\alpha_1,\alpha_3)\simeq\mathbb{Q}[x_1,x_3]/\langle g_1,g_3\rangle.$$

Les corps $\mathbb{Q}(\underline{\alpha})$ et $\mathbb{Q}(\alpha_1,\alpha_3)$ sont identiques car ils sont tout deux de degré 24 sur $\mathbb{Q}$. Pour calculer dans le corps $\mathbb{Q}(\underline{\alpha})$, les polynômes g_1 et g_3 sont insuffisants. Nous utiliserons l'algorithme `GaloisIdéal` étendu appliqué à l'idéal J_{12} pour calculer un ensemble triangulaire de 8 polynômes engendrant l'idéal $\mathcal{M}_{12}$.

Remarque 3. Pour calculer (uniquement) le groupe de Galois, R.P. Stauduhar en considère un conjugué quelconque et réordonne les racines approximées numériquement afin qu'elles correspondent à ce conjugué (voir [25]). Ici, le conjugué du groupe de Galois ne peut être quelconque car il doit être l'injecteur de l'un des deux idéaux maximaux contenant l'idéal J_{12}.

3. Idéaux triangulaires

Rappelons ci-dessous la définition d'un ensemble triangulaire séparable.

Un sous-ensemble T de n polynômes de $k[x_1, \ldots, x_n]$ est dit *triangulaire* si $T = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ où chaque polynôme f_i est unitaire en tant que polynôme en x_i avec $\deg(f_i, x_i) > 0$.

Cet ensemble triangulaire est dit *séparable* si chaque polynôme f_i de T vérifie la condition suivante : pour tout $(\beta_1, \ldots, \beta_n) \in \hat{k}^n$, si $\forall j \in [\![1, n]\!]$, $f_j(\beta_1, \ldots, \beta_j) = 0$, alors le polynôme d'une variable $f_i(\beta_1, \ldots, \beta_{i-1}, x)$ n'a pas de racine multiple dans $\hat{k}[x]$.

La liste $(\deg(f_1, x_1), \deg(f_2, x_2), \ldots, \deg(f_n, x_n))$ est appelée la *liste des degrés initiaux* de l'ensemble T (ou de l'idéal qu'il engendre).

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

Lorsque l'injecteur d'un idéal de Galois est un groupe, cet idéal est triangulaire et la liste de ses degrés initiaux est facilement calculable à partir de ce groupe (voir [9]). Tout idéal de Galois n'est pas triangulaire. Réciproquement :

Théorème 3.1. *Un idéal triangulaire de $k[x_1, \ldots, x_n]$ contenant les relations symétriques de f est un idéal de Galois de f.*

Démonstration. Comme, par hypothèse, $Id(S_n.\underline{\alpha}) \subset I$, nous avons $V(I) \subset S_n.\underline{\alpha}$. Il existe donc une partie H de S_n telle que $V(I) = H.\underline{\alpha}$. Comme l'idéal I est engendré par un ensemble triangulaire séparable, il est radical. Donc $I = Id(V(I)) = Id(H.\underline{\alpha})$ est un idéal de Galois de f. □

Exemple 3.2. L'idéal J_{12} est triangulaire (il est radical par construction) engendré par les polynômes de T_{12}. Comme il contient les relations symétriques, par le théorème 3.1, l'idéal J_{12} est un idéal de Galois de f. La liste de ses degrés initiaux est $(8, 1, 3, 2, 1, 1, 1, 1)$. L'idéal maximal $\mathcal{M}_{12}$ possède le groupe de Galois G_{12} pour injecteur. Le calcul montre que la liste de ses degrés initiaux est $(8, 1, 3, 1, 1, 1, 1, 1)$. Alors les polynômes g_1, g_2, g_3 et g_5, g_6, g_7, g_8 de l'ensemble T_{12} appartiennent à un ensemble triangulaire engendrant l'idéal $\mathcal{M}_{12}$ (car $J_{12} \subset \mathcal{M}_{12}$). Pour connaître un ensemble triangulaire l'engendrant, il reste à trouver un polynôme de la forme $x_4 + h(x_1, x_3)$ (avec $h \in \mathbb{Q}[x_1, x_3]$) qui appartienne à $\mathcal{M}_{12}$ (cela se voit également avec l'identité $\mathbb{Q}(\alpha_1, \alpha_3) = \mathbb{Q}(\underline{\alpha})$).

4. L'algorithme GaloisIdéal et sa généralisation

Supposons que I soit un idéal de Galois de f engendré par un ensemble triangulaire T et admettant un sous-ensemble S du groupe symétrique S_n pour injecteur relatif à $\underline{\alpha}$, un élément de $\hat{k}^n$ annulant les polynômes de l'ensemble T.

Muni des paramètres S et T, l'algorithme `GaloisIdéal` calcule un idéal de Galois I' contenant strictement l'idéal I (i.e. un injecteur S' de I' et un ensemble triangulaire T' l'engendrant). Si l'idéal I' est maximal alors l'algorithme s'arrête sinon il

recommence récursivement avec les paramètres S' et T'. Nous reviendrons ci-après sur le test d'arrêt de cet algorithme lors de sa description. À chaque étape, nous préciserons ce qui sera fait par la suite afin qu'elle puisse être réalisée sans supposer que S soit un groupe.

Au départ, est choisi un sous-groupe H de S_n inclus dans l'injecteur S de l'idéal I. Il s'agit de calculer $I' = Id(H.\underline{\alpha})$. Si S n'est pas un groupe, le groupe H est choisi dans une liste de groupes candidats inclus dans S (voir plus loin).

La première étape consiste à calculer un polynôme d'une variable appelé H-résolvante S-relative de $\underline{\alpha}$ (voir Paragraphe 7). À partir de l'ensemble triangulaire T, l'algorithme de [9] calcule une puissance de cette résolvante que S soit ou non un groupe. Si S est un groupe, le degré de la résolvante étant connu (c'est l'indice de H dans S), la résolvante l'est aussi (cela a son importance car seuls ses facteurs simples sont exploitables). Nous allons montrer comment calculer le degré de la résolvante dans le cas où S n'est pas un groupe (voir Paragraphe 7).

Une fois obtenu un facteur simple de cette résolvante, l'algorithme `GaloisIdéal` applique le théorème 3.27 de [27] pour en déduire des générateurs de l'idéal I'. Mais ce théorème n'est applicable que dans le cas où les injecteurs des idéaux I et I' sont des groupes. Au paragraphe 9, nous généraliserons ce théorème en s'affranchissant de cette condition sur les injecteurs des idéaux I et I'.

Dans l'algorithme `GaloisIdéal`, un des paramètres est une liste de groupes, dite *liste de candidats*, pouvant être le groupe de Galois de $\underline{\alpha}$ sur k. Avec une résolvante S-relative, en utilisant la matrice des groupes relative à S ou celle des partitions (voir Paragraphe 8), il est possible d'exclure des groupes de cette liste de candidats. Le calcul de la chaîne (1) d'idéaux de Galois aboutissant à l'idéal maximal $\mathcal{M}$ s'en trouve grandement simplifié. En particulier, le groupe H est choisi parmi ces groupes candidats et l'algorithme se termine lorsqu'il n'existe plus qu'un seul groupe dans la liste de candidats (à conjugaison près dans S). Seulement, les matrices des groupes et des partitions ne sont définies et utilisables que lorsque l'injecteur S de I est un groupe. Le paragraphe 8 les généralisera au cas où S est quelconque.

Ces nouveaux résultats suffisent à la généralisation de l'algorithme `GaloisIdéal`.

5. Notations et Hypothèses générales

Pour toute la suite, nous fixons J un idéal de Galois de f et $\underline{\alpha}$ un n-uplet des racines de f tel que l'idéal $\mathcal{M}$ des $\underline{\alpha}$-relations contienne l'idéal J. Posons $L = \mathrm{Inj}(J, \mathcal{M})$. L'intérêt de tout ce qui va suivre est de ne pas supposer que L soit un groupe.

Nous notons $G = \mathrm{Gal}_k(\underline{\alpha})$ le groupe de Galois de $\underline{\alpha}$ sur k et M le groupe engendré par L dans S_n. Comme le groupe de Galois G est un sous-groupe de M (car $G \subset L$ d'après (3)), le groupe M est l'injecteur de l'idéal de Galois $Id(M.\underline{\alpha})$. Nous fixons H un sous-groupe de M contenu dans l'injecteur L.

L'objectif est de pouvoir calculer l'idéal $Id(H.\underline{\alpha})$ et un injecteur de cet idéal connaissant l'idéal J et L, un injecteur de J. Nous avons les inclusions suivantes :

$$Id(M.\underline{\alpha}) \subset J \subset Id(H.\underline{\alpha}) \subset \mathcal{M} = Id(\underline{\alpha}) \quad \text{et} \tag{7}$$

$$G = \mathrm{Inj}(\mathcal{M}) \subset \mathrm{Inj}(Id(H.\underline{\alpha}), \mathcal{M}) \subset L = \mathrm{Inj}(J, \mathcal{M}) \subset M = \mathrm{Inj}(Id(M.\underline{\alpha})) \; . \tag{8}$$

Exemple 5.1. Nous savons que L_{12} (de cardinal 48) est l'injecteur de l'idéal J_{12} dans l'idéal maximal $\mathcal{M}_{12}$. Le groupe engendré par L_{12} est le groupe M_{12} d'ordre 192 et engendré dans S_8 par les permutations (1, 5)(2, 8)(3, 4)(6, 7), (1, 4)(2, 7)(3, 5)(6, 8), (1, 6)(2, 3)(4, 8)(5, 7), (1, 3, 4)(2, 6, 7) et (1, 2)(3, 4, 6, 7).

6. Décomposition de l'idéal J et de sa variété

Lemme 6.1. *Pour toute permutation $\tau \in S_n$, nous avons les trois identités suivantes :*

1. $\mathrm{Gal}_k(\tau.\underline{\alpha}) = \tau^{-1}G\tau$;
2. $Id(\tau.\underline{\alpha}) = Id(G\tau.\underline{\alpha})$;
3. $V(Id(\tau.\underline{\alpha})) = G\tau.\underline{\alpha}$.

L'idéal $Id(\tau.\underline{\alpha})$ étant maximal, sa variété est irréductible.

Démonstration. Montrons l'égalité *1.* Soient $g \in G$ et $R \in Id(\tau.\underline{\alpha})$. Posons $\sigma = \tau^{-1}g\tau$. Pour montrer que $\sigma \in \mathrm{Gal}_k(\tau.\underline{\alpha})$, il suffit de montrer que $\sigma.R(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = 0$. Nous savons, par hypothèse sur R, que $\tau.R(\alpha_1, \ldots, \alpha_n) = R(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = 0$. Comme g appartient au groupe de Galois de $\underline{\alpha}$ sur k, nous avons, par sa définition, $g\tau.R(\alpha_1, \ldots, \alpha_n) = 0$ et donc $\tau^{-1}g\tau.R(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = 0$. Ainsi, $\tau^{-1}G\tau \subset \mathrm{Gal}_k(\tau.\underline{\alpha})$. Pour l'inclusion réciproque, il suffit de poser $\underline{\beta} = (\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})$.

Pour l'égalité *3.* Puisque $\sigma.R(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = \tau\sigma.R(\alpha_1, \ldots, \alpha_n)$ et que $\mathrm{Gal}_k(\tau.\underline{\alpha})$ est l'injecteur de l'idéal $Id(\tau.\underline{\alpha})$, l'identité (4) montre les égalités :

$$\begin{aligned} V(Id(\tau.\underline{\alpha})) &= \{\tau\sigma.\underline{\alpha} \mid \sigma \in \mathrm{Gal}_k(\tau.\underline{\alpha})\} \\ &= \{\tau\sigma.\underline{\alpha} \mid \sigma \in \tau^{-1}G\tau\} \text{ , d'où le résultat.} \end{aligned}$$

L'égalité *2.* portant sur l'idéal radical $Id(\tau.\underline{\alpha})$, elle découle de l'égalité *3.* □

Théorème 6.2. *La variété $V(J)$ de l'idéal de Galois J est l'union disjointe de $s = \mathrm{Card}(L)/\mathrm{Card}(G)$ variétés irréductibles $V(Id(\tau_i.\underline{\alpha}))$, où i parcourt $[\![1, s]\!]$ et $\tau_i \in L$. L'idéal J est l'intersection de s idéaux de Galois maximaux :*

$$J = \bigcap_{i=1}^{s} I_{\tau_i.\underline{\alpha}} \quad et$$

$$\mathrm{Inj}(J, \mathcal{M}) = G\tau_1 + G\tau_2 + \cdots + G\tau_s \; .$$

Démonstration. Soient les $e = [S_n : G]$ permutations $\tau_1 = id, \ldots, \tau_e$ telles que S_n s'écrive comme l'union disjointe : $S_n = G\tau_1 + G\tau_2 + \cdots + G\tau_e$. La variété $S_n.\underline{\alpha}$ de l'idéal des relations symétriques se décompose donc en e variétés irréductibles (d'après le lemme 6.1) et disjointes (car les α_j sont distincts deux à deux) :

$$V_i = G\tau_i.\underline{\alpha} \; ,$$

où i parcourt $[\![1,e]\!]$. Puisque $V(J) \subset S_n.\underline{\alpha}$, en ordonnant correctement les permutations τ_i, il existe $s \leq e$ tel que $V(J) = V_1 \cup V_2 \cup \cdots \cup V_s$. Les idéaux de Galois étant radicaux, le lemme 6.1 et l'identité (6) montre le théorème. □

Exemple 6.3. Poursuivons notre exemple et considérons un 8-uplet $\underline{\alpha}$ des racines du polynôme f_{12} tel que l'idéal $\mathcal{M}_{12} = Id(\underline{\alpha})$ des $\underline{\alpha}$-relations admette pour injecteur le groupe $G_{12} = \mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$ (voir Exemple 2.1). Nous avons $L_{12} = \mathrm{Inj}(J, \underline{\alpha}) = G_{12} + G_{12}\sigma$, où $\sigma = (3,4)(5,6)$, et l'égalité :

$$J_{12} = Id(\underline{\alpha}) \cap Id(\sigma.\underline{\alpha}) \; .$$

7. Résolvantes L-relatives

Soit Θ un polynôme de $k[x_1, \ldots, x_n]$. La *résolvante L-relative de $\underline{\alpha}$ par Θ* est le polynôme défini par :

$$R_{\Theta,J} = \prod_{\Psi \in \{\sigma.\Theta \mid \sigma \in L\}} (x - \Psi(\alpha_1, \ldots, \alpha_n)) \; .$$

Lorsque $\underline{\alpha}$ est fixé, nous utiliserons la notation simplifiée $R_{\Theta,L}$ pour désigner la résolvante $R_{\Theta,J}$.

Le polynôme caractéristique $C_{\Theta,J}$ de l'endomorphisme multiplicatif induit par Θ dans l'anneau quotient $k[x_1, \ldots, x_n]/J$ est une puissance de cette résolvante. Nous avons $R_{\Theta,J} \in k[x]$ puisque le corps k est parfait.

Soit H le sous-groupe de M inclus dans L. Supposons que Θ soit un *H-invariant M-primitif* (i.e. un polynôme $\Theta \in k[x_1, \ldots, x_n]$ tel que $H = \{\sigma \in M \mid \sigma.\Theta = \Theta\}$). La résolvante $R_{\Theta,L}$ est alors appelée une *H-résolvante L-relative*.

Si L est un groupe alors le degré des H-résolvantes L-relatives est l'indice de H dans L. Le théorème suivant nous donne le degré des H-résolvantes L-relatives dans le cas général :

Théorème 7.1. *Soient $\sigma_1 H, \sigma_2 H, \ldots, \sigma_e H$ (avec $\sigma_1 = id$) les classes à gauche de H dans M numérotées de telle sorte que $(\sigma_j H) \cap L \neq \emptyset$ pour $j \in \{1, \ldots, r\}$ et $(\sigma_j H) \cap L = \emptyset$ pour $j \in \{r+1, \ldots, e\}$ (avec $r \leq e$). Nous avons l'union disjointe :*

$$L = [(\sigma_1 H) \cap L] + \cdots + [(\sigma_r H) \cap L] \; . \tag{9}$$

La H-résolvante L-relative $R_{\Theta,L}$ est de degré r et est donnée par

$$R_{\Theta,L} = \prod_{j=1}^{r} (x - \Theta(\alpha_{\sigma_j(1)}, \ldots, \alpha_{\sigma_j(n)})) \; .$$

(Cette résolvante est un facteur de la résolvante $R_{\Theta,M}$ avec $\Theta(\alpha_1, \ldots, \alpha_n)$ comme racine commune.)

Démonstration. D'après l'identité (9), les racines de la résolvante $R_{\Theta,L}$ sont les $\sigma_i h.\Theta$ tels que $i \in [\![1,r]\!]$ et $h \in H$. Cherchons les racines distinctes de cette résolvante. Soient τ et σ deux permutations de S_n telles que $\tau = \sigma\, h \in \sigma H$. Puisque Θ est invariant par les permutations de H, nous avons $\tau.\Theta = \sigma.(h.\Theta) = \sigma.\Theta$. Soient $i, j \in [\![1,r]\!]$ tels que $\sigma_i.\Theta = \sigma_j.\Theta$. Nous avons donc $\sigma_j^{-1}\sigma_i.\Theta = \Theta$. Comme M est un groupe, $\sigma_j^{-1}\sigma_i \in M$ et donc $\sigma_j^{-1}\sigma_i \in H$ puisque Θ est un H-invariant M-primitif. Comme $\sigma_i \in \sigma_j H$, nous avons $i = j$. Donc les racines distinctes de la résolvante $R_{\Theta,L}$ sont les $\sigma_i.\Theta$ avec $i \in [\![1,r]\!]$. □

L'invariant Θ est dit $(L,\underline{\alpha})$-*séparable* si, pour tout $\sigma \in L$ tel que $\sigma.\Theta \neq \Theta$, alors :

$$\Theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) \neq \Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)\ .$$

Soit h le facteur k-irréductible de la résolvante $R_{\Theta,L}$ s'annulant en $\Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Le polynôme h est un facteur simple de la résolvante si et seulement si Θ est $(L,\underline{\alpha})$-séparable.

Remarque 4. Si Θ est $(L,\underline{\alpha})$-séparable alors $\Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ est racine simple de la résolvante $R_{\Theta,L}$. Inversement, supposons que la résolvante $R_{\Theta,L}$ possède un facteur h simple et irréductible sur k. En considérant $\underline{\alpha} \in V(J)$ tel que $\Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ soit une racine de ce facteur, l'invariant Θ est alors $(L,\underline{\alpha})$-séparable. Nous expliquerons par la suite la nécessité de cette séparabilité.

Exemple 7.2. Prenons le groupe $H = G_{12}$ d'indice $e = 8$ dans M_{12}. Nous calculons d'abord le degré des G_{12}-résolvantes L_{12}-relatives. Seules cinq des huits classes à gauche σH de H dans M satisfont $\sigma H \cap L \neq \emptyset$; donc, d'après le théorème 7.1, le degré est $r = 5$ avec $\sigma_1 = id$, $\sigma_2 = (4,5)(7,8)$, $\sigma_3 = (1,6,2,3)(5,8)$, $\sigma_4 = (1,7,8,3)(2,4,5,6)$ et $\sigma_5 = (1,8,4,3)(2,5,7,6)$.

Ensuite, nous calculons

$$\begin{aligned}\Theta_{12} \;=\; & -3x_1x_3^2x_4 + 2x_1^6x_3x_4 + 14x_1^4x_3x_4 + 22x_1^2x_3x_4 + 2x_3x_4 - x_1^7x_4 \\ & -9x_1^5x_4 - 21x_1^3x_4 - 6x_1x_4 + x_1^6x_3^2 + 7x_1^4x_3^2 + 11x_1^2x_3^2 + x_3^2 \\ & -x_1^7x_3 - 9x_1^5x_3 - 20x_1^3x_3 + 3x_1x_3 - 2x_1^6 - 15x_1^4 - 27x_1^2 - 11\ ,\end{aligned}$$

un G_{12}-invariant M_{12}-primitif tel que la résolvante associée ait au moins un facteur simple (voir [1], [2] pour le calcul et [14] pour la séparabilité).

Pour terminer, calculons la résolvante par Θ_{12} en exécutant pas-à-pas l'algorithme de [9] qui en calcule une puissance. Soit p_1 la réduction modulo l'idéal J_{12} du résultant en x_4 de $x - \Theta_{12}$ et du polynôme g_4 de l'ensemble T_{12}. La factorisation de p_1 sur $\mathbb{Q}[x_1, x_3, x]$ donne :

$$p_1 = (x+6)p_2, \text{ où } p_2 = x_1^6 + 6x_1^4 + 8x_1^2 + x + 10\ .$$

Le résultant en x_1 des polynômes p_2 et g_1 de l'ensemble T_{12} est le polynôme $\mathbb{Q}$-irréductible $p_3 = x^4 + 28x^3 + 239x^2 + 487x - 1093$. Le polynôme $(x+6)p_3$ est la forme sans facteur carré du polynôme caractéristique $C_{\Theta_{12},J_{12}}$ et son degré 5 est celui de la résolvante $R_{\Theta_{12},L_{12}}$. Ainsi,

$$R_{\Theta_{12},L_{12}} = (x+6)(x^4 + 28x^3 + 239x^2 + 487x - 1093)\ .$$

8. Matrices des groupes et des partitions

Nous nous plaçons toujours dans les hypothèses du paragraphe 5.

Nous considérons Θ un H-invariant M-primitif. La résolvante $R_{\Theta,M}$ est de degré e, l'indice de H dans M. Pour $\sigma \in S_n$, posons $\theta^\sigma = \Theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$ et $\theta = \theta^{id}$.

8.1. Matrices des groupes et des partitions relatives à M (rappels).

Ce paragraphe reprend des résultats des articles [6] et [26].

Uniquement à partir des groupes G, M et H, nous savons calculer une partition $P_M(G,H) = (i_1, \ldots, i_s)$ de e et une liste de groupes $Gr_M(G,H) = (G_1, \ldots, G_s)$ (où $G_j \subset S_{i_j}$ pour $j \in [\![1, s]\!]$) telles que si la résolvante $R_{\Theta,M}$ n'a pas de racine double alors elle possède exactement s facteurs k-irréductibles tels que $P_M(G,H)$ soit la liste de leur degré respectif et $Gr_M(G,H)$ celle de leur groupe de Galois respectif sur k.

Les listes $P_M(G,H)$ et $Gr_M(G,H)$ ne dépendent que des classes de conjugaison de G et H dans le groupe M. Supposons que les classes de conjugaison des sous-groupes de M soient indicées par $1, 2, \ldots, m$, que la i-ième soit celle du groupe G et que la j-ième soit celle du groupe H. La *matrice des partitions* (resp. *des groupes*) *relative à* M est la matrice $m \times m$ où $P_M(G,H)$ (resp. $Gr_M(G,H)$) est à l'intersection de la ligne i et de la colonne j.

Les lignes de la matrice des partitions étant distinctes deux à deux, il est toujours possible de calculer le groupe de Galois d'un polynôme avec des résolvantes sans racine double. Ces matrices sont utilisées par l'algorithme `GaloisIdéal` afin de réduire la liste des groupes candidats.

Notons $\mathcal{C}$ l'ensemble $\{\sigma_1 H, \ldots, \sigma_e H\}$ des classes à gauche de H dans M. Soit $\mathcal{O} = \{g_1 H, g_2 H, \ldots, g_d H\}$ une G-orbite par action à gauche dans $\mathcal{C}$. Alors la résolvante $R_{\Theta,M}$ possède un facteur h sur k de degré $d = \mathrm{Card}(\mathcal{O})$ s'écrivant :

$$h(x) = \prod_{i=1}^{d} (x - \theta^{g_i}) \,. \tag{10}$$

Pour simplifier, nous pouvons supposer que θ est une racine de h. Nous pouvons alors choisir $g_1 = id$ et $g_i \in G$ pour $i \in [\![1, d]\!]$. Si le polynôme h est sans racine multiple alors $\theta^{g_1}, \ldots, \theta^{g_d}$ sont les éléments distincts de l'ensemble $\{\, \theta^\tau \mid \tau \in G\}$. Par la théorie de Galois classique, le polynôme h est donc k-irréductible ; c'est le polynôme minimal de θ sur k. Dans ce cas, le groupe de Galois du polynôme h sur k est le sous-groupe de S_d obtenu par opération à gauche de G sur l'orbite $\mathcal{O}$. Ainsi, les cardinaux des G-orbites de $\mathcal{C}$ forment la liste $P_M(G,H)$ et la liste $Gr_M(G,H)$ est construite par l'action à gauche de G sur ces G-orbites.

L'idée de calculer des listes $P_M(G,H)$ et $Gr_M(G,H)$ est ancienne (voir [10] et [16]) mais elles n'étaient considérées que dans les cas où $M = S_n$ avec des groupes H

transitifs. En se limitant aux partitions $P_{S_n}(G,H)$, elle a été reprise avec succès jusqu'en degré 7 avec des groupes H ayant des H-invariants S_n-primitifs linéaires (voir [22]). Dans le paragraphe suivant, nous allons généraliser cette idée aux matrices des groupes et des partitions relatives à la partie $L = \mathrm{Inj}(J, \mathcal{M})$ de S_n (qui n'est donc pas nécessairement un groupe) et aux H-résolvantes L-relatives.

8.2. **Matrices des groupes et des partitions relatives à L.**

Il s'agit ici de construire des matrices des groupes et des partitions relatives à L, qui n'est pas nécessairement un groupe, et de les associer aux résolvantes L-relatives de la même manière que pour M.

Soit $\mathcal{O}$ la G-orbite associée au facteur h donné en (10). Posons $\mathcal{F} = \{C \in \mathcal{C} \mid C \cap L \neq \emptyset\}$ et $C_0 = \sigma H \in \mathcal{O}$, où σ désigne une permutation de M. Le polynôme h possède θ^σ comme racine.

Si le polynôme h est un facteur simple de la résolvante $R_{\Theta,M}$ alors il est k-irréductible. Dans ce cas, d'après le théorème 7.1, nous avons que $C_0 \in \mathcal{F}$ si et seulement si h est aussi un facteur simple de la résolvante $R_{\Theta,L}$ (car h et $R_{\Theta,L}$ ont une racine en commun et h est k-irréductible). Donc h est un facteur de la résolvante $R_{\Theta,L}$ si et seulement si $\mathcal{O}$ est la G-orbite de C_0 dans $\mathcal{F}$.

La différence entre le calcul de la matrice des groupes (resp. partitions) relative à M et celle relative à L est donc infime : il suffit de déterminer le sous-ensemble $\mathcal{F}$ de $\mathcal{C}$. Toute G-orbite d'une classe à gauche du groupe H appartenant à $\mathcal{C}$ est ou bien incluse $\mathcal{F}$ ou bien d'intersection vide avec $\mathcal{F}$. Pour chaque G-orbites $\mathcal{O}$ incluse dans $\mathcal{F}$, nous savons donc calculer le degré et le groupe de Galois sur k du facteur commun des résolvantes $R_{\Theta,M}$ et $R_{\Theta,L}$ et associé à l'orbite $\mathcal{O}$ dans le cas où ce facteur est k-irréductible simple de la résolvante (voir Paragraphe 8.1).

Nous notons $Gr_L(G,H)$ (resp. $P_L(G,H)$) la liste des groupes de Galois sur k (resp. des degrés) des facteurs irréductibles (supposés simples) de la résolvante $R_{\Theta,L}$. La fonction `Groups` suivante, écrite dans le langage du logiciel de calcul formel `GAP` (voir [17]), retourne la liste $Gr_L(G,H)$ (la liste $P_L(G,H)$ s'en déduit aisément) :

```
Groups := function(M,L,G,H)
          local rc,orbits;
          rc := Filtered(RightCosets(M,H),rc->(Intersection(rc,L) <> []));
          orbits :=Orbits(G,rc,OnRight);
          return List(orbits,D->AsSubgroup(
                      SymmetricGroup(Length(D)),Operation(G,D,OnRight)));
          end;
```

La fonction `Groups` se comprend aisément en remplaçant `Right` (droite) par gauche car en `GAP` les actions dites à droite sont celles à gauche de notre article. Cette fonction est déduite de celle écrite par Claude Quitté qui, elle, retourne $Gr_M(G,H)$ (communication privée).

Exemple 8.1. La résolvante séparable $R_{\Theta_{12},L_{12}}$ calculée dans l'exemple 7.2 possède deux facteurs (simples) irréductibles sur $\mathbb{Q}$: le premier, $x+6$, est linéaire et l'autre, $g(x) = x^4 + 28x^3 + 239x^2 + 487x - 1093$, a pour groupe de Galois sur $\mathbb{Q}$ le groupe alterné A_4. D'après l'exemple 7.2 :

$$L_{12} = \bigcup_{i=1}^{5} (\sigma_i G_{12}) \cap L_{12} \ .$$

L'exécution de la fonction `Groups`, avec $M = M_{12}$, $L = L_{12}$, $G = G_{12}$ et $H = G_{12}$ comme paramètres réels, retourne une liste constituée de deux groupes : le groupe S_1, groupe de Galois sur $\mathbb{Q}$ du facteur linéaire $x+6$, et le groupe A_4, groupe de Galois sur $\mathbb{Q}$ du facteur g. Ces groupes correspondent aux 2 G_{12}-orbites que sont $\{H\}$ de longueur 1 et $\{(\sigma_i H) \cap L \mid i \in \{2,3,4,5\}\}$ de longueur 4.

Si nous ne savions pas déjà que le groupe de Galois de f sur $\mathbb{Q}$ est G_{12}, le facteur linéaire simple de cette résolvante nous assurerait qu'il est inclus dans G_{12}. Il faudrait alors calculer des résolvantes G_{12}-relatives (en utilisant un ensemble triangulaire engendrant l'idéal $Id(G_{12}.\underline{\alpha})$) pour déterminer que le groupe de Galois de $\underline{\alpha}$ sur $\mathbb{Q}$ est bien G_{12}.

Pour cet exemple, les matrices de groupes et de partitions ne sont pas utiles car nous savons déjà que le groupe de Galois de f_{12} sur $\mathbb{Q}$ est G_{12}. Mais dans bien d'autres exemples elles le sont.

9. Polynôme primitif et générateurs d'un idéal de Galois

Soit I un idéal de Galois de f (sur k) vérifiant :

$$J \subset I \subset \mathcal{M} \quad .$$

Avec le théorème 9.3 de ce paragraphe, nous saurons calculer un système de générateurs de l'idéal I à partir de celui de l'idéal J.

Un polynôme P de $k[x_1, \ldots, x_n]$ est dit *J-primitif de l'idéal I* si

$$\mathrm{Inj}(I, \mathcal{M}) = \{\sigma \in \mathrm{Inj}(J, \mathcal{M}) \mid \sigma.P \in \mathcal{M}\} \ .$$

Rappelons que nous avions posé $L = \mathrm{Inj}(J, \mathcal{M})$. La proposition suivante donne une méthode constructive pour le calcul d'un polynôme J-primitif d'un idéal de Galois.

Proposition 9.1. *Soit $\Theta \in k[x_1, x_2, \ldots, x_n]$ tel que $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$ et tel que la résolvante $R_{\Theta,L}$ ait un facteur simple h irréductible sur k. Soit $\underline{\alpha} \in V(J)$ tel que $\Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ soit une racine du polynôme h (i.e. Θ est $(L, \underline{\alpha})$-séparable). Alors le polynôme $h(\Theta)$ est un polynôme J-primitif de l'idéal de Galois $Id(H.\underline{\alpha})$.*

Remarquons qu'il suffit que Θ soit un H-invariant M-primitif pour que $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$.

Démonstration. Posons $P = h(\Theta)$, $\theta^\sigma = \Theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$, où σ est une permutation de S_n, et

$$A = \{\sigma \in L \mid P(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = 0\} .$$

Le polynôme k-irréductible h étant le polynôme minimal de θ sur k, par la théorie de Galois, nous savons que :

$$h = \prod_{\psi \in \{\theta^\sigma \mid \sigma \in G\}} (x - \psi) .$$

Comme, pour tout $\sigma \in S_n$, $P(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = h(\theta^\sigma)$, nous aurons $\sigma \in A$ si et seulement si il existe $\tau \in G$ tel que $\theta^\sigma = \theta^\tau$; ce qui est équivalent à $\theta^{\tau^{-1}\sigma} = \theta$, par définition du groupe de Galois G de $\underline{\alpha}$ sur k auquel la permutation τ appartient. Puisque $GL = L$ (voir identité (2) appliquée à L=Inj$(J, \underline{\alpha})$), nous avons $\tau^{-1}\sigma \in L$ pour $\sigma \in L$ et $\tau \in G$. Comme, par hypothèse, le polynôme Θ est $(L, \underline{\alpha})$-séparable, nous obtenons :

$$A = \{\sigma \in L \mid (\exists \tau \in G)\ \tau^{-1}\sigma.\Theta = \Theta\} .$$

Puisque $\tau^{-1}\sigma \in L$ et que $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$, nous obtenons :

$$A = \{\sigma \in L \mid (\exists \tau \in G)\ \tau^{-1}\sigma \in H\} = GH .$$

Le polynôme P est donc bien un polynôme J-primitif de l'idéal $Id(H.\underline{\alpha})$ puisque, d'après l'identité (2), nous avons Inj$(Id(H.\underline{\alpha}), \mathcal{M}) = GH$. □

Remarque 5. Pour calculer le degré de la résolvante $R_{\Theta,L}$, le théorème 7.1 impose que Θ soit un H-invariant M-primitif alors que cette proposition ne lui impose que d'être L-primitif.

Exemple 9.2. Le polynôme $x + 6$ est un facteur simple et irréductible sur k de la résolvante $R_{\Theta_{12},L_{12}}$ (voir Exemple 7.2). Pour un ordre $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_8)$ des racines de f_{12}, $\Theta_{12}(\alpha_1, \alpha_2, \ldots, \alpha_8)$ est une racine du polynôme $x+6$ et le polynôme $P_{12} = \Theta_{12} + 6$ est un polynôme J_{12}-primitif de l'idéal $Id(\underline{\alpha}) = Id(G_{12}.\underline{\alpha})$. C'est un tel $\underline{\alpha}$ que nous considèrerons par la suite.

Le théorème suivant à déjà été prouvé dans le cas où Inj$(J, \mathcal{M})$ et Inj$(I, \mathcal{M})$ sont des groupes (voir Théorème 3.27 de [27]).

Théorème 9.3. *Soit P un polynôme J-primitif de l'idéal I. Alors, nous avons :*

$$I = J + \langle P \rangle ,$$

où $\langle P \rangle$ est l'idéal engendré par P dans $k[x_1, x_2, \ldots, x_n]$.

Démonstration. Posons $U =$ Inj$(I, \mathcal{M})$. D'après le théorème 6.2 et puisque $U \subset L$, nous avons les unions disjointes suivantes :

$$U = G\tau_1 + \cdots + G\tau_e \qquad et \qquad L = U + G\tau_{e+1} + \cdots + G\tau_s ,$$

pour une numérotation bien choisie des τ_i, avec $\tau_1 = id$ et $e.\,\mathrm{Card}(G) = \mathrm{Card}(U)$.

Posons $U' = G\tau_{e+1} + \cdots + G\tau_s$ et $I' = Id(U'.\underline{\alpha})$. Pour $i \in [\![1, s]\!]$, nous avons $Id(\tau_i.\underline{\alpha}) = Id(G\tau_i.\underline{\alpha})$ (voir Lemme 6.1). Les idéaux I, I' et J s'expriment comme suit (voir Identité (6)) :

$$I = \bigcap_{i=1}^{e} Id(\tau_i.\underline{\alpha}) \quad , \qquad I' = \bigcap_{i=e+1}^{s} Id(\tau_i.\underline{\alpha}) \qquad \text{et} \qquad J = I \cap I' \, .$$

Comme P est un polynôme J-primitif de l'idéal I et d'après l'identité (4) sur les variétés affines des idéaux de Galois, nous avons :

$$\begin{aligned} V(J + \langle P \rangle) &= \{(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in L \text{ et } P(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = 0\} \\ &= \{(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in \mathrm{Inj}(I, \underline{\alpha})\} \\ &= V(I) \, . \end{aligned}$$

Donc $I = \sqrt{J + \langle P \rangle}$, le radical de l'idéal $J + \langle P \rangle$. Il existe donc un entier $m > 0$ tel que :

$$I^m \subset J + \langle P \rangle \subset I \, .$$

D'après le lemme 9.4, les idéaux I et I' sont comaximaux et, par conséquent, les idéaux I^m et I' le sont aussi. Prenons $x \in I$. Il existe $u \in I^m$ et $v \in I'$ tels que :

$$x = xu + xv \, .$$

Nous avons $xu \in J + \langle P \rangle$ et $xv \in I\,I'$. Les idéaux $I_{\tau_i.\underline{\alpha}}$ étant maximaux et distincts deux à deux (donc comaximaux deux à deux), nous avons :

$$I\,I' = \prod_{i=1}^{e} Id(\tau_i.\underline{\alpha}) \prod_{i=e+1}^{s} Id(\tau_i.\underline{\alpha}) = \bigcap_{i=1}^{s} Id(\tau_i.\underline{\alpha}) = I \cap I' = J \, .$$

Donc $xv \in J$ et $x \in J + \langle P \rangle$, ce qui termine la démonstration. □

Lemme 9.4. *Les idéaux I et I' de la démonstration du théorème 9.3 sont comaximaux.*

Démonstration. Nous savons que $V(J) = V(I) \cup V(I')$ est l'union des s variétés affines irréductibles disjointes $V_i = V(Id(\tau_i.\underline{\alpha}))$, $i \in [\![1, s]\!]$ (voir Théorème 6.2). De même $V(I) = \bigcup_{i=1}^{e} V_i$ et donc $V(I') = \bigcup_{i=e+1}^{s} V_i$. Nous avons donc $V(I + I') = V(I) \cap V(I') = \emptyset$ et les idéaux I et I' sont bien comaximaux. □

Exemple 9.5. Soit $P_{12} = \Theta_{12} + 6$, le polynôme J_{12}-primitif de l'idéal $\mathcal{M}_{12} = Id(G_{12}.\underline{\alpha})$ calculé dans l'exemple 9.2. Alors, pour $\underline{\alpha}$ dans $V(J_{12})$ tel que $\Theta(\underline{\alpha})$ soit une racine de $x + 6$ (i.e. $P_{12}(\underline{\alpha}) = 0$), nous avons $\underline{\alpha} \in V(\mathcal{M}_{12})$ et :

$$\mathcal{M}_{12} = J_{12} \, + \langle P_{12} \rangle \, .$$

Calculons le corps de décomposition du polynôme f_{12}. Bien que nous disposons de l'isomorphisme $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_8) \simeq \mathbb{Q}[x_1, x_2, \ldots, x_8]/\mathcal{M}_{12}$, la liste des générateurs de $\mathcal{M}_{12}$ dont nous disposons n'est pas adaptée pour calculer dans le corps $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_8)$ (car ce n'est pas une base de Gröbner). Il faut pour cela disposer

d'un ensemble triangulaire engendrant l'idéal $\mathcal{M}_{12}$. D'après l'exemple 3.2, il suffit de calculer un polynôme de la forme $x_4 + h(x_1, x_3)$ appartenant à $\mathcal{M}_{12}$

En partant des polynômes de l'ensemble T_{12} et du polynôme P_{12}, des calculs rapides avec des pseudo-restes aboutissent au polynôme :

$$h_4 = x_4 - x_1^3x_3^2 - 4x_1x_3^2 + x_1^6x_3 + 8x_1^4x_3 + 15x_1^2x_3 + x_3 - x_1^7 - 9x_1^5 - 23x_1^3 - 13x_1 \ .$$

L'ensemble triangulaire $T_{\underline{\alpha}} = \{g_1, g_2, g_3, h_4, g_5, g_6, g_7, g_8\}$ engendre l'idéal $\mathcal{M}_{12}$.

10. Un autre exemple d'application

Nous présentons un autre exemple d'application de la proposition 9.1 et du théorème 3.1. Bien que ne soit connu aucun injecteur de l'idéal de Galois triangulaire J_1 que nous calculons, l'algorithme `GaloisIdéal` pourra être poursuivi avec cet idéal.

Nous considérons le polynôme $f = x^8+x^4+2$ calculé par Mattman, McKay et Smith. Soit M le sous-groupe transitif de S_8 d'ordre 1152 et engendré par les permutations

$$a = (5,6),\ b = (1,2),\ c = (7,8),\ d = (3,4),\ e = (1,5)(2,6)(3,7)(4,8) \text{ et } f = (2,3).$$

Posons $P = x_1x_2x_3x_4 + x_5x_6x_7x_8 - 1$. Avec l'algorithme `GaloisIdéal` non étendu, nous obtenons que pour tout n-uplet $\underline{\alpha}$ vérifiant $P(\underline{\alpha}) = 0$:

$$Id(M.\underline{\alpha}) = Id(S_8.\underline{\alpha}) + \langle P \rangle$$

avec $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) \subset M = \mathrm{Inj}(Id(M.\underline{\alpha}), \underline{\alpha})$.

Pour calculer un ensemble triangulaire engendrant l'idéal $Id(M.\underline{\alpha})$, nous utilisons l'implantation de P. Aubry en `AXIOM` pour décomposer un idéal en ensembles triangulaires (voir [7] et [8]). Le calcul intermédiaire fournit trois ensembles triangulaires engendrant respectivement trois idéaux J_1, J_2 et J_3 tels que

$$Id(M.\underline{\alpha}) = J_1 \cap J_2 \cap J_3 \text{ , avec}$$

$$J_1 = \langle x_1^8+x_1^4+2,\ x_2+x_1,\ x_3^2+x_1^2,\ x_4+x_3,\ x_5^4+x_1^4+1,\ x_6^3+x_6^2x_5+x_6x_5^2+x_5^3,$$
$$x_7^2+x_7x_6+x_7x_5+x_6^2+x_6x_5+x_5^2,\ x_8+x_7+x_6+x_5\rangle \ .$$

Pour chacun des idéaux J_1, J_2 et J_3, le produit de leurs degrés initiaux est 384. L'idéal $Id(M.\underline{\alpha})$ est radical et le cardinal de sa variété est $\mathrm{Card}(M) = 3.384$. Donc les trois idéaux J_1, J_2 et J_3 sont aussi radicaux. Par le théorème 3.1, ce sont donc trois idéaux de Galois du polynôme f.

Pour des raisons évidentes d'efficacité, il est préférable de poursuivre le calcul avec l'idéal J_1 plutôt qu'avec l'idéal $Id(M.\underline{\alpha})$. Pour calculer les degrés des résolvantes, le théorème 7.1 est inapplicable à l'idéal J_1 car aucun injecteur de cet idéal n'est connu. Nous utilisons une méthode adaptée à cette situation particulière.

Soit $\Theta = x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ un H-invariant M-primitif où H est le sous-groupe de M d'ordre 128 et engendré par les permutations

$$bd, ac, cd, e, g = (1,3,2,4) \text{ et } h = (5,7,6,8) \ .$$

Avec l'algorithme décrit dans [9], nous obtenons :

$M_{\Theta,J_1} = x(x^4 - 4x^2 + 32)$ et $M_{\Theta,J_2} = M_{\Theta,J_3} = (x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112)$,

où, pour I un idéal de $k[x_1, \ldots, x_n]$ de dimension 0, $M_{\Theta,I}$ est la forme sans facteur carré du polynôme caractéristique de l'endomorphisme multiplicatif induit par le polynôme Θ dans l'anneau $\mathbb{Q}[x_1, x_2, \ldots, x_8]/I$. Comme la résolvante $R_{\Theta,Id(M.\underline{\alpha})}$ est de degré 9, l'indice de H dans M, et que les trois polynômes M_{Θ,J_j} sont des facteurs de cette résolvantes, nous avons :

$$R_{\Theta,Id(M.\underline{\alpha})} = x(x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112)\ .$$

Les résolvantes R_{Θ,J_j} étant des facteurs de cette résolvante, elles sont sans facteur carré (i.e. $R_{\Theta,J_j} = M_{\Theta,J_j}$ pour $j = 1, 2, 3$). Le polynôme x est donc un facteur simple de la résolvante R_{Θ,J_1}. Imposons à $\underline{\alpha}$ de vérifier $\Theta(\underline{\alpha}) = 0$. Nous avons alors $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) \subset H$. D'après la proposition 9.1, le polynôme Θ est J_1-primitif de l'idéal $Id(H.\underline{\alpha})$. Donc, avec le théorème 9.3, nous obtenons :

$$\begin{aligned} (11) \qquad Id(H.\underline{\alpha}) &= J_1 + \langle \Theta \rangle \\ &= \langle x_1^8 + x_1^4 + 2,\ x_2 + x_1,\ x_3^2 + x_1^2, x_4 + x_3,\ x_5^4 + x_1^4 + 1, \\ &\qquad x_6 + x_5,\ x_7^2 + x_5^2,\ x_8 + x_7 \rangle\ . \end{aligned}$$

En poursuivant l'algorithme `GaloisIdéal` avec l'idéal $Id(H.\underline{\alpha})$ d'injecteur H, nous aboutissons à l'idéal de Galois maximal :

$\mathcal{M} = \langle x_1^8{+}x_1^4{+}2,\ x2{+}x_1,\ x_3^2{+}x_1^2,\ x_4{+}x_3,\ x_5^4{+}x_1^4{+}1,\ x_6{+}x_5,\ 2x_7{+}x_5x_3x_1^7{+}x_5x_3x_1^3,\ x_8{+}x_7 \rangle$

d'injecteur le groupe de Galois relatif à tout $\underline{\alpha} \in V(\mathcal{M})$ engendré par les permutations bd, ac, e, g, h et cd. Pour aboutir à cet idéal maximal, nous avons construit la chaîne ascendante suivante :

$$Id(S_8.\underline{\alpha}) \subset J_1 \subset Id(H.\underline{\alpha}) \subset \mathcal{M}\ .$$

Le théorème 9.3, nous a permis d'éviter :
- le calcul d'un ensemble triangulaire engendrant l'idéal $Id(M.\underline{\alpha})$ et
- le calcul d'un ensemble triangulaire engendrant l'idéal $Id(H.\underline{\alpha})$ en utilisant l'identité $Id(H.\underline{\alpha}) = Id(M.\underline{\alpha}) + \langle \Theta \rangle$ (voir Théorème 3.27 de [27]) plutôt que le calcul moins coûteux induit par l'identité (11).

Remarque 6. Suite aux calculs de résolvantes, les informations fournies par les matrices de groupes ne sont pas retranscrites car ne sont utilisées que des matrices relatives à des groupes.

Conclusion

Nous avons donné tous les éléments permettant d'étendre naturellement l'algorithme `GaloisIdéal` au cas des idéaux de Galois triangulaires dont les injecteurs ne sont pas des groupes. Désormais, il est en particulier possible de calculer le corps de décomposition du polynôme f à partir d'un idéal de Galois déduit de la factorisation de f dans un ou plusieurs sous-corps du corps de décomposition K de f (voir

[24]). Sans le travail présenté ici, il faudrait ou bien calculer l'idéal maximal des $\underline{\alpha}$-relations à partir de l'idéal des relations symétriques ou bien factoriser le polynôme f dans la tour d'extensions $k(\alpha_1), \ldots, K = k(\alpha_1, \ldots \alpha_m)$ (avec $m \leq n-1$).

Références

[1] I. Abdeljaouad, *Calculs d'invariants primitifs de groupes finis*, Theorical Informatics and Applications, **33**, N^o 1, (1999), 59-77.

[2] I. Abdeljaouad, Package Primitive Invariants du logiciel GAP, http ://www-history.mcs.st-and.ac.uk/ gap/Info/deposit.html.

[3] I. Abdeljaouad, S. Orange, G. Renault, A. Valibouze, *Decomposition group of triangular ideals, application to Galois theory*, Submitted to AAECC, (2003).

[4] H. Anai,, M. Noro, K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials.*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., eds. Birkhauser, Basel, **143**,(1996) 29–50.

[5] J.M. Arnaudiès, A. Valibouze, *Résolvantes de Lagrange*, Rapport LITP 93.61, (1993).

[6] J.M. Arnaudiès, A. Valibouze, *Lagrange resolvents*, special issue of MEGA'96 (A. Cohen and M-F- Roy Eds), Journ. of Pure and Appl. Algeb. **117&118** (1997), 23–40.

[7] P. Aubry, Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Ph.D. Thesis, Université Paris 6, (1999).

[8] P. Aubry, M. Moreno Mazat, *Triangular sets for solving polynomial systems : a comparative implantation of four methods*, J. Symb. Comp.,**28** (1999), 125–154.

[9] P. Aubry, A. Valibouze, *Using Galois ideals for computing relative resolvents*, Special Issue on Algorithmic Galois Theory, Jour. Symb. Compu., **30**, num. 6, (2000), 635–651.

[10] E.H. Berwick, *On Soluble Sextic equations* Proc. London Math. Soc. (2) **29**(1929), 1-28.

[11] G. Butler, J. McKay, *The transitive groups of degree up to 11*, Comm. Algebra **11** (1983), 863-911.

[12] D. Casperson, J. McKay, *Symmetric functions, m-sets, and Galois groups, Math. Comp.* **63**, (1994) 749-757.

[13] A. Cauchy, *Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée.* Oeuvre Volume **5** p.473 extrait 108.

[14] A. Colin, *Formal computation of Galois groups with relative resolvents*, AAECC'95 Conference (G. Cohen, A. Giusti and T. Mora Eds) LNCS **948** (1995) , 169-182.

[15] Y. Eichenlaub, Problèmes effectifs de théorie de Galois en degrés 8 à 11, PhD thesis, Université de Bordeaux 1, 1996.

[16] H.O. Foulkes, *The resolvents of an equation of seventh degree*, Quart. J. Math. Oxford Ser. (2)(1931) , 9-19.

[17] GAP `Groups, Algorithms and Programming, GAP 3.3` Martin Schönert and others, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, **93.**

[18] E. Galois, **Oeuvres Mathématiques,** publiées sous les auspices de la SMF, Gauthier-Villars, 1897

[19] K. Geissler, J. Klüners, *Galois Group Computation for Rational Polynomials*, Journal of Symbolic Computation **30**, N. 6, (2000), 653-674.

[20] A. Hulpke, Konstruktion transitiver Permutationsgruppen. PhD thesis, Rheinisch-Westfälische Technische Hocschule, Aachen, Germany.

[21] T. Mattman, J. McKay, *Computation of Galois group over function fields*, Math. Comp., **66**, (1997), 823-831.

[22] J. McKay, L. Soicher, *Computing Galois Groups over the rationals*, Journal of number theory **20** (1985) , 273-281.

[23] J. McKay, R.P. Stauduhar, *Finding relations among the roots of an irreducible polynomial*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), ACM, New York (1997),75-77,

[24] S. Orange, G. Renault, A. Valibouze, *Calcul efficace de corps de décompositions*, *Publication interne LIP6* lip6.2003.005 (2003), http ://www.lip6.fr/reports/lip6.2003.005.html.

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

[26] A. Valibouze, *Computation of the Galois group of the Resolvent Factors for the Direct and Inverse Galois Problems*, AAECC'10 conference (Paris, July 1995), LNCS **948** (1995), 456-468 (LITP Report 94-58 (1994)).

[27] A. Valibouze, *Etude des relations algébriques entre les racines d'un polynôme d'une variable*, Bulletin of The Belgian Math. Soc. S. Stevin **6** (1999), 507-535.

[28] A. Valibouze Théorie de Galois constructive, mémoire d'HDR, Université P. et M. Curie, 1994.

[29] B.L. Van der Waerden, Modern Algebra : volume 2, New-York, Frederic Ungar, 1950.

[30] K. Yokoyama, A modular method for computing the Galois group of polynomial, A. Cohen et M.F. Roy, editors, MEGA'96, **117-118**, J. Pure Appl. Alg., 617-636.