Généralisation de résultats sur les idéaux de Galois

Annick Valibouze

GÉNÉRALISATIONS DE RÉSULTATS SUR LES IDÉAUX DE GALOIS

ANNICK VALIBOUZE

Résumé

Cet article a pour but de généraliser des propriétés sur les idéaux de Galois pour le calcul efficace de corps de décomposition.

Abstract

The goal of this paper is to generalize some properties about Galois ideals in order to compute efficiently splitting fields.

1. Introduction

La construction du corps de décomposition K d'un polynôme f d'une variable sur un corps parfait k se réalise dans [21] avec des idéaux de $k[x_1, x_2, \ldots, x_n]$, dit idéaux de Galois (avec $x_1, \ldots, x_n$ des variables algébriquement indépendantes). L'algorithme `GaloisIdéal` qui y est proposé construit une chaîne ascendante de tels idéaux :

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

où l' idéal I_1 est par défaut l'idéal des relations symétriques qui contient tous les idéaux de Galois du polynôme f, et $\mathcal{M}$ est un idéal maximal tel que le corps K soit isomorphe à l'anneau quotient $k[x_1, x_2, \ldots, x_n]/\mathcal{M}$.

Pour chaque idéal I_j de la chaîne (1), il s'agit de calculer un ensemble triangulaire T_j l'engendrant et un *stabilisateur* L_j, une partie de S_n, le groupe symétrique de degré n. L'idéal des relations symétriques est engendré par les modules de Cauchy et possède S_n comme stabilisateur ; l'idéal maximal $\mathcal{M}$ a comme stabilisateur un groupe isomorphe au groupe de Galois de K sur k.

L'algorithme `GaloisIdéal` impose que chaque stabilisateur L_j soit un groupe. Or, dans [18] sont construits efficacement des idéaux de Galois dont les stabilisateurs ne sont pas des groupes (voir aussi Paragraphe 10). Pour calculer l'idéal $\mathcal{M}$ à partir de tout idéal de Galois, nous devons généraliser l'algorithme `GaloisIdéal`. C'est ce que vont permettre les résultats de cet article.

Cet article se décompose ainsi : le paragraphe 2 définit les idéaux de Galois, leurs stabilisateurs, le groupe de Galois et rappelle des résultats de [21] qui seront utiles pour

Date: 9 Mai 2003.

AMS Subject Classification 2OOO: 12F10 12Y05 11Y40.

Keywords: Galois group, Galois ideal, Triangular ideal, splitting field.

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 explique quels sont les résultats à obtenir pour généraliser l'algorithme `GaloisIdéal` ; les paragraphes suivant vont fournir les résultats théoriques permettant cette généralisation ; 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 stabilisateur ; le paragraphe 7 est dédié au calcul des résolvantes ; le paragraphe 8 généralise les matrices des groupes et des partitions (voir [5] et [20]) ; le paragraphe 9 contient les théorèmes permettant de calculer un idéal de Galois contenant un idéal de Galois donné (i.e. il sera aussi possible de calculer I_j à partir de I_{j-1} lorsque le stabilisateur L_{j-1} n'est pas un groupe) ; au paragraphe 10, nous traiterons un exemple illustrant les résultats de cet article. Cet exemple vient compléter l'exemple du polynôme f_{12} qui nous suivra tout au long de l'article pour en illustrer les résultats (voir Exemple 1.1). Nous aboutirons ainsi au calcul d'un ensemble triangulaire engendrant un idéal maximal, noté $\mathcal{M}_{12}$, associé au polynôme f_{12}.

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 $\mathbb{Q}$ et calculé par Mattman, McKay et Smith (communication privée). L'idéal des relations symétriques engendré par les 8 modules de Cauchy du polynôme f_{12}, de degrés respectifs 8 en x_1, 7 en x_2,..., 1 en x_8, est par défaut le point de départ de l'algorithme `GaloisIdéal`. Or, avec les résultats de [18], à partir de la factorisation de f_{12} dans $\mathbb{Q}(\alpha_1)$, nous construisons rapidement l'idéal de Galois J_{12} engendré par T_{12}, l'ensemble triangulaire séparable suivant :

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

Simultanément au calcul de J_{12}, nous savons :
- que le groupe G_{12} d'ordre 24 et engendré dans S_{12} par les permutations $(1,3,2,6)(4,5,7,8)$ et $(1,3,7)(2,6,4)$ est, à un isomorphisme près, le groupe de Galois du corps de décomposition du polynôme f_{12} sur $\mathbb{Q}$,
- et qu'un stabilisateur de J_{12} est la partie L_{12} de S_{12} qui s'exprime comme une union (disjointe) de deux classes à droite du groupe G_{12} :

$$L_{12} = G_{12} + G_{12}(3,4)(6,7) \qquad .$$

Remarquons qu'il est impossible de considérer n'importe quel conjugué du groupe de Galois de f_{12} pour étudier l'idéal J_{12} et en déduire un idéal maximal qui le contient. 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 [19]). Ici, le conjugué ne peut être quelconque et nous précisons au fur et à mesure les contraintes sur l'ordre des racines de f_{12} sans jamais les calculer. Au départ, la contrainte est que le 8-uplet $\underline{\alpha}$ de ses racines appartienne à la k-variété affine de l'idéal J_{12}.

L'idéal J_{12} est l'intersection de deux idéaux maximaux dont l'un, $\mathcal{M}_{12}$, possède le groupe G_{12} comme stabilisateur et l'autre le groupe $(3,4)(6,7)G_{12}(3,4)(6,7)$. Nous cherchons à calculer l'idéal $\mathcal{M}_{12}$. Il est éventuellement possible de le calculer par une méthode classique : la décomposition de J_{12} en idéaux premiers. Mais cette méthode générale est bien plus coûteuse qu'un algorithme adapté aux idéaux de Galois comme `GaloisIdéal`. Notons g_i, le i-ième polynôme de T_{12}. Il est également possible de factoriser le polynôme g_4 de degré 2 en x_4 dans le corps $\mathbb{Q}(\alpha_1, \alpha_3)$ isomorphe à l'anneau quotient $\mathbb{Q}[x_1, x_3]/ < g_1(x_1), g_3(x_1, x_3) >$ qui est de degré 24 sur $\mathbb{Q}$ (voir [3]). Cette factorisation est également moins efficace que ce que nous proposons. Elle le sera encore moins pour de nombreux autres exemples (voir [18]).

Or, avec les connaissances actuelles, l'idéal J_{12} est inutilisable pour l'algorithme `GaloisIdéal` puisque son stabilisateur L_{12} n'est pas un groupe. L'idéal des relations symétriques, argument possible de l'algorithme `GaloisIdéal`, est quant à lui l'intersection de 1680=8!/card(G_{12}) idéaux maximaux. La généralisation de `GaloisIdéal` aux idéaux de Galois qui comme J_{12} ont des stabilisateurs qui ne sont pas des groupes induira donc un gain très important pour le calcul de corps de décomposition (i.e. de l'idéal $\mathcal{M}$).

2. Rappels

Cette partie reprend les résultats de [21] que nous ne redémontrons donc pas.

Nous nous donnons un polynôme f d'une variable sur k et de racines supposées distinctes $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ 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 notons $\mathcal{M}$ l'*idéal des $\underline{\alpha}$-relations* défini par :

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

Cet idéal est maximal puisqu'il est le noyau du morphisme surjectif d'évaluation qui à P dans $k[x_1, x_2, \ldots, x_n]$ associe $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ dans $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

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

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

Pour une partie H du groupe symétrique S_n (non nécessairement un groupe), l'$(\underline{\alpha}, H)$-*idéal de Galois* (sur k), noté $I_{\underline{\alpha}}^H$, est défini par :

$$I_{\underline{\alpha}}^H = \{R \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in H)\ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\} \quad .$$

Un tel idéal est appelé un *idéal de Galois de f (sur k).*

L'idéal $I_{\underline{\alpha}}^{S_n}$ est appelé l'*idéal des relations symétriques* (entre les racines du polynôme f). L'idéal des $\underline{\alpha}$-relations $\mathcal{M}$ est l'idéal $I_{\underline{\alpha}}^{I_n}$ où I_n est le sous-groupe identité de S_n. Nous simplifions cette notation en posant $I_{\underline{\alpha}} = I_{\underline{\alpha}}^{I_n}$.

Fixons un idéal de Galois J de f et choisissons le n-uplet $\underline{\alpha}$ de racines de f de telle sorte qu'il appartienne à $V(J) = \{\underline{\beta} \in \hat{k}^n \mid (\forall R \in J)\ R(\underline{\beta}) = 0\}$, la k-variété affine de J.

Le *stabilisateur de J relatif à $\underline{\alpha}$*, noté $\mathrm{Stab}(J, \underline{\alpha})$, est défini par :

$$\mathrm{Stab}(J, \underline{\alpha}) = \{\sigma \in S_n \mid (\forall R \in J)\ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\} \quad .$$

Ce stabilisateur est l'union des parties H de S_n telles que J soit l'$(\underline{\alpha}, H)$-idéal de Galois (i.e. $J = I_{\underline{\alpha}}^H$). L'idéal J est aussi appelé l'$\underline{\alpha}$-*idéal de Galois de stabilisateur Stab*$(J, \underline{\alpha})$.

L'exemple de l'idéal J_{12} de l'introduction montre qu'un stabilisateur n'est pas nécessairement un groupe. Une condition nécessaire et suffisante pour que $\mathrm{Stab}(J, \underline{\alpha})$ soit un groupe est qu'il existe un sous-groupe H de S_n tel que $J = I_{\underline{\alpha}}^H$ et que H contienne le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$. Dans ce cas, l'idéal J ne possède qu'un stabilisateur, le groupe H, que nous appelons le *stabilisateur de l'idéal J* et que nous notons $\mathrm{Stab}(J)$.

Remarque 1. Le stabilisateur de l'idéal des relations symétriques est le groupe symétrique S_n et celui de l'idéal des $\underline{\alpha}$-relations, $\mathcal{M} = I_{\underline{\alpha}}$, est le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$. En particulier, nous avons :

$$I_{\underline{\alpha}} = I_{\underline{\alpha}}^{\mathrm{Gal}_k(\underline{\alpha})} \quad .$$

Nous avons les identités suivantes :

$$V(J) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \in \hat{k}^n \mid \sigma \in \mathrm{Stab}(J, \underline{\alpha})\} \quad \text{et} \tag{2}$$

$$\mathrm{Stab}(J, \underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})H = \{gh \mid g \in \mathrm{Gal}_k(\underline{\alpha})\ ,\ h \in H\} \tag{3}$$

pour toute partie H de S_n telle que J soit l'$(\underline{\alpha}, H)$-idéal de Galois et donc en particulier pour $H = \mathrm{Stab}(J, \underline{\alpha})$. Nous constatons que $\mathrm{Gal}_k(\underline{\alpha}) \subset \mathrm{Stab}(J, \underline{\alpha})$.

Si I est un idéal de Galois de f (sur k) contenant J et tel que $\underline{\alpha} \in V(I)$ alors :

$$\mathrm{Stab}(I, \underline{\alpha}) \subset \mathrm{Stab}(J, \underline{\alpha}) \quad . \tag{4}$$

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

$$I_{\underline{\alpha}}^{\cup_{H\in\mathcal{G}}H} = \bigcap_{H\in\mathcal{G}} I_{\underline{\alpha}}^{H} \quad . \tag{5}$$

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 :

$\forall(\beta_1,\ldots,\beta_n)\in\hat{k}^n$ tel que $\forall j\in[\![1,n]\!]$, $f_j(\beta_1,\ldots,\beta_j)=0$, 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 le stabilisateur d'un idéal de Galois est un groupe alors la liste de ses degrés initiaux est calculable à partir de ce groupe (voir [8]).

Exemple 3.1. L'idéal de Galois J_{12} est triangulaire engendré par les polynômes de T_{12}. 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} comme stabilisateur. Le calcul montre que la liste de ses degrés initiaux est $(8,1,3,1,1,1,1,1)$. Notons $g_i(x_1,\ldots,x_i)$ le i-ème polynôme de l'ensemble T_{12}. Alors g_1,g_2,g_3 et g_5,g_6,g_7,g_8 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 $\mathcal{M}_{12}$.

Nous avons le théorème suivant qui nous donne une condition suffisante pour qu'un idéal triangulaire soit de Galois :

Théorème 3.2. *Soit I un idéal triangulaire sur $k[x_1,\ldots,x_n]$ tel que sa variété $V(I)$ soit incluse dans la variété $V(I_{\underline{\alpha}}^{S_n}) = \{(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}) \mid \sigma\in S_n\}$. Alors I est un idéal de Galois de f.*

Démonstration. Par hypothèse, $V(I) = \{(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}) \mid \sigma\in H\}$ où H est une partie S_n. Comme l'idéal I est engendré par un ensemble triangulaire séparable, il est radical. Donc I est l'idéal de $V(I)$, c'est-à-dire que :

$$I = \{R\in k[x_1,\ldots,x_n] \mid (\forall\sigma\in H)\ R(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)})=0\} = I_{\underline{\alpha}}^{H}$$

et que I est un idéal de Galois dont H est le stabilisateur relatif à $\underline{\alpha}$. □

4. L'algorithme GaloisIdéal et sa généralisation

Supposons que I soit un idéal de Galois de f engendré par un ensemble triangulaire T et ayant S comme stabilisateur relatif à $\underline{\alpha} \in V(I)$.

L'algorithme `GaloisIdéal` calcule un idéal de Galois I' contenant strictement I (i.e. un stabilisateur de I' et un ensemble triangulaire l'engendrant) et recommence avec cet idéal I'. L'algorithme se termine sur l'idéal maximal $\mathcal{M}$ (nous verrons plus loin le test d'arrêt).

La première étape consiste à choisir un sous-groupe H de S_n inclus dans S et à calculer un polynôme d'une variable appelé H-résolvante S-relative de $\underline{\alpha}$ (voir Paragraphe 7).

Pour calculer une telle résolvante, il faut appliquer l'algorithme de [8] qui, à partir de l'ensemble triangulaire T, 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 un facteur simple de cette résolvante obtenu, `GaloisIdéal` applique le théorème 3.27 de [21] pour en déduire des générateurs de l'idéal $I' = I_{\underline{\alpha}}^{H}$. Mais ce théorème n'est applicable que dans le cas où S et $\mathrm{Stab}(I', \underline{\alpha})$ sont des groupes. Au paragraphe 9, nous généraliserons ce théorème sans condition sur les stabilisateurs 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 et l'algorithme se termine lorsque qu'il n'existe plus qu'un seul groupe dans cette liste (à conjugaison près dans S). Seulement les matrices des groupes et des partitions ne sont définies et utilisables que lorsque S est un groupe. Le Paragraphe 8 les généralisera au cas où S est quelconque.

Ainsi, avec les résultats de cet article, nous pourrons appliquer l'algorithme `GaloisIdéal` à tous idéaux de Galois.

5. Notations et Hypothèses générales

Pour toute la suite, nous fixons J un idéal de Galois de f. Nous considérons $\underline{\alpha} \in V(J)$ et nous posons $L = \mathrm{Stab}(J, \underline{\alpha})$. L'intérêt de tout ce qui va suivre est de ne pas supposer que L est un groupe.

Nous posons $G = \mathrm{Gal}_k(\underline{\alpha})$, le groupe de Galois de $\underline{\alpha}$ sur k, et nous notons M le groupe engendré par L dans S_n. Comme le groupe M contient G, il est le stabilisateur de l'idéal $I_{\underline{\alpha}}^{M}$. Nous fixons H un sous-groupe de M tel que $H \subset L$.

Nous avons donc les inclusions suivantes :

$$G = \mathrm{Stab}(\mathcal{M}) \subset L = \mathrm{Stab}(J, \underline{\alpha}) \subset M = \mathrm{Stab}(I_{\underline{\alpha}}^{M}, \underline{\alpha}) \qquad \text{et} \tag{6}$$

$$I_{\underline{\alpha}}^{M} \subset J \subset I_{\underline{\alpha}}^{H} \subset \mathcal{M} = I_{\underline{\alpha}} \quad . \tag{7}$$

Exemple 5.1. Nous savons que L_{12} (de cardinal 48) est le stabilisateur de l'idéal J_{12} relatif à un certain $\underline{\alpha}$ dans $V(J_{12})$. 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

Pour $\tau \in S_n$ et $R \in k[x_1, x_2, \ldots, x_n]$, posons $\tau.\underline{\alpha} = (\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})$ et $\tau.R = R(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Lemme 6.1. *Soit $\tau \in S_n$. Nous avons les trois identités suivantes :*

$$Gal_k(\tau.\underline{\alpha}) = \tau^{-1} G \tau \quad , \quad I_{\tau.\underline{\alpha}} = I_{\underline{\alpha}}^{G\tau} \quad \text{et} \quad V(I_{\tau.\underline{\alpha}}) = \{\sigma.\underline{\alpha} \mid \sigma \in G\tau\} \quad .$$

L'idéal $I_{\tau.\underline{\alpha}}$ étant maximal, la variété $V(I_{\tau.\underline{\alpha}})$ est irréductible.

Démonstration. Soit $\sigma = \tau^{-1} g \tau \in \tau^{-1} G \tau$, avec $g \in G$ et $R \in I_{\tau.\underline{\alpha}}$; 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 $\underline{\alpha}$, nous avons, par 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 $\tau^{-1} G \tau \subset \mathrm{Gal}_k \tau.\underline{\alpha}$. Par symétrie, en posant $\underline{\beta} = (\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})$, nous obtenons l'inclusion réciproque ; d'où l'égalité. Pour les variétés, comme $\sigma.R(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = \tau\sigma.R(\alpha_1, \ldots, \alpha_n)$, et puisque $\mathrm{Gal}_k(\tau.\underline{\alpha})$ est le stabilisateur de $I_{\underline{\alpha}}$, nous avons, d'après l'identité (2), :

$$\begin{aligned} V(I_{\tau.\underline{\alpha}}) &= \{\tau\sigma.\underline{\alpha} \mid \sigma \in \mathrm{Gal}_k(\tau.\underline{\alpha})\} \\ &= \{\tau\sigma.\underline{\alpha} \mid \sigma \in \tau^{-1} G \tau\} \quad . \end{aligned}$$

D'où le résultat. L'identité sur l'idéal $I_{\tau.\underline{\alpha}}$ découle de celle sur $V(I_{\tau.\underline{\alpha}})$. □

Théorème 6.2. *La k-variété affine $V(J)$ de l'idéal de Galois J est l'union disjointe de s=Card(L)/Card(G) k-variétés affine irréductibles*

$$V(I_{\tau_i.\underline{\alpha}}) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in G\tau_i\} \qquad i \in [\![1, s]\!].$$

Pour $i \in [\![1, s]\!]$, l'idéal de la variété $V(I_{\tau_i.\underline{\alpha}})$ est l'idéal $I_{\tau_i.\underline{\alpha}}$ des $\tau_i.\underline{\alpha}$-relations ayant pour stabilisateur le groupe de Galois $Gal_k(\tau_i.\underline{\alpha}) = \tau_i^{-1} G \tau_i$. Par conséquent,

$$J = \bigcap_{i=1}^{s} I_{\tau_i.\underline{\alpha}} \qquad et \qquad Stab(J,\underline{\alpha}) = G\tau_1 + G\tau_2 + \cdots + G\tau_s \qquad .$$

Démonstration. Soient les $e = [S_n : G]$ permutations $\tau_1 = id, \ldots, \tau_e$ telles que S_n soit l'union disjointe : $S_n = G\tau_1 + G\tau_2 + \cdots + G\tau_e$. La variété de l'idéal des relations symétriques est donnée par (voir (2)) :

$$V = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in S_n\}$$

qui, d'après le lemme 6.1, se décompose en e k-variétés affines irréductibles disjointes (car les α_j sont distincts deux à deux)

$$V_i = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in G\tau_i\} \qquad i \in [\![1, e]\!].$$

Comme V contient $V(J)$ (car $I_{\underline{\alpha}}^{S_n} \subset J$), en choisissant correctement l'ordre des τ_i, nous obtenons qu'il existe $s \leq e$ tel que $V(J) = V_1 \cup V_2 \cup \cdots \cup V_s$. Comme les idéaux de Galois sont radicaux, en appliquant le lemme 6.1 et l'identité (5), nous obtenons le résultat. □

Exemple 6.3. Toujours en poursuivant notre exemple. Considérons $\underline{\alpha}$ un 8-uplet des racines du polynôme f_{12} tel que l'idéal $I_{\underline{\alpha}}$ des $\underline{\alpha}$-relations ait le groupe G_{12} $=\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$ comme stabilisateur. Puisque L_{12} $=\mathrm{Stab}(J,\underline{\alpha}) = G_{12} + G_{12}(3,4)(5,6)$, nous obtenons :

$$J_{12} = I_{\underline{\alpha}} \cap I_{(3,4)(6,7).\underline{\alpha}} \qquad .$$

7. Résolvantes L-relatives

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

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

Lorsque $\underline{\alpha}$ est fixé, pour simplifier, nous noterons parfois cette résolvante $R_{\Theta,L}$.

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 un sous-groupe de M et inclus dans L. Supposons que Θ soit un *H-invariant M-primitif* ; c'est-à-dire que $H = \{\sigma \in M \mid \sigma.\Theta = \Theta\}$. La résolvante $R_{\Theta,L}$ est 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 :

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 numérotée de telle sorte que $(\sigma_j H) \bigcap L \neq \emptyset$ pour $j = 1, \ldots, r$ avec $r \leq e$ et $(\sigma_j H) \bigcap L = \emptyset$ pour $j = r+1, \ldots, e$. Nous avons l'union disjointe :*

$$L = (\sigma_1 H) \cap L + \cdots + (\sigma_r H) \cap L \qquad . \tag{8}$$

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

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

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

Démonstration. Les racines de la résolvante $R_{\Theta,L}$ sont, d'après (8), les $\sigma_i h.\Theta$ tels que $i \in [\![1, r]\!]$ et $h \in H$. Cherchons les racines distinctes de cette résolvante. Soit $\tau, \sigma \in S_n$ tels que $\tau \in \sigma H$. 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 $\sigma \in L$ si $\sigma.\Theta \neq \Theta$ alors

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

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

Remarque 2. Posons $\theta = \Theta(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Si Θ est $(L, \underline{\alpha})$-séparable alors θ 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 θ soit une racine de ce facteur, l'invariant Θ est alors $(L, \underline{\alpha})$-séparable. Nous verrons par la suite la nécessité que Θ soit $(L, \underline{\alpha})$-séparable.

Exemple 7.2. Prenons le groupe $H = G_{12}$ d'indice $e = 8$ dans M_{12}.

Calculons un G_{12}-invariant M_{12}-primitif tel que la résolvante associée ait au moins un facteur simple. Le module `PrimitiveInvariant` écrit en `GAP` (voir [1] et [2]) calcule le polynôme $P = x_6x_7x_8 + x_3x_4x_5 + x_2x_5x_7 + x_2x_4x_6 + x_2x_3x_8 + x_1x_5x_6 + x_1x_4x_8 + x_1x_3x_7$ qui est un G_{12}-invariant M_{12}-primitif mais qui se réduit à zéro modulo l'idéal J_{12}. Puisque $P \in J_{12}$, la résolvante $R_{P,L_{12}} = x^5$. Nous appliquons donc la méthode de [12] pour obtenir un invariant $(L_{12}, \underline{\alpha})$-séparable : soit $\phi(x) = x^2 + x$; alors le polynôme $P(\phi(x1), \ldots, \phi(x_8))$ est aussi un G_{12}-invariant M_{12}-primitif. Sa réduction modulo J_{12} fournit le polynôme :

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

Nous calculons ensuite le degré de la résolvante. Cinq des huits classes à gauche σH de H dans M vérifient $\sigma H \cap L \neq \emptyset$; donc la résolvante $R_{\Theta_{12},L_{12}}$ est de degré $r = 5$. Elle est donnée par :

$$R_{\Theta_{12},L_{12}} = \prod_{\sigma \in F} (x - \Theta(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$$

où $F = \{\sigma_1 = id, (4,5)(7,8), (1,6,2,3)(5,8), (1,7,8,3)(2,4,5,6), (1,8,4,3)(2,5,7,6)\}$.

Pour terminer, calculons cette résolvante en exécutant pas-à-pas l'algorithme de [8] qui en calcule une puissance. C'est le système de calcul formel `MAXIMA` qui a été utilisé pour ces calculs (voir [17]). Soit p_1 le résultant en x_4 de $x - \Theta_{12}$ et du polynôme g_4 réduit modulo l'idéal J_{12}. La factorisation de g_1 sur $\mathbb{Q}[x_1, x_3, x]$ donne :

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

Le résultant en x_1 des polynômes p_2 et g_1 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 est identique à celui de la résolvante. Donc

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

8. Matrices des groupes et des partitions

Nous considérons Θ un H-invariant M-primitif. La résolvante $R_{\Theta,M}$ de degré $e = [M : H]$.

Nous notons $\mathcal{C}$ les classes à gauche de H dans M.

Nous prenons comme convention que le groupe de Galois d'un polynôme de degré m sur k est celui de son corps de décomposition sur k qui, par isomorphisme, appartient au groupe symétrique S_m.

Pour $\sigma \in S_n$, posons $\theta^\sigma = \Theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$.

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

Ce paragraphe reprend des résultats des articles [5] et [20] et précise les liens entre les facteurs des résolvantes M-relatives et l'action du groupe de Galois G sur les classes de $\mathcal{C}$.

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 la résolvante $R_{\Theta,M}$, si elle n'a pas de racine double,

ait exactement s facteurs k-irréductibles dont les degrés et les groupes de Galois sur k respectifs soient $i_1, \ldots, i_s$ et $G_1, \ldots, G_s$.

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 ques les classes de conjugaisons dans 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.

Soit $\mathcal{O} = \{g_1H, g_2H, \ldots, g_dH\}$ 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=card($\mathcal{O}$) et qui s'écrit :

$$h(x) = \prod_{i=1}^{d} (x - \theta^{g_i}) \qquad . \qquad , \tag{9}$$

Pour simplifier, nous pouvons supposer que θ est 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 $\{\theta^\tau \mid \tau \in G\} = \{\theta^{g_i} \mid i \in [\![1, d]\!]\}$. 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 $\mathcal{O}$. C'est ainsi que sont calculées les listes $P_M(G,H)$ et $Gr_M(G,H)$.

Dans la pratique, nous ne disposons que de la résolvante $R_{\Theta,M}$ et nous cherchons à savoir lesquels de ses facteurs sur k sont associés à des G-orbites de $\mathcal{C} = \{\sigma_1 H, \ldots, \sigma_e H\}$.

Soit g un facteur sur k de cette résolvante ayant θ^{σ_i} comme racine où $i \in [\![1, e]\!]$.

Si g est un facteur simple de la résolvante $R_{\Theta,M}$, alors $\forall j \in [\![1, e]\!] \backslash \{i\}$ $\theta^{\sigma_j} \neq \theta^{\sigma_i}$. C'est donc en particulier vrai pour les $j \neq i$ tels que $\sigma_j \in G\sigma_i H$. Si le polynôme g est un facteur k-irréductible simple de la résolvante $R_{\Theta,M}$, alors il est associé à la G-orbite de $\sigma_i H$.

Remarque 3. Supposons que le polynôme g soit k-irréductible et associé à une G-orbite et qu'un autre facteur g' de la résolvante vérifie $g = g'$. Dans ce cas, le polynôme g n'est pas simple et pourtant bien associé à une G-orbite. Il faut alors étudier la matrice des partitions relative à M pour éventuellement le détecter.

L'idée de calculer des listes $P_M(G,H)$ et $Gr_M(G,H)$ est ancienne (voir [9] et [13]). Mais n'étaient considérés que le 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 [16]). Dans le paragraphe suivant, nous allons généraliser cette idée aux matrices des groupes et des partitions relatives à la partie L de S_n (donc qui n'est 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 et de les associer aux résolvantes L-relatives de la même manière que pour M.

Posons $\mathcal{F} = \{C \in \mathcal{C} \mid C \cap L \neq \emptyset\}$ et $C_0 = \sigma H \in \mathcal{O}$ ($\sigma \in M$), la G-orbite associée au facteur h donné en (9). Le polynôme h possède θ^σ comme racine.

Si h est irréductible, il est un facteur simple de la résolvante $R_{\Theta,M}$. 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 $\mathcal{F}$.

Nous pouvons étudier les matrices des partitions et des groupes relative à L sans utiliser les propriétés algébriques des polynômes et en ne considérant que les groupes. C'est ce que nous faisons ci-dessous en utilisant l'outil classique que sont les classes doubles.

Soit la relation d'équivalence définie $\mathcal{R}$ dans S_n par

$$\sigma \,\mathcal{R}\, \tau \text{ si et seulement si } \tau \in G\sigma H.$$

La classe d'équivalence de σ, notée $(G\sigma H)$, est appelée une *classe double*. Nous avons également $\sigma \,\mathcal{R}\, \tau$ si et seulement si $\sigma H \cap G\tau \neq \emptyset$.

Lemme 8.1. *Nous avons $(G\sigma H) = \sum_{K \in \mathcal{O}} K$ (union disjointe). Soit $\tau \in G\sigma H$ (i.e. $\sigma H \cap G\tau \neq \emptyset$). Alors nous avons l'union disjointe :*

$$G\tau = \sum_{K \subset \mathcal{O}} K \cap G\tau \qquad .$$

Démonstration. Évident, par la définition de la G-orbite $\mathcal{O}$ et celle de la relation d'équivalence $\mathcal{R}$. □

Le proposition suivante traduit en terme de groupe le fait suivant : si θ^σ est une racine de la résolvante $R_{\Theta,L}$ alors les $\theta^{\sigma'}$ tels que $\sigma' H \in \mathcal{O}$ sont aussi des racines de cette résolvante et par conséquent le polynôme h est un facteur de cette résolvante que h soit ou non k-irréductible.

Proposition 8.2. *Si $C_0 \in \mathcal{F}$. Alors toute classe C dans la G-orbite $\mathcal{O}$ appartient $\mathcal{F}$.*

Démonstration. Comme L est une union de classes à droite $G\tau$ (voir Théorème 6.2) et que $C_0 = \sigma H \in \mathcal{F}$, nous pouvons choisir $\tau \in L$ tel que $\sigma H \cap G\tau \neq \emptyset$. Nous avons alors $\tau \in G\sigma H$ et donc $\tau \in G\sigma' H$ si $C = \sigma' H$ appartient à $\mathcal{O}$. D'où $C \cap G\tau \neq \emptyset$ et $C \in \mathcal{F}$. □

Lemme 8.3. *Soit $\tau \in M$ tels que $\tau \in G\sigma H$. En posant $c = card(\sigma H \cap G\tau) \neq 0$ (car $\tau \in G\sigma H$), nous avons $c = card(\sigma' H \cap G\tau')$ pour tout $\sigma', \tau' \in G\sigma H$.*

Démonstration. Soit $\sigma' \in G\sigma H$, donc $\sigma' H \in \mathcal{O}$. Supposons que $\sigma H = \{h_1, \ldots, h_r\}$ et que $\sigma H \cap G\tau = \{h_1, \ldots, h_c\}$. Comme $\sigma' H \in \mathcal{O}$, nous avons $\sigma' H = \{g_1 h_1, \ldots, g_r h_r\}$ où $g_i \in G$. Nous avons forcément $g_1 h_1, \ldots, g_c h_c \in \sigma' H \cap G\tau$ et si pour $s \in [\![1, r]\!]$ nous avons

$g_s h_s \in \sigma' H \cap G\tau$ alors $h_s \in G\tau$ et $s \in [\![1, c]\!]$. Donc $c = \text{card}(\sigma' H \cap G\tau)$ et, comme il s'agit d'une relation d'équivalence, le résultat énoncé est vrai. □

Théorème 8.4. *Supposons que $C_0 = \sigma H \in \mathcal{F}$ (i.e. θ^σ est une racine commune de h et de la résolvante $R_{\Theta,L}$). Soit $\tau \in G\sigma H$ et $c = card(\sigma H \cap G\tau)$. Alors*

$$card(G) \quad = \quad c.card(\mathcal{O}) = c.deg(h) \qquad .$$

Démonstration. Soit d le cardinal de $\mathcal{O}$ et donc aussi le degré du polynôme h. Soit $\{\sigma_1 H, \ldots, \sigma_d H\}$, l'orbite $\mathcal{O}$. D'après le lemme 8.1, nous avons :

$$\sum_{i=1}^{\lambda} (\sigma_i H \cap G\tau) = G\tau$$

Comme cette union est disjointe, puisque les $\sigma_i H$ le sont deux à deux, nous avons :

$$d.\text{card}(\sigma_i H \cap G\tau) = \text{card}(G\tau) = \text{card}(G) \qquad .$$

Pour finir, nous appliquons le lemme 8.3 pour obtenir $c.d = \text{card}(G)$. □

Théorème 8.5. *Le nombre de facteurs k-irréductibles d'une H-résolvante L-relative sans racine double est le nombre de classes doubles distinctes $(G\sigma H)$ auxquelles appartiennent les permutations $\tau_1, \ldots, \tau_s$ de L telles que L est l'union disjointe $G\tau_1 + \cdots + G\tau_s$.*

Démonstration. Car à chaque facteur irréductible (simple) de la résolvante $R_{\Theta,L}$ (i.e. une orbite $\mathcal{O}$) correspond une et une unique classe double. □

Remarque 4. Nous retrouvons le résultat bien connu qui dit que si la résolvante possède un facteur simple $h = x - \theta^\sigma$ ($\sigma \in S_n$ étant forcément inconnu), alors $G \subset \sigma H \sigma^{-1}$. En effet, si c'est le cas alors $(G\sigma H) = \{\sigma H\}$, soit $G \subset \sigma H \sigma^{-1}$. Dans la pratique, nous considérons $\underline{\alpha} \in V(J)$ tel que $h = x - \theta$ (i.e. $\sigma = id$). Ce qui permet d'affirmer que $G \subset H$.

Remarque 5. Avec les résultats précédents, il apparaît que si un facteur est simple dans la résolvante $R_{\Theta,L}$ alors il est associé à un G-orbite dans $\mathcal{F}$ (donc dans $\mathcal{C}$). Or ce facteur n'est pas nécessiarement un facteur simple de la résolvante $R_{\Theta,M}$. Cette remarque est à rapprocher de la remarque 3.

8.3. Calcul des matrices de partitions et de groupes en GAP.

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 $\mathcal{C}$. Par la proposition 8.2, toute G-orbite d'une classe de $\mathcal{C}$ est ou bien dans $\mathcal{F}$ ou bien complètement en dehors de $\mathcal{F}$. Or, avec chacune de ces G-orbites $\mathcal{O}$, nous savons 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 (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 (simples) de la résolvante $R_{\Theta,L}$. La fonction `Groups` suivante écrite dans le langage du logiciel de calcul formel `GAP` (voir [14]) 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 (communication privée) qui retourne $Gr_M(G,H)$.

Remarque 6. Il est possible de calculer autrement $Gr_L(G,H)$. Il suffit de calculer les classes doubles $(G\sigma H)$ dans M contenant $\tau_1,\ldots,\tau_s$. Le nombre de ces classes doubles est m, le nombre de facteurs irréductibles des H-résolvantes L-relatives séparables de polynômes de groupe de Galois G. Soit $\sigma H \in \mathcal{C}$ telle que $(G\sigma H)$ soit une de ces classes doubles (i.e. $\sigma H \in \mathcal{F}$). La G-orbite de σH est formée des classes à gauche ρH dans $\mathcal{C}$ telles que $\rho \in (G\sigma H)$.

Exemple 8.6. Nous savons que $L_{12} = G_{12} + G_{12}(3,4)(6,7)$. Donc, d'après le théorème 8.5, toute G_{12}-résolvante L_{12}-relative séparable est ou bien $\mathbb{Q}$-irréductible, ou bien le produit de deux polynômes $\mathbb{Q}$-irréductibles. La résolvante séparable $R_{\Theta_{12},L_{12}}$ calculée dans l'exemple 7.2 a effectivement 2 facteurs (simples) 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 :

$$L_{12} = \bigcup_{\sigma \in F} (\sigma G_{12}) \cap L_{12} \qquad .$$

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 $\{(\sigma H) \cap L \mid \sigma \in F\ ,\ \sigma \neq id\}$ 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 $I_{\underline{\alpha}}^{G_{12}}$) 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. Elément primitif d'un idéal de Galois

Soit I un idéal de Galois de f (sur k) contenant l'idéal J et tel que $\underline{\alpha} \in V(I)$. Un polynôme P de $k[x_1, \ldots, x_n]$ est dit *L-primitif de l'idéal I* si

$$\mathrm{Stab}(I, \underline{\alpha}) = \{\sigma \in L \mid P(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\} \quad .$$

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 L-primitif de l'idéal $I^H_{\underline{\alpha}}$.

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

Démonstration. Posons $P = h(\Theta)$, $\theta^\sigma = \Theta(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$ pour $\sigma \in S_n$ et

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

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

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

Comme $P(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = h(\theta^\sigma)$, 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 (3) appliquée à L=Stab$(J, \underline{\alpha})$), nous avons $\tau^{-1}\sigma \in L$. Comme, par hypothèse, le polynôme Θ est $(L, \underline{\alpha})$-séparable, nous obtenons :

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

Puisque $\tau^{-1}\sigma \in L$ et que H est le stabilisateur de Θ dans L, nous obtenons :

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

Le polynôme P est donc bien un polynôme L-primitif de l'idéal $I^H_{\underline{\alpha}}$ puisque, d'après l'identité (3), nous avons $\mathrm{Stab}(I^H_{\underline{\alpha}}, \underline{\alpha}) = GH$. □

Remarque 7. Pour calculer le degré de la résolvante $R_{\Theta,L}$, le théorème 7.1 impose que Θ soit un H-invariant M-primitif et cette proposition lui impose seulement d'être L-primitif.

Exemple 9.2. La 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 L_{12}-primitif de l'idéal $I_{\underline{\alpha}} = I^{G_{12}}_{\underline{\alpha}}$. C'est un tel $\underline{\alpha}$ que nous considèrerons par la suite.

Le théorème suivant à déjà été prouvé dans le cas où L et $\mathrm{Stab}(I,\underline{\alpha})$ sont des groupes (voir Théorème 3.27 de [21]).

Théorème 9.3. *Soit P un polynôme L-primitif de l'idéal I. Alors*

$$I = J + < P > \qquad .$$

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

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

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

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 $I' = I_{\underline{\alpha}}^{U'}$. Pour $i \in [\![1, s]\!]$, nous avons $I_{\tau_i.\underline{\alpha}} = I_{\underline{\alpha}}^{G\tau_i}$ (voir Lemme 6.1). Les idéaux I, I' et J s'expriment comme suit (voir Identité (5)) :

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

Comme P est un élément L-primitif de l'idéal I et d'après l'identité (2) sur les variétés affines des idéaux de Galois, nous avons :

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

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

$$I^m \subset J + < P > \subset\ I \qquad .$$

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

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

Nous avons $xu \in J + < P >$ 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

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

Donc $xv \in J$ et $x \in J + < P >$. 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 $V_i = V(I_{\tau_i.\underline{\alpha}})$, $i \in [\![1, s]\!]$ (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 L_{12}-primitif de l'idéal $\mathcal{M}_{12} = I_{\underline{\alpha}} = I_{\underline{\alpha}}^{G_{12}}$ calculé dans l'exemple 9.2. Alors, pour $\underline{\alpha} \in V(J_{12})$ tel que $\Theta(\underline{\alpha})$ soit racine de $x+6$ (i.e. $P(\underline{\alpha}) = 0$), nous avons $\underline{\alpha} \in V(\mathcal{M}_{12})$ et :

$$\mathcal{M}_{12} = J_{12} + < P_{12} > \quad .$$

Calculons le corps de décomposition du polynôme f_{12}. Bien que $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_8) \simeq \mathbb{Q}[x_1, x_2, \ldots, x_8]/\mathcal{M}_{12}$, la liste des générateurs de $\mathcal{M}_{12}$ dont nous disposons n'est pas adaptée pour calculer dans le corps $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_8)$. Il faut pour cela disposer d'un ensemble triangulaire engendrant l'idéal $\mathcal{M}_{12}$. Nous savons d'après l'exemple 3.1 qu'il suffit de calculer un polynôme de la forme $x_4 + h(x_1, x_3)$.

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

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

qui appartient à $J_{12} + < P_{12} >= \mathcal{M}_{12}$. L'idéal $\mathcal{M}_{12}$ est donc engendré par l'ensemble triangulaire $T_{\underline{\alpha}} = \{g_1, g_2, g_3, h_4, g_5, g_6, g_7, g_8\}$.

10. Un autre exemple d'application

Nous allons choisir un autre exemple dans lequel sont construits des idéaux de Galois triangulaires dont les stabilisateurs ne sont pas des groupes. Ces stabilisateurs sont inconnus mais nous parviendrons tout de même à calculer un élément primitif d'un idéal de Galois afin de poursuivre la construction de la chaîne ascendante. Nous utiliserons cet exemple pour illustrer les résultats du paragraphe 8.

Nous considérons le polynôme $f = x^8 + x^4 + 2$ calculé par Mattman,McKay et Smith. Choisissons au départ $\underline{\alpha}$ un 8-uplet quelconque des racines du polynôme f sur lequel nous imposerons des contraintes au fur et à mesure de l'avancée des calculs. Tout d'abord, remarquons que le groupe de Galois de f sur $\mathbb{Q}$ est un groupe impair puisque son discriminant $2^{19}7^4$ n'est pas un carré dans $\mathbb{Q}$.

10.1. Calcul d'un idéal maximal des $\underline{\alpha}$-relations.

Notons I_1 l'idéal des relations symétriques entre les racines du polynôme f. Considérons le sous-groupe H_2 de S_8 d'ordre 1152 et engendré par les permutations

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

Choisissons le H_2-invariant H_1-primitif suivant :

$$\Theta_2 = x_1x_2x_3x_4 + x_5x_6x_7x_8 \quad .$$

Pour cet invariant, il existe une formule permettant de calculer la résolvante (voir [4]) de $\underline{\alpha}$ par Θ_2 . Nous obtenons :

$$R_{\Theta_2, I_1} = (x-1)x^8(x^2-8)^5(x^4-8x^2+14)^4 \quad .$$

Cette résolvante possède le facteur linéaire simple $x - 1$. Décidons que $\underline{\alpha}$ soit tel que $\Theta_2(\underline{\alpha}) - 1 = 0$. Nous avons alors $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) \subset H_2$. Notons I_2 l'$\underline{\alpha}$-idéal de Galois de

stabilisateur H_2. D'après le théorème 3.27 de [21] (dont le théorème 9.3 de cet article est une généralisation), nous avons :

$$I_2 = I_1 + < \Theta_2 - 1 > \quad .$$

Nous cherchons à calculer un ensemble triangulaire engendrant l'idéal I_2. Nous utilisons l'implantation de P. Aubry en `AXIOM` pour décomposer un idéal en ensembles triangulaires (voir [6] et [7]). Nous obtenons trois ensembles triangulaires engendrant respectivement trois idéaux J_1, J_2 et J_3 tels que

$$I_2 = J_1 \cap J_2 \cap J_3 \quad .$$

En particulier, nous avons :

$$\begin{aligned} J_1 \;=\; & < x_1^8 + x_1^4 + 2, x_2 + x_1, x_3^2 + x_1^2, x_4 + x_3, x_5^4 + x_1^4 + 1, x_6^3 + x_6^2 x_5 + x_6 x_5^2 + x_5^3, \\ & x_7^2 + x_7 x_6 + x_7 x_5 + x_6^2 + x_6 x_5 + x_5^2, x_8 + x_7 + x_6 + x_5 > \quad . \end{aligned}$$

Pour chacun des idéaux J_1, J_2 et J_3, le produit de leurs degrés initiaux est 384. L'idéal I_2 est radical et le cardinal de sa variété est $\mathrm{Card}(H_2) = 3.384 = 1152$. Donc les trois idéaux J_1, J_2 et J_3 sont aussi radicaux. Par le théorème 3.2, ce sont donc trois idéaux de Galois du polynôme f.

Posons $I_3 = J_1$ et imposons à $\underline{\alpha}$ d'appartenir à $V(I_3)$. Nous avons la chaîne :

$$I_1 \subset I_2 \subset I_3 \quad .$$

Pour des raisons évidentes d'efficacité, nous aimerions poursuivre notre calcul avec l'idéal I_3 plutôt qu'avec l'idéal I_2. Pour ce faire, il faut pouvoir calculer des résolvantes H_3-relatives où H_3 est le stabilisateur de I_3 relatif à $\underline{\alpha}$. La définition du stabilisateur montre que H_3 ne peut être calculé qu'avec l'idéal maximal des $\underline{\alpha}$-relation que nous recherchons. Nous ne pouvons donc pas appliquer le théorème 7.1 qui donne le moyen de calculer les degrés des résolvantes H_3-relatives. Pour y parvenir, nous utiliserons une autre méthode adaptée à notre situation.

Avec la matrice des partitions relative à S_8 et la résolvante R_{Θ_2, I_1}, nous obtenons le résultat suivant : le groupe de Galois de f sur $\mathbb{Q}$ est un sous-groupe H_4 de H_2 d'ordre 128 et engendré par les permutations

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

Avec le module `PrimitiveInvariant`, nous calculons l'H_4-invariant H_3-primitif

$$\Theta_4 = x_1 x_2 + x_3 x_4 + x_5 x_6 + x_7 x_8 \quad .$$

Avec l'algorithme de [8] nous obtenons :

$$M_{\Theta_4, J_1} = x(x^4 - 4x^2 + 32) \quad \text{et} \quad M_{\Theta_4, J_2} = M_{\Theta_4, J_3} = (x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112) \; .$$

où $M_{\Theta, I}$ est la forme sans facteur carré du polynôme caractéristique de l'endomorphisme multiplicatif induit par le polynôme Θ dans l'anneau quotient $\mathbb{Q}[x_1, x_2, \ldots, x_8]/I$. Comme la résolvante R_{Θ_4, I_2} est de degré 9, l'indice de H_4 dans H_2, et que les trois polynômes M_{Θ_4, J_j} sont des facteurs de cette résolvantes, nous avons :

$$R_{\Theta_4,I_2} = x(x^4 - 4x^2 + 32)(x^4 - 8x^2 - 112) \quad .$$

Comme les résolvantes R_{Θ_4,J_j} sont aussi des facteurs de cette résolvante, nous avons $R_{\Theta_4,J_j} = M_{\Theta_4,J_j}$ pour $j = 1, 2, 3$. Le polynôme x est donc un facteur simple de la résolvante R_{Θ_4,J_1}. Imposons à $\underline{\alpha}$ de vérifier $\Theta_4(\underline{\alpha}) = 0$. Nous avons alors $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) \subset H_3$. Notons I_4 l'$\underline{\alpha}$-idéal de Galois de stabilisateur H_4. Avec le théorème 9.3, nous obtenons :

$$I_4 = I_3 + < \Theta_4 > = < x_1^8 + x_1^4 + 2, x_2 + x_1, x_3^2 + x_1^2, x_4 + x_3, x_5^4 + x_1^4 + 1, x_6 + x_5, x_7^2 + x_5^2, x_8 + x_7 > .$$

Nous pouvons utiliser les matrices des groupes et des partitions. Le calcul montre que les deux facteurs de degré 4 de la résolvante R_{Θ_{35},I_2} ont le groupe diédral D_4 comme groupe de Galois sur $\mathbb{Q}$. Nous déterminons 5 sous-groupes H de H_2 tels que $Gr_{H_2}(H, H_4) = (1, D_4, D_4)$ (voir Paragraphe 8.1). Parmi eux, nous choisissons le sous-groupe H_5 d'indice 2 dans H_4 et engendré par les permutations bd, ac, e, g, h et cd.

Avec le module `PrimitiveInvariant`, nous calculons Θ_5 un H_5-invariant H_4-primitif. Cet invariant se réduit à zéro modulo l'idéal I_4. Nous transformons cet invariant, comme dans l'exemple 7.2, avec ici $\phi(x) = x^2 + x + 1$. Le polynôme $\Theta_5(\phi(x_1), \ldots, \phi(x_8))$ se réduit modulo l'idéal I_4 au polynôme :

$$\Psi_5 = 128x_1^3x_3x_5^3x_7 + 352 \quad .$$

Nous trouvons que le résultant en x_7 de $x - \Psi_5$ et de $x_7^2 + x_5^2$ (polynôme de I_4) se réduit modulo I_4 au polynôme $x^2 - 704x + 58368 = (x - 608)(x - 96)$. Imposons à $\underline{\alpha}$ de vérifier $\Psi_5(\underline{\alpha}) - 96 = 0$. Ainsi $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) \subset H_5$ et $I_5 = I_4 + < \Psi_5 - 96 >$. Soit

$$I_5 = < x_1^8 + x_1^4 + 2, x2 + x_1, x_3^2 + x_1^2, x_4 + x_3, x_5^4 + x_1^4 + 1, x_6 + x_5, 2x_7 + x_5x_3x_1^7 + x_5x_3x_1^3, x_8 + x_7 > .$$

est l'$\underline{\alpha}$-idéal de Galois de stabilisateur H_5. Le groupe de Galois est donc H_5 ou bien un de ses sous-groupes. Le seul de ses sous-groupes H qui vérifie $Gr_{H_2}(H, H_4) = (1, D_4, D_4)$ est le groupe H_6 d'indice 2 dans H_5 engendré par les permutations bd, ac, e, g et h. Un calcul rapide d'une H_6-résolvante H_5-relative de degré 2 séparable et réductible montre que H_5 est le groupe de Galois de $\underline{\alpha}$ sur $\mathbb{Q}$ et que I_5 est l'idéal maximal $\mathcal{M}$ des $\underline{\alpha}$-relations. Nous avons construit la chaîne ascendante d'idéaux de Galois suivante :

$$I_1 \subset I_3 \subset I_4 \subset I_5 = \mathcal{M} \quad .$$

Remarque 8. En factorisant le polynôme f dans $\mathbb{Z}/11\mathbb{Z}$, nous trouvons le polynôme $(x - 3)(x + 3)(x^2 - 2)(x^2 - 5x - 4)(x^2 + 5x - 4)$ qui correspond au cycle type $1^2, 2^3$. D'après les tables de Butler et McKay (voir [10]), le groupe de Galois de f sur $\mathbb{Q}$ ne peut être le groupe H_6 conjugué au groupe au groupe $8T_{17}$ de leur nomenclature.

10.2. **Illustration des résultats du paragraphe 8.**

Posons M_1=Stab$(J_1, \underline{\alpha})$, M_2 =Stab$(J_2, \underline{\alpha})\cup$Stab$(J_3, \underline{\alpha})$, $G = H_5$ et $H = H_4$. Nous avons $\mathrm{Card}(H) = 2.\mathrm{card}(G) = 128$. Nous savons qu'il existe des permutations $\tau_1 = id, \ldots, \tau_{18}, \sigma_1 = id, \ldots, \sigma_9$ de H_3 telles que nous ayons les unions disjointes :

$$H_3 = G\tau_1 + \cdots + G\tau_{18} = \sigma_1 H + \cdots + \sigma_9 H \quad .$$

Nous allons étudier le lien qui existe entre les trois résolvantes $R_u = R_{\Theta_4,J_u}$ $(u = 1,2,3)$ et les $\sigma_i H \cap G\tau_j$ $(i \in [\![1,9]\!]$ et $j \in [\![1,18]\!])$. Comme $3.\mathrm{card}(V(J_u)) = \mathrm{card}(H_3)$ pour $u = 1,2,3$, nous avons, en numérotant correctement les τ_j, (voir Théorème 6.2) :

$$M_1 = G\tau_1 + \cdots + G\tau_6 \quad \text{et} \quad M_2 = G\tau_7 + \cdots + G\tau_{18} \quad .$$

Choisissons l'ordre des σ_i de telle sorte que les facteurs de la résolvante R_{Θ_4,I_3} vérifient :

$$\begin{aligned} g_1 = x &= x - \sigma_1.\Theta_4(\underline{\alpha}) \\ g_2 = x^4 - 4x^2 + 32 &= \prod_{i=2}^{5}(x - \sigma_i.\Theta_4(\underline{\alpha})) \quad \text{et} \\ g_3 = x^4 - 8x^2 - 112 &= \prod_{i=6}^{9}(x - \sigma_i.\Theta_4(\underline{\alpha})) \quad . \end{aligned}$$

Regardons d'abord la G-orbite de $\sigma_1 H$ (réduite à $\sigma_1 H$ puisque $G \subset H$) à laquelle le polynôme $g_1 = x$ est associé. Comme $\tau_1 = \sigma_1 = id$, nous avons $\tau_1 \in G\sigma_1 H$ et d'après le lemme 8.1, nous avons $G\tau_1 = \sigma_1 H \cap G\tau_1$ (i.e. $G \subset H$). Nous avons $c_1 = \mathrm{card}(\sigma_1 H \cap G\tau_1) = \mathrm{Card}(G) = 64$. Comme x n'est facteur que de la résolvante R_1, les 64 autres permutations de $\sigma_1 H$ appartiennent aussi à M_1. Choisissons la permutation τ_2 de M_1 telle que $\sigma_1 H \cap G\tau_2 \neq \emptyset$. D'après le lemme 8.3, nous avons $c_1 = 64 = \mathrm{card}(\sigma_1 H \cap G\tau_2)$. Nous avons $G\tau_2 = \sigma_1 H \cap G\tau_2$ (i.e. $G\tau_2 \subset H$). D'où $H = (\sigma_1 H \cap G\tau_1) + (\sigma_1 H \cap G\tau_2) = G + G\tau_2$.

Intéressons nous maintenant à la G-orbite $\{\sigma_2 H, \ldots, \sigma_5 H\}$ à laquelle est associé le facteur g_2 commun aux trois résolvantes R_i, $i = 1,2,3$. Nous avons nécessairement pour $i = 1,2,3,4$ et $j = 3,4,5,6$:

$$\sigma_i H \cap G\tau_j \neq \emptyset \qquad \text{avec} \qquad c_2 = \mathrm{card}(\sigma_i H \cap G\tau_j) = \mathrm{card}(G)/4 = 16 \quad .$$

Nous avons $4.c_2 = 64$ et $\mathrm{card}(\sigma_2 H) = 2.64$. Il y a donc 64 permutations de $\sigma_2 H$ appartenant à M_1 (en fait à $G\tau_3 + G\tau_4 + G\tau_5 + G\tau_6$). Les 64 autres permutations de $\sigma_2 H$ appartiennent donc à M_2. D'après les lemmes 8.1 et 8.3, en numérotant correctement les τ_j, nous savons que les 4 classes à droites $G\tau_j$, $j = 7,8,9,10$, dans M_2 vérifient pour $i = 2,3,4,5$

$$G\tau_j = \sum_{i=2}^{5} \sigma_i H \cap G\tau_j \quad , \quad c_2 = \mathrm{card}(\sigma_i H \cap G\tau_j) \quad \text{et} \quad \sigma_i H = \sum_{j=3}^{10} (\sigma_i H \cap G\tau_j) \quad .$$

Pour terminer, le facteur g_3 est associé à la G-orbite $\{\sigma_6 H, \ldots, \sigma_9 H\}$. Ce polynôme est uniquement un facteur des résolvantes R_2 et R_3. Les 8 classes à droite $G\tau_{11}, \ldots, G\tau_{18}$ vérifient donc pour $i = 6,7,8,9$ et $j \in [\![11,18]\!]$:

$$G\tau_j = \sum_{i=6}^{9} \sigma_i H \cap G\tau_j \quad , \qquad \mathrm{card}(\sigma_i H \cap G\tau_j) = 16 \quad \text{et} \quad \sigma_i H = \sum_{j=11}^{18} (\sigma_i H \cap G\tau_j) \quad .$$

Conclusion

À partir de l'idéal des relations symétriques, pour calculer en une étape l'ensemble triangulaire $T_{\underline{\alpha}}$ engendrant l'idéal maximal $\mathcal{M}_{12}$, il faudrait calculer une résolvante de degré 1680 $=[S_8 : G_{12}]$ (i.e. la résolvante de Galois) et en extraire au moins un facteur linéaire simple pour obtenir un polynôme S_8-primitif de l'idéal $\mathcal{M}_{12}$ (i.e. un ensemble de générateurs de cet idéal). Resterait ensuite un calcul extrêmement coûteux en temps et en espace pour en déduire $T_{\underline{\alpha}}$. De plus, ce calcul n'est possible en une étape que si le groupe de Galois est déjà connu.

Ici, à partir d'une factorisation dans $\mathbb{Q}(\alpha_1)$ de degré 8 sur $\mathbb{Q}$, l'idéal J_{12} a pu être calculé et le groupe de Galois G_{12} déterminé. Puis le calcul de $T_{\underline{\alpha}}$ s'est réalisé en une étape par le biais d'une résolvante de degré 5 et de quelques pseudo-restes. Cette méthode efficace pour calculer le corps de décomposition a été en partie possible grâce aux résultats de cet article qui permettent d'exploiter ceux de [18].

References

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

[2] I. Abdeljaouad, Package `Primitive Invariants` du logiciel `GAP`, ftp:pub/gap/gap-3.4.4/deposit/gap/priminv.g ou bien http://www-history.mcs.st-and.ac.uk/ gap/Info/deposit.html.

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

[4] J.M. Arnaudiès, A. Valibouze, *Calculs de Résolvantes*, Rapport LITP 94.46, (1994).

[5] 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.

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

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

[8] 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.

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

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

[11] 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.

[12] 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.

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

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

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

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

[17] `Maxima DOE`, maintenu par William Schelter (Austin, Unversity of Texas) jusqu'à son décès juillet 2001.
[18] Orange, S., Renault, G., Valibouze, A., *Calcul efficace de corps de décompositions*, (2003), communication privée.
[19] R.P. Stauduhar, *The determination of Galois groups*, Math. Comp.,**27** (1973) , 981–996.
[20] 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)).
[21] 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.

L.I.P.6 Université Paris VI 4, place Jussieu F-75252 Paris Cedex 05
E-mail address: `Annick.Valibouze@lip6.fr`