

INES ABDELJAOUAD

Calculs d'invariants primitifs de groupes finis

RAIRO. Theoretical Informatics and Applications, tome 33, n° 1
(1999), p. 59-77

http://www.numdam.org/item?id=ITA_1999__33_1_59_0

© AFCET, 1999, tous droits réservés.

L'accès aux archives de la revue « RAIRO. Theoretical Informatics and Applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

CALCULS D'INVARIANTS PRIMITIFS DE GROUPES FINIS *

INES ABDELJAOUAD¹

Abstract. We introduce in this article a new method to calculate all absolute and relatif primitive invariants of finite groups. This method is inspired from K. Girstmair which calculate an absolute primitive invariant of minimal degree. Are presented two algorithms, the first one enable us to calculate all primitive invariants of minimal degree, and the second one calculate all absolute or relative primitive invariants with distincts coefficients. This work take place in Galois Theory and Invariant Theory.

Résumé. Nous introduisons dans cet article un nouvel outil de calcul de tous les invariants primitifs relatifs et absolus de groupes finis. Cette méthode est inspirée par l'algorithme de K. Girstmair qui calcule un invariant primitif absolu de degré minimal. Sont présentés deux algorithmes : le premier algorithme calcule tous les invariants primitifs de degré minimal et le deuxième algorithme calcule tous les invariants primitifs à coefficients distincts. Ce travail entre dans le cadre de la théorie de Galois et la théorie des Invariants.

INTRODUCTION

Les invariants auxquels nous faisons référence tout au long de cet article sont des invariants dits primitifs : un *invariant primitif* d'un groupe de permutations est un polynôme qui à lui seul, permet d'identifier ce groupe.

Il existe deux types d'invariants primitifs : les *invariants primitifs absolus* et les *invariants primitifs relatifs*. Ces polynômes sont un outil fondamental dans la résolution des équations polynomiales (voir [8]) et dans la théorie de Galois effective (voir [20]). Dans ces applications, il est important d'avoir plusieurs invariants primitifs relatifs ou absolus d'un même groupe qui soient de petits degrés.

* Recherche supportée par le Projet Galois du GDR de Calcul Formel MEDICIS, <http://medicis.polytechnique.fr/medicis/projetGalois>

¹ CalFor - LIP6, Université Paris VI, 4 place Jussieu, 75252 Paris Cedex 05, France; e-mail: Ines.Abdeljaouad@lip6.fr

Les invariants primitifs les plus célèbres sont donnés par des mathématiciens tels que Vandermonde [21], Luther [15], Cayley [6], Berwick [4, 5], Foulkes [9] et les méthodes utilisées, appelées *méthodes classiques*, s'appuyaient sur les caractéristiques propres à chaque sous-groupe du groupe symétrique pour construire, par étapes successives, des invariants de plus en plus sophistiqués (voir par exemple [5] et [21]). Chaque groupe demandait donc une stratégie spécifique alors que nous préférons maintenant avoir des algorithmes généraux.

Une autre méthode dite *méthode naturelle* permet de calculer un invariant primitif d'un sous-groupe H du groupe symétrique de degré n (voir [22]). En effet, nous remarquons que la somme des images du monôme $(x_2x_3^2 \dots x_n^{n-1})$ par les permutations de H est invariant absolu de H de degré $\frac{n(n-1)}{2}$.

L'inconvénient de ces méthodes est qu'elles donnent des invariants primitifs absolus de degrés élevés. Elles ne sont pas économiques et elles ne se généralisent pas facilement au calcul d'invariants primitifs relatifs.

Une représentation des polynômes assez particulière, due à Jordan [12], a permis à Girstmair [11] d'exhiber une technique de calcul d'un invariant absolu de degré minimal pour tout groupe de permutation. Le but de cet article est de présenter la généralisation de cette technique au calcul de tous les invariants primitifs absolus et relatifs, et en particulier au calcul des invariants primitifs relatifs ou absolus de degré minimal et de degrés inférieurs ou égaux à $\frac{n(n-1)}{2}$. Les invariants calculés par la méthode naturelle ou les méthodes classiques sont aussi retrouvés par les algorithmes présentés dans cet article.

Les trois premiers paragraphes introduisent les définitions et notations ainsi que les théorèmes sur lesquels se basent les algorithmes de calcul d'invariants primitifs ; le paragraphe 4 présente les algorithmes nécessaires au calcul d'invariants primitifs relatifs ou absolus à coefficients distincts : l'algorithme 4.3 calcule la liste de ces invariants de *degré minimal* et l'algorithme 4.4 calcule pour des sous-groupes de permutations de degré n , la liste des invariants primitifs de degrés $\leq \frac{n(n-1)}{2}$.

Les principaux outils de calcul sont les *ensembles essentiels*. Le paragraphe 5 est consacré à la représentation des données utilisées pour l'implantation des algorithmes : nous introduisons la notion de *partition*, définissons la correspondance entre les monômes et les partitions et nous montrons que grâce à cette représentation de données, nous calculons tous les invariants primitifs de tous les degrés possibles.

Le dernier paragraphe est consacré à des exemples d'applications de ces algorithmes.

1. DÉFINITIONS ET NOTATIONS

Dans tout l'article k désigne un corps commutatif de caractéristique nulle et $k[X_1, \dots, X_n]$ l'anneau des polynômes en X_1, \dots, X_n à coefficients dans k , où X_1, \dots, X_n sont n indéterminées algébriquement indépendantes sur k .

Le groupe symétrique de degré n est noté S_n . L'action de S_n sur $k[X_1, \dots, X_n]$

est définie de façon naturelle par :

$$\begin{aligned} S_n \times k[X_1, \dots, X_n] &\longrightarrow k[X_1, \dots, X_n] \\ (\sigma, P) &\longmapsto \sigma(P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}). \end{aligned}$$

Soient L un sous-groupe de S_n et P un polynôme de $k[X_1, \dots, X_n]$. Le *stabilisateur de P sous l'action de L* est

$$\text{Stab}_L(P) = \{g \in L \mid g(P) = P\}.$$

Le *stabilisateur d'une partie U de $k[X_1, \dots, X_n]$ sous l'action de L* est

$$\text{Stab}_L(U) = \{g \in L \mid \forall P \in U, g(P) \in U\}.$$

Soit H un sous-groupe de L tels que $H \subset L$. L'*orbite du polynôme P sous l'action de H* appelé aussi la *H -orbite de P* est définie par

$$\text{Orb}_H(P) = \{\sigma(P) \mid \sigma \in H\}.$$

Définition 1.1. Un polynôme $P \in k[X_1, \dots, X_n]$ est un *H -invariant (relatif à L)* si $H \subset \text{Stab}_L(P)$. Si de plus $L = S_n$ alors P est appelé un *H -invariant (absolu)*.

Définition 1.2. Un polynôme $P \in k[X_1, \dots, X_n]$ est dit *H -invariant L -primitif* si

$$\text{Stab}_L(P) = H.$$

Si $L = S_n$, alors P est appelé *H -invariant primitif (absolu)*.

Un polynôme P H -invariant L -primitif est de *degré minimal* si le degré de tout polynôme H -invariant L -primitif est supérieur ou égal au degré de P .

Parmi tous les H -invariants L -primitifs de degré minimal, un polynôme dont le nombre de monômes est minimal et dont le PGCD des coefficients est égal à 1, est appelé un *H -invariant L -primitif minimal*.

Exemple 1. Notons A_n le groupe alterné de degré n . Le déterminant de Vandermonde $\delta_n = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ est un A_n -invariant primitif absolu.

Notation 2. Soient g_1, \dots, g_r des permutations de S_n , alors $\langle g_1, \dots, g_r \rangle$ désigne le sous-groupe de S_n engendré par les permutations g_1, \dots, g_r .

Exemple 3. Soient $n = 4$, $H_1 = \langle (3, 4), (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ un sous-groupe de S_4 et $H_2 = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ un sous-groupe de H_1 . Les polynômes suivants sont des polynômes H_2 -invariants H_1 -primitifs de degré minimal :

$$X_2X_4 + X_1X_3 \quad \text{et} \quad X_2X_3 + X_1X_4.$$

Le polynôme H_2 -invariant H_1 -primitif de degré $\frac{n(n-1)}{2} = 6$ est égal à :

$$a(X_2X_3^2X_4^3 + X_1X_4^2X_3^3 + X_4X_1^2X_2^3 + X_3X_2^2X_1^3),$$

où a est un élément non nul de k .

Remarque 4. Soient τ_1, \dots, τ_e des permutations de L vérifiant $L = \tau_1 H + \dots + \tau_e H$. Un polynôme P est un H -invariant L -primitif, lorsque $\forall \sigma \in H, \sigma(P) = P$ et $\forall i \neq j \tau_i(P) \neq \tau_j(P)$. Le nombre de conjugués de P sous l'action des τ_i est égal à l'indice de H dans L c'est-à-dire e .

Définition 1.3. Un monôme de $k[X_1, \dots, X_n]$ sera unitaire et de la forme $X_1^{r_1} \dots X_n^{r_n}$ où les r_i sont des entiers positifs ou nuls. Soit Q un monôme de $k[X_1, \dots, X_n]$, nous notons

$$N_H(Q) = \sum_{Q' \in \text{Orb}_H(Q)} Q'.$$

Le polynôme $N_H(Q)$ est appelé *Trace réduite de Q par H* .

Définition 1.4. Soit U un ensemble fini de monômes de $k[X_1, \dots, X_n]$. Le (L, H) -groupe de U , noté $H_L(U)$, est défini par :

$$H_L(U) = \bigcap_{Q \in U} \text{Stab}_L(N_H(Q)).$$

Définition 1.5. Soit U un ensemble fini de monômes de $k[X_1, \dots, X_n]$.

Une U -fonction élémentaire est un polynôme \mathcal{P}_U donné par la formule suivante :

$$\mathcal{P}_U = \sum_{Q \in U} a_Q N_H(Q)$$

où les a_Q sont des éléments de k non nuls et deux à deux distincts.

Exemple 5. Soient $U = \{X_1 X_2, X_2 X_3\}$ et $H = \langle (1, 4) \rangle$ un sous-groupe de S_4 . La famille des U -fonctions élémentaires est donnée par $\mathcal{P}_U = a(X_1 X_2 + X_2 X_4) + b(X_2 X_3)$ avec $a \neq b$ deux éléments non nuls de k .

Définition 1.6. Le degré d'un ensemble U de monômes de $k[X_1, \dots, X_n]$ est par définition égal au maximum des degrés des monômes dans U .

2. RÉSULTATS EFFECTIFS POUR CALCULER DES INVARIANTS PRIMITIFS

Le théorème et le corollaire suivants ont été énoncés dans [11], dans le cas où $L = S_n$.

Théorème 2.1. Soit U un ensemble fini de monômes de $k[X_1, \dots, X_n]$. Toute U -fonction élémentaire \mathcal{P}_U est un polynôme $H_L(U)$ -invariant L -primitif.

Preuve. Montrons qu'un polynôme $\mathcal{P}_U = \sum_{Q \in U} a_Q N_H(Q)$ ($a_Q \in k$, non nuls et deux à deux distincts) est un $H_L(U)$ -invariant L -primitif. D'après la définition 1.4

du (L, H) -groupe $H_L(U)$ et la définition 1.2 des H -invariants L -primitifs, ceci revient à montrer que :

$$\text{Stab}_L \left(\sum_{Q \in U} a_Q N_H(Q) \right) = \bigcap_{Q \in U} \text{Stab}_L(N_H(Q)).$$

Soit g un élément du groupe $\text{Stab}_L(\mathcal{P}_U)$, alors $g(\mathcal{P}_U) = \mathcal{P}_U$, soit :

$$g(\mathcal{P}_U) = \sum_{Q \in U} a_Q N_H(Q).$$

Comme les a_Q sont deux à deux distincts on a : $g(N_H(Q)) = N_H(Q)$ pour tout $Q \in U$ et donc $g \in \text{Stab}_L(N_H(Q))$ pour tout $Q \in U$. D'où :

$$g \in \bigcap_{Q \in U} \text{Stab}_L(N_H(Q)).$$

Réciproquement, si $g \in \bigcap_{Q \in U} \text{Stab}_L(N_H(Q))$ alors pour tout $Q \in U$ on a : $g \in \text{Stab}_L(N_H(Q))$ et donc $g \in \text{Stab}_L(\sum_{Q \in U} a_Q N_H(Q))$. □

Remarque 6. En d'autres termes, le (L, H) -groupe $H_L(U)$ est le stabilisateur de chaque U -fonction élémentaire $\mathcal{P}_U : \text{Stab}_L(\mathcal{P}_U) = H_L(U)$.

Définition 2.1. Si $H_L(U) = H$, alors U est appelé *ensemble essentiel pour (L, H)* .

Corollaire 2.1. Soit U un ensemble fini de monômes. Si U est un ensemble essentiel pour (L, H) alors chaque U -fonction élémentaire est un H -invariant L -primitif.

Proposition 2.1. Si U est un ensemble essentiel pour (L, H) , alors tout ensemble V contenant U est un ensemble essentiel pour (L, H) .

Preuve. $U \subset V \Rightarrow H_L(V) \subset H_L(U)$, d'autre part, $H_L(U) = H$ et $H \subset H_L(V)$, d'où l'égalité $H_L(V) = H$. □

Définition 2.2. Soit U un ensemble essentiel pour (L, H) . Une U -fonction primitive est un polynôme $P = \sum_{Q \in U} a_i N_H(Q)$ où les a_Q sont des éléments de k non nuls et où $\text{Stab}_L(P) = H$.

Remarque 7. Si U est un ensemble essentiel pour (L, H) alors chaque U -fonction élémentaire est une U -fonction primitive dont les coefficients sont deux à deux distincts.

Nous avons montré que toute U -fonction élémentaire où U est un ensemble essentiel pour (L, H) , est un H -invariant L -primitif à coefficients distincts. Il reste à montrer que tout H -invariant L -primitif est égal à une U -fonction primitive où U est un ensemble essentiel pour (L, H) . Ainsi, nous calculerons à l'aide d'ensembles essentiels pour (L, H) tous les H -invariants L -primitifs.

3. ENSEMBLES ESSENTIELS ET INVARIANTS PRIMITIFS

Proposition 3.1 (K. Girstmair). *Soit Q un monôme de $k[X_1, \dots, X_n]$. La trace réduite de Q par H est un polynôme H -invariant.*

Preuve. D'après la définition 1.1 des polynômes invariants, il faut montrer que H est inclus dans le stabilisateur de $N_H(Q)$.

Prenons $g \in H$. La linéarité de l'action de g sur $k[X_1, \dots, X_n]$ implique que $g(N_H(Q)) = \sum_{Q' \in \text{Orb}_H(Q)} g(Q')$. La permutation $g \in H$ est une bijection sur $\text{Orb}_H(Q)$.

En effet : si $Q' \in \text{Orb}_H(Q)$ alors $g(Q') \in \text{Orb}_H(Q)$ et pour tous monômes Q_1 et Q_2 de $\text{Orb}_H(Q)$, si $g(Q_1) = g(Q_2)$ alors $Q_1 = g^{-1}g(Q_1) = g^{-1}g(Q_2) = Q_2$.

Ainsi $\sum_{Q' \in \text{Orb}_H(Q)} g(Q') = \sum_{Q' \in \text{Orb}_H(Q)} Q'$, et donc $g(N_H(Q)) = N_H(Q)$. \square

Définition 3.1. Soit Q un monôme de $k[X_1, \dots, X_n]$. Tout monôme Q' de $\text{Orb}_H(Q)$ est dit *représentant de $N_H(Q)$* . Le monôme Q' est aussi appelé *représentant de la H -orbite de Q* .

Proposition 3.2. *Un polynôme $P \in k[X_1, \dots, X_n]$ est un H -invariant s'il existe Q_1, \dots, Q_l des monômes de $k[X_1, \dots, X_n]$ tels que $P = \sum_{i=1}^l c_i N_H(Q_i)$ avec $c_i \in k$ non nuls.*

Preuve. Soit P un polynôme de $k[X_1, \dots, X_n]$ vérifiant $P = \sum_{i=1}^s a_i Q_i$ tel que pour tout $i \in [1, s]$, les a_i sont des éléments deux à deux distincts de k et $Q_i \in k[X_1, \dots, X_n]$. En regroupant les monômes de P en polynômes de même coefficients, nous obtenons $P = \sum_{i=1}^r b_i (\sum_{j \in I_i} Q_j)$ avec $r \leq s$, les b_i sont des éléments deux à deux distincts de k , $\bigcup_{i=1}^r I_i = \{1, \dots, s\}$ et pour $i, j \in [1, r]$ tels que $i \neq j$, nous avons $I_i \cap I_j = \emptyset$. Notons $P_i = \sum_{j \in I_i} Q_j$.

P est un H -invariant alors pour tout $h \in H$, $h(\sum_{i=1}^r b_i P_i) = \sum_{i=1}^r b_i P_i$. Comme les b_i sont deux à deux distincts, nous obtenons pour tout $i \in [1, r]$: $h(P_i) = P_i$ pour tout $h \in H$.

Chaque polynôme P_i est un H -invariant. En regroupant les monômes de P_i en monômes de même H -orbite nous obtenons $P_i = \sum_{j \in J_i} N_H(Q_j)$ avec $J_i \subset I_i$. (D'après la proposition 3.1, $N_H(Q_j)$ est un H -invariant).

Ainsi $P = \sum_{i=1}^r b_i (\sum_{j \in J_i} N_H(Q_j)) = \sum_{i=1}^l c_i N_H(Q_i)$ avec $l \geq r$ et les c_i sont des éléments non nuls de k . \square

Remarque 8. Les monômes Q_i pour $i \in [1, l]$ de la proposition précédente peuvent être remplacés par d'autres représentants de H -orbites de Q_i . En effet, si pour tout $i \in [1, l]$ nous notons $Q'_i \in \text{Orb}_H(Q_i)$ un représentant de la H -orbite de Q_i , alors $P = \sum_{i=1}^l c_i N_H(Q_i) = \sum_{i=1}^l c_i N_H(Q'_i)$.

Définition 3.2. Chaque H -orbite pouvant être représentée par un de ses monômes, l'ensemble de ces représentants forme un *système de représentants des orbites de H* .

Nous fixons un système de représentants des orbites de H que nous notons \mathcal{S} .

Théorème 3.1. *Soit $P \in k[X_1, \dots, X_n]$ un H -invariant L -primitif à coefficient distincts. Il existe un unique sous-ensemble U de \mathcal{S} tel que P soit une U -fonction primitive.*

Preuve. Soit P un H -invariant L -primitif. D'après la proposition 3.2, P s'écrit sous la forme $P = \sum_{i=1}^l c_i N_H(Q_i)$ avec c_i des éléments de k deux à deux distincts et où Q_i sont des éléments de \mathcal{S} pour tout $i \in [1, l]$. Le choix des monômes Q_i est unique.

Soit $U = \{Q_1, \dots, Q_l\}$. D'après la définition 2.2, il reste à montrer que U est un ensemble essentiel pour (L, H) , ce qui revient à montrer d'après la définition 2.1 que $H_L(U) = H$.

Le (L, H) -groupe de U est défini par $H_L(U) = \bigcap_{i=1}^l \text{Stab}_L(N_H(Q_i))$.

$H \subset H_L(U)$, en effet : pour tout $i \in [1, l]$ $H \subset \text{Stab}_L(N_H(Q_i))$ car les $N_H(Q_i)$ sont des H -invariants (voir Prop. 3.1). D'autre part, si $g \in H_L(U)$ alors $g \in \bigcap_{i=1}^l \text{Stab}_L(N_H(Q_i))$ et donc pour tout $i \in [1, l]$, $g(N_H(Q_i)) = N_H(Q_i) \Rightarrow g \in \text{Stab}_L(P)$. Ainsi $H_L(U) = \text{Stab}_L(P) = H$. \square

Corollaire 3.1. *Pour calculer tous les H -invariants L -primitifs à coefficients distincts, il suffit de calculer tous les ensembles essentiels pour (L, H) .*

Preuve. D'après le théorème 3.1 et la remarque 7, tout H -invariant L -primitif à coefficients distincts s'écrit sous la forme d'une U -fonction élémentaire où U est un ensemble essentiel pour (L, H) . D'autre part, toute U -fonction élémentaire où U est un ensemble essentiel pour (L, H) est un H -invariant L -primitif (voir Cor. 2.1). Ainsi, le calcul de tous les H -invariants L -primitifs à coefficients distincts, revient à calculer toutes les U -fonctions élémentaires c'est-à-dire à calculer tous les ensembles U essentiels pour (L, H) . \square

Pour le calcul de tous les H -invariants L -primitifs, il faut d'abord calculer tous les ensembles essentiels pour (L, H) . Pour chaque ensemble essentiel U pour (L, H) il faut tester si chaque polynôme de la forme $\sum_{Q \in U} a_Q N_H(Q)$ où les a_Q sont non nuls, est un H -invariant L -primitif.

Si les coefficients a_Q sont deux à deux distincts alors d'après le corollaire 3.1, les polynômes $\sum_{Q \in U} a_Q N_H(Q) = \mathcal{P}_U$ sont des H -invariants L -primitifs.

Sinon, si les coefficients a_Q ne sont pas distincts, alors il faut vérifier que le nombre de conjugués du polynôme $\sum_{Q \in U} a_Q N_H(Q)$ sous l'action des éléments de la classe de conjugaison de L par H , est égal à l'indice de H dans L (voir Rem. 4).

4. ALGORITHMES DE CALCULS D'ENSEMBLES ESSENTIELS

Pour calculer un H -invariant S_n -primitif, Girstmair [11] utilise une technique semblable à celle de l'algorithme 4.3 sauf qu'il n'obtient qu'un seul ensemble essentiel pour (L, S_n) de degré minimal. De plus, le choix de cet ensemble se fait d'une manière aléatoire de sorte qu'il n'a pas toujours un H -invariant primitif absolu et minimal. Nous présentons, dans la première partie de ce paragraphe, un algorithme de calcul de l'ensemble essentiel de \mathcal{S} de degré minimal et contenant

tous les autres ensembles essentiels de degré minimal. Dans la deuxième partie de ce paragraphe, nous donnons un algorithme de calcul de tous les invariants primitifs relatifs ou absolus et de degré minimal ainsi qu'un algorithme de calcul de tous les ensembles essentiels de degrés $\leq \frac{n(n-1)}{2}$ de \mathcal{S} et donc de calcul de tous les invariants primitifs relatifs ou absolus de degrés $\leq \frac{n(n-1)}{2}$ et à coefficients distincts (voir Cor. 3.1).

4.1. SYSTÈME DE REPRÉSENTANTS ET ENSEMBLES ESSENTIELS

Algorithme 4.1 (SystèmeDeReprésentant). Cet algorithme calcule un système de représentants des H -orbites de monômes de degré $\leq \frac{n(n-1)}{2}$.

Entrée : Un entier n et un sous-groupe H de S_n .

Sortie : Un système de représentants des orbites de H de degré $\leq \frac{n(n-1)}{2}$.

1. Soit \mathcal{A} l'ensemble des monômes de degrés $\leq \frac{n(n-1)}{2}$.

Pour Tout m et m' dans \mathcal{A} de même degré **Faire**

Si $Orb_H(m) = Orb_H(m')$

Alors retirer m' de \mathcal{A}

Fin Si

Fin Pour

2. **Rendre**(\mathcal{A}) ;

Fin.

Preuve de l'algorithme 1. L'algorithme termine au bout d'un nombre fini d'étapes puisque l'ensemble \mathcal{A} est fini. D'autre part, en remarquant que deux monômes de degrés distincts n'ont pas la même H -orbite, il suffit de ne comparer que les monômes de même degré.

Notations 9. Soit \mathcal{A} un ensemble fini de monômes. Notons $\text{premier}(\mathcal{A})$ la liste de tous les éléments de \mathcal{A} de degré minimal et $\text{rest}(\mathcal{A})$ la liste des éléments de \mathcal{A} privé de $\text{premier}(\mathcal{A})$.

Algorithme 4.2 (EnsembleEssentiel). Soit \mathcal{A} un sous-ensemble fini de \mathcal{S} . Nous présentons l'algorithme pour le calcul d'un ensemble essentiel pour (L, H) dans \mathcal{A} . L'ensemble U essentiel pour (L, H) obtenu grâce à cet algorithme est, parmi tous les ensembles essentiels dans \mathcal{A} , celui de degré minimal d qui contient tous les autres ensembles essentiels pour (L, H) dans \mathcal{A} de degré d .

Entrée : Un ensemble \mathcal{A} fini de \mathcal{S} .

Sortie : Un ensemble essentiel $U \subset \mathcal{A}$ pour (L, H) , s'il existe.

1. $U := [1]$;

2. **Tant que** $H_L(U) \neq H$ **Et** $\mathcal{A} \neq \{ \}$ **Faire**

$U := U \cup \text{premier}(\mathcal{A})$;

$\mathcal{A} := \text{rest}(\mathcal{A})$;

Fin Tant que

3. **Si** $\mathcal{A} \neq \emptyset$

Alors **Rendre**(U) ;

Sinon \mathcal{A} ne contient pas d'ensemble essentiel pour (L, H) .

Fin Si

Fin.

Preuve de l'algorithme 2. Puisque \mathcal{A} est fini, cet algorithme récursif s'arrête au bout d'un nombre fini d'étapes avec $\mathcal{A} = \{ \}$ ou $H_L(U) = H$. En effet : à chaque étape de l'algorithme, si $H_L(U) \neq H$ alors aucun sous-ensemble U n'est un ensemble essentiel pour (L,H) . En effet, supposons qu'il existe $V \subset U$ un ensemble essentiel pour (L,H) . Alors, d'après la proposition 2.1, U est aussi un ensemble essentiel pour (L,H) et donc $H_L(U) = H$, d'où l'absurdité.

Soit U l'ensemble essentiel pour (L,H) obtenu au bout d'un nombre fini d'étapes de la boucle 2. de l'algorithme. Parmi tous les autres ensembles essentiels pour (L,H) contenus dans \mathcal{A} , U est un ensemble essentiel de degré minimal parce que c'est le premier trouvé.

Enfin, U contient tous les monômes de \mathcal{A} de degré inférieur ou égal à d . Il contient donc tous les ensembles dans \mathcal{A} essentiels pour (L,H) et de degré d .

Remarque 10. Soit U un système de représentants des H -orbites des monômes de degré égal à $\frac{n(n-1)}{2}$, alors U contient nécessairement un représentant de la H -orbite du monôme $X_2 X_3^2 \dots X_n^{n-1}$. D'autre part, la trace réduite du représentant de ce monôme est un H -invariant L -primitif (voir la méthode classique de l'introduction). Ainsi d'après la proposition 2.1, U est aussi un ensemble essentiel pour (L,H) .

4.2. INVARIANTS PRIMITIFS DE DEGRÉ MINIMAL

Définition 4.1. Soit U un ensemble essentiel pour (L,H) . Si U ne contient aucun ensemble essentiel pour (L,H) alors U est dit *réduit*. Toutes les U -fonctions primitives sont alors *réduites*.

Notations 11. Pour U un ensemble fini de monômes, $\text{partie}(U)$ est la liste de tous les sous-ensembles de U classés par ordre croissant suivant leurs tailles et $\text{diff}(U,V)$ est la liste des sous-ensembles de U privée des ensembles contenant V .

Algorithme 4.3 (InvariantsPrimitifsDeDegréMinimal). L'algorithme suivant calcule tous les ensembles essentiels réduits pour (L,H) et de degré minimal dans \mathcal{S} . À chaque ensemble essentiel U nous donnons en guise d'exemples les polynômes H -invariants L -primitifs à coefficients distincts \mathcal{P}_U .

Entrées : Deux sous-groupes L et H de S_n vérifiant $H \subset L$.

Sortie : Une liste de polynômes H -invariants L -primitifs réduits et de degré minimal et à coefficients deux à deux distincts.

1. $\mathcal{A} := \text{SystèmeDeReprésentant}(n,H)$;
2. $U := \text{EnsembleEssentiel}(\mathcal{A},L,H)$;
3. $\mathcal{I} := \{ \}$; *contient tous les ensembles essentiels réduits pour (L,H) de degré minimal*
4. $E := \text{partie}(U)$;
5. **Pour tout** $V \subset E$ **faire**
 Si $H_L(V) = H$;

Alors Rajouter V dans \mathcal{I} ;
 $E := \text{diff}(U, V)$;

Fin Si

Fin Pour

6. Rendre(\mathcal{I}) ;
7. Pour tout U dans \mathcal{I} , donner les polynômes \mathcal{P}_U .

Fin.

Preuve de l'algorithme 3. Soit \mathcal{A} un système de représentants des H -orbites de monômes de degrés $\leq \frac{n(n-1)}{2}$ obtenu par l'algorithme 4.1 appliqué à (n, H) .

L'algorithme 4.2, termine avec un ensemble essentiel. En effet, U contient nécessairement un représentant de la H -orbite du monôme $X_2 X_3^2 \dots X_n^{n-1}$ et d'après la remarque 10 nous savons qu'au pire des cas, c'est-à-dire lorsque U est de degré $\frac{n(n-1)}{2}$, l'algorithme 4.1 termine avec la condition d'arrêt $H_L(U) = H$ et $\mathcal{A} = \{ \}$. L'ensemble U obtenu à l'étape 2 de l'algorithme, est un ensemble essentiel de degré minimal parmi les ensembles essentiels dans \mathcal{A} et il contient tous les autres ensembles essentiels de degré minimal dans \mathcal{A} (voir la preuve de l'algorithme 4.2). La boucle 5 de l'algorithme calcule tous les sous-ensembles V de U qui sont essentiels et réduits et donne les polynômes \mathcal{P}_V qui sont des H -invariants L -primitifs à coefficients distincts (voir Cor. 3.1).

Remarque 12. Le calcul d'ensembles essentiels réduits revient à ne pas calculer les polynômes invariants primitifs somme de deux autres.

Remarque 13. Pour le calcul de tous les H -invariants L -primitifs de degré minimal dont les coefficients peuvent être égaux, il faut d'abord calculer tous les ensembles essentiels pour (L, H) de degré minimal (voir algorithme 4.3) et il faut vérifier que le nombre de conjugués des polynômes $\sum_{Q \in U} a_Q N_H(Q)$ avec a_Q des éléments non nuls de k , sous l'action des éléments de la classe de conjugaison de L par H , est égal à l'indice de H dans L (voir Rem. 4).

4.3. REMARQUES SUR LE CALCUL DE TOUS LES INVARIANTS PRIMITIFS

Nous avons montré dans les paragraphes précédents que le calcul de tous les invariants primitifs à coefficients distincts, est le calcul de toutes les U -fonctions primitives où U sont des ensembles essentiels. L'algorithme précédent nous donne tous les ensembles essentiels U réduits de degré minimal, ainsi nous obtenons toutes les U -fonctions élémentaires réduites par le simple calcul de polynômes dont les monômes sont les traces réduites des éléments de U et dont les coefficients sont deux à deux distincts. Le calcul des U -fonctions primitives qui ne sont pas des U -fonctions élémentaires nécessite, à part le calcul de l'ensemble essentiel U , de tester que le nombre de conjugués de ces polynômes est égal à l'indice de H dans L (voir Rems. 13 et 4), et ce test est très coûteux à cause du nombre de polynômes à tester.

Le plus important, selon notre avis, dans le calcul d'invariants primitifs est de trouver les monômes qui forment ces polynômes c'est-à-dire les ensembles essentiels.

4.4. ALGORITHME DE CALCUL DES INVARIANTS PRIMITIFS DE DEGRÉS $\leq \frac{n(n-1)}{2}$

Notation 14. Soit U un ensemble fini de monômes, $\text{degre}(U)$ est le degré de l'ensemble U .

Algorithme 4.4 (Girstmair-Jordan). Cet algorithme calcule tous les ensembles essentiels réduits pour (L, H) de degrés $\leq \frac{n(n-1)}{2}$. Nous allons voir que grâce à la représentation de données (paragraphe 5), nous calculons avec ce même algorithme tous les ensembles essentiels pour (L, H) .

Entrées : Deux sous-groupes L et H de S_n vérifiant $H \subset L$.

Sortie : Tous les ensembles essentiels réduits pour (L, H) de degré $\leq \frac{n(n-1)}{2}$.

1. $\mathcal{A} := \text{SystèmeDeReprésentant}(n, H)$;
 2. $d := 1$;
 3. $\mathcal{I} := \{ \}$; contient tous les ensembles essentiels réduits pour (L, H) de degrés inférieurs ou égaux à $\frac{n(n-1)}{2}$
 4. **Tant que** $d \leq \frac{n(n-1)}{2}$ **Faire**
 $U := \text{EnsembleEssentiel}(\mathcal{A}, L, H)$;
 5. **Pour tout** $V \subset E$ **faire**
Si $H_L(V) = H$;
Alors Rajouter V dans \mathcal{I} ;
 $E := \text{diff}(U, V)$;
Fin Si
 - Fin Pour**
 $d := \text{degre}(U) + 1$;
 - Fin Tant que**
 6. **Rendre** (\mathcal{I}) ;
- Fin.**

Preuve de l'algorithme 4. À chaque étape de la boucle 4. \mathcal{A} change de valeur et ne contient plus que des monômes de degré supérieur strictement au degré du dernier ensemble essentiel obtenu. À la fin de la boucle 4, l'ensemble essentiel obtenu est de degré $\frac{n(n-1)}{2}$ et l'algorithme termine avec $d = \frac{n(n-1)}{2} + 1$.

Tous les ensembles essentiels obtenus sont réduits, en effet : soit U un ensemble essentiel obtenu à l'étape (p) de la boucle 4, alors $U = \text{EnsembleEssentiel}(\mathcal{A}, L, H)$ et \mathcal{A} change de valeur et ne contient plus que les monômes de degré supérieur strictement au degré de U (voir l'algorithme 4.2). Ainsi, le nouvel ensemble essentiel calculé à la $(p+1)$ -ième étape de la boucle 4. sera contenu dans ce nouvel \mathcal{A} et l'intersection de l'ensemble essentiel obtenu à l'étape $(p+1)$ avec U est l'ensemble vide. D'autre part, la boucle 5 nous donne tous les ensembles essentiels réduits d'un même degré.

5. PARTITIONS ET INVARIANTS PRIMITIFS

Dans ce paragraphe est présentée la notion de partitions, qui a été introduite pour la première fois par Jordan [12] et ses contemporains du siècle dernier. Nous

mettons en évidence la correspondance entre monômes et partitions et nous montrons comment le problème de calcul d'invariants primitifs qui, à première vue, est purement algébrique se transforme en un problème de combinatoire des groupes et des ensembles.

En effet, vis-à-vis d'un groupe de permutation, un monôme ou son carré donnent la même information. Ce qui compte donc c'est la partition de l'ensemble $\{1, \dots, n\}$ associée à un monôme.

5.1. PARTITIONS

Le cardinal d'un sous-ensemble I de $\{1, \dots, n\}$ est noté $|I|$.

Définition 5.1. Une *partition* $T = (T_1, \dots, T_s)$ de l'ensemble $\{1, \dots, n\}$ est une liste de sous-ensembles non vides de $\{1, \dots, n\}$ classés par cardinal décroissant tels que les ensembles T_1, \dots, T_s soient deux à deux disjoints et que leur réunion soit égale à l'ensemble $\{1, \dots, n\}$.

Notons \mathcal{T} l'ensemble des partitions de $\{1, \dots, n\}$. D'après la définition 5.1, une partition $T = (T_1, \dots, T_s)$ de \mathcal{T} vérifie donc les quatre propriétés suivantes :

- (i) $\forall i \in [1, n] \quad T_i \subset \{1, \dots, n\}$.
- (ii) $\bigcup_{i=1}^s T_i = \{1, \dots, n\}$.
- (iii) $\forall i, j \in [1, n] \quad i \neq j \implies T_i \cap T_j = \emptyset$.
- (iv) $\forall i \in [1, n] \quad |T_i| \neq 0$ et $|T_1| \geq |T_2| \geq \dots \geq |T_s| \geq 1$.

5.2. REPRÉSENTATION DES DONNÉES

Notation 15. Soient I un sous-ensemble de $\{1, \dots, n\}$ et α un entier. Par convention, notons :

$$X_I^\alpha = \left(\prod_{i \in I} X_i \right)^\alpha .$$

Un monôme Q de $k[X_1, \dots, X_n]$ peut toujours s'écrire de manière unique sous la forme :

$$Q = X_{T_1}^{\alpha_1} \dots X_{T_s}^{\alpha_s}$$

où $\alpha_1, \dots, \alpha_s$ sont des entiers deux à deux distincts et (T_1, \dots, T_s) est une partition de $\{1, \dots, n\}$ vérifiant pour tout $i, j \in [1, s]$ tels que $i < j$: ou bien $|T_i| > |T_j|$ ou bien $|T_i| = |T_j|$ et $\alpha_i < \alpha_j$.

Introduisons l'application surjective Ψ définie par :

$$\Psi: \left\{ \prod_{i=1}^n X_i^{r_i} \mid (r_1, \dots, r_n) \in \mathbf{N}^n \right\} \longrightarrow \mathcal{T}$$

$$Q = X_{T_1}^{\alpha_1} \dots X_{T_s}^{\alpha_s} \quad \mapsto \quad \Psi(Q) = (T_1, \dots, T_s) .$$

Définitions 5.1. Soit $T = (T_1, \dots, T_s) \in \mathcal{T}$. Nous définissons le monôme Q_T et un ensemble de monômes \mathcal{M} par :

$$Q_T = \prod_{i=1}^s X_{T_i}^{(i-1)} \quad \text{et} \quad \mathcal{M} = \{Q_T \mid T \in \mathcal{T}\}.$$

Le degré d'une partition T est par définition égal au degré du monôme Q_T c'est-à-dire égal à $\sum_{i=1}^s (i-1) |T_i|$.

Proposition 5.1. L'application Φ définie par :

$$\begin{aligned} \Phi: \mathcal{T} &\longrightarrow \mathcal{M} \\ T &\longmapsto Q_T \end{aligned}$$

est bijective.

Preuve. Évident. □

Exemple 16. Soient $Q = X_1 X_2 X_3^2 X_4^3 X_5^2 X_6^2 X_7$ et $n = 8$ alors :

$$\Psi(Q) = (\{1, 2, 7\}, \{3, 5, 6\}, \{8\}, \{4\}).$$

En effet : $Q = (X_1 X_2 X_7)^1 (X_3 X_5 X_6)^2 X_8^0 X_4^3$.

Exemple 17. Soient $n = 9$ et $T = (\{2, 3, 4, 5\}, \{7, 8, 9\}, \{1\}, \{6\})$ un élément de \mathcal{T} . Alors, $\Phi(T) = Q_T = X_7 X_8 X_9 X_1^2 X_6^3$ et le degré de T est égal à 8.

La correspondance entre partitions et monôme étant démontrée, il suffit d'appliquer les algorithmes de la section 4 à l'ensemble des partitions plutôt qu'aux monômes et de faire le calcul d'ensembles essentiels de partitions. En effet, la manipulation des listes et des ensembles d'entiers (partitions) est beaucoup plus facile que la manipulation des monômes et des polynômes.

5.3. CALCUL DE TOUS LES INVARIANTS PRIMITIFS AVEC DES PARTITIONS

Nous remarquons tout d'abord que l'ensemble de partitions \mathcal{T} est un ensemble fini et que le degré d'un ensemble de partitions varie entre 1 et $\frac{n(n-1)}{2}$.

En remplaçant dans les algorithmes 4.1 et 4.4 appelés *SystèmeDeReprésentant* et *Algorithme de Girstmair-Jordan*, les monômes par les partitions, nous obtenons un algorithme qui calcule tous les ensembles essentiels de partitions à partir desquels, nous obtenons tous les invariants primitifs à coefficients distincts.

Voici un exemple de la représentation des données utilisée dans l'implantation de l'*algorithme de Girstmair-Jordan* dans le cas où $n = 3$.

La liste des partitions en degré 3 est égale à :

$$\begin{aligned} &[[[1, 2, 3]], \\ &[[[1, 2], [3]], [[1, 3], [2]], \\ &[[[2, 3], [1]], \\ &[[[1], [2], [3]], [[[1], [3], [2]], \end{aligned}$$

$$\begin{aligned} & [[2] , [1] , [3]] , [[2] , [3] , [1]] , \\ & [[3] , [1] , [2]] , [[3] , [2] , [1]]] \end{aligned}$$

Un système de représentants des S_2 -orbites de partitions est égal à :

$$\begin{aligned} & [[[1 , 2 , 3]] , [[1 , 2] , [3]]] , \\ & [[[1 , 3] , [2]] , [[1] , [2] , [3]]] , \\ & [[[1] , [3] , [2]] , [3] , [1] , [2]]] \end{aligned}$$

La liste des ensembles essentiels réduits pour (S_2, S_3) est égale à :

$$\begin{aligned} & [[[[1 , 2] , [3]]]] , \\ & [[[[1 , 3] , [2]]]] , \\ & [[[[1] , [2] , [3]]]] , \\ & [[[[1] , [3] , [2]]]] , \\ & [[[[3] , [1] , [2]]]] \end{aligned}$$

La famille des polynômes S_2 -invariants S_3 -primitifs réduits est égale à :

$a(X_1 X_2)^\alpha X_3^\beta$, $a((X_1 X_3)^\alpha X_2^\beta + (X_2 X_3)^\alpha X_1^\beta)$, $a(X_1^\alpha X_2^\beta X_3^\gamma + X_2^\alpha X_1^\beta X_3^\gamma)$,
avec α, β, γ trois entiers distincts et a un élément de k .

6. EXEMPLES D'APPLICATIONS

L'implantation des algorithmes 4.3 et 4.4 dans le système de Calcul Formel GAP (voir [10]), a été possible grâce à la manipulation des partitions. Pour plus de détails sur l'implantation le lecteur pourra consulter les références [1] et [2].

6.1. EXEMPLES D'UTILISATION

Les polynômes invariants primitifs suivis de $*$ peuvent être obtenus par les méthodes classiques ou par la méthode naturelle discutées dans l'introduction.

Notation 18. Le monôme $X_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$ sera représenté par la liste $[r_1 r_2 \dots r_n]$.

Exemple 19. Soient $H_1 = \langle (4, 5, 6), (2, 3), (1, 2), (5, 6) \rangle$, $H_2 = \langle (4, 5, 6), (5, 6), (1, 2, 3) \rangle$ et $H_3 = \langle (5, 6), (1, 2)(3, 4), (1, 3, 2, 4) \rangle$ trois sous-groupes de S_6 . La table suivante présente des H -invariants L -primitifs minimaux calculés à partir de l'algorithme 4.3 :

| L | H | H-Invariant L-Primitif minimal |
|-------------------|-----------------------------|---|
| S_4 | A_4 | δ_4^* |
| S_4 | D_4 | $X_3X_4 + X_1X_2^*$ |
| D_4 | C_4 | $X_2X_4^2 + X_4X_1^2 + X_3X_2^2 + X_1X_3^{2*}$ |
| $S_2 \times S_2$ | S_2 | $X_2X_4 + X_1X_3$ |
| $S_2 \times S_2$ | $S_1 \times S_1 \times S_2$ | X_2 |
| $S_2 \times S_2$ | Id_4 | $X_2 - X_4$ |
| D_5 | C_5 | $X_4X_5^2 + X_5X_1^2 + X_3X_4^2 + X_2X_3^2 + X_1X_2^{2*}$ |
| S_5 | $S_2 \times A_3$ | $X_1 + X_2$ |
| $S_2 \times S_3$ | $S_2 \times A_3$ | $X_2X_3^2 + X_3X_1^2 + X_1X_2^2$ |
| $S_2 \times S_3$ | $S_2 \times A_3$ | $X_2X_3^2 + X_3X_1^2 + X_1X_2^2$ |
| $S_2 \times S_3$ | $S_1 \times S_2 \times S_2$ | X_1 |
| $S_2 \times S_3$ | $A_3 \times Id_2$ | $X_2X_3^2 + X_3X_1^2 + X_1X_2^2 - X_4X_5^2$ |
| $S_2 \times S_3$ | $Id_3 \times S_2$ | $X_2 - X_3$ |
| $H_1 \subset S_6$ | $H_2 \subset S_6$ | $X_2X_3^2 + X_3X_1^2 + X_1X_2^2$ |
| $H_1 \subset S_6$ | $H_3 \subset S_6$ | $X_2X_4^2 + X_4X_1^2 + X_3X_2^2 + X_1X_3^2$ |

Exemple 20. Soient $n = 5$, $L = S_5$ et $H = \langle (2,3)(4,5), (4,5), (3,4) \rangle$. Un H -invariant L -primitif minimal est égal à X_1 . Un autre H -invariant L -primitif de degré minimal est $X_5 + X_4 + X_3 + X_2$.

Remarque 21. Soient P un H -invariant L -primitif et Q un polynôme tels que $P + Q$ est un L -invariant. Alors Q est aussi un H -invariant L -primitif, car $\forall \sigma \in L$, $\sigma(P) = P$ équivaut à $\forall \sigma \in L$, $\sigma(Q) = Q$.

Exemple 22. Soient $n = 5$, $L = \langle (2,3)(4,5), (2,4)(3,5), (4,5), (3,4) \rangle$ et $H = \langle (2,3), (2,4)(3,5) \rangle$. Nous adoptons la notation 18 et nous supposons que les entiers i, j, l, h, m sont deux à deux distincts.

L'algorithme 4.4 calcule la liste suivante des H -invariants L -primitifs réduits :

$$\begin{aligned}
 & [iiij] + [ijji], \\
 & [iijj] + [iijj] + [ijji] + [ijji], \\
 & [iijh] + [iihj] + [ijhi] + [ihji], \\
 & [iijih] + [iihij] + [iijhi] + [ihji] + [ijjih] + [ihij] + [ijhi] + [ihji], \\
 & [iijjh] + [iijhj] + [ijijh] + [ijihj] + [ijhij] + [ihji] + [ijhji] + [ihjji], \\
 & [iijhj] + [ihijj] + [ijjih] + [ijjhi], \\
 & [jiijh] + [jihij] + [jihii] + [jhjii], \\
 & [hiij] + [hjii], \\
 & [jijih] + [jihij] + [jihhi] + [jihji] + [jjih] + [jhii] + [jjhi] + [jhji], \\
 & [hijij] + [hijji] + [hjii] + [hjji], \\
 & [iijhl] + [iijlh] + [ijihl] + [ijilh] + [ihlij] + [ihlij] + [ihlji] + [ihlji], \\
 & [iijhl] + [iijlh] + [ihijl] + [ihilj] + [ijlih] + [iljih] + [ijlhi] + [iljhi],
 \end{aligned}$$

$$\begin{aligned}
& [iiljh] + [iilhj] + [ilijh] + [ilihj] + [ijhil] + [ihjil] + [ijhli] + [ihjli], \\
& \quad [jiihl] + [jiilh] + [jhlii] + [jlihi], \\
& \quad [hiijl] + [hiilj] + [hjlii] + [hljii], \\
& \quad [liijh] + [liihj] + [ljhii] + [lhjii], \\
& [jihil] + [jilih] + [jihli] + [jilhi] + [jhii] + [jliih] + [jhili] + [jlihi], \\
& [hijil] + [hilij] + [hijli] + [hilji] + [hjii] + [hliij] + [hjili] + [hlijii], \\
& [lijih] + [lihi] + [lijhi] + [lihji] + [ljiih] + [lhii] + [ljihii] + [lhajii], \\
& [ijhlm] + [ijhml] + [ihjlm] + [ihjml] + [ilmjh] + [imljh] + [ilmhj] + [imlhj]*, \\
& [ijlhm] + [ijlhm] + [iljhm] + [iljmh] + [ihmj] + [imhjl] + [ihmlj] + [imhlj]*, \\
& [ijmhl] + [ijmhl] + [imjhl] + [imjhl] + [ihljm] + [ilhjm] + [ihlmj] + [ilmhj]*, \\
& [jihlm] + [jihml] + [jhilm] + [jhiml] + [jlmih] + [jmlih] + [jlmhi] + [jmlhi]*, \\
& [jilhm] + [jilmh] + [jlihm] + [jlimh] + [jhmil] + [jmhil] + [jhmli] + [jmhli]*, \\
& [jimhl] + [jimhl] + [jmihl] + [jmihl] + [jhljm] + [jhljm] + [jhlmi] + [jhlmi]*, \\
& [hijlm] + [hijml] + [hjilm] + [hjiml] + [hlmij] + [hmlij] + [hlmji] + [hmlji]*, \\
& [lijhm] + [lijmh] + [ljihm] + [ljimh] + [lhmij] + [lmhij] + [lhmji] + [lmhji]*, \\
& [mijhl] + [mijhl] + [mjihl] + [mjihl] + [mhlij] + [mlhij] + [mhlji] + [mlhji]*, \\
& [hiljm] + [hilmj] + [hljhm] + [hljm] + [hjmil] + [hjmil] + [hjml] + [hmjli]*, \\
& [himjl] + [himjl] + [hmi] + [hmil] + [hjljm] + [hjljm] + [hjlmi] + [hjlmi]*, \\
& [lihjm] + [lihmj] + [lhijm] + [lhimj] + [ljmih] + [lmjih] + [ljmhi] + [lmjhi]*, \\
& [mihjl] + [mihjl] + [mhi] + [mhil] + [mjlih] + [mljih] + [mjli] + [mljhi]*, \\
& [limjh] + [limjh] + [lmijh] + [lmihj] + [ljhim] + [lhjim] + [ljhmi] + [lhjmi]*, \\
& [miljh] + [miljh] + [mljih] + [mlihj] + [mjhil] + [mhjil] + [mjhli] + [mhjli]*.
\end{aligned}$$

Exemple 23. Soient L et H deux sous-groupes de S_8 définis par :

$$\begin{aligned}
H = \langle & (1, 2, 6, 7)(3, 4, 8, 5), (1, 4, 7, 5)(2, 3, 8, 6), (2, 7, 8)(4, 5, 6), (2, 5, 6)(3, 4, 8), (3, 6, 7) \\
& (4, 5, 8), (3, 4, 7, 8, 6, 5) \rangle
\end{aligned}$$

et

$$L = \langle (1, 2, 6, 7)(3, 4, 8, 5), (1, 4, 7, 5)(2, 3, 8, 6) \rangle.$$

Nous adoptons la notation 18 et nous supposons que les entiers i et h sont distincts.

Le polynôme suivant est un H -Invariant L -Primitif ; il est un H -Invariant L -Primitif minimal pour $i = 0$ et $h = 1$:

$$\begin{aligned}
& [iiiihhhh] + [iiahhhhh] + [iiahhhhh] + [ihihihih] + [ihihhhii] + [ihhhiihi] + [ihhhiihi] + [ihhhiihi] + \\
& [hihhiihi] + [hihhiihi] + [hihhiihi] + [hihhiihi] + [hhiiiii] + [hhiiiii] + [hhhhiiiii].
\end{aligned}$$

Le polynôme suivant est un H -Invariant S_8 -Primitif minimal :

$$\begin{aligned}
& [00001111] + [00010111] + [00101101] + [00110011] + [00111010] + [00111100] + [01001110] + \\
& [01010101] + [01011001] + [01011010] + [01100011] + [01100110] + [01101001] + [01110100] + \\
& [10001011] + [10010110] + [10011001] + [10011100] + [10100101] + [10100110] + [10101010] + \\
& [10110001] + [11000011] + [11000101] + [11001100] + [11010010] + [11101000] + [11110000].
\end{aligned}$$

Ces deux derniers calculs ont été réalisés en trois minutes sur une machine PC Pentium Pro 200 MHz avec 512 Mo de mémoire RAM.

6.2. COÛT DE L'ALGORITHME 4.3

Sous GAP, les temps nécessaires au calcul d'ensembles essentiels avec l'algorithme 4.3 pour des degrés inférieurs ou égaux à 6 varient de moins d'une seconde à une heure. Ces temps augmentent avec le degré n ; le tableau suivant marque en moyenne cette évolution pour n allant de 5 à 9 (sur une machine PC Pentium Pro 200 MHz avec 512 Mo de mémoire RAM) :

| Degré | Temps (CPU) | Mémoire (Mo) |
|-------|-------------|--------------|
| 5 | < 1'' | < 1 |
| 7 | 2' | 7 |
| 8 | 100' | 30 |
| 9 | 120' | 36 |

La mémoire utilisée varie entre moins d'un Mo en degré 4 et plus de 500 Mo lors du calcul d'ensembles essentiels pour (S_{15}, A_{15}) . Rappelons que, même si le calcul d'ensembles essentiels est coûteux en temps et en espace, il ne sera fait qu'une seule fois.

6.3. APPLICATION À LA THÉORIE DE GALOIS

Le calcul du groupe de Galois d'un polynôme se fait en utilisant des propriétés de groupes et de certains polynômes assez particuliers appelés *résolvantes*. Le calcul de ces polynômes se fait en calculant d'abord les polynômes invariants primitifs : en effet une résolvente d'un groupe H par rapport à L est un polynôme dont les racines sont les différents conjugués d'un H -invariant L -primitif. Pour calculer le groupe de Galois d'un polynôme f de degré n , A. Valibouze et J.M. Arnaudès ont mis en place (voir [3]) une méthode déterministe pour le calcul du groupe de Galois d'un polynôme, s'appuyant sur la factorisation de *résolvantes absolues* (ou polynômes associés à des H -invariants S_n -primitif). Dans ce cas H est un sous-groupe appelé *groupe test*) et le calcul de la résolvente absolue associée à H est d'autant plus rapide que le degré de l'invariant primitif utilisé est petit.

Souvent, le degré des résolvents absolues est assez grand et leur factorisation est difficile (voir le travail de Lehobey [14] sur la factorisation de résolvents), et une autre méthode appelée *la méthode de Stauduhar* (voir [7, 18, 20], etc.) qui utilise la factorisation de *résolvantes relatives* associés à des H -invariants L -primitifs relatifs ($H \subset L \subset S_n$), est plus rapide car de degré plus petit. Il est donc recommandé, pour calculer le groupe de Galois d'un polynôme, d'avoir plusieurs invariants primitifs relatifs et absolus de degrés petits.

CONCLUSION

Les méthodes de calculs de polynômes invariants primitifs connus sont intuitifs et donnent souvent des polynômes de degrés élevés. L'algorithme de Girstmair

calcule un invariant primitif absolu de degré minimal, mais pas nécessairement minimal.

Une autre façon de calculer des invariants de groupes finis a été introduite par Sturmfels [19] et améliorée et implantée en MAGMA par Kemper [13]. Cette méthode consiste à calculer des invariants primaires et secondaires d'un groupe fini H , qui forment une base de l'anneau des polynômes H -invariants.

Malgré la rapidité de l'algorithme de Kemper qui arrive à calculer une base de l'anneau des polynômes H -invariants en quelques secondes pour le degré 6, cet algorithme n'arrive pas à calculer des H -invariants primitifs directement. En effet, les invariants primaires et secondaires ne sont pas nécessairement des invariants primitifs, et il faut faire des tests pour vérifier que les polynômes obtenus sont bien des invariants primitifs.

L'algorithme 4.3 présenté dans le paragraphe 4, nous donne des invariants différents et de degré minimal, utilisés essentiellement pour la résolution d'équations polynomiales et les calculs de résolvantes dans la théorie de Galois (voir [20] et [16]) et nous avons mis au point l'algorithme de Girstmair-Jordan qui, grâce à la représentation de données utilisées, calcule tous les polynômes invariants primitifs (relatifs ou absolus) à coefficients distincts de groupes finis.

Cet algorithme peut se généraliser au calcul de polynômes invariants vérifiant d'autres propriétés et nous pouvons l'utiliser pour le calcul de *résolvantes* et autres types d'invariants utiles en théorie de Galois.

Je tiens à remercier le professeur Annick Valibouze pour l'encadrement de ce travail et sa disponibilité. Je remercie également le rapporteur pour ses remarques pertinentes.

RÉFÉRENCES

- [1] I. Abdeljaouad, *Calculs d'invariants primitifs minimaux et implantation en Axiom*, Mémoire de stage, DEA Algorithmique (1996). Disponible sur la page web du Projet Galois du GDR MEDICIS : <http://medicis.polytechnique.fr/medicis/projetGalois>
- [2] I. Abdeljaouad, *Package PrimitiveInvariant* sous GAP, (1997). Disponible sur la page web du Projet Galois du GDR MEDICIS : <http://medicis.polytechnique.fr/medicis/projetGalois>
- [3] J.M. Arnaudiès and A. Valibouze, Lagrange resolvents. *J. Pure Appl. Algebra* (1997).
- [4] E.H. Berwick, The condition that a quintic equation should be soluble by radicals. *Proc. London Math. Soc.* **14** (1915) 301-307.
- [5] E.H. Berwick, On soluble sextic equations. *Proc. London Math. Soc.* **29** (1929) 1-28.
- [6] A. Cayley, On a new auxiliary equation in the theory of equation of fifth order. *Philos. Trans. Roy. Soc. London*, CLL (1861).
- [7] A. Colin, Formal computation of Galois groups with relative resolvents, AAEECC'95, Springer Verlag, *Lecture Notes in Computer Science* **948** (1995) 169-182.
- [8] A. Colin, Solving a system of algebraic equations with symmetries. *J. Pure and Appl. Algebra* (1996).
- [9] H.O. Foulkes, The resolvents of an equation of seventh degree. *Quart. J. Math. Oxford Ser.* (1931) 9-19.
- [10] G.A.P. Groups, algorithms and programming, Martin Schönert and others, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, gap@samson.math.rwth-aachen.de (1993).
- [11] K. Girstmair, On invariant polynomials and their application in field theory. *Maths of Comp.* **48** (1987) 781-797.

- [12] C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villard, Paris (1870).
- [13] G. Kemper, Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Computation* (1995).
- [14] F. Lehobey, Resolvent computation by resultants without extraneous powers. *J. Pure Appl. Algebra* (1999) à paraître.
- [15] E. Luther, Ueber die factoren des algebraisch lösbaren irreducible Gleichungen vom sechsten Grade und ihren Resolventen. *Journal für Math.* **37** (1848) 193-220.
- [16] N. Rennert and A. Valibouze, *Modules de Cauchy*, Rapport interne LIP6 (1997).
- [17] L. Soicher, *The computation of the Galois groups*, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada (1981).
- [18] R.P. Stauduhar, The computation of Galois groups. *Math. Comp.* **27** (1973) 981-996.
- [19] B. Sturmfels, *Algorithms in invariant theory*, Wien, New-York: Springer Verlag (1993).
- [20] A. Valibouze, *Groupes de Galois jusqu'en degré 7*. Rapport interne LIP6 (1997).
- [21] A. Vandermonde, *Mémoire de l'Académie des Sciences de Paris* (1771).
- [22] R.L. Wilson, *A method for the determination of the Galois group*, *Amer. Math. Soc.* (1949).

Communicated by Ch. Choffrut.

Received September, 1997. Accepted November, 1998.