CALCULS D'INVARIANTS PRIMITIFS DE GROUPES FINIS

INES ABDELJAOUAD

CalFor - LIP6, Université Paris VI,
4 Place Jussieu, F-75252 PARIS CEDEX 05
Ines.Abdeljaouad@calfor.lip6.fr

ABSTACT. 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 algorithm 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 me'thode est inspire' par l'algorithme de Girstmair qui calcule un invariant primitif absolu de degre' minimal. Sont pre'sente's deux algorithmes : le premier algorithme calcule tous les invariants primitifs de degre' minimal et le deuxie'me algorithme calcule tous les invariants primitifs a 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. Les invariants primitifs les plus célèbres sont donnés par des mathématiciens tels que A. Vandermonde [20], E. Luther [14], A. Cayley [6], E.H. Berwick [5] [4], H.O. Foulkes [9]. Ces invariants furent obtenus de manières intuitives. Une méthode automatique (voir [21]) permet de calculer un invariant primitif d'un sous-groupe H du groupe symétrique de degré n, en prenant la somme de toutes les images, par les permutations de H, du monôme $(x_2x_3^2 \dots x_n^{n-1})$. Nous appelons cette méthode la *méthode naïve* et remarquons que les invariants obtenus ont un degré égal à $\frac{n(n-1)}{2}$.
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 [19]). 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.

Une méthode de calcul des invariants primitifs absolus de groupes de permutations se base sur la connaissance des propriétés des générateurs de ces groupes (voir par exemple [5], [20] et [19]). Cette méthode plutôt intuitive, donne des invariants primitifs de degrés assez grands et ne se généralise pas au calcul d'invariants primitifs relatifs, il est donc intéressant d'avoir un algorithme qui calcule ce type d'invariants. Une représentation des polynômes assez particulière, due à C. Jordan [12], a permis à K. 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 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 $k[X_1, \ldots, X_n]$ l'anneau des polynômes en $X_1, \ldots, X_n$ à coefficients dans k, où $X_1, \ldots, X_n$ sont n indéterminées algébriquement indépendantes sur k.
Le groupe symétrique de degré n est noté S_n. L'action de S_n sur $k[X_1, \ldots, X_n]$ est définie de façon naturelle par :

$$\begin{array}{lcc} S_n \times k[X_1, \ldots, X_n] & \longrightarrow & k[X_1, \ldots, X_n] \\ (\sigma \ , \ P) & \mapsto & \sigma(P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \end{array}$$

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

$$Stab_L(P) = \{g \in L \mid g(P) = P\} \quad .$$

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

$$Stab_L(U) = \{g \in L \mid \forall P \in U \ , \ g(P) \in U\} \quad .$$

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

$$Orb_H(P) = \{\sigma(P) \mid \sigma \in H\} \quad .$$

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

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

$$Stab_L(P) = H \quad .$$

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

Soit P un H-invariant L-primitif. P 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 est appelé *H-invariant L-primitif minimal.*

Exemple 1.1. 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 1.1. Soient $g_1, \ldots, g_r$ des permutations de S_n, alors $< g_1, \ldots, g_r >$ désigne le sous-groupe de S_n engendré par les permutations $g_1, \ldots, g_r$.

Exemple 1.2. Soient $n = 4$, $H_1 =< (3,4), (1,2)(3,4), (1,3)(2,4) >$ un sous-groupe de S_4 et $H_2 =< (1,2)(3,4), (1,3)(2,4) >$ un sous-groupe de H_1. Les polynômes suivants sont des polynômes H_2-invariants H_1-primitifs de degré minimal :

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

Le polynôme H_2-invariant H_1-primitif calculé par la méthode naïve décrite en introduction est le polynôme :

$$X_2X_3^2X_4^3 + X_1X_4^2X_3^3 + X_4X_1^2X_2^3 + X_3X_2^2X_1^3 \qquad .$$

Remarque 1.1. Soient $\tau_1, \ldots, \tau_e$ des permutations de L vérifiant $L = \tau_1 H + \cdots + \tau_e H$. 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 $k[X_1, \ldots, X_n]$ sera unitaire et de la forme $X_1^{r_1} \ldots X_n^{r_n}$ où les r_i sont des entiers positifs ou nuls. Soit Q un monôme de $k[X_1, \ldots, X_n]$, nous notons

$$N_H(Q) \ = \sum_{Q' \in Orb_H(Q)} Q' \qquad .$$

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

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

$$H_L(U) \ = \ \bigcap\nolimits_{Q \in U} Stab_L(N_H(Q)) \qquad .$$

Définition 1.5. Soit U un ensemble fini de monômes de $k[X_1, \ldots, X_n]$.
Une *U-fonction élémentaire* est un polynôme $\mathcal{P}_U$ donné par la formule suivante :

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

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

Exemple 1.3. Soient $U = \{X_1X_2, X_2X_3\}$ et $H =< (1,4) >$ un sous-groupe de S_4. La famille des U-fonctions élémentaires est donnée par $\mathcal{P}_U = a(X_1X_2 + X_2X_4) + b(X_2X_3)$ avec $a \neq b$ deux éléments non nuls de k.

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

Remarque 1.2. Soit U un ensemble fini de monômes de $k[X_1, \ldots, X_n]$. Le degré de U correspond aussi au degré de chacune des U-fonctions élémentaires $\mathcal{P}_U$.

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 $k[X_1, \ldots, X_n]$. 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 :

$$Stab_L\left(\sum\nolimits_{Q \in U} a_Q \; N_H(Q)\right) = \bigcap\nolimits_{Q \in U} Stab_L(N_H(Q)) \qquad .$$

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

$$g(\mathcal{P}_U) = \sum\nolimits_{Q \in U} a_Q \; N_H(Q) \qquad .$$

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 $g \in Stab_L(N_H(Q))$ pour tout $Q \in U$. D'où :

$$g \in \bigcap\nolimits_{Q \in U} Stab_L(N_H(Q)) \qquad .$$

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

Remarque 2.1. En d'autres termes, le (L,H)-groupe $H_L(U)$ est le stabilisateur de chaque U-fonction élémentaire $\mathcal{P}_U$: $Stab_L(\mathcal{P}_U) = H_L(U)$.

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 $Stab_L(P) = H$.

Remarque 2.2. 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 $k[X_1,\ldots,X_n]$. La trace réduite de Q par H, $N_H(Q)$, 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 $k[X_1,\ldots,X_n]$ implique que $g(N_H(Q))$ $= \sum_{Q' \in Orb_H(Q)} g(Q^{'})$. La permutation $g \in H$ est une bijection sur $Orb_H(Q)$.
En effet : si $Q^{'} \in Orb_H(Q)$ alors $g(Q^{'}) \in Orb_H(Q)$ et pour tous monômes Q_1 et Q_2 de $Orb_H(Q)$, si $g(Q_1) = g(Q_2)$ alors $Q_1 = g^{-1}g(Q_1) = g^{-1}g(Q_2) = Q_2$.
Ainsi $\sum_{Q' \in Orb_H(Q)} g(Q^{'}) = \sum_{Q' \in Orb_H(Q)} Q^{'}$, et donc $g(N_H(Q)) = N_H(Q)$. □

Définition 3.1. Soit Q un monôme de $k[X_1,\ldots,X_n]$. Tout monôme Q' de $Orb_H(Q)$ 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 $P \in k[X_1,\ldots,X_n]$ est un H-invariant si et seulement si il existe $Q_1,\ldots,Q_l$ des monômes de $k[X_1,\ldots,X_n]$ 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 $k[X_1,\ldots,X_n]$ 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 $Q_i \in k[X_1,\ldots,X_n]$. En regroupant les monômes de P en polynômes de même coefficients, nous obtenons $P = \sum_{i=1}^{r} b_i \left(\sum_{j \in I_i} Q_j\right)$ avec $r \leq s$, les b_i sont des éléments deux à deux distincts de k, $\bigcup_{i=1}^{r} I_i = \{1,\ldots,s\}$ et pour $i,j \in [1,r]$ tels que $i \neq j$, nous avons $I_i \bigcap I_j = \emptyset$. 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 $P = \sum_{i=1}^{r} b_i \left(\sum_{j \in J_i} N_H(Q_j)\right) = \sum_{i=1}^{l} c_i N_H(Q_i)$ avec $l \geq r$ et les c_i sont des éléments non nuls de k. □

Remarque 3.1. 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 $Q_i^{'} \in Orb_H(Q_i)$ 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. Un *système de représentants des orbites de H*, noté $\mathcal{S}$, est un ensemble de tous les monômes de $k[X_1,\ldots,X_n]$ de H-orbites deux à deux distinctes.

Théorème 3.1. *Soit $P \in k[X_1,\ldots,X_n]$ un H-invariant L-primitif. 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 $U = \{Q_1,\ldots,Q_l\}$. 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 $H_L(U) = \bigcap_{i=1}^{l} Stab_L(N_H(Q_i))$.
$H \subset H_L(U)$, en effet: pour tout $i \in [1,l]$ $H \subset Stab_L(N_H(Q_i))$ car les $N_H(Q_i)$ sont des H-invariants (voir proposition 3.1). D'autre part, si $g \in H_L(U)$ alors $g \in \bigcap_{i=1}^{l} Stab_L(N_H(Q_i))$ et donc pour tout $i \in [1,l]$, $g(N_H(Q_i)) = N_H(Q_i) \Rightarrow g \in Stab_L(P)$. Ainsi $H_L(U) = Stab_L(P) = H$ et U est un ensemble essentiel pour (L,H). ☐

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 2.2, 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 corollaire 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). ☐

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 remarque 1.1).

4. Algorithmes De Calculs D'ensembles Essentiels

Pour calculer un H-invariant S_n-primitif, K. Girstmair (voir [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 corollaire 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. **Pour Tout** m et m' dans $\mathcal{A}$ de même degré **Faire**
   Si $Orb_H(m) = Orb_H(m')$

Alors retirer m' de A
Fin Si
Fin Pour
2. **Rendre**($\mathcal{A}$) ;
Fin.

Preuve de l'algorithme 1. Il existe un nombre fini de monômes de degrés $\leq \frac{n(n-1)}{2}$, cet algorithme termine donc au bout d'un nombre fini d'étapes. 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 4.1. Soit $\mathcal{A}$ un ensemble fini de monômes. Notons $\texttt{premier}(\mathcal{A})$ la liste de tous les éléments de $\mathcal{A}$ de degré minimal et $\texttt{rest}(\mathcal{A})$ la liste des éléments de $\mathcal{A}$ privé de $\texttt{premier}(\mathcal{A})$.

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**
$U := U \bigcup \texttt{premier}(\mathcal{A})$;
$\mathcal{A} := \texttt{rest}(\mathcal{A})$;
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 4.1. 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 $X_2X_3^2\ldots X_n^{n-1}$. D'autre part, la trace réduite du représentant de ce monôme est un H-invariant L-primitif (voir la méthode naïve 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 4.2. Pour U un ensemble fini de monômes, $\texttt{partie}(U)$ est la liste de tous les sous-ensembles de U classés par ordre croissant suivant leurs tailles et $\texttt{diff}(U,V)$ 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'exemple 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. $\mathcal{A} := \texttt{SystèmeDeReprésentant}(n,H)$;
2. $U := \texttt{EnsembleEssentiel}(\mathcal{A},L,H)$;
3. $\mathcal{I} := \{\ \}$; *contient tous les ensembles essentiels réduits pour (L,H) de degré minimal*
4. $E := \texttt{partie}(U)$;
5. **Pour tout** $V \subset E$ **faire**
    - **Si** $H_L(V) = H$;
        - **Alors** Rajouter V dans $\mathcal{I}$;
          $E := \texttt{diff}(U,V)$;
    - **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 $X_2X_3^2\ldots X_n^{n-1}$ et d'après la remarque 4.1 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 corollaire 3.1).

Remarque 4.2. Le calcul d'ensembles essentiels réduits revient à ne pas calculer les polynômes invariants primitifs somme de deux autres.

Remarque 4.3. 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 remarque 1.1).

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 remarques 4.3 et 1.1), 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 4.1. Soit U un ensemble fini de monômes, $\texttt{degre}(U)$ 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. $\mathcal{A} :=$ $\texttt{SystèmeDeReprésentant}(n,H)$;
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**
   $U :=$ $\texttt{EnsembleEssentiel}(\mathcal{A},L,H)$;
   5. **Pour tout** $V \subset E$ **faire**
      Si $H_L(V) = H$;
         Alors Rajouter V dans $\mathcal{I}$;
            $E := \texttt{diff}(U,V)$;
      Fin Si
   Fin Pour
   $d := \texttt{degre}(U) + 1$;
   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=`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 $(p+1)$-ème 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 C. 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.

5.1. **Partitions et Représentation Des Données.**

Notation 5.1. Soit $I \subset \{1,\dots,n\}$ alors le cardinal de I est noté $\mid I \mid$.

Définition 5.1. Une *partition* $T = (T_1,\dots,T_s)$ *de* $\{1,\dots,n\}$ est une liste vérifiant les 5 conditions suivantes :

(i)	Pour tout $i \in [1,n]$, $T_i \subset \{1,\dots,n\}$.	*(ii)*	$\sum_{i=1}^{s} \mid T_i \mid = n.$
(iii)	$\bigcup_{i=1}^{s} T_i = \{1,\dots,n\}$	*(iv)*	$\mid T_1 \mid \geq \mid T_2 \mid \geq \cdots \geq \mid T_s \mid \geq 1.$
(v)	$\forall\ i,j \in [1,n] : i \neq j \Longrightarrow T_i \cap T_j = \emptyset$		

Notation 5.2. Nous notons $\mathcal{T}$ l'ensemble des partitions de $\{1,\dots,n\}$.

Proposition 5.1. *Pour tout monôme Q de $k[X_1,\dots,X_n]$, il existe une partition unique $T = (T_1,\dots,T_s) \in \mathcal{T}$ vérifiant :*

$$Q = \prod_{i=1}^{s} \Big(\prod_{j\in T_i} X_j\Big)^{\alpha_i} \qquad .$$

Preuve. Soit $Q = X_{i_1}^{r_1} \dots X_{i_n}^{r_n}$ avec $r_i \geq 0$ un monôme de $k[X_1,\dots,X_n]$. En regroupant les monômes X_j de Q en blocs de même degré, et en classant ces blocs par ordre décroissant suivant les degrés nous obtenons :

$$Q = \Big(\prod_{j\in I_1} X_j\Big)^{\alpha_1} \dots \Big(\prod_{j\in I_s} X_j\Big)^{\alpha_s} \qquad ,$$

avec $\mid I_1 \mid \geq \cdots \geq \mid I_s \mid \geq 1$. En remarquant que si deux blocs ont la même taille, c'est à dire si $\mid I_i \mid = \mid I_j \mid$, alors nous les classons suivant le degré croissant : (si $\alpha_i < \alpha_j$ alors I_i se situe avant I_j sinon, c'est le contraire). Nous obtenons ainsi un nouvel ordre sur les indices :

$$(T_1,\dots,T_s) \in \mathcal{T} \qquad \text{tels que} \qquad Q = \prod_{i=1}^{s} \Big(\prod_{j\in T_i} X_j\Big)^{\alpha_i} \qquad ,$$

d'où le résultat. □

Définition 5.2. Nous considérons l'application Ψ définie par :

$$\begin{array}{rcccc} \Psi & : & \text{Monômes de } k[X_1,\dots,X_n] & \longrightarrow & \mathcal{T} \\ & & Q = \prod_{i=1}^{s} (\prod_{j\in T_i} X_j)^{\alpha_i} & \mapsto & \Psi(Q) = (T_1,\dots,T_s) \end{array}$$

Remarque 5.1. Nous avons montré dans la proposition 5.1 que pour n'importe quel monôme de $k[X_1, \ldots, X_n]$, il existe une unique partition de $\mathcal{T}$ qui le représente. L'application Ψ est donc bien définie.

Proposition 5.2. *l'application Ψ est surjective.*

Preuve. soit $T = (T_1, \ldots, T_s) \in \mathcal{T}$. Montrer que Ψ est surjective revient à montrer qu'il existe au moins un monôme Q vérifiant $\Psi(Q) = T$. Il suffit donc de considérer le monôme $Q_T = \prod_{i=1}^{s}(\prod_{j \in T_i} X_j)^{(i-1)}$ qui vérifie $\Psi(Q_T) = T$. □

Exemple 5.1. Soient $Q = X_1X_2X_3^2X_4^3X_5^2X_6^2X_7$ et $n = 8$, alors :

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

En effet : $Q = (X_1X_2X_7)^1(X_3X_5X_6)^2{X_8}^0{X_4}^3$.

Définitions 5.1. Soit $T = (T_1, \ldots, T_s) \in \mathcal{T}$. Nous définissons le monôme Q_T et l'ensemble de monômes $\mathcal{M}$ par :

$$Q_T = \prod_{i=1}^{s}(\prod_{j \in T_i} X_j)^{(i-1)} \qquad , \qquad \mathcal{M} = \{Q_T \mid T \in \mathcal{T}\} \qquad .$$

Soit la fonction Φ définie par :

$$\begin{array}{cccc} \Phi & : & \mathcal{T} & \longrightarrow & \mathcal{M} \\ & & \mathrm{T} & \mapsto & Q_T \end{array}$$

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

Théorème 5.1. *L'application Φ est une bijection.*

Preuve. Φ est bien une application, en effet à une partition $T \in \mathcal{T}$, est associé un unique monôme Q_T de $\mathcal{M}$ et l'application réciproque de Φ est une restriction de Ψ sur l'ensemble $\mathcal{M}$. Φ est une application surjective : il existe T tel que $\Psi(Q_T) = T$ et nous pouvons dire que Φ est surjective par construction. Enfin, il est évident que l'application Φ est injective. □

Les monômes de $k[X_1, \ldots, X_n]$ sont représentés par les partitions de $\mathcal{T}$ de $\{1, \ldots, n\}$, et au lieu de calculer des ensembles essentiels de monômes, nous calculons des ensembles essentiels de partitions. L'application Φ transforme les partitions en monômes, nous obtenons donc, grâce à Φ, des polynômes invariants primitifs associés aux ensembles essentiels de partitions.

5.2. **Exemple de Calcul de Tous les Invariants Primitifs.** 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 l'algorithme 4.4 que nous avons appelé *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 donnés 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 :

```
[ [ [ 1, 2, 3 ] ],
  [ [ 1, 2 ], [ 3 ] ], [ [ 1, 3 ], [ 2 ] ],
```

```
[ [ 2, 3 ], [ 1 ] ],
[ [ 1 ], [ 2 ], [ 3 ] ], [ [ 1 ], [ 3 ], [ 2 ] ],
[ [ 2 ], [ 1 ], [ 3 ] ],  [ [ 2 ], [ 3 ], [ 1 ] ],
[ [ 3 ], [ 1 ], [ 2 ] ], [ [ 3 ], [ 2 ], [ 1 ] ] ]
```

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

```
[ [ [ 1, 2, 3 ] ], [ [ 1, 2 ], [ 3 ] ],
[ [ 1, 3 ], [ 2 ] ], [ [ 1 ], [ 2 ], [ 3 ] ],
[ [ 1 ], [ 3 ], [ 2 ] ], [ 3 ], [ 1 ], [ 2 ] ] ]
```

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

```
[ [ [ [ 1, 2 ], [ 3 ] ] ],
  [ [ [ 1, 3 ], [ 2 ] ] ],
  [ [ [ 1 ], [ 2 ], [ 3 ] ] ],
  [ [ [ 1 ], [ 3 ], [ 2 ] ] ],
  [ [ [ 3 ], [ 1 ], [ 2 ] ] ] ]
```

La famille des polynômes S_2-invariants S_3-primitifs réduits est égale à : $a(X_1X_2)^{\alpha}{X_3}^{\beta}$, $a((X_1X_3)^{\alpha}{X_2}^{\beta}+(X_2X_3)^{\alpha}{X_1}^{\beta})$, $a({X_1}^{\alpha}{X_2}^{\beta}{X_3}^{\gamma}+{X_2}^{\alpha}{X_1}^{\beta}{X_3}^{\gamma})$, 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]), à été possible grâce à la manipulation des partitions. Pour plus de détails sur l'implantation le lecteur pourra consulter [1] et [2].

6.1. Exemples d'utilisation.

Exemple 6.1. Soient $H_1 = <(4,5,6),(2,3),(1,2),(5,6)>$, $H_2 = <(4,5,6),(5,6),(1,2,3)>$ et $H_3 = <(5,6),(1,2)(3,4),(1,3,2,4)>$ dans S_6. La table suivante présente le H-invariant L-primitif minimal calculé 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 6.2. Soient $n = 5$, $L = S_5$ et $H =< (2,3)(4,5),(4,5),(3,4) >$. Le H-invariant L-primitif minimal est égal à X_1. L'autre H-invariant L-primitif de degré minimal est $X_5 + X_4 + X_3 + X_2$.

Exemple 6.3. Soient $n = 5$, $L =<(2,3)(4,5),(2,4)(3,5),(4,5),(3,4)>$ et $H =<(2,3),(2,4)(3,5)>$. La liste des H-invariants L-primitifs réduits de degrés petits, obtenue par l'algorithme 4.4 est égale à :

$$
\begin{gathered}
X_4X_5 + X_2X_3, \qquad X_3X_5 + X_3X_4 + X_2X_5 + X_2X_4, \qquad X_4X_5^2 + X_5X_4^2 + X_2X_3^2 + X_3X_2^2,\\
X_3X_5^2 + X_5X_3^2 + X_3X_4^2 + X_4X_3^2 + X_2X_5^2 + X_5X_2^2 + X_2X_4^2 + X_4X_2^2,\\
X_3X_4X_5^2 + X_3X_5X_4^2 + X_2X_4X_5^2 + X_2X_5X_4^2 + X_2X_5X_3^2 + X_3X_5X_2^2 + X_2X_4X_3^2 + X_3X_4X_2^2,\\
X_4X_5X_3^2 + X_4X_5X_2^2 + X_2X_3X_5^2 + X_2X_3X_4^2, \qquad X_4X_5X_1^2 + X_2X_3X_1^2, \qquad X_1X_4X_5^2 + X_1X_5X_4^2 + X_1X_2X_3^2 + X_1X_3X_2^2,\\
X_1X_3X_5^2 + X_1X_5X_3^2 + X_1X_3X_4^2 + X_1X_4X_3^2 + X_1X_2X_5^2 + X_1X_5X_2^2 + X_1X_2X_4^2 + X_1X_4X_2^2,\\
X_3X_5X_1^2 + X_3X_4X_1^2 + X_2X_5X_1^2 + X_2X_4X_1^2,\\
X_3X_4^2X_5^3 + X_3X_5^2X_4^3 + X_2X_4^2X_5^3 + X_2X_5^2X_4^3 + X_5X_2^2X_3^3 + X_5X_3^2X_2^3 + X_4X_2^2X_3^3 + X_4X_3^2X_2^3,\\
X_4X_3^2X_5^3 + X_5X_3^2X_4^3 + X_4X_2^2X_5^3 + X_5X_2^2X_4^3 + X_2X_5^2X_3^3 + X_3X_5^2X_2^3 + X_2X_4^2X_3^3 + X_3X_4^2X_2^3,\\
X_4X_5^2X_3^3 + X_5X_4^2X_3^3 + X_4X_5^2X_2^3 + X_5X_4^2X_2^3 + X_2X_3^2X_5^3 + X_3X_2^2X_5^3 + X_2X_3^2X_4^3 + X_3X_2^2X_4^3,\\
X_1X_4^2X_5^3 + X_1X_5^2X_4^3 + X_1X_2^2X_3^3 + X_1X_3^2X_2^3,\\
X_4X_1^2X_5^3 + X_5X_1^2X_4^3 + X_2X_1^2X_3^3 + X_3X_1^2X_2^3,\\
X_4X_5^2X_1^3 + X_5X_4^2X_1^3 + X_2X_3^2X_1^3 + X_3X_2^2X_1^3,\\
X_1X_3^2X_5^3 + X_1X_5^2X_3^3 + X_1X_3^2X_4^3 + X_1X_4^2X_3^3 + X_1X_2^2X_5^3 + X_1X_5^2X_2^3 + X_1X_2^2X_4^3 + X_1X_4^2X_2^3,\\
X_3X_1^2X_5^3 + X_5X_1^2X_3^3 + X_3X_1^2X_4^3 + X_4X_1^2X_3^3 + X_2X_1^2X_5^3 + X_5X_1^2X_2^3 + X_2X_1^2X_4^3 + X_4X_1^2X_2^3,\\
X_3X_5^2X_1^3 + X_5X_3^2X_1^3 + X_3X_4^2X_1^3 + X_4X_3^2X_1^3 + X_2X_5^2X_1^3 + X_5X_2^2X_1^3 + X_2X_4^2X_1^3 + X_4X_2^2X_1^3,\\
X_2X_3^2X_4^3X_5^4+X_2X_3^2X_5^3X_4^4+X_3X_2^2X_4^3X_5^4+X_3X_2^2X_5^3X_4^4+X_4X_5^2X_2^3X_3^4+X_4X_5^2X_3^3X_2^4+X_5X_4^2X_2^3X_3^4+X_5X_4^2X_3^3X_2^4,\\
X_2X_4^2X_3^3X_5^4+X_2X_5^2X_3^3X_4^4+X_3X_4^2X_2^3X_5^4+X_3X_5^2X_2^3X_4^4+X_4X_2^2X_5^3X_3^4+X_4X_3^2X_5^3X_2^4+X_5X_2^2X_4^3X_3^4+X_5X_3^2X_4^3X_2^4,\\
X_2X_4^2X_5^3X_3^4+X_2X_5^2X_4^3X_3^4+X_3X_4^2X_5^3X_2^4+X_3X_5^2X_4^3X_2^4+X_4X_2^2X_3^3X_5^4+X_4X_3^2X_2^3X_5^4+X_5X_2^2X_3^3X_4^4+X_5X_3^2X_2^3X_4^4,\\
X_1X_3^2X_4^3X_5^4+X_1X_3^2X_5^3X_4^4+X_1X_2^2X_4^3X_5^4+X_1X_2^2X_5^3X_4^4+X_1X_5^2X_2^3X_3^4+X_1X_5^2X_3^3X_2^4+X_1X_4^2X_2^3X_3^4+X_1X_4^2X_3^3X_2^4,\\
X_1X_4^2X_3^3X_5^4+X_1X_5^2X_3^3X_4^4+X_1X_4^2X_2^3X_5^4+X_1X_5^2X_2^3X_4^4+X_1X_2^2X_5^3X_3^4+X_1X_3^2X_5^3X_2^4+X_1X_2^2X_4^3X_3^4+X_1X_3^2X_4^3X_2^4,\\
X_1X_4^2X_5^3X_3^4+X_1X_5^2X_4^3X_3^4+X_1X_4^2X_5^3X_2^4+X_1X_5^2X_4^3X_2^4+X_1X_2^2X_3^3X_5^4+X_1X_3^2X_2^3X_5^4+X_1X_2^2X_3^3X_4^4+X_1X_3^2X_2^3X_4^4,\\
X_3X_1^2X_4^3X_5^4+X_3X_1^2X_5^3X_4^4+X_2X_1^2X_4^3X_5^4+X_2X_1^2X_5^3X_4^4+X_5X_1^2X_2^3X_3^4+X_5X_1^2X_3^3X_2^4+X_4X_1^2X_2^3X_3^4+X_4X_1^2X_3^3X_2^4,\\
X_3X_4^2X_1^3X_5^4+X_3X_5^2X_1^3X_4^4+X_2X_4^2X_1^3X_5^4+X_2X_5^2X_1^3X_4^4+X_5X_2^2X_1^3X_3^4+X_5X_3^2X_1^3X_2^4+X_4X_2^2X_1^3X_3^4+X_4X_3^2X_1^3X_2^4,\\
X_3X_4^2X_5^3X_1^4+X_3X_5^2X_4^3X_1^4+X_2X_4^2X_5^3X_1^4+X_2X_5^2X_4^3X_1^4+X_5X_2^2X_3^3X_1^4+X_5X_3^2X_2^3X_1^4+X_4X_2^2X_3^3X_1^4+X_4X_3^2X_2^3X_1^4,\\
X_4X_1^2X_3^3X_5^4+X_5X_1^2X_3^3X_4^4+X_4X_1^2X_2^3X_5^4+X_5X_1^2X_2^3X_4^4+X_2X_1^2X_5^3X_3^4+X_3X_1^2X_5^3X_2^4+X_2X_1^2X_4^3X_3^4+X_3X_1^2X_4^3X_2^4,\\
X_4X_1^2X_5^3X_3^4+X_5X_1^2X_4^3X_3^4+X_4X_1^2X_5^3X_2^4+X_5X_1^2X_4^3X_2^4+X_2X_1^2X_3^3X_5^4+X_3X_1^2X_2^3X_5^4+X_2X_1^2X_3^3X_4^4+X_3X_1^2X_2^3X_4^4,\\
X_4X_3^2X_1^3X_5^4+X_5X_3^2X_1^3X_4^4+X_4X_2^2X_1^3X_5^4+X_5X_2^2X_1^3X_4^4+X_2X_5^2X_1^3X_3^4+X_3X_5^2X_1^3X_2^4+X_2X_4^2X_1^3X_3^4+X_3X_4^2X_1^3X_2^4,\\
X_4X_3^2X_5^3X_1^4+X_5X_3^2X_4^3X_1^4+X_4X_2^2X_5^3X_1^4+X_5X_2^2X_4^3X_1^4+X_2X_5^2X_3^3X_1^4+X_3X_5^2X_2^3X_1^4+X_2X_4^2X_3^3X_1^4+X_3X_4^2X_2^3X_1^4,\\
X_4X_5^2X_1^3X_3^4+X_5X_4^2X_1^3X_3^4+X_4X_5^2X_1^3X_2^4+X_5X_4^2X_1^3X_2^4+X_2X_3^2X_1^3X_5^4+X_3X_2^2X_1^3X_5^4+X_2X_3^2X_1^3X_4^4+X_3X_2^2X_1^3X_4^4,\\
X_4X_5^2X_3^3X_1^4+X_5X_4^2X_3^3X_1^4+X_4X_5^2X_2^3X_1^4+X_5X_4^2X_2^3X_1^4+X_2X_3^2X_5^3X_1^4+X_3X_2^2X_5^3X_1^4+X_2X_3^2X_4^3X_1^4+X_3X_2^2X_4^3X_1^4.
\end{gathered}
$$

Exemple 6.4. Soient L et H deux sous-groupes de S_8 définis par :
$H =< (1,2,6,7)(3,4,8,5),(1,4,7,5)(2,3,8,6),(2,7,8)(4,5,6),(2,5,6)(3,4,8),(3,6,7)(4,5,8),(3,4,7,8,6,5) >$ et $L =< (1,2,6,7)(3,4,8,5),(1,4,7,5)(2,3,8,6) >$.

Le H-Invariant L-Primitif minimal est égal à :

$$
\begin{gathered}
X_5X_6X_7X_8 + X_3X_4X_7X_8 + X_3X_4X_5X_6 + X_2X_4X_6X_8 + X_2X_4X_5X_7 + X_2X_3X_6X_7 + X_2X_3X_5X_8 +\\
X_1X_4X_6X_7 + X_1X_4X_5X_8 + X_1X_3X_6X_8 + X_1X_3X_5X_7 + X_1X_2X_7X_8 + X_1X_2X_5X_6 + X_1X_2X_3X_4 \quad .
\end{gathered}
$$

Le H-Invariant S_8-Primitif minimal est égal à :

$$
\begin{gathered}
X_5X_6X_7X_8 + X_4X_6X_7X_8 + X_3X_5X_6X_8 + X_3X_4X_7X_8 + X_3X_4X_5X_7 + X_3X_4X_5X_6 + X_2X_5X_6X_7 +\\
X_2X_4X_6X_8 + X_2X_4X_5X_8 + X_2X_4X_5X_7 + X_2X_3X_7X_8 + X_2X_3X_6X_7 + X_2X_3X_5X_8 + X_2X_3X_4X_6 +\\
X_1X_5X_7X_8 + X_1X_4X_6X_7 + X_1X_4X_5X_8 + X_1X_4X_5X_6 + X_1X_3X_6X_8 + X_1X_3X_6X_7 + X_1X_3X_5X_7 +\\
X_1X_3X_4X_8 + X_1X_2X_7X_8 + X_1X_2X_6X_8 + X_1X_2X_5X_6 + X_1X_2X_4X_7 + X_1X_2X_3X_5 + X_1X_2X_3X_4 \quad .
\end{gathered}
$$

Ces calculs ont été fait 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.** Le temps de calcul d'ensembles essentiels avec l'algorithme 4.3 sous GAP pour des degrés inférieurs ou égaux à 6 varie entre moins d'une seconde et une heure. Les temps de calcul augmentent au fur et à mesure que le degré n augmente ; le tableau suivant nous donne une idée sur cette évolution, en moyenne, 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 pour le calcul d'ensembles essentiels pour (S_{15},A_{15}). Rappelons que même si le calcul d'ensembles essentiels est assez lourd, il ne sera fait qu'une seule fois.

6.3. **Application à La Théorie de Galois.** La connaissance de polynômes invariants primitifs nous permet à partir de son polynôme minimal, appelé *résolvante de Lagrange*, de calculer le groupe de Galois d'un polynôme f de degré n.
En effet, A. Valibouze et J. M. Arnaudiès 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 minimaux de H-invariants S_n-primitif) H est un sous-groupe de S_n appelé *groupe test*).
Souvent, le degré de ces résolvantes absolues est assez grand et leur factorisation est difficile surtout lorsque n est grand. Une autre méthode appelée *la méthode de Stauduhar* (voir [17], [7], [19], etc) qui utilise la factorisation de polynômes minimaux de H-invariants L-primitifs relatifs ($H \subset L \subset S_n$), est plus rapide car de degré plus petit. Il est donc recommandé d'avoir plusieurs invariants primitifs relatifs et absolus de degrés petits. D'où l'intérêt de l'*algorithme de Girstmair-Jordan.*

Conclusion

Les méthodes de calculs de polynômes invariants primitifs connus sont intuitifs et donnent souvent des polynômes de degrés élevés. L'algorithme de K. Girstmair calcule un invariant primitif absolu de degré minimal, mais pas nécessairement minimal. Une autre façon de calculer des invariants de groupes finis à été introduite par B. Sturmfels [18] et améliorée et implantée en MAGMA par G. 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 G. 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 [19] et [15]). Grâce à l'algorithme 4.4 que nous avons appelé Algorithme de Girstmair-Jordan, et grâce à la représentation de données utilisée, nous calculons tous les polynômes invariants primitifs à coefficients distincts et de tous les degrés possibles. Ce sont des polynômes invariants relatifs ou absolus par rapport à des groupes de permutations.

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).

[3] J.M. Arnaudiès, A. Valibouze, *Lagrange Resolvents*, Journal Of Pure And Applied Algebra, (1997).

[4] E.H. Berwick, *The Condition That A quintic Equation Should Be Soluble By Radicals* Proc. London Math. Soc.(2) 14, 301-307, (1915).

[5] E.H. Berwick, *On soluble Sextic Equations* Proc. London Math. Soc.(2) 29, 1-28, (1929).

[6] A. Cayley, *On a new auxiliary equation in the theory of equation of fifth order*, Philosophical transactions of the Royal Society of London, CLL, (1861).

[7] A. Colin, *Formal Computation of Galois groups with relative resolvents*, AAECC'95, Lecture Notes in Computer Science, volume 948, p 169-182. Sprniger Verlag, (1995).

[8] A. Colin, *Solving a system of algebraic equations with symmetries*, J. of Pure and Applied Algebra, (1996).

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

[10] G.A.P. `Groups, Algorithms and Programming` Martin Schönert and others, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochoschule, Aachem, `gap@samson.math.rwth-aachen.de`, (1993).

[11] K. Girstmair, *On invariant Polynomials and Their Application in Field Theory*, Maths of Comp., vol 48, no 178, p.781-797, (1987).

[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] E. Luther *Ueber die Factoren des algebraisch lôsbaren irreducible Gleichungen vom sechsten Grade und ihren Resolvanten*,Journal für Math., 37, 193-220, (1848).

[15] N. Rennert, A. Valibouze, *Modules de Cauchy*, Rapport interne LIP6, (1997).

[16] L. Soicher, *The computation of the Galois groups*, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).

[17] R.P. Stauduhar, *The computation of Galois groups*, Math.Comp. volume 27, 981-996, (1973).

[18] B. Sturmfels, *Algorithms in Invariant Theory*, Wien, New York : Springer Verlag, (1993).

[19] A. Valibouze, *Groupes de Galois jusqu'en degré 7*, Rapport interne LIP6, (1997).

[20] A. Vandermonde, *Mémoire de l'Académie des Sciences de Paris*, (1771).

[21] R.L. Wilson, *A method for the determination of the Galois group*, American Mathematical Society, (1949).