ÉTUDE DES RELATIONS ALGÉBRIQUES ENTRE LES RACINES D'UN POLYNÔME D'UNE VARIABLE

ANNICK VALIBOUZE

Résumé. Cet article développe une vision effective de la théorie de Galois algébrique en apportant des propriétés inhérentes aux idéaux associés à un polynôme d'une variable. Il débouche sur un algorithme de calcul du groupe de Galois d'un polynôme et de l'idéal des relations entre ses racines.

About the relations among the roots of a univariate polynomial

Abstract. *Galois theory allows us to deal with effective computation in algebraic extensions of fields. In this aim, the present paper is devoted to an inductive construction of a generating system for the ideal of relations among the roots of a univariate polynomial over a field. The idea is to define new ideals between the ideal of symmetric relations and the ideal of relations and to give a correspondence between these ideals and finite sets of permutations. The fundamental tools of this construction are multivariate polynomials called minimal polynomials associated to our ideals. These polynomials characterize the considered ideals and allow to construct a generating system for them.*

Introduction

La recherche du *groupe de Galois d'un polynôme* f d'une variable fut d'abord motivée par la résolution par radicaux de ses racines, puis par l'étude de son corps de décomposition et les manipulations des nombres algébriques qui lui appartiennent. Ce qui est exposé ici suppose que le corps k des coefficients du polynôme f est parfait.

La première étude fondamentale est due à Lagrange (voir [19]) qui, en introduisant les *résolvantes*, a défini l'outil algébrique fondamental de la théorie de Galois constructive. Il a montré que toutes les méthodes de résolution par radicaux connues alors revenaient à choisir de "bonnes" résolvantes, à les calculer puis à les factoriser sur le corps k des coefficients du polynôme f. S'appuyant sur ces travaux Galois (voir [14]) utilisa une résolvante particulière, connue sous le nom de *résolvante de Galois*, pour définir un groupe appelé aujourd'hui *groupe de Galois du polynôme* f. Ce groupe décrit le comportement des racines du polynôme f. Les études ultérieures mirent en évidence la *correspondance entre les sous-groupes du groupe de Galois de* f *et les sous-corps de son corps de décomposition* (voir [5]). Par ailleurs, de nombreux auteurs ont trouvé empiriquement des résolvantes permettant de déterminer les groupes de Galois jusqu'en degré 7 (voir [7], [8], [13], [21] et [22]). La *correspondance entre les résolvantes et les groupes* montre qu'il est toujours possible de

---

soutenue par le projet *Galois* du GDR-CNRS MEDICIS et par le *Dipartimento di Matematica di la Università di Pisa*

Mathematics Subject Classification. 12F10, 12Y05, 11Y40.

Key words and phrases. Galois group, univariate polynomials, resolvents, primitive elements of Galois ideals, computation of the ideal of the relations among the roots of univariate polynomials.

calculer le groupe de Galois d'un polynôme à partir des résolvantes et détermine les résolvantes adéquates pour y parvenir (voir [4] et [25]) .

Une autre façon d'aborder la théorie de Galois est d'étudier les relations entre les racines du polynôme f. (Une relation est un polynôme de n variables à coefficients dans le corps k où n est le degré du polynôme f.) Lorsque l'*idéal de toutes les relations* entre les racines de f est connu, le groupe de Galois et le corps de décomposition du polynôme f le sont également. Dans [2] est proposé un algorithme de construction d'une base de Gröbner de cet idéal (voir aussi [23]) ; il consiste à factoriser le polynôme dans des extensions successives du corps k de base jusqu'au corps de décomposition du polynôme f. Un autre idéal étudié jusqu'alors est l'*idéal des relations symétriques* entre les racines du polynôme f.

Cet article propose une étude approfondie des relations entre les racines du polynôme f à travers des idéaux particuliers contenant l'idéal des relations symétriques et inclus dans l'idéal (maximal) des relations entre les racines du polynôme f. Les principaux résultats de cette étude sont la *correspondance entre les idéaux étudiés et des ensembles de permutations* et un *algorithme de construction d'un système de générateurs de l'idéal des relations.* Cet algorithme ne nécessite aucune factorisation dans une extension algébrique du corps des coefficients du polynôme f. Il construira une chaîne croissante d'idéaux :

$$I_1 \subset I_2 \subset \cdots \subset I_m$$

où I_1 est l'idéal des relations symétriques entre les racines du polynôme f et I_m est l'idéal des relations entre ces racines. Pour chaque idéal I_j de la chaîne sera déterminé un polynôme R_j, appelé *polynôme primitif* de l'idéal I_j, vérifiant

$$I_j = I_{j-1} + < R_j > \quad .$$

Passons à une présentation plus détaillée de cet article. L'étude des relations entre les racines du polynôme f nécessite un ordonnancement des ses racines. Un ensemble ordonné des racines du polynôme f, noté Ω, sera donc fixé afin d'étudier les Ω-relations (i.e. les polynômes de n variables qui, évalués en Ω, s'annulent).

Le premier paragraphe sera consacré aux définitions. Au paragraphe 1.3 seront définis l'*idéal des Ω-relations*, noté I_Ω, et le *groupe de Galois* , noté G_Ω. Au paragraphe 1.4 seront introduits les *idéaux des Ω-relations invariantes par des permutations*, notés sous la forme I_Ω^L, où L est un ensemble de permutations. Deux ensembles de permutations associés à un idéal I_Ω^L seront alors définis : le *fixateur*, noté $\mathrm{Max}(I_\Omega^L)$, et le *groupe de décomposition*, noté $\mathrm{Gr}(I_\Omega^L)$.

Les hypothèses générales de l'article feront l'objet du second paragraphe.

Le troisième paragraphe sera consacré aux résultats théoriques. Les idéaux I_Ω^L forment une chaîne croissante commençant par l'idéal des relations symétriques et terminant par l'idéal maximal I_Ω. Au paragraphe 3.1 se trouveront des résultats préliminaires. Au paragraphe 3.2 sera montré que pour chaque idéal I_Ω^L, où L est un groupe, il existe un polynôme qui le caractérise par rapport à un idéal I_Ω^M, où M est un groupe qui contient les groupes L et G_Ω (voir Théorème 3.10). Ce polynôme sera appelé un *polynôme M-primitif de l'idéal I_Ω^L* et servira à identifier le fixateur (voir Corollaire 3.12). La correspondance entre les idéaux I_Ω^L et les fixateurs sera décrite au paragraphe 3.3 (voir Théorème 3.14). Aux paragraphes 3.4 et 3.5 seront exprimés les variétés, les polynômes caractéristiques et minimaux ainsi que les résolvantes associés aux idéaux I_Ω^L. Au paragraphe 3.6, il sera montré comment obtenir un *système de générateurs de l'idéal I_Ω^L* à partir d'un de ses polynômes M-primitifs (voir Théorème

3.27). Au paragraphe 3.7 sera étudiée l'effectivité de l'hypothèse d'induction de la construction de l'idéal des Ω-relations à partir de l'idéal des relations symétriques. Cette hypothèse d'induction est celle du second paragraphe. Au paragraphe 4 seront rappelés les résultats sur les *matrices de groupes* et de *partitions.*

Le cinquième paragraphe comportera un algorithme de construction d'un système de générateurs de l'idéal des Ω-relations.

Pour terminer, un exemple explicite sera donné au sixième paragraphe.

Ces résultats ont été enseignés en troisième cycle universitaire à Marrakech (Octobre 1996), à Paris (Janvier 1997) et à Pise (Avril 1997).

1. Définitions et notations préliminaires

1.1. **Les données.**

Nous nous donnons :
- k un corps supposé parfait,
- $\hat{k}$ une clôture algébrique de k,
- f un polynôme séparable d'une variable à coefficients dans k et de degré n,
- $\Omega = (\alpha_1, \ldots, \alpha_n) \in \hat{k}^n$, composé des racines (distinctes) du polynôme f,
- $x_1, \ldots, x_n$ et T des indéterminées

et nous adoptons les notations suivantes :
- $k[x_1, \ldots, x_n]$ désigne l'anneau des polynômes en $x_1, \ldots, x_n$ à coefficients dans k,
- $k(x_1, \ldots, x_n)$ désigne le corps des fractions de $k[x_1, \ldots, x_n]$,
- pour un polynôme P de$k[x_1, \ldots, x_n]$, $P(\Omega) = P(\alpha_1, \ldots, \alpha_n)$.

1.2. **Action du groupe symétrique.**

Fixons, pour ce paragraphe, une fraction Θ dans le corps $k(x_1, \ldots, x_n)$ et deux sous-groupes L et H du groupe symétrique de degré n qui sera noté $\mathfrak{S}_n$. Supposons que H soit inclus dans L.

Le groupe symétrique de degré n agit naturellement sur le corps $k(x_1, \ldots, x_n)$. Pour $\sigma \in \mathfrak{S}_n$, l'action de σ sur Θ, notée $\sigma.\Theta$ ou $(\sigma.\Theta)$, est définie ainsi :

$$\sigma.\Theta(x_1, \ldots, x_n) = \Theta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \ .$$

L'action de σ sur Ω, notée $\sigma.\Omega$, est définie par $\sigma.\Omega = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

Définition 1.1. L' *orbite de Θ sous l'action d'un groupe L* est définie par :

$$L.\Theta = \{\sigma.\Theta \ \mid \ \sigma \in L\} \ .$$

La fraction Θ est appelée un *invariant de L* (ou un *L-invariant*) si $L.\Theta = \{\Theta\}$. Le corps des L-invariants sera noté $k(x_1, \ldots, x_n)^L$.

Définition 1.2. Le *stabilisateur de Θ dans L*, noté $\mathrm{Stab}_L(\Theta)$, est défini par :

$$\mathrm{Stab}_L(\Theta) = \{\sigma \in L \mid \Theta = \sigma.\Theta\} \ .$$

Le *stabilisateur du groupe H dans le groupe L* sera noté $\mathrm{Stab}_L(H)$.

Définition 1.3. La fraction Θ est appelée un *H-invariant L-primitif* si Θ est un polynôme et $H = \mathrm{Stab}_L(\Theta)$.

Des méthodes efficaces permettent de calculer des H-invariants L-primitifs (voir [1] ou [17]).

Exemple 1.4. Soit A_n, le groupe alterné dans $\mathfrak{S}_n$, alors le déterminant de Vandermonde $\delta_n := \prod_{1\leq i<j\leq n}(x_i - x_j)$ est un A_n-invariant $\mathfrak{S}_n$-primitif.

Définition 1.5. Soit Θ un H-invariant L-primitif. Le polynôme Θ est dit *séparable pour* Ω si $H = \{\sigma \in L \mid \Theta(\Omega) = (\sigma.\Theta)(\Omega)\}$.

Lorsque le corps k est infini, il est toujours possible de construire pour chaque polynôme des H-invariant L-primitif séparables (voir [3]). Il existe aussi pour certains groupes des invariants "universels" qui sont séparables pour tous les polynômes.

Exemple 1.6. Comme le polynôme f est séparable (i.e. ses racines sont distinctes), le déterminant de Vandermonde est séparable. En effet $\mathfrak{S}_n.\delta_n = \{\delta_n, -\delta_n\}$ et le discriminant non nul de f est à une constante près $\delta_n^2(\Omega)$. Si $\delta_n(\Omega) = -\delta_n(\Omega)$ alors $\delta_n(\Omega) = 0$ et le discriminant du polynôme f est nul.

Exemple 1.7. L'invariant de Cayley qui est un invariant $\mathfrak{S}_5$-primitif du groupe métacyclique est séparable pour tous les polynômes séparables (voir [4]).

Définition 1.8. Soit $\{\sigma_1 H, \dots, \sigma_e H\}$ l'ensemble des classes à gauche (resp. à droite) de $L \mod H$, noté $(L/H)_g$. L'ensemble $\{\sigma_1, \dots, \sigma_n\}$ est appelé une *transversale à gauche de* $L \mod H$ (resp. *à droite*).

Notation 1.9. Pour G et H deux sous-groupes de $\mathfrak{S}_n$, la notation GH désigne le sous-ensemble $\{gh \mid g \in G\,,\, h \in H\}$ de $\mathfrak{S}_n$.

1.3. **Idéal des relations et groupe de Galois.**

Cet article se propose d'étudier les racines du polynôme f par les relations qui existent entre elles. Pour ce faire, l'ordre des racines a été fixé dans Ω.

Définition 1.10. Un polynôme $P \in k[x_1, \dots, x_n]$ est appelé une Ω-*relation* si $P(\Omega) = 0$.

Définition 1.11. L'idéal I_Ω de $k[x_1, \dots, x_n]$ défini par

$$I_\Omega = \{R \in k[x_1, \dots, x_n] \mid R(\Omega) = 0\} \tag{1}$$

est connu sous le nom d'*idéal des* Ω-*relations.*

Définition 1.12. Le *groupe de Galois de* Ω est le sous-groupe G_Ω de $\mathfrak{S}_n$ défini par

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid (\forall R \in I_\Omega)\ \sigma.R \in I_\Omega\}\ . \tag{2}$$

Le lemme 3.4 assure que G_Ω est effectivement un groupe. Ce groupe est communément appelé le groupe de Galois du polynôme f car il est isomorphe au groupe des k-automorphismes de $k(\Omega)$, le groupe de Galois de l'extension $k(\Omega)$ de k.

De par sa définition, le groupe de Galois G_Ω agit sur l'anneau quotient $A_{I_\Omega} := k[x_1, \dots, x_n]/I_\Omega$ de la manière suivante :

$$\begin{array}{rcl} G_\Omega \times A_{I_\Omega} & \longrightarrow & A_{I_\Omega} \\ (\sigma, P) & \mapsto & (\sigma.P)(\Omega) = P(\sigma.\Omega)\ . \end{array}$$

Comme A_{I_Ω} est k-isomorphe au corps $k(\Omega)$, le corps de décomposition du polynôme f, cette action induit une action, notée $\star$, de G_Ω sur $k(\Omega)$. C'est ce qui, avec la correspondance galoisienne, rend essentielle la connaissance du groupe de Galois ou mieux encore celle de l'idéal I_Ω.

1.4. **Idéal invariant par un ensemble de permutations.**

L'étude de l'idéal des Ω-relations va être abordée avec celle d'une famille d'idéaux particuliers définis ci-dessous :

Définition 1.13. Soit un sous-ensemble L de $\mathfrak{S}_n$, l'idéal

$$I_\Omega^L \quad = \quad \{R \in k[x_1, \ldots, x_n] \ | \ (\forall \sigma \in L)\ (\sigma.R)(\Omega) = 0\}$$

est appelé *idéal des Ω-relations invariantes par L*. En particulier l'idéal des relations, I_Ω, est défini comme l'idéal des Ω-relations invariantes par l'identité et l'idéal $I_\Omega^{\mathfrak{S}_n}$ est connu sous le nom d'*idéal des relations symétriques entre les racines du polynôme f*.

Remarque 1. L'idéal des relations symétriques ne dépend pas de l'ordre donné aux racines du polynôme f. Il peut aussi être noté $I_f^{\mathfrak{S}_n}$.

Définition 1.14. Soit L un sous-ensemble du groupe symétrique $\mathfrak{S}_n$. Le plus grand des sous-ensembles, G, de $\mathfrak{S}_n$ qui vérifient :

$$I_\Omega^L = I_\Omega^G \tag{3}$$

est appelé le *fixateur de l'idéal* I_Ω^L et sera noté $\mathrm{Max}(I_\Omega^L)$.

Le fixateur existe puisqu'il s'exprime sous la forme :

$$\mathrm{Max}(I_\Omega^L) = \bigcup_{G \in \mathfrak{S}_n \,|\, I_\Omega^L = I_\Omega^G} G$$

et que pour tout ensemble $\mathcal{G}$ d'ensembles de permutations :

$$I_\Omega^{\bigcup_{G\in\mathcal{G}} G} = \bigcap_{G \in \mathcal{G}} I_\Omega^G \quad .$$

Définition 1.15. Le *groupe de décomposition d'un idéal* $I \subset k[x_1, \ldots, x_n]$, noté $\mathrm{Gr}(I)$, est défini par :

$$\mathrm{Gr}(I) = \{\sigma \in \mathfrak{S}_n \ | \ \sigma(I) = I\} \quad . \tag{4}$$

Cette terminologie est choisie en référence à la théorie des nombres. (Le lemme 3.4 assure que le groupe de décomposition est effectivement un groupe.)

2. Hypothèses générales

Désormais, deux sous-groupes M et L du groupe symétrique $\mathfrak{S}_n$ seront fixés. Le groupe L et le groupe de Galois G_Ω seront inclus dans le groupe M.

La situation est la suivante (voir Lemme 3.3) :

$$I_\Omega^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset I_\Omega \quad . \tag{5}$$

Pour assurer de l'existence d'invariants primitifs séparables, le corps k est supposé infini.

Le polynôme $\Theta \in k[x_1, \ldots, x_n]$ désignera un L-invariant M-primitif séparable pour Ω. Lui seront associés $\theta \in k(\Omega)$ et le polynôme $R_{L,M}$ de $k[x_1, \ldots, x_n]$ définis par :

$$\theta := \Theta(\Omega) \quad \text{et} \quad R_{L,M} := \mathrm{Min}_{\theta,k}(\Theta)$$

où $\mathrm{Min}_{\theta,k}$ désigne le polynôme minimal de θ sur k.

Exemple 2.1. Supposons le polynôme f unitaire et notons $\Delta(f)$ son discriminant. Choisissons $M = \mathfrak{S}_n$ et $L = A_n$, le groupe alterné dans $\mathfrak{S}_n$. Le déterminant de Vandermonde, noté δ_n, est toujours un A_n-invariant $\mathfrak{S}_n$-primitif séparable puisque f n'a que des racines simples. Il est alors possible de choisir $\Theta := \delta_n$. Si le groupe de Galois est pair alors $\theta \in k$ (voir Lemme 3.7) et

$$R_{L,M} = \Theta - \theta \quad .$$

Sinon $\mathrm{Min}_{\theta,k}(T) = T^2 - \theta^2 = T^2 - \Delta(f)$ et donc

$$R_{L,M} = \Theta^2 - \Delta(f) \quad .$$

3. Résultats théoriques

3.1. **Premières propriétés.**

La notation $\sigma.P(\Omega)$ n'est pas ambiguë : $\sigma.P(\Omega) = (\sigma.P)(\Omega)$. Néanmoins, le lemme suivant précise cette notation :

Lemme 3.1. *Soit $\sigma, \tau \in \mathfrak{S}_n$ et $P \in k(x_1, \ldots, x_n)$, alors $(\sigma.P)(\tau.\Omega) = P(\tau\sigma.\Omega)$.*

Démonstration. Soit $\sigma, \tau \in \mathfrak{S}_n$ et $P \in k(x_1, \ldots, x_n)$. En appliquant les notations et définitions il vient :

$$\begin{aligned}(\sigma.P)(x_1, \ldots, x_n)(\tau.\Omega) &= P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) \\ &= P(\tau\sigma.\Omega)\end{aligned}$$

car l'évaluation de x_j est $\alpha_{\tau(j)}$ pour tout $j \in [1, n]$ et donc celle $x_{\sigma(i)}$ est $\alpha_{\tau\sigma(i)}$ pour tout $i \in [1, n]$ (en posant $j := \sigma(i)$). □

Lemme 3.2. *Pour chaque ensemble de permutations H inclus dans le groupe symétrique $\mathfrak{S}_n$, l'idéal I_Ω^H est radical.*

Démonstration. Soit n un entier positif non nul et $P \in k[x_1, \ldots, x_n]$ tel que $P^n \in I_\Omega^H$. Soit $\sigma \in L$, alors $0 = (\sigma.P)^n(\Omega) = (\sigma.P(\Omega))^n$ et, puisque k est un corps parfait, $\sigma.P(\Omega) = 0$. D'où $P \in I_\Omega^L$. □

Lemme 3.3. *Soient H et G deux sous-ensembles de $\mathfrak{S}_n$ tels que $H \subset G$. Alors $I_\Omega^G \subset I_\Omega^H$.*
En particulier, si G contient l'identité alors $I_\Omega^G \subset I_\Omega$.

Démonstration. Supposons que H soit inclus dans G. Soit $R \in I_\Omega^G$. Nous avons $\sigma.R \in I_\Omega$ pour tout $\sigma \in G$ et ce en particulier pour tout $\sigma \in H$. Donc $R \in I_\Omega^H$. □

Remarque 2. La réciproque du lemme 3.3 n'est pas toujours vraie (voir Théorème 3.14).

Lemme 3.4. *Soit I un idéal de $k[x_1, \ldots, x_n]$ et H l'ensemble de permutations défini par :*

$$H := \{\sigma \in \mathfrak{S}_n \mid \sigma(I) \subset I\} \quad .$$

Alors H est un groupe et donc $H = \{\sigma \in \mathfrak{S}_n \mid \sigma(I) = I\} = Gr(I)$.

Démonstration. Pour σ et $\tau \in H$, alors $\tau\sigma \in H$ puisque $\tau\sigma.I \subset \tau.I \subset I$. Donc H est stable par composition et puisqu'il est fini, c'est un groupe. □

Les idéaux I_Ω et $I_\Omega^{\mathfrak{S}_n}$ sont égaux si et seulement si le groupe de Galois G_Ω est identique au groupe symétrique $\mathfrak{S}_n$ puisque

$$G_\Omega = \mathrm{Max}(I_\Omega) = \mathrm{Gr}(I_\Omega) \quad \text{et que} \tag{6}$$

$$\mathfrak{S}_n = \mathrm{Max}(I_\Omega^{\mathfrak{S}_n}) = \mathrm{Gr}(I_\Omega^{\mathfrak{S}_n}) \ . \tag{7}$$

Les propositions 3.5 et 3.6 montrent ce qu'il en est pour les idéaux I_Ω^L intermédiaires entre l'idéal des Ω-relations et l'idéal des relations symétriques.

Proposition 3.5. *Si L est un sous-groupe de $\mathfrak{S}_n$, alors :*

$$L \subset Gr(I_\Omega^L) \ \ et \tag{8}$$

$$I_\Omega^{Gr(I_\Omega^L)} \subset I_\Omega^L \ . \tag{9}$$

Démonstration. Pour prouver (8), prenons $\tau \in L$ et $R \in I_\Omega^L$. D'après le lemme 3.4, il suffit de prouver que $\tau(I_\Omega^L) \subset I_\Omega^L$. Pour tout $\sigma \in L$, le polynôme $\sigma\tau.R$ appartient à l'idéal I_Ω puisque $\sigma\tau \in L$. D'où $\tau.R \in I_\Omega^L$ (i.e. $\tau \in \mathrm{Gr}(I_\Omega^L)$). l'inclusion (9) découle du lemme 3.3. □

Proposition 3.6. *Soit I un idéal de $k[x_1, \ldots, x_n]$.*
(i) Si $I \subset I_\Omega$ alors $I \subset I_\Omega^{Gr(I)}$.
(ii) Si $I = I_\Omega^L$, où L est un sous-groupe de $\mathfrak{S}_n$, alors

$$I_\Omega^L = I_\Omega^{Gr(I)} = I_\Omega^{Max(I)} \ \ et \tag{10}$$

$$L \subset Gr(I_\Omega^L) \subset Max(I_\Omega^L) \ . \tag{11}$$

(iii) Si, de plus, $Max(I_\Omega^L)$ est un groupe alors $Gr(I_\Omega^L) = Max(I_\Omega^L)$.

Démonstration. Montrons d'abord (i). Soit $R \in k[x_1, \ldots, x_n]$. Si $R \in I$ alors , par définition du groupe de décomposition, $\forall \sigma \in \mathrm{Gr}(I)$ $\sigma.R \in I \subset I_\Omega$. Finalement, $R \in I_\Omega^{\mathrm{Gr}(I)}$. Maintenant, prenons L un sous-groupe de $\mathfrak{S}_n$ et posons $I := I_\Omega^L$ qui est contenu dans l'idéal I_Ω puisque L contient l'identité. Montrons (ii). D'après (i), $I_\Omega^L \subset I_\Omega^{\mathrm{Gr}(I_\Omega^L)}$. Réciproquement, par la proposition 3.5, puisque L est un groupe, il est inclus dans le groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$ et donc $I_\Omega^{\mathrm{Gr}(I_\Omega^L)} \subset I_\Omega^L$, d'après le lemme 3.3. Si, de plus, le fixateur $\mathrm{Max}(I)$ est un groupe, alors la proposition 3.5, appliquée à $\mathrm{Max}(I)$ à la place de L, implique $\mathrm{Max}(I) \subset \mathrm{Gr}(I)$. L'inclusion inverse est la conséquence de la définition de $\mathrm{Max}(I)$ et de (10). □

3.2. **Polynôme primitif d'un idéal.**

Ce paragraphe montre que le polynôme $R_{L,M}$ caractérise l'idéal I_Ω^L relativement à l'idéal I_Ω^M et identifie le fixateur avec le groupe de Galois G_Ω.

Rappelons ce résultat standard (voir, par exemple, [22]) :

Lemme 3.7. *Soit Θ_L un L-invariant M-primitif. Alors :*
(i) si $G_\Omega \subset L$ alors $\Theta_L(\Omega) \in k$;
(ii) si $\Theta_L(\Omega) \in k$ et si Θ_L est M-séparable pour Ω alors $G_\Omega \subset L$.

Démonstration. Le (i) est évident. Montrons le (ii). Si $\theta = \Theta_L(\Omega) \in k$, alors $R_L := \Theta_L - \theta \in I_\Omega^L \subset I_\Omega$ puisque L contient l'identité. S'il existe $\sigma \in G_\Omega$ tel que $\sigma \notin L$ alors $\sigma.R_L(\Omega) = \sigma.\Theta_L - \theta \neq 0$, puisque $\sigma \in M$ et Θ_L est M-séparable pour Ω. Ce qui aboutit à la contradiction $R_L \notin I_\Omega^{G_\Omega} = I_\Omega$. □

Mais que dire lorsque le groupe de Galois G_Ω n'est pas inclus dans le groupe L ? Le lemme suivant permet d'aborder la situation générale.

Lemme 3.8. *Soit H un sous-ensemble de $\mathfrak{S}_n$. Alors, il existe un polynôme $R_M \in I_\Omega^M$ tel que la condition $R_M \in I_\Omega^H$ soit équivalente à $H \subset M$.*

Démonstration. Prenons Θ_M un M-invariant $\mathfrak{S}_n$-primitif séparable pour Ω. Comme le groupe M contient le groupe de Galois G_Ω, d'après le lemme 3.7, le polynôme $R_M = \Theta_M - \Theta_M(\Omega)$ appartient à I_Ω^M. Soit $\sigma \in \mathfrak{S}_n$. Si $\sigma \notin M$ alors $\sigma.\Theta_M \neq \Theta_M$ et donc $\sigma.\Theta_M(\Omega) \neq \Theta_M(\Omega)$ puisque Θ_M est séparable pour Ω . □

Proposition 3.9. *Soit H un sous-ensemble de $\mathfrak{S}_n$. Si $I_\Omega^M \subset I_\Omega^H$ alors $H \subset Max(I_\Omega^H) \subset M$. Si, de plus, H est un sous-groupe de $\mathfrak{S}_n$ alors $Gr(I_\Omega^H) \subset M$.*

Démonstration. Il suffit de montrer que $H \subset M$ puisque $I_\Omega^H = I_\Omega^{\mathrm{Max}(I_\Omega^H)}$ et que si H est un sous-groupe de $\mathfrak{S}_n$ alors $I_\Omega^H = I_\Omega^{\mathrm{Gr}(I_\Omega^H)}$. Soit R_M le polynôme de la démonstration du lemme 3.8. Par hypothèse, $R_M \in I_\Omega^H$ et par conséquent $H \subset M$. □

Théorème 3.10. *Soient M et L deux sous-groupes du groupe symétrique $\mathfrak{S}_n$ tels que M contienne le groupe L et le groupe de Galois G_Ω. Soit Θ un L-invariant M-primitif séparable pour Ω. Posons $\theta := \Theta(\Omega)$ et $R_{L,M} :=Min_{\theta,k}(\Theta)$. Alors*

$$\begin{array}{ll} a) & R_{L,M} \in I_\Omega^L \;\; ; \\ b) & \{\sigma \in M \mid \sigma.R_{L,M}(\Omega) = 0\} = G_\Omega L \;\; . \end{array}$$

Démonstration. a) Pour $\sigma \in L$, comme Θ est un L-invariant M-primitif, nous avons :

$$\sigma.R_{L,M} = \mathrm{Min}_{\theta,k}(\sigma.\Theta) = \mathrm{Min}_{\theta,k}(\Theta) = R_{L,M} \;\; .$$

Par conséquent, $\sigma.R_{L,M}(\Omega) = \mathrm{Min}_{\theta,k}(\theta) = 0$.

b) Par la théorie de Galois, le polynôme minimal de θ sur k est donné par :

$$\mathrm{Min}_{\theta,k}(x) = \prod_{\phi \in G_\Omega \star \theta} (x - \phi) = \prod_{\phi \in \{\tau.\Theta(\Omega) \mid \tau \in G_\Omega\}} (x - \phi) \;\; . \tag{12}$$

Posons $A := \{\sigma \in M \mid \; \sigma.R_{L,M}(\Omega) = 0\}$. D'après (12),

$$\begin{aligned} A &= \{\sigma \in M \mid \; (\exists\, \tau \in G_\Omega)\; \sigma.\Theta(\Omega) = \tau.\Theta(\Omega)\} \\ &= \{\sigma \in M \mid \; (\exists\, \tau \in G_\Omega)\; \tau^{-1}\sigma.\Theta(\Omega) = \Theta(\Omega)\} \end{aligned}$$

puisque $\tau^{-1} \in G_\Omega$. Finalement, comme Θ est M-séparable pour Ω et $\tau^{-1}\sigma \in M$,

$$A = \{\sigma \in M \mid \; (\exists\, \tau \in G_\Omega)\; \tau^{-1}\sigma \in L\} = G_\Omega L \;\; .$$

□

Définition 3.11. Le polynôme $R_{L,M}$ est appelé un *polynôme M-primitif de l'idéal I_Ω^L*.

Cette terminologie est justifiée par le corollaire suivant :

Corollaire 3.12. *Le fixateur de l'idéal I_Ω^L est donné par :*

$$Max(I_\Omega^L) = G_\Omega L = \{\sigma \in M \mid \; \sigma.R_{L,M}(\Omega) = 0\} \;\; . \tag{13}$$

Démonstration. Soient $R \in I_\Omega^L$, $\tau \in G_\Omega$ et $l \in L$. Puisque $l.R \in I_\Omega$ et par définition de G_Ω, $\tau.(l.R) \in I_\Omega$. Par conséquent, $\tau l \in \mathrm{Max}(I_\Omega^L)$. Inversement, soit $\sigma \in \mathrm{Max}(I_\Omega^L)$. D'après la proposition 3.9, $\sigma \in M$. D'après le a) du théorème 3.10, $R_{L,M}(\sigma.\Theta)(\Omega) = 0$ et, d'après le b) du théorème 3.10, $\sigma \in G_\Omega L$. □

Corollaire 3.13. *Si $\tau \in \mathfrak{S}_n$ alors $Max(I_\Omega^{\tau L}) = G_{\tau.\Omega}L$.*

Démonstration. Puisque $I_\Omega^{\tau L} = I_{\tau.\Omega}^L$. □

3.3. **Correspondance entre idéaux et les fixateurs.**

Nous aboutissons à cette correspondance entre les fixateurs et les idéaux de relations invariantes par des permutations :

Théorème 3.14. *Soit H un sous-groupe de $\mathfrak{S}_n$, alors*
(i) la condition $H \subset Max(I_\Omega^L)$ est équivalente à $I_\Omega^L \subset I_\Omega^H$.
(ii) $H \subset Max(I_\Omega^L)$ est équivalent à $Max(I_\Omega^H) = G_\Omega H \subset G_\Omega L = Max(I_\Omega^L)$.

Démonstration. L'équivalence de (ii) avec l'hypothèse est évidente ainsi que la condition nécessaire de (i) (voir Lemme 3.3). Montrons la condition suffisante de (i) : pour $h \in H$, $h.R_{L,M}(\Theta)(\Omega) = 0$ car $R_{L,M}(\Theta) \in I_\Omega^L \subset I_\Omega^H$. Comme $I_\Omega^M \subset I_\Omega^H$, par la proposition 3.9, $H \subset M$. Finalement, $h \in \mathrm{Max}(I_\Omega^L)$, d'après le corollaire 3.12. □

Le groupe de décomposition de l'idéal I_Ω^L n'est pas nécessairement égal au fixateur. C'est le cas lorsque le groupe de Galois G_Ω est inclus dans le groupe de décomposition et que L est un groupe puisque L est inclus dans le groupe de décomposition. La proposition suivante donne une condition suffisante pour que cela ait lieu :

Proposition 3.15. *Si le groupe L est inclus dans le normalisateur dans $\mathfrak{S}_n$ du groupe de Galois G_Ω alors $G_\Omega \subset Gr(I_\Omega^L)$. Par conséquent, le fixateur $Max(I_\Omega^L) = G_\Omega L$ est un groupe et est identique au groupe de décomposition $Gr(I_\Omega^L)$.*

Démonstration. Supposons que L vérifie les hypothèses de la proposition 3.15. Pour $\sigma \in G_\Omega$ et $R \in I_\Omega^L$, il faut montrer que $\sigma.R \in I_\Omega^L$. Pour $l \in L$, il existe $\sigma' \in G_\Omega$ tel que $l.(\sigma.R) = l\sigma.R = \sigma' l.R$ puisque L est inclus dans le normalisateur de G_Ω. Ainsi, $l.r(\Omega) = 0$ et, par définition du groupe de Galois G_Ω, $0 = \sigma'.(l.R)(\Omega) = l.(\sigma.R(\Omega))$. La première assertion est prouvée.

Lorsque L est un groupe, le groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$ est inclus dans le fixateur $\mathrm{Max}(I_\Omega^L) = G_\Omega L$. Si, par hypothèse, G_Ω et L sont des sous-groupes du groupe $\mathrm{Gr}(I_\Omega^L)$, alors le fixateur $G_\Omega L$ est inclus dans $\mathrm{Gr}(I_\Omega^L)$. □

La proposition 3.34 donnera des conditions nécessaires et suffisantes pour que le fixateur et le groupe de décomposition soient égaux.

3.4. **Variétés.**

La détermination de la variété de l'idéal I_Ω^L, utilisera celle de l'idéal des relations symétriques qui sera rappelée dans la proposition 3.16. Notons $V(I)$ la variété dans $\hat{k}^n$ d'un idéal I de $k[x_1, \dots, x_n]$.

Proposition 3.16. *La variété de l'idéal des relations symétriques $I_f^{\mathfrak{S}_n}$ est donnée par :*

$$V(I_f^{\mathfrak{S}_n}) = \{\sigma.\Omega \mid \sigma \in \mathfrak{S}_n\} \quad . \tag{14}$$

Comme le polynôme f est séparable, son cardinal est $card(V(I_f^{\mathfrak{S}_n})) = card(\mathfrak{S}_n) = n!$.

Démonstration. Posons $\mathcal{W} := \{\sigma.\Omega \mid \sigma \in \mathfrak{S}_n\}$. Notons e_i la i-ème fonction symétrique élémentaire. Sans perte de généralité, il est possible de supposer le polynôme f unitaire qui s'écrit alors sous la forme $f(x) = x^n - e_1(\Omega)x^{n-1} + \cdots +$

$(-1)^n e_n(\Omega) = \prod_{i=1}^{n}(x-\alpha_i)$. Ainsi, $\beta \in \mathcal{W}$ si et seulement si $e_i(\beta) - e_i(\Omega) = 0$ pour tout $i \in [1, \ldots, n]$. Autrement dit, $\mathcal{W} = V(e_1 - e_1(\Omega), \ldots, e_n - e_n(\Omega))$. Comme pour $i \in [1, n]$ le polynôme $e_i - e_i(\Omega)$ appartient à l'idéal $I_f^{\mathfrak{S}_n}$, la variété $V(I_f^{\mathfrak{S}_n})$ est incluse dans $\mathcal{W}$. Réciproquement, prenons $\sigma \in \mathfrak{S}_n$ et $R \in I_f^{\mathfrak{S}_n}$. Alors $R(\sigma.\Omega) = \sigma.R(\Omega) = 0$, par définition de l'idéal $I_f^{\mathfrak{S}_n}$. D'où $\mathcal{W} \subset V(I_f^{\mathfrak{S}_n})$. □

Proposition 3.17. *Soit H un sous-ensemble du groupe symétrique $\mathfrak{S}_n$, la variété de son idéal associé est donnée par :*

$$V(I_\Omega^H) = \{\sigma.\Omega \mid \sigma \in Max(I_\Omega^H)\} \ . \tag{15}$$

En particulier, si H est un groupe

$$V(I_\Omega^H) \ = \ \{\sigma.\Omega \mid \sigma \in G_\Omega H\} \ \textit{ et aussi} \tag{16}$$

$$V(I_\Omega) \ = \ \{\sigma.\Omega \mid \sigma \in G_\Omega\} \ . \tag{17}$$

Démonstration. Un élément β de la variété $V(I_\Omega^H)$ s'exprime sous la forme $\beta = \sigma.\Omega$, où $\sigma \in \mathfrak{S}_n$, puisque $V(I_\Omega^H) \subset V(I_\Omega^{\mathfrak{S}_n})$. Soit $\sigma \in \mathfrak{S}_n$. Par définition du fixateur $\mathrm{Max}(I_\Omega^H)$, la condition $(\forall P \in I_\Omega^H)\ \sigma.P(\Omega) = 0$ est équivalente à $\sigma \in \mathrm{Max}(I_\Omega^H)$. □

3.5. **Polynôme caractéristique, polynôme minimal et résolvante.**

Soit $\Psi \in k[x_1, \ldots, x_n]$. Notons
- A_L l'anneau quotient $k[x_1, \ldots, x_n]/I_\Omega^L$;
- $\overline{\Psi}$ la classe de Ψ dans A_L ;
- $\hat{\Psi}$ l'endomorphisme de multiplication par $\overline{\Psi}$ dans A_L ;
- C_{Ψ, I_Ω^L} le polynôme caractéristique de $\hat{\Psi}$;
- M_{Ψ, I_Ω^L} le polynôme minimal de $\hat{\Psi}$.

L'idéal I_Ω^L étant radical et f étant séparable, d'après la proposition 3.17, le polynôme caractéristique s'exprime sous la forme :

$$C_{\Psi, I_\Omega^L}(T) \ = \ \prod_{\sigma \in G_\Omega L} (T - \sigma.\Psi(\Omega)) \ . \tag{18}$$

Comme l'idéal I_Ω^L est radical et que le corps k est parfait, le polynôme minimal de l'endomorphisme $\hat{\Theta}$ est la forme sans facteur carré sur k de son polynôme caractéristique :

$$M_{\Psi, I_\Omega^L}(T) \ = \ \prod_{\phi \in \{\sigma.\Psi(\Omega) \mid \sigma \in G_\Omega L\}} (T - \phi) \ . \tag{19}$$

Par l'algèbre linéaire ou la théorie de Galois, les coefficients de ces deux polynômes appartiennent au corps k.

L'intérêt du calcul de ces polynômes est qu'ils ont chacun comme facteur irréductible sur k le polynôme minimal de $\Psi(\Omega)$ sur k. Ils permettent donc de déterminer des polynômes minimaux d'idéaux. Il faudrait pouvoir calculer le polynôme minimal M_{Ψ, I_Ω^L} qui est de degré inférieur à celui du polynôme caractéristique. Dans une démarche inductive de recherche du groupe de Galois, G_Ω, le fixateur $\mathrm{Max}(I_\Omega^L)$ est connu (voir le paragraphe 5). Ainsi, le calcul du polynôme caractéristique est réalisable alors que celui du polynôme minimal ne l'est pas. L'idée est donc d'introduire un polynôme de degré inférieur à celui du polynôme caractéristique et qui puisse être calculé sans connaître le groupe de Galois G_Ω. Cet autre polynôme est défini ci-dessous :

Définition 3.18. La *résolvante (de Lagrange) par* Ψ *associée à l'idéal* I_Ω^L, notée $\mathcal{L}_{\Psi,I_\Omega^L}$, est le polynôme de $k[T]$ défini par :

$$\mathcal{L}_{\Psi,I_\Omega^L}(T) \quad = \prod_{\Phi\in G_\Omega L.\Psi} (T - \Phi(\Omega)) \quad . \tag{20}$$

Le polynôme caractéristique est une puissance de la résolvante, dont les coefficients appartiennent au corps k puisqu'il est parfait.

La résolvante a été introduite par Lagrange (voir [19]) dans le cas où $L = \mathfrak{S}_n$ et par Stauduhar (voir [22]) dans celui où L est un groupe contenant le groupe de Galois G_Ω. La définition donnée ici est plus globale. Son degré étant inférieur à celui du polynôme caractéristique, elle constitue l'outil fondamental de la théorie de Galois constructive (voir [4]).

Remarque 3. Lorsque $L = \mathfrak{S}_n$, la résolvante $\mathcal{L}_{\Psi,I_\Omega^{\mathfrak{S}_n}}$ est indépendante de l'ordre de Ω choisi pour les racines du polynôme f. Elle est appelée *résolvante absolue* et peut être aussi notée $\mathcal{L}_{\Psi,f}$.

Exemple 3.19. Soit V un I_n-invariant $\mathfrak{S}_n$-primitif. La résolvante $\mathcal{L}_{V,f}$ est la *résolvante de Galois* du polynôme f. Galois l'utilisa pour démontrer l'existence du groupe de Galois.

Exemple 3.20. Soit D_4 le groupe diédral de $\mathfrak{S}_4$ dont $\Psi = x_1x_2 + x_3x_4$ est un D_4-invariant $\mathfrak{S}_4$-primitif. La résolvante

$$\mathcal{L}_{\Psi,f} = (T - (\alpha_1\alpha_2 + \alpha_3\alpha_4))(T - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(T - (\alpha_1\alpha_4 + \alpha_2\alpha_4))$$

est connue sous le nom de *résolvante diédrale* du polynôme f.

Définition 3.21. Si Ψ est un H-invariant L-primitif alors la résolvante $\mathcal{L}_{\Psi,I_\Omega^L}$ est appelée une *H-résolvante L-relative de* Ω.

Remarque 4. Soit Ψ_H un H-invariant L-primitif. L'invariant Ψ_H est L-séparable pour Ω si et seulement si $\Psi_H(\Omega)$ est une racine simple de la résolvante $\mathcal{L}_{\Psi_H,I_\Omega^L}$. Dans ce cas, le polynôme minimal de $\Psi_H(\Omega)$ sur k est un facteur (irréductible) simple de la résolvante $\mathcal{L}_{\Psi_H,I_\Omega^L}$. Si Ψ_H est H-séparable pour Ω (le groupe H suffit) alors

$$\mathcal{L}_{\Psi_H,I_\Omega^H} = M_{\Psi_H,I_\Omega^H} = \mathrm{Min}_{\Psi_H(\Omega),k} \quad .$$

Lemme 3.22. *Soit Ψ_L un L-invariant M-primitif et $\psi_L = \Psi_L(\Omega)$. Alors le polynôme minimal de l'endomorphisme $\hat{\Psi}_L$ de A_L et le polynôme minimal de ψ_L sur k sont identiques :*

$$M_{\Psi_L,I_\Omega^L} = Min_{\psi_L,k} = \prod_{\phi\in G_\Omega\star\psi_L} (T - \phi) \quad . \tag{21}$$

Démonstration. Évidente. □

Lemme 3.23. *Soit $\Psi \in k[x_1, \ldots, x_n]$ et $\psi := \Psi(\Omega)$. Alors*

$$Min_{\psi,k} = M_{\Psi,I_\Omega} \quad .$$

Démonstration. Évidente. □

3.6. Générateurs de l'idéal I_Ω^L.

Rappelons que M et L sont deux sous-groupes de $\mathfrak{S}_n$ tels que M contienne le groupe L et le groupe de Galois G_Ω. Le polynôme Θ est un L-invariant M-primitif séparable pour Ω et $\theta = \Theta(\Omega)$. Le polynôme minimal de θ sur k est un facteur irréductible simple sur k de la résolvante M-relative $\mathcal{L}_{\Theta, I_\Omega^M}$.

Notation 3.24. Pour un ensemble $E \subset k[x_1, \ldots, x_n]$, l'idéal engendré par E dans $k[x_1, \ldots, x_n]$ sera noté $< E >$.

Dans [6], il est montré que l'idéal I_Ω^M est engendré par un système triangulaire séparable de n polynômes. À partir de ces générateurs, il est aisé de calculer des résolvantes M-relatives. Ce paragraphe propose une méthode explicite pour calculer, sous certaines conditions, un système de générateurs de l'idéal I_Ω^L.

Le résultat connu jusqu'alors s'applique au cas où $L = G_\Omega$ (voir [3]) : Si Ψ est un G_Ω-invariant $\mathfrak{S}_n$-primitif séparable pour Ω alors

$$I_\Omega = I_\Omega^{\mathfrak{S}_n} + < \Psi - \Psi(\Omega) > = I_\Omega^M + < \Psi - \Psi(\Omega) > \quad .$$

Le lemme suivant donne une première approche du résultat cherché :

Lemme 3.25. *Soit F un polynôme M-primitif de l'idéal I_Ω^L. Nous avons l'identité suivante:*

$$I_\Omega^{G_\Omega L} = I_\Omega^L = \sqrt{I_\Omega^M + < F >} \quad . \tag{22}$$

Démonstration. Nous avons $I_\Omega^L = \sqrt{I_\Omega^M + < F >}$ puisque les variétés sont identiques et que l'idéal I_Ω^L est radical. □

Lemme 3.26. *Si $Q \in k[x_1, \ldots, x_n]^M$ alors $Q = Q(\Omega) \mod I_\Omega^M$ et $Q(\Omega) \in k$.*

Démonstration. Puisque $G_\Omega \subset M$. □

Théorème 3.27. *Supposons que $f \in k[x]$ soit un polynôme séparable de degré n. Soient L et M deux sous-groupes du groupe symétrique $\mathfrak{S}_n$ vérifiant*

$$G_\Omega \subset Gr(I_\Omega^L) \subset M \quad ,$$

où $Gr(I_\Omega^L)$ est le groupe de décomposition de l'idéal I_Ω^L. Soit F un polynôme M-primitif de l'idéal I_Ω^L (i.e. $G_\Omega L = \{\sigma \in M \mid \sigma.F(\Omega) = 0\}$). Alors

$$I_\Omega^L = I_\Omega^M + < F > \quad . \tag{23}$$

En particulier, si $L \subset G_\Omega$ alors

$$I_\Omega = I_\Omega^L = I_\Omega^M + < F > \quad . \tag{24}$$

Démonstration. Si le théorème est vrai dans le cas où $\mathrm{Gr}(I_\Omega^L) = L$ alors il l'est également pour tout groupe L vérifiant les hypothèses du théorème puisque $I_\Omega^L = I_\Omega^{\mathrm{Gr}(I_\Omega^L)}$. Nous pouvons donc supposer que $\mathrm{Gr}(I_\Omega^L) = L$, et donc $L = G_\Omega L$ puisque G_Ω est supposé être un sous-groupe du groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$.

Choisissons des permutations $\tau_1 = id, \ldots, \tau_e$ constituant une transversale à droite $M \mod L$, et posons

$$I := I_\Omega^L \ \text{ et } \ J := \bigcup_{i=2}^{e} I_\Omega^{L\tau_i} = I_\Omega^{\bigcap_{i=2}^{e} L\tau_i} \quad .$$

D'après le lemme 3.28, les idéaux I et J sont comaximaux puisque les idéaux $I_\Omega^{L\tau_1},\dots,I_\Omega^{L\tau_e}$ sont deux à deux comaximaux. Par ailleurs, un polynôme g est un polynôme M-primitive de I_Ω^L si et seulement si $g\in I\backslash J$.

D'après le lemme 3.25, il existe un entier $l>0$ vérifiant :

$$I^l\subset I_\Omega^M+<F>\subset I \quad .$$

Comme les idéaux I et J sont comaximaux, les idéaux I^l et J le sont aussi. Maintenant, prenons x dans I. Il existe donc $u\in I^l$ et $v\in J$ tels que

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

Nous avons $xu\in I_\Omega^M+<F>$ et $xv\in IJ=M$ car les idéaux $I_\Omega^{L\tau_1},\dots,I_\Omega^{L\tau_e}$ sont deux à deux comaximaux et donc

$$IJ=\prod_{i=1}^{e} I_\Omega^{L\tau_i}=\bigcap_{i=1}^{e} I_\Omega^{L\tau_i}=M \quad .$$

□

Lemme 3.28. *Sous les hypothèses du théorème 3.27, choisissons $\tau_1,\dots,\tau_e$ une transversale à droite de $M \mod L$ et supposons que L vérifie $G_\Omega L=L$. Lorsque le polynôme f est séparable, les idéaux $I_\Omega^{L\tau_1},\dots,I_\Omega^{L\tau_e}$ sont deux à deux comaximaux.*

Démonstration. Soient $i,j\in[1,n]$. La variété de chaque l'idéal $I_\Omega^{L\tau_i}$ est donnée par

$$V(I_\Omega^{L\tau_i})=\{\sigma.\Omega \mid \sigma\in L\}$$

puisque $G_\Omega L=L$. Lorsque le polynôme f est séparable, nous avons $V(I_\Omega^{L\tau_i}+I_\Omega^{L\tau_j})=V(I_\Omega^{L\tau_i})\bigcap V(I_\Omega^{L\tau_j})=\emptyset$. Les idéaux $I_\Omega^{L\tau_i}$ et $I_\Omega^{L\tau_j}$ sont donc comaximaux. □

Nous en déduisons le corollaire suivant :

Corollaire 3.29. *Sous les hypothèses du théorème 3.27, nous considérons un sous-groupe H du groupe M. Alors la conditions $I_\Omega^H=I_\Omega^M+<F>$ est équivalente à $L\subset G_\Omega H=G_\Omega L$.*

Démonstration. Triviale puisque chacune des conditions est équivalente à $I_\Omega^H=I_\Omega^L$. □

La proposition ci-dessous donne des conditions nécessaires et suffisantes dans lesquelles le groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$ contient le groupe de Galois G_Ω.

Proposition 3.30. *Il existe un groupe G tel que $I_\Omega^G=I_\Omega^L$ et G contient le groupe de Galois G_Ω si et seulement si l'une des conditions équivalentes suivantes est vérifiée :*
(i) $G_\Omega L$ est un groupe ;
(ii) $LG_\Omega\subset G_\Omega L$;
(iii) $Gr(I_\Omega^L)=G_\Omega L$;
(iv) $G_\Omega\subset Gr(I_\Omega^L)$.
En particulier, lorsque G_Ω est un sous-groupe de L, G_Ω est aussi un sous-groupe du groupe de décomposition $Gr(I_\Omega^L)$.

Démonstration. Comme $\mathrm{Gr}(I_\Omega^L)$ contient tous les groupes G tels que $I_\Omega^G=I_\Omega^L$, l'hypothèse de la proposition est équivalente à (iv).

Prouvons que (i) est équivalente à (ii). Si (i) est vérifiée, le groupe $G_\Omega L$ est stable par composition et contient le groupe de Galois G_Ω. Ainsi $(G_\Omega L)G_\Omega\subset G_\Omega L$ et comme G_Ω est un groupe alors $LG_\Omega\subset G_\Omega L$ et (ii) est vraie. Réciproquement, si (ii) est vérifiée, alors (i) aussi puisque $(G_\Omega L)(G_\Omega L)\subset G_\Omega(G_\Omega L)L\subset G_\Omega L$.

Supposons que (iv) soit vérifiée et montrons qu'alors (iii) l'est également. Comme $L \subset \mathrm{Gr}(I_\Omega^L)$, le fixateur $G_\Omega L$ est inclus dans $G_\Omega \mathrm{Gr}(I_\Omega^L)$ qui lui-même est identique au groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$, d'après (iv). L'assertion (iii) est donc vraie puisque l'inclusion inverse est vérifiée dès que L est un groupe.

Pour les autres équivalences, voir la proposition 3.6. □

Remarque 5. La proposition 3.15 donne une condition suffisante pour que $G_\Omega L$ soit un groupe. Nous connaissons maintenant des conditions nécessaires et suffisantes.

3.7. **Construction de l'idéal des relations I_Ω.**

Il s'agit de préparer l'algorithme aboutissant au calcul d'un système de générateurs de l'idéal I_Ω des Ω-relations.

Un idéal I_Ω^L sera dit *connu* lorsqu'un système de générateurs de cet idéal a pu être déterminé à partir du polynôme f.

Exemple 3.31. L'idéal $I_\Omega^{\mathfrak{S}_n}$ est connu. Les polynômes $e_1 - e_1(\Omega), \ldots, e_n - e_n(\Omega)$ forment un système de générateurs bien connu de l'idéal $I_\Omega^{\mathfrak{S}_n}$. De plus, les n polynômes appelés *modules de Cauchy du polynôme f* forment une base de Gröbner réduite pour l'ordre lexicographique de l'idéal des relations symétriques (voir [9]).

Il existe des chaînes croissantes finies d'idéaux :

$$I_\Omega^{\mathfrak{S}_n} = I_1 \subset I_2 \subset \cdots \subset I_m = I_\Omega$$

où chaque idéal I_j $(j \in [1, m])$ est un idéal de la forme I_Ω^H avec H un sous-ensemble de $\mathfrak{S}_n$.

L'idée est de construire une telle chaîne par le calcul inductif de systèmes de générateurs des idéaux $I_2, \ldots, I_m$. Le théorème 3.27 sera utilisé pour calculer un système de générateurs des idéaux I_Ω^H.

Considérons M notre sous-groupe de $\mathfrak{S}_n$ contenant le groupe de Galois G_Ω et un sous-groupe L de $\mathfrak{S}_n$. Le groupe M vérifie donc les hypothèses du théorème 3.27. Supposons que l'idéal I_Ω^M soit connu. Au départ, le seul idéal connu qui contienne le groupe de Galois est l'idéal des relations symétriques, $I_f^{\mathfrak{S}_n}$.

La situation est la suivante :

$$I_f^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset \cdots \subset I_\Omega \quad . \tag{25}$$

Il faut chercher les conditions (minimales) dans lesquelles la construction de cette chaîne d'idéaux peut être poursuivie jusqu'à connaître l'idéal des Ω-relations. La condition minimale est que le groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$ contienne le groupe de Galois G_Ω. Ainsi, si nous savons calculer F un polynôme M-primitif de l'idéal I_Ω^L alors, d'après le théorème 3.27,

$$I_\Omega^L = I_\Omega^M + < F >$$

et, de plus, $\mathrm{Gr}(I_\Omega^L)$ peut remplacer le groupe M.

Remarque 6. Rappelons que Θ est un L-invariant M-primitif *séparable* pour Ω et que

$$R_{L,M} := \mathrm{Min}_{\Theta(\Omega),k}(\Theta) \quad .$$

Le polynôme $R_{L,M}$ est un polynôme M-primitif de l'idéal I_Ω^L (voir Définition 3.11). Le polynôme minimal $\mathrm{Min}_{\Theta(\Omega),k}$ de $\Theta(\Omega)$ sur k est un facteur irréductible (simple) de la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$. L'idéal I_Ω^M étant connu, cette résolvante est calculable (voir [6]).

D'après la proposition 3.30, si le fixateur $G_\Omega L$ n'est pas un groupe (i.e. $\mathrm{Gr}(I_\Omega^L)$ ne contient pas le groupe de Galois), il n'est pas possible de poursuivre la construction en remplaçant l'idéal I_Ω^M par l'idéal I_Ω^L. Le proposition suivante permet de tester cette condition dans certains cas particuliers :

Proposition 3.32. *Soit Θ un L-invariant M-primitif séparable pour Ω. Les conditions suivantes sont équivalentes :*

(i) $I_\Omega^L = I_\Omega^M$

(ii) $G_\Omega L = M$*; et dans ce cas,* $Gr(I_\Omega^L) = G_\Omega L$*;*

(iii) la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ *est irréductible sur* k*; et dans ce cas, elle est égale à* $Min_{\Theta(\Omega),k}$.

Supposons que L soit un sous-groupe maximal du groupe M. Il existe un groupe H conjugué du groupe L dans M tel que $G_\Omega H$ soit un groupe si, et seulement si, une des conditions suivante est vérifiée :

(a) la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ *est irréductible sur k ; et, dans ce cas,* $Gr(I_\Omega^L) = G_\Omega L = M$*;*

(b) la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ *a un facteur linéaire dans* $k[x]$.

Démonstration. Prouvons d'abord les trois premières équivalences. Si $I_\Omega^L = I_\Omega^M$ alors $G_\Omega L = G_\Omega M = M$ (et $\mathrm{Gr}(I_\Omega^L) = \mathrm{Gr}(I_\Omega^M) = M$). Réciproquement, si $G_\Omega L = M$ alors, par définition du fixateur, $I_\Omega^L = I_\Omega^M$. Donc (i) est équivalente à (ii). Si $G_\Omega L = M$ alors

$$\mathcal{L}_{\Theta, I_\Omega^M} = \mathcal{L}_{\Theta, I_\Omega^L} = \mathrm{Min}_{\Theta(\Omega),k}$$

car Θ est M-séparable pour Ω. Réciproquement, si (iii) est vraie alors

$$G_\Omega \star \Theta(\Omega) = \{\Psi(\Omega) \mid \Psi \in M.\Theta\} \ .$$

Soit $m \in M$. Il existe $g_m \in G_\Omega$ tel que $g_m.\Theta(\Omega) = m.\Theta(\Omega)$. Comme $g_m^{-1} \in G_\Omega$, $g_m^{-1}m.\Theta(\Omega) = \Theta(\Omega)$. Nous avons $m \in G_\Omega L$ puisque le polynôme L-invariant M-primitif Θ est M-séparable pour Ω et que $g_m^{-1}m \in M$. D'où $G_\Omega L = M$ puisque l'inclusion inverse est toujours vraie. En conclusion, (ii) est équivalente à (iii).

Maintenant, supposons que L est un sous-groupe maximal du groupe M.

Nous savons que l'égalité $\mathrm{Gr}(I_\Omega^G) = G_\Omega G = M$ est équivalente à (a) pour tout sous-groupe G de M.

Supposons donc que $\mathrm{Gr}(I_\Omega^L) = G_\Omega L \neq M$. Comme $L \subset \mathrm{Gr}(I_\Omega^L) \subset M$ et L est un sous-groupe maximal de M, $L = \mathrm{Gr}(I_\Omega^L) = G_\Omega L$. Donc $G_\Omega \subset L$ et (b) est vérifiée. Réciproquement, si (b) est vraie alors $G_\Omega \subset \tau L \tau^{-1}$ avec $\tau \in M$ (voir Lemme 3.7). □

Dans le cas où L n'est pas un sous-groupe maximal du groupe M, si la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ est réductible sur k et n'a pas de facteur linéaire dans $k[x]$ alors il n'est pas possible de tester si l'un des conjugués de L dans M vérifie l'hypothèse du théorème 3.27 (i.e. l'une des conditions de la proposition 3.30). Omettons ce problème pour le moment et travaillons sur les facteurs irréductibles sur k de la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$.

Soient $\tau_1, \dots, \tau_e$ des permutations d'une transversale à gauche de $M \mod L$ telles que :

- $\mathcal{O} := (\tau_1.\Theta, \dots, \tau_e.\Theta)$ soit la G_Ω-orbite de l'invariant Θ et

- $\mathcal{L} = (\tau_1 L, \dots, \tau_e L)$ soit la G_Ω-orbite du groupe L dans $(M/L)_g$, l'ensemble des classes à gauche de $M \mod L$

(la correspondance entre ces deux ensembles est dans [7]). Les e éléments distincts (car Θ est séparable pour Ω) de $\hat{k}$ contenus dans

$$\mathcal{O}(\Omega) = (\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega))$$

sont les conjugués de $\theta = \Theta(\Omega)$ sur k (i.e. les racines du polynôme minimal de θ sur k) et la G_Ω-orbite de θ est donc :

$$G_\Omega \star \theta = \mathcal{O}(\Omega) = (\tau_1.\Theta(\Omega), \ldots, \tau_e.\Theta(\Omega)) \ .$$

Notons S le sous-groupe de M ainsi défini :

$$S := \mathrm{Stab}_M(\mathcal{O}) = \mathrm{Stab}_M(\mathcal{L}) = \mathrm{Stab}_M(G_\Omega L) \ .$$

Dans [3], avec $M = \mathfrak{S}_n$ il est prouvé que :

$$G_\Omega \subset S \subset \bigcup_{i=1}^{e} \tau_i L = \bigcup_{L_i \in \mathcal{L}} L_i \ .$$

Le lemme suivant étend ce résultat à tout groupe M contenant le groupe de Galois G_Ω.

Lemme 3.33. *Soient L un sous-groupe de $\mathfrak{S}_n$ et $S = Stab_M(G_\Omega L)$. Alors*

$$G_\Omega \subset S \subset G_\Omega L \quad \textit{et donc}$$

$$I_\Omega^L = I_\Omega^{G_\Omega L} \subset I_\Omega^S \subset I_\Omega \ . \tag{26}$$

Nous avons $L \subset Gr(I_\Omega^L) \subset G_\Omega L$ et $S = Gr(I_\Omega^S) = G_\Omega S = Max(I_\Omega^S)$ puisque $G_\Omega S$ est un groupe.

Démonstration. Comme l'ensemble $\mathcal{L}$ est stable sous l'action du groupe de Galois G_Ω, $G_\Omega \subset S$. Et $S \subset G_\Omega L$ car $SL \subset SG_\Omega L \subset G_\Omega L$ et L est un groupe. □

Avec le groupe S, nous pouvons compléter la proposition 3.30 pour tester si, dans la construction inductive de la chaîne (25), le groupe M peut être remplacé par le groupe de décomposition $\mathrm{Gr}(I_\Omega^L)$:

Proposition 3.34. *Le fixateur $G_\Omega L$ est un groupe si et seulement si une des conditions équivalentes suivantes est vérifiée :*

(i) $L \subset S$;

(ii) $I_\Omega^L = I_\Omega^S$;

(iii) $G_\Omega L = S$;

(iv) $S = Gr(I_\Omega^L)$.

Démonstration. Évidente. □

Remarque 7. Lorsque l'ensemble $\mathcal{L}$ est réduit à un élément alors le groupe L contient le groupe de Galois. Donc $G_\Omega L = L$ est un groupe et $L = S$. Pour le vérifier, il suffit de prouver que $\Theta(\Omega) \in k$. Mais il se peut que $G_\Omega L$ soit un groupe sans que les groupes L et S soient égaux. En effet, supposons que f ne se factorise pas entièrement sur k (G_Ω est donc différent du groupe identité). Prenons pour L le groupe identité I_n. Alors $I_\Omega^L = I_\Omega^{G_\Omega} = I_\Omega$ et $S = G_\Omega \neq L$.

Cette remarque nous amène à la proposition suivante utilisée comme test d'arrêt de la construction de la chaîne (25) :

Proposition 3.35. *Les conditions suivantes sont équivalentes :*

(i) $G_\Omega = S = G_\Omega L$ *;*

(ii) $L \subset G_\Omega$ *;*

(iii) $I_\Omega = I_\Omega^M + < R_{L,M} >$ *.*

(L'équivalence entre (i) et (iii) est démontrée dans [3] *dans le cas où* $S = \mathfrak{S}_n$*.)*

Démonstration. Soit F un polynôme M-primitive de l'idéal I_Ω^L. La condition $G_\Omega L = \mathrm{Max}(I_\Omega^L) = G_\Omega$ est équivalente à

$$I_\Omega = I_\Omega^L = I_\Omega^M + < F >$$

qui est elle-même équivalente à $L \subset G_\Omega$ (voir Corollaire 3.29). □

Remarque 8. Avec V un I_n-invariant primitif séparable pour Ω, l'idéal des Ω-relations s'obtient en une étape :

$$I_\Omega = I_f^M + < \mathrm{Min}_{V(\Omega),k}(V) > \quad . \tag{27}$$

Mais le problème est de calculer la *résolvante de Galois* $\mathcal{L}_{V,I_\Omega^M}$ de degré card(M) dont le polynôme minimal de $V(\Omega)$ sur k est un facteur (irréductible) simple sur k. Au départ comme $M = \mathfrak{S}_n$, la résolvante de Galois est de degré $n!$.

À partir de l'idéal I_Ω^L, nous avons trouvé un groupe S contenant le groupe de Galois et permettant de poursuivre (théoriquement) notre construction d'une chaîne croissante d'idéaux :

$$I_\Omega^M \subset I_\Omega^L \subset I_\Omega^S = I_\Omega^M + < R_{S,M} > \subset \cdots \subset I_\Omega \quad , \tag{28}$$

pour tout polynôme M-primitif $R_{S,M}$ de l'idéal I_Ω^S. Posons $A_G = k[x_1, \ldots, x_n]/I_\Omega^G$ pour tout sous-ensemble G de $\mathfrak{S}_n$. Cette chaîne se traduit ainsi sur ces algèbres :

$$A_{\mathfrak{S}_n} \supset A_M \quad \supset \quad A_S \supset A_{G_\Omega} \cong k(\Omega) \quad ,$$

avec d'après les inclusions de (28) et l'article [26] :

$$A_S \quad = \quad k[x_1, \ldots, x_n]/(I_\Omega^M + < R_{S,M} >) \cong A_M/\hat{R}_{S,M} A_M \quad .$$

Nous constatons que les polynômes primitifs des idéaux jouent également des rôles d'éléments primitifs des algèbres associées.

Si l'une des conditions de la proposition 3.34 est vérifiée alors le groupe S est identique au fixateur $G_\Omega L$ de l'idéal I_Ω^L et

$$I_\Omega^L = I_\Omega^S = I_\Omega^M + < R_{L,M} > \quad .$$

Sinon, il reste encore à calculer un polynôme M-primitif $R_{S,M}$ de l'idéal I_Ω^S.

Soit $\Theta_{S,M}$ un S-invariant M-primitif séparable pour Ω. Comme le polynôme minimal de $\Theta_{S,M}(\Omega)$ sur k est $T - \Theta_{S,M}(\Omega)$ (le groupe de Galois G_Ω est inclus dans le groupe S), le polynôme

$$R_{S,M} := \Theta_{S,M} - \Theta_{S,M}(\Omega)$$

est un polynôme M-primitif de l'idéal I_Ω^S. Pour calculer un S-invariant M-primitif, A. Colin propose de choisir pour $\Theta_{S,M}$ une fonction symétrique sur $\mathcal{O}$, la G_Ω-orbite de l'invariant Θ (voir [11]). Le calcul de $\Theta_{S,M}(\Omega)$ est alors réalisé avec le théorème fondamental des fonctions symétriques appliqué aux racines du polynôme $\mathrm{Min}_{\theta,k}$ (voir [24] pour les calculs de polynômes symétriques). Il existe nécessairement une fonction symétrique élémentaire ou une fonction symétrique puissance qui soit M-séparable pour Ω (voir [20]).

Nous avons en théorie une méthode pour construire une chaîne croissante d'idéaux partant de l'idéal $I_\Omega^{\mathfrak{S}_n}$ et arrivant à l'idéal I_Ω. Mais il faut savoir identifier le groupe S sans connaître le groupe de Galois G_Ω. Avec la remarque 7, nous savons que $S = L$ si $T - \theta$ est un facteur simple sur k de la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$. En dehors de ce cas, nous n'avons aucun moyen d'identifier le groupe S. L'algorithme effectif de calcul de l'idéal I_Ω du paragraphe 5 introduira l'utilisation des matrices de groupes. Ces matrices permettent non seulement de calculer le groupe G_Ω (et donc l'idéal I_Ω) plus rapidement mais aussi de remplacer le groupe S par un autre groupe qui est calculable.

4. Matrices de groupes et de partitions

Dans [4] et [25] sont définies les *matrices de groupes et de partitions*. Ces matrices permettent toujours de calculer le groupe de Galois d'un polynôme à partir des degrés ou des groupes des facteurs simples irréductibles sur k des résolvantes. Leur utilisation est brièvement rappelée dans ce paragraphe.

Soit la résolvante $F = \mathcal{L}_{\Psi, I_\Omega^M}$ où M contient le groupe de Galois et un groupe H de $\mathfrak{S}_n$ et Ψ est un H-invariant M-primitif. Il est montré que les degrés et les groupes de Galois sur k des facteurs simples irréductibles sur k de la résolvante F ne dépendent que des classes de conjugaison des groupes H et G_Ω dans M. Les formules permettant de calculer ces groupes et ces degrés sont aisées à programmer dans un logiciel comme `GAP` (voir [15]). Donnons une définition (qui est en fait un théorème) de ces matrices :

Définition 4.1. La matrice *de groupes (resp. de partitions) relative au groupe M* est la matrice telle que :
1- les lignes et les colonnes sont indicées par toutes les classes de conjugaison de sous-groupes de M ; les classes de conjugaison des lignes sont appelées les *classes candidates* et celles des colonnes les *classes tests* ; le groupe M est appelé quant à lui le *groupe de référence* ;
2- soient $\mathcal{G}$ et $\mathcal{H}$ deux classes de conjugaison dans M de deux sous-groupes G et H de M ; soient Ψ un H-invariant M-primitif et g un polynôme de $k[x]$ tel que $G = G_{\Omega_g}$ (si g existe) ; alors à l'intersection de la ligne de $\mathcal{G}$ et de la colonne de $\mathcal{H}$ se trouve la liste des groupes de Galois sur k (resp. des degrés) des facteurs irréductibles de la résolvante $\mathcal{L}_{\Psi,k}$ si elle est séparable.

Si la résolvante n'est pas séparable, la définition s'applique aux facteurs simples de la résolvante.

Comme il est montré dans [4], les lignes de la matrice de partitions (et donc de groupes) étant toutes distinctes, il est toujours possible de déterminer le groupe de Galois d'un polynôme avec ces matrices. La méthode consiste à utiliser les classes tests pour éliminer des classes candidates. Supposons que l'on ait déterminé un groupe M contenant le groupe de Galois. Ou bien les calculs sont toujours effectués avec le même groupe de référence M et la même matrice de groupes (resp. partitions) relative à M, ou bien, si un sous-groupe S de M est déterminé comme contenant le groupe de Galois G_Ω, il est possible de prendre S comme nouveau groupe de référence. Le choix de changement de groupe de référence est dépendant des temps de calculs. Au départ, le groupe de référence est $\mathfrak{S}_n$ qui est le seul groupe M contenant de façon certaine le groupe de Galois et tel que l'idéal I_Ω^M soit connu.

5. Construction de l'idéal des relations : algorithme

5.1. Préparation de l'algorithme.

Dans la pratique, nous combinons la recherche du groupe de Galois par la méthode des matrices de groupes et de partitions avec celle de l'idéal des relations. Nous n'utiliserons en fait que les matrices de groupes qui incluent les informations des matrices de partitions.

Dans le paragraphe 3.7 nous avions une méthode théorique pour construire l'idéal des Ω-relations nécessitant le calcul impossible d'une G_Ω-orbite. Nous cherchons à contourner cette difficulté.

Nous supposons toujours que nous avons déterminé un groupe M contenant le groupe de Galois G_Ω et que nous connaissons un système de générateurs de l'idéal I_Ω^M. Nous avons choisi un sous-groupe L du groupe M et nous avons calculé la résolvante $F = \mathcal{L}_{\Theta, I_\Omega^M}$ où Θ est un L-invariant M-primitif séparable pour Ω.

Nous supposons également disposer d'un ensemble $\mathcal{S}_M$ de groupes candidats à être le groupe de Galois (un par classe de conjugaison dans M). Par exemple, lorsque $M = \mathfrak{S}_n$ et qu'aucune résolvante n'a été calculée, l'ensemble $\mathcal{S}_{\mathfrak{S}_n}$ contient toutes les classes de conjugaison de sous-groupes de $\mathfrak{S}_n$. Le groupe de Galois étant contenu dans le groupe M, tous les groupes non inclus dans M n'appartiennent pas à $\mathcal{S}_M$.

La matrice de groupes relative au groupe M et la factorisation de la résolvante $F = \mathcal{L}_{\Theta, I_\Omega^M}$ éliminent des groupes candidats de l'ensemble $\mathcal{S}_M$. Elles déterminent donc un sous-ensemble $\mathcal{S}$ de l'ensemble $\mathcal{S}_M$ de groupes étant encore candidats à être le groupe de Galois G_Ω.

Soit G le plus petit sous-groupe de M contenant l'union des groupes de l'ensemble $\mathcal{S}$ et H l'intersection des groupes de $\mathcal{S}$:

$$G = < \bigcup_{H' \in \mathcal{S}} H' > \ \text{ et } H = \bigcap_{H' \in \mathcal{S}} H' \ .$$

Comme l'ensemble $\mathcal{S}$ est connu, les groupes G et H le sont également et ils vérifient :

$$H \subset G_\Omega \subset G \ .$$

Un des tests d'arrêt de l'algorithme applique l'identité (24) à un sous-groupe H' quelconque du groupe H dès qu'une H'-résolvante sera calculable : $I_\Omega = I_\Omega^{H'} + < R_{H',M} >$. Si aucun sous-groupe du groupe H ne permet de stopper l'algorithme, nous poursuivons notre construction pour nous approcher de l'idéal des Ω-relations.

Remarque 9. Le groupe G étant connu et contenant le groupe de Galois, nous pouvons être tentés de lui appliquer le théorème 3.27 et de remplacer le groupe M par le groupe G. Mais en ce cas, nous devons calculer une G-résolvante M-relative et n'exploitons pas jusqu'au bout la résolvante F déjà calculée. A moins qu'une G-résolvante M-relative puisse se calculer rapidement, ce n'est pas G qui sera choisi pour continuer la construction.

Reprenons l'idée de la section 3.7. Comme les groupes G et L sont connus, l'ensemble $GL = \{gl \mid g \in G \ , l \in L\}$ l'est également et il est possible de calculer le groupe $\mathrm{Stab}_M(GL)$, le stabilisateur de GL dans le groupe M. Posons

$$S' = \mathrm{Stab}_M(GL) \ .$$

Le groupe S' contient le groupe de Galois G_Ω (voir la figure (29)). Il est donc possible de lui appliquer le théorème 3.27 et si F est un polynôme M-primitif de l'idéal $I_\Omega^{S'}$ alors

$$I_\Omega^{S'} = I_\Omega^M + < F > \quad .$$

Voyons si le groupe $S = \mathrm{Stab}_M(G_\Omega L)$ du paragraphe 3.7, qui n'est pas toujours calculable, peut être remplacé par le groupe S' qui lui l'est. La situation du point de vue des groupes est la suivante :

$$\begin{array}{ccccccc} L & \subset & G_\Omega L & \subset & GL & \subset & M \\ & & \cup & & \cup & & \\ & & S = \mathrm{Stab}_M(G_\Omega L) & \subset & S' = \mathrm{Stab}_M(GL) & & \\ & & \cup & & \cup & & \\ H & \subset & G_\Omega & \subset & G & & \end{array} \tag{29}$$

où H, G, L, M et S' sont des groupes connus. Les chaînes d'idéaux que nous considérons sont donc les suivantes :

$$I_\Omega^{\mathfrak{S}_n} \subset \cdots \subset I_\Omega^M \subset I_\Omega^{S'} \subset I_\Omega^G \subset \cdots \subset I_\Omega = I_\Omega^H \quad .$$

Regardons maintenant ce qui se passe du côté des polynômes afin de pouvoir calculer un polynôme M-primitif de l'idéal $I_\Omega^{S'}$ comme nous l'avons fait pour l'idéal I_Ω^S au paragraphe 3.7.

Soit $G.L$ la G-orbite de L dans $(M/L)_g$:

$$G.L = \{\tau_1 L, \ldots, \tau_s L\} \quad .$$

Nous définissons alors le polynôme

$$W(T) = \prod_{i=1}^{s} (T - \tau_i.\Theta(\Omega)) \quad . \tag{30}$$

Comme $G_\Omega \subset G \subset M$, ce polynôme est un facteur de la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ et ses coefficients, invariants par le groupe G et donc par G_Ω, appartiennent au corps k. Puisque l'invariant Θ est M-séparable pour Ω :

$$\mathcal{L}_{\Theta, I_\Omega^L} = \prod_{\Psi \in G_\Omega L.\Theta} (T - \Psi(\Omega)) = \mathcal{L}_{\Theta, I_\Omega} = M_{\Theta, I_\Omega} = \mathrm{Min}_{\Theta(\Omega), k} \quad . \tag{31}$$

Nous savons que $G_\Omega L \subset GL$. Donc la résolvante $\mathcal{L}_{\Theta, I_\Omega^L}$ est un facteur irréductible (simple) sur k du polynôme W. Mais si GL et $G_\Omega L$ ne sont pas identiques alors le polynôme W est différent de la résolvante $\mathcal{L}_{\Theta, I_\Omega^L}$ et n'est donc pas irréductible. Le fixateur $G_\Omega L$ n'est pas nécessairement égal à l'ensemble GL comme le montre l'exemple ci-dessous.

Exemple 5.1. Supposons que les groupes G et M soient égaux et que donc $GL = M$. Si $M = GL = G_\Omega L$, alors

$$\mathcal{L}_{\Theta, I_\Omega^M} = \mathcal{L}_{\Theta, I_\Omega^L} = \mathrm{Min}_{\Theta(\Omega), k}$$

d'après (31). Cette situation n'arrive que si la résolvante $\mathcal{L}_{\Theta, I_\Omega^M}$ est irréductible. Dans ce cas le fixateur $G_\Omega L$ est un groupe qui agit transitivement sur les classes à gauche $(M/L)_g$. Or, si le groupe test L est mal choisi, il peut n'apporter aucune information (i.e. $G = M$) sans que les L-résolvantes M-relatives séparables soient irréductibles sur le corps k.

Donc l'orbite $G.L$ est connue et elle correspond à un facteur W sur k de la résolvante $\mathcal{L}_{\Theta,I_\Omega^M}$. Le stabilisateur de l'orbite $G.L$ est connu. Il reste à identifier le polynôme W à partir de la résolvante F. Dans le cas où les degrés ou les groupes de Galois des facteurs de la résolvante F n'apportent rien, il est possible d'utiliser la proposition 5.2 :

Proposition 5.2. *Supposons que la résolvante $\mathcal{L}_{\Theta,I_\Omega^M}$ soit séparable. Soit V un facteur de la résolvante $\mathcal{L}_{\Theta,I_\Omega^M}$. La condition $V = W$ est équivalente à $V(\Theta) \in I_\Omega^G$.*

Démonstration. Par définition de W, nous avons $W(\Theta) \in I_\Omega^G$. Supposons que $V(\Theta) \in I_\Omega^G$. Alors $(\forall \tau \in G)\ V(\tau.\Theta(\Omega)) = 0$ et il existe donc un entier $i \in [1, e]$ vérifiant $\tau.\Theta(\Omega) = \tau_i.\Theta(\Omega)$. Comme $\tau_i.\Theta(\Omega)$ est une racine simple de la résolvante, nous avons $\tau.\Theta = \tau_i.\Theta$. Comme $\tau_i^{-1}\tau \in M$ et Θ est un L-invariant M-primitif, $\tau_i \in \tau L$. Finalement $\tau_i \in GL$. □

Maintenant un polynôme M-primitif de l'idéal $I_\Omega^{S'}$ est calculable à partir du polynôme W de la même manière qu'un polynôme M-primitif de l'idéal I_Ω^S est calculable à partir du polynôme $\mathrm{Min}_{\theta,k}$ (voir le paragraphe 3.7).

Nous disposons désormais de tous les éléments pour décrire notre algorithme de construction de l'idéal des Ω-relations.

5.2. **L'algorithme `GaloisIdéal`.**

L'algorithme `GaloisIdéal` est présenté sous la forme d'une fonction récursive. Il sera exécuté avec l'appel

`GaloisIdéal(f,n,`$\mathfrak{S}_n$`,Generateurs,Candidats)`

où
- `n` est le degré n du polynôme f représenté par `f`;
- `Generateurs` est une liste qui contient le groupe symétrique $\mathfrak{S}_n$ et les n modules de Cauchy du polynôme f qui engendrent l'idéal $I_\Omega^{\mathfrak{S}_n}$;
- `Candidats` contient toutes les classes de conjugaison de sous-groupes de $\mathfrak{S}_n$.

À chaque appel récursif

`GaloisIdéal(f,n,M,Generateurs,Candidats)` ,

- `M` est un sous-groupe de $\mathfrak{S}_n$ contenant le groupe de Galois G_Ω;
- `Generateurs` est une liste contenant les modules de Cauchy du polynôme f, des sous-groupes distincts

$$M_1 = \mathfrak{S}_n \supset M_2 \supset \cdots \supset M_m$$

de $\mathfrak{S}_n$ et des polynômes $R_2, \ldots, R_m$ de $k[x_1, \ldots, x_n]$ tels que pour $i \in [2, m]$ le polynôme R_i est un polynôme $M_{(i-1)}$-primitif de l'idéal $I_\Omega^{M_i}$;
- `Candidats` est la liste des classes de conjugaison de sous-groupes de M contenant les groupes candidats à être le groupe de Galois G_Ω.

À chaque appel de l'algorithme, la liste `Candidats` est amenée à diminuer et la liste de `Generateurs` est amenée à grossir. La première fait converger vers le groupe de Galois par élimination de classes de conjugaison et la deuxième fait converger vers l'idéal maximal des Ω-relations par la construction d'une chaîne ascendante d'idéaux.

Résultat de l'algorithme `GaloisIdéal`.

L'algorithme retourne en valeur la liste `Generateurs`. Le dernier groupe M_m qu'elle contient vérifie

$$I_\Omega = I_\Omega^{M_m}$$

avec $M_m \subset G_\Omega$. Si $M_m \neq G_\Omega$, il est facile de déduire le groupe de Galois G_Ω de l'idéal des relations I_Ω. En effet, G_Ω est le groupe de décomposition de l'idéal I_Ω. Le groupe G_Ω est donc celui dont les générateurs envoient tous les générateurs de I_Ω dans I_Ω. Le test de l'appartenance se réalise avec une base de Gröbner de l'idéal I_Ω.

Définitions de deux fonctions utilisées dans l'algorithme.

- La fonction `Retourner` a pour effet l'arrêt de l'exécution de la fonction `GaloisIdéal` en renvoyant un résultat. C'est pourquoi l'alternance `Sinon` dans `Si-Alors-Sinon` est absente.
- Soient S le groupe $\mathrm{Stab}_M(GL)$ et W le polynôme défini en (30) ; la fonction `R(M,`S`,`W`)` calcule un polynôme `M`-primitif de l'idéal I_Ω^S en appliquant le théorème fondamental des fonctions symétriques avec les coefficients du polynôme W.

Hypothèse de l'algorithme `GaloisIdéal`.

À la première étape, il est trop coûteux de calculer une résolvante associée au groupe identité. Cette résolvante, appelée *résolvante de Galois*, détermine l'idéal des relations I_Ω (voir l'identité (24)).

Commentaires des lignes (A) à (E) l'algorithme `GaloisIdéal`.

- (A) Le choix judicieux d'un sous-groupe L de M doit tenir compte de la complexité du calcul des résolvantes relatives à M, de l'intérêt des informations fournies par la matrice de groupes relative à M et de la vitesse de convergence vers l'idéal des Ω-relations.
- (B) Il est impossible que tous les sous-groupes de `M` aient été testés car le groupe de Galois est déterminé avant que cela n'arrive. En effet, lorsque tous les sous-groupes de `M` sont utilisés comme groupes tests, la matrice de groupes de `M` suffit à déterminer le groupe de Galois.
- (C) Pour déterminer le facteur associé à une orbite, il faut utiliser le degré ou le groupe de Galois de ce facteur ou encore la proposition 5.2.
- (D) Le stabilisateur `S` de l'orbite, sera identique à l'union des groupes de cette orbite si cette union est un groupe.
- L'étape (E) est indispensable puisque deux sous-groupes conjugués dans le groupe M ne le sont pas nécessairement dans son sous-groupe `S`.

Variante de l'algorithme `GaloisIdéal`.

Le calcul d' une résolvante relative à un idéal, nécessite celui d'une base de Gröbner de cet idéal (voir [6]). Donc, avant de changer le groupe M par son sous-groupe S, il faut parfois exploiter la matrice de groupes de M et amortir le calcul de la base de Gröbner de l'idéal I_Ω^M. Le choix est déterminé par la comparaison du temps de calcul d'une résolvante relative à l'idéal I_Ω^M avec les temps de calcul d'une base de Gröbner de l'idéal I_Ω^S et d'une résolvante relative à cet idéal. L'avantage du sous-groupe S sur le groupe M est que les degrés des résolvantes sont moindres (ils sont majorés par l'ordre du groupe).

Fonction `GaloisIdéal(f, n, M, Generateurs, Candidats)`

```
(A) Choisir L un sous-groupe de M
*   Calculer Θ un L-invariant M-primitif
    Calculer Et Factoriser F la résolvante ℒ_{Θ,I_Ω^M}
    (supposons le polynôme  F  séparable)
    Choisir V un facteur de F irréductible sur k
    Si L est un sous-groupe du groupe de Galois
       Alors Rajouter V(Θ) à Generateurs Et Retourner Generateurs
    Retirer de la liste Candidats les groupes exclus
             (par la matrice de groupes ou une autre méthode)
    Si Candidats ne contient qu'un groupe G (i.e.  G=G_Ω)
       Alors Si M=G Alors Retourner Generateurs
       Calculer P un polynôme M-primitif de l'idéal des Ω-relations
       Rajouter P et G à Generateurs Et Retourner Generateurs
    Soit H l'intersection des groupes de Candidats
    Si pour SH un sous-groupe de H
       il est facile de calculer une SH-résolvante M-relative
       Alors L:=SH Et Refaire * avec L (L est un sous-groupe de G_Ω)
    Calculer G un sous-groupe minimal de M qui contient G_Ω
    Si G=M (le groupe test L a été mal choisi)
(B)    Alors Choisir un autre sous-groupe L de M
             Refaire * avec L (un échappement sera produit)
    Calculer les G-orbites de (M/L)_g (ici G≠ M)
**  Choisir une G-orbite Or
(C) Déterminer le facteur W de F qui correspond à Or
    Si ce n'est pas possible
       Alors Changer d'orbite
             Si toutes les orbites sont testées
(B)             Alors Choisir un autre sous-groupe L de M
                      Refaire * avec L
             Refaire ** avec la nouvelle orbite
(D) Calculer S le stabilisateur de Or dans M
    Si S=M pour chaque orbite Or
(B)    Alors Choisir un autre sous-groupe L de M
             Refaire * avec L
    Rajouter R(M,S,W) Et S à Generateurs
(E) Changer les classes de conjugaison dans Candidats
    GaloisIdéal(f,n,S,Generateurs,Candidats)
```

Démonstration. L'algorithme `GaloisIdéal` se termine puisqu'il inclut celui des matrices de groupes. □

6. Exemple

Ce paragraphe décrit un exemple explicite. Nous reprenons les notations de l'algorithme `GaloisIdéal`.

Choisissons $f = x^6 + 2$ qui est irréductible sur $\mathbb{Q}$ et cherchons le groupe de Galois de f sur $\mathbb{Q}$ ainsi que l'idéal des relations entre ses racines.

Au départ $M = \mathfrak{S}_6$, le groupe symétrique de degré 6. La première étape consiste à calculer les n modules de Cauchy du polynôme f qui forment un ensemble triangulaire engendrant l'idéal $I_\Omega^{\mathfrak{S}_6}$:

$$\begin{aligned}
I_\Omega^{\mathfrak{S}_6} \quad = \quad & < x_6 + x_5 + x_4 + x_3 + x_2 + x_1, \\
& x_5^2 + x_4x_5 + x_3x_5 + x_2x_5 + x_1x_5 + x_4^2 + x_3x_4 + x_2x_4 + x_1x_4 \\
& + x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2, \\
& x_4^3 + x_3x_4^2 + x_2x_4^2 + x_1x_4^2 + x_3^2x_4 + x_2x_3x_4 + x_1x_3x_4 + x_2^2x_4 + x_1x_2x_4 + x_1^2x_4 \\
& + x_3^3 + x_2x_3^2 + x_1x_3^2 + x_2^2x_3 + x_1x_2x_3 + x_1^2x_3 + x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3, \\
& x_3^4 + x_2x_3^3 + x_1x_3^3 + x_2^2x_3^2 + x_1x_2x_3^2 + x_1^2x_3^2 + x_2^3x_3 + x_1x_2^2x_3 \\
& + x_1^2x_2x_3 + x_1^3x_3 + x_2^4 + x_1x_2^3 + x_1^2x_2^2 + x_1^3x_2 + x_1^4, \\
& x_2^5 + x_1x_2^4 + x_1^2x_2^3 + x_1^3x_2^2 + x_1^4x_2 + x_1^5, x_1^6 + 2 > \quad .
\end{aligned}$$

Choisissons d'abord $L = \mathfrak{S}_1 \times \mathfrak{S}_5$. Le polynôme $\Theta_1 = x_1$ est un L-invariant M-primitif. La résolvante par Θ_1 associée à l'idéal des relations symétrique est le polynôme f lui-même. Comme le polynôme f est irréductible sur $\mathbb{Q}$, son groupe de Galois est transitif. Les groupes non transitifs sont exclus des groupes candidats et $S = \mathfrak{S}_6$.

Choisissons ensuite $L = A_6$ où A_6 est le groupe alterné dans $\mathfrak{S}_6$. Le déterminant de Vandermonde Θ_2 est un A_6-invariant $\mathfrak{S}_6$-primitif séparable. Puisque le discriminant de f n'est pas un carré son groupe de Galois n'est pas un groupe pair (voir Lemme 3.7). Les sous-groupes de A_6 sont exclus des groupes candidats et $S = \mathfrak{S}_6$.

Maintenant, soit L=PGL$(2,5)$, le sous-groupe maximal transitif de $\mathfrak{S}_6$ et de degré degré 120. Choisissons le L-invariant $\mathfrak{S}_6$-primitif donné dans [16] que nous nommons Θ_3 (cet invariant est long à exprimer). La factorisation sur $\mathbb{Q}$ de la résolvante par Θ_3 associée à l'idéal $I_f^{\mathfrak{S}_6}$ aboutit à :

$$\mathcal{L}_{\Theta_3, I_f^{\mathfrak{S}_6}} = (T-42)(T-24)^2(T+6)^3 \quad .$$

La matrice de partitions de $\mathfrak{S}_6$ indique qu'alors le groupe de Galois du polynôme f est un des groupes suivants : PGL$(2,5)$, PSL$(2,5)$, D_6, le groupe diédral, ou C_6, le groupe cyclique, qui sont inclus dans L. Puisque le groupe de Galois est inclus dans L, le groupe S est identique à L. D'autre part, d'après le théorème 3.27,

$$I_\Omega^L = I_f^{\mathfrak{S}_6} + < \Theta_3 - 42 > \quad ,$$

où 42 est la valeur du facteur linéaire de $\mathcal{L}_{\Theta_3, I_f^{\mathfrak{S}_6}}$ sur $\mathbb{Q}$. Le logiciel `FGb` (voir [12]) a calculé le système triangulaire suivant engendrant l'idéal I_Ω^L :

$$\begin{aligned}
I_\Omega^{\mathrm{PGL}(2,5)} \quad = \quad & < 24x_6 + x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + 6x_3^3x_2x_1^3 + 5x_3^3x_1^4 + 8x_3^2x_2^3x_1^2 + 4x_3^2x_2^2x_1^3 + 8x_3^2x_2x_1^4 \\
& + 6x_3x_2^3x_1^3 + 8x_3x_2^2x_1^4 - 4x_3x_2x_1^5 + 12x_3 + 5x_2^3x_1^4 + 12x_2 + 14x_1, \\
& 24x_5 - 5x_3^3x_2^4 - 7x_3^3x_2^3x_1 - 16x_3^3x_2^2x_1^2 - 7x_3^3x_2x_1^3 - 5x_3^3x_1^4 - 8x_3^2x_2^4x_1 - 12x_3^2x_2^3x_1^2 \\
& - 12x_3^2x_2^2x_1^3 - 8x_3^2x_2x_1^4 - 12x_3x_2^4x_1^2 - 16x_3x_2^3x_1^3 - 12x_3x_2^2x_1^4 + 8x_3 - 5x_2^4x_1^3 \\
& - 5x_2^3x_1^4 - 2x_2 - 2x_1, \\
& 24x_4 + 5x_3^3x_2^4 + 6x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + x_3^3x_2x_1^3 + 8x_3^2x_2^4x_1 + 4x_3^2x_2^3x_1^2 + 8x_3^2x_2^2x_1^3 \\
& + 12x_3x_2^4x_1^2 + 10x_3x_2^3x_1^3 + 4x_3x_2^2x_1^4 + 4x_3x_2x_1^5 + 4x_3 + 5x_2^4x_1^3 + 14x_2 + 12x_1, \\
& x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 + x_3x_2^3 \\
& + x_3x_2^2x_1 + x_3x_2x_1^2 + x_3x_1^3 + x_2^4 + x_2^3x_1 + x_2^2x_1^2 + x_2x_1^3 + x_1^4, \\
& x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5, x_1^6 + 2 > \quad .
\end{aligned}$$

Nous avons maintenant M =PGL$(2,5)$. Choisissons $L = D_6$. La situation est la suivante :

$$I_f^{\mathfrak{S}_6} \subset I_\Omega^{\mathrm{PGL}(2,5)} \subset I_\Omega^{D_6} \subset I_\Omega \quad .$$

Le polynôme $\Theta_4 = x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1$ qui est un D_6-invariant $\mathfrak{S}_6$-primitif est a fortiori un D_6-invariant M-primitif. Le calcul de la résolvante associée et sa factorisation sur $\mathbb{Q}$ aboutissent à :

$$\mathcal{L}_{\Theta_4, I_\Omega^M} = T(T^3 - 2)(T^3 + 2)^2 \quad .$$

La matrice de partitions associée à M indique qu'alors le groupe de Galois de f est D_6 ou C_6. Comme $G_\Omega \subset D_6$, nous avons $S = D_6$. L'idéal $I_\Omega^{D_6}$ s'exprime alors ainsi :

$$I_\Omega^{D_6} = I_\Omega^{\mathrm{PGL}(2,5)} + < \Theta_4 - 0 > \quad .$$

Nous en déduisons le système triangulaire suivant :

$$I_\Omega^{D_6} =< x_6 - x_3 - x_1, x_5 + x_3 + x_1, x_4 + x_3, x_3^2 + x_1x_3 + x_1^2, x_2 + x_1, x_1^6 + 2 > \quad .$$

Finalement, prenons $L = C_6$, le groupe cyclique inclus dans D_6, et choisissons comme C_6-invariant D_6-primitif le polynôme $\Theta_5 = x_4x_5^2 + x_3x_6^2 + x_5x_2^2 + x_2x_3^2 + x_6x_1^2 + x_1x_4^2$. Le degré de la résolvante par Θ_5 associée à l'idéal $I_\Omega^{D_6}$ est 2, l'indice de C_6 dans D_6. Le calcul montre que $\mathcal{L}_{\Theta_5, I_\Omega^{D_6}} = T^2$ et que donc Θ_5 n'est pas séparable pour Ω. Adoptons donc la méthode donnée dans [10] pour chercher un invariant séparable pour Ω et remplaçons $\Theta_5(x_1, \ldots, x_6)$ par $\Psi = \Theta_5(p(x_1), \ldots, p(x_6))$ où $p(x) = x^2 + 1$. Nous aboutissons alors à la résolvante

$$\mathcal{L}_{\Psi, I_\Omega^{D_6}} = T^2 - 24T + 252$$

qui est irréductible sur $\mathbb{Q}$. Le groupe de Galois n'est donc pas C_6 (voir Lemme 3.7).

Les calculs réalisés dans ce paragraphe ont montré que le groupe de Galois de $x^6 + 2$ est D_6 et que l'idéal des relations est $I_\Omega^{D_6}$.

Conclusion. De l'étude des idéaux invariants par des permutations, a été exhibée une construction de l'idéal des relations sans avoir à factoriser dans des extensions de k. Cette méthode est réellement effective, puisque nous savons calculer les résolvantes apparaissant dans l'algorithme.

Remerciements *Je remercie le Professeur C. Traverso de m'avoir éclairée sur certains points indispensables à l'aboutissement de ce travail.*

References

[1] **Abdeljaouad, I., 1997**, Calcul d'invariants primitifs de groupes finis, Rapport LIP6 1997-020.

[2] **Anai H., Noro M., Yokoyama K., 1994** Computation of the splitting field and the Galois groups of polynomials, Progress in Mathematics, **143** (conference MEGA'94), Birkhaüser Verlag, pp. 29–50.

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

[4] **Arnaudiès J.M., Valibouze A., 1996.** Lagrange resolvents, special issue of MEGA'96 (A. Cohen and M-F- Roy Eds), Journ. of Pure and Appl. Algeb. **117&118** (1997), 23-40.

[5] **Artin, E., 1959** *Galois Theory*, Notre Dame Mathematical Lectures No. 2, Notre Dame, IN: Notre Dame University Press.

[6] **Aubry, P., Valibouze, A., 1998**, Using Galois ideals for computing relative resolvents, International Conference MEGA'98 (LITP Report 1998/004).

[7] **Berwick, E.H., 1915**, The condition that a quintic equation should be soluble by radicals, Proc. London Math. Soc. (2) **14**. 301-307.

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

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

[10] **Colin, A., 1995** Formal computation of Galois groups with relative resolvents Conference AAECC'10, (Paris, July 1995), LNCS **948**, 169-182

[11] **Colin A., 1997** Identification of the Galois group thanks to symbolic computation of relative resolvents and tables of partitions, ISSAC'97 Conference (Hawaii, July 1997).

[12] **Faugère, J.C., 1997** A new efficient algorithm for computing Gröbner Basis (F4), Task 3.3.2.1 Frisco report, preprint.

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

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

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

[16] **Girstmair, K., 1987** On invariant polynomials and their application in field theory Maths of Comp., vol. **48**, no 178, 781-797.

[17] **Kemper, G., 1996**, Calculating invariant rings of finite groups over arbitrary fields, JSC **21** 351-366.

[18] **Kemper, G., 1994** The *Invar* package for calculating rings of invariants, IWR Preprint **93-34**, Heidelberg.

[19] **Lagrange, J.L., 1770**, Réflexions sur la résolution algébrique des équations, Mémoires de l'Académie de Berlin, 205-421, (*Œuvres de Lagrange*, tome IV, 205-421)

[20] **Lazard, D,, Valibouze, A., 1991**, Computing subfields: Reverse of the primitive element problem, proc. de Mega'92 (Nice, april 1992). Progress in Mathematics **109**, 163-176.

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

[22] **Stauduhar, R.P., 1973**, The determination of Galois groups, Math. Comp. **27**, 981-996.

[23] **Tchebotarev N., 1950** *Grundzüge des Galois'shen Theorie*, P. Noordhoff.

[24] **Valibouze A., 1989**, Symbolic computation with symmetric polynomials, an extension to Macsyma. Conference Computers and Mathematics (1989, MIT, Cambridge, Mass.). Springer-Verlag, 308-320.

[25] **Valibouze A., 1995**, Computation of the Galois group of the resolvent factors for the direct and inverse Galois problems, AAECC'10 conference (Paris, July 1995), LNCS **948**, 456-468 (LITP Report 94-58).

[26] **Yokoyama, K., Noro, M., Takeshima, T. , 1992** Solution of systems of algebraic equations and linear maps on Residue Class ring, Journal of Symbolic Computation **14**, 399-417 .

LIP6, Université Paris VI, 4, place Jussieu, F-75252 Paris Cedex 05, e-mail : avb@medicis.polytechnique.fr