Calcul efficace de corps de décomposition

Sébastien Orange, Guénaël Renault, Annick Valibouze

CALCUL EFFICACE DE CORPS DE DÉCOMPOSITION

SÉBASTIEN ORANGE, GUÉNAËL RENAULT, ANNICK VALIBOUZE

Résumé

Nous proposons de nouvelles idées pour le calcul efficace du corps de décomposition d'un polynôme d'une variable sur un corps parfait. Ces idées accélèrent tous les algorithmes existants mais aussi les rendent compatibles en compensant leurs faiblesses respectives. Il s'agit d'exploiter d'une part les groupes de Galois des facteurs du polynôme dans les extensions mais aussi de calculer, voir de pré-calculer, des relations avec les modules de Cauchy ou en permutant d'autres relations.

Abstract

In this paper, we propose new ideas for the computation of the splitting field of an univariate polynomial over a perfect field. This ideas can mixe two known algorithms in a faster one by avoiding their respective drawbacks.

1. Introduction

Dans cet article, k désignera un corps parfait et f un polynôme irréductible sur k et de degré n. Sous ces hypothèses, les racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ de f dans une clôture algébrique $\overline{k}$ de k sont distinctes et, en tant que groupe de permutations, le groupe de Galois $\mathrm{Gal}_k(f)$ de f sur k est isomorphe à un sous-groupe transitif de S_n, le groupe symétrique de degré n.

Déterminer le corps de décomposition $k(\alpha_1, \ldots, \alpha_n)$ du polynôme f revient à calculer un ensemble triangulaire séparable $\mathfrak{T}$ de $k[x_1, \ldots, x_n]$ engendrant un idéal maximal $\mathfrak{M}$, appelé *idéal des relations*, vérifiant :

$$k(\alpha_1, \ldots, \alpha_n) \simeq k[x_1, \ldots, x_n]/\mathfrak{M}.$$

L'objet de cet article est l'élaboration d'un algorithme efficace de calcul de l'idéal $\mathfrak{M}$, c'est-à-dire celui de l'ensemble triangulaire $\mathfrak{T}$.

Plusieurs méthodes exploitent les factorisations successives du polynôme f dans les extensions algébriques $k(\alpha_1)$, $k(\alpha_1, \alpha_2)$, $\ldots$, $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ (voir [20], [13], [2] et [15]). Mais ces méthodes, dans leurs dernières étapes, peuvent s'avérer très coûteuses (voir infaisables) lorsque l'ordre du groupe de Galois de f est élevé.

Date: 08/04/2006.

2000 *Mathematics Subject Classification.* Primary 12F10; Secondary 12Y05, 11Y40.

Key words and phrases. Splitting field, Galois ideal, Galois group.

L'algorithme `GaloisIdéal` basé sur les *idéaux de Galois* évite les factorisations dans les extensions (voir Paragraphe 9.2) Cet algorithme, appliqué à un idéal I_1, construit récursivement une chaîne strictement ascendante d'idéaux de Galois de f :

$$I_1 \subset I_2 \subset \cdots \subset I_r = \mathfrak{M} .$$

Il est toujours possible de prendre pour I_1 l'idéal $\mathcal{S}$ des relations symétriques engendré par l'ensemble triangulaire formé des modules de Cauchy de f (voir [8], [18] et [20]). À partir de $\mathcal{S}$, l'idéal $\mathfrak{M}$ est algorithmiquement calculable en une étape (i.e. $r = 2$) (voir [3]). Mais ce calcul dépend de celui du polynôme minimal d'un élément k-primitif du corps des racines de f. L'algorithme `GaloisIdéal` diminue la complexité du problème en le décomposant en plusieurs étapes. La complexité du calcul de l'idéal I_{i+1} dépend fortement de la dimension du k-e.v. $k[x_1, \ldots, x_n]/I_i$ qui vaut $n!$ lorsque $i = 1$ et $\mathcal{S} = I_1$. Plus la dimension de $k[x_1, \ldots, x_n]/\mathfrak{M}$ est moindre (c'est l'ordre du groupe de Galois), plus il est essentiel de calculer un idéal de Galois distinct de $\mathcal{S}$ en un temps plus rapide que `GaloisIdéal` partant de $I_1 = \mathcal{S}$.

Pour calculer $\mathfrak{M}$, nous disposons d'une troisième voie proposée dans [26]. L'auteur y calcule les degrés des monômes initiaux de l'ensemble triangulaire $\mathfrak{T}$ engendrant $\mathfrak{M}$ (voir [5]) puis, par l'algèbre linéaire et les nombres p-adiques, il détermine les coefficients des monômes de $\mathfrak{T}$. Cette méthode suppose le groupe de Galois pré-déterminé et pourtant n'exploite cette information que pour le calcul des degrés initiaux.

Dans l'algorithme de factorisations dans les extensions, il est possible d'extraire des informations sur le groupe de Galois à travers les *tables de rupture* (voir Paragraphe 4). De plus, les modules de Cauchy des facteurs sont des relations dont certaines appartiennent à $\mathfrak{T}$ (voir Paragraphe 5). Nous évitons ainsi des factorisations dans les extensions. Au lieu de poursuivre les factorisations "à l'aveugle", il est possible de construire un idéal de Galois dit induit (voir Paragraphe 5) et de calculer l'objet indispensable à son utilisation : son injecteur dans $\mathfrak{M}$ (voir Paragraphe 7.3). À partir d'un idéal de Galois dont l'injecteur n'est pas un groupe, nous verrons que nous pouvons calculer extrêmement rapidement un nouvel idéal J le contenant (voir Paragraphe 8). À cette étape, nous disposons d'une liste de groupes de Galois candidats. À partir de l'idéal J, il est alors possible de poursuivre la construction de $\mathfrak{T}$ avec l'une des trois méthodes évoquées plus haut. Ces idées donnent des résultats excellents puisqu'elles permettent de mixer toutes les méthodes connues en les optimisant individuellement. De plus, mixer ces méthodes compense leurs faiblesses respectives (ordre élevé pour la factorisation, bas pour `GaloisIdéal`, pré-calcul du groupe de Galois pour la troisième).
Au paragraphe 9, nous décrivons une méthode pour construire un algorithme de construction de $\mathfrak{T}$. Pour simplifier la présentation, cette description s'arrête à la factorisation dans la première extension et termine la construction avec `GaloisIdéal` sans faire appel à d'autres outils de détermination du groupe de Galois ou à d'autres méthodes pour calculer des relations de $\mathfrak{T}$. Pour l'élaboration d'un algorithme efficace, il faut poursuivre l'étude dans les extensions supérieures et mixer toutes les méthodes. Dans le paragraphe 10 et à titre d'illustration, nous étudierons cet algorithme simplifié

en degré 8 car il offre un panel complet des situations possibles. Le paragraphe 11 est dédié à l'implantation et à l'expérimentation.
Les polynômes utilisés à titre d'illustration sont extraits de la base de données de G. Malle et J. Klüners (voir [11] et [12]).

2. Notations

Nous adopterons les notations et conventions suivantes :

- Pour tout idéal I de $k[x_1,\ldots,x_n]$, la variété affine de I dans $\overline{k}^n$, i.e. l'ensemble des n-uplets de $\overline{k}^n$ annulant l'idéal I, est notée $V(I)$ et $\mathcal{M}(I)$ désigne l'ensemble des idéaux maximaux contenant I.
- Soit $V \subset \overline{k}^n$; l'idéal $Id_k(V)$ est l'ensemble des polynômes de $k[x_1,\ldots,x_n]$ s'annulant sur V.
- L'ensemble des permutations d'un ensemble fini E est noté S_E. Lorsque E désigne l'ensemble $\{1,\ldots,n\}$, S_E est noté S_n.
- Si L un sous-groupe de S_E, le fixateur dans L d'un élément $e \in E$ est noté $L_{\{e\}}$ et est considéré comme un sous-groupe de $S_{E\setminus\{e\}}$.
- Le produit direct $S_{n_1} \times \cdots \times S_{n_m}$ de groupes symétriques est noté $S_{n_1,\ldots,n_m}$.
- Pour tout sous-groupe H de S_n et tout $\sigma \in S_n$, nous posons $H^\sigma = \sigma H \sigma^{-1}$.
- L'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action naturelle d'un sous-groupe G de S_n est noté $Orb(G)$.
- Soit $\sigma \in S_n$. Pour tout n-uplet $\underline{u}$, nous posons $\sigma.\underline{u} = (u_{\sigma(1)},\ldots,u_{\sigma(n)})$ et, pour tout $P \in k[x_1,\ldots,x_n]$, nous posons $\sigma.P = P(x_{\sigma(1)},\ldots,x_{\sigma(n)})$.
- Soit $\sigma \in S_n$. Soit E un ensemble sur lequel S_n agit. Notons . cette action. Pour toute partie $\mathcal{P} \subset E$, toute partie L de S_n et tout élément $e \in E$, nous posons $\sigma.\mathcal{P} = \{\sigma.p \,|\, p \in \mathcal{P}\}$, $L.\mathcal{P} = \{\sigma.\mathcal{P} \mid \sigma \in L\}$ et $L.e = L.\{e\}$.
- Pour tout anneau $\mathcal{A}$ et toute partie non vide E de $\mathcal{A}$, nous noterons $\langle E\rangle_{\mathcal{A}}$ l'idéal engendré par E dans $\mathcal{A}$.

Si G est un sous-groupe d'un sous-groupe H de S_n et $\{\sigma_1 G,\ldots,\sigma_e G\}$ sont les classes à gauche de $H \mod G$ alors l'ensemble $\{\sigma_1,\ldots,\sigma_e\}$ est appelé *une transversale à gauche de* $H \mod G$. Les transversales à droite se définissent de la même manière.
Dans toute la suite de cet article, $\underline{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \bar{k}^n$ désignera un n-uplet de n racines distinctes de f (supposé irréductible).

3. Idéaux de Galois

Les définitions et les résultats non démontrés ci-après sont repris des articles [23] et [24]. La notion de stabilisateur a toutefois été étendue à celle d'injecteur.

Dans tout ce paragraphe, nous noterons K une extension algébrique de k, nous fixons L un sous-ensemble de S_n et l'idéal $I = Id_K(L.\underline{\alpha})$.

Définition 3.1. L'idéal I est appelé un *idéal de Galois de* f (sur K). Deux idéaux de Galois particuliers sont l'*idéal des* $\underline{\alpha}$*-relations*

$$\mathfrak{M} = Id_K(\{\underline{\alpha}\}) \quad et \quad \mathcal{S} = Id_K(S_n.\underline{\alpha}) \quad .$$

La proposition suivante donne une caractérisation des idéaux de Galois.

Proposition 3.2. *Un idéal propre de $K[x_1, \ldots, x_n]$ est un idéal de Galois de f si et seulement si il contient les modules de Cauchy de f.*

Il s'ensuit naturellement le nouveau corollaire suivant :

Corollaire 3.3. *Soient K_1, K_2 deux extensions algébriques de k telles que $K_1 \subset K_2$. Si I (resp. J) est un idéal de Galois de $K_1[x_1, \ldots, x_n]$ (resp. $K_2[x_1, \ldots, x_n]$) alors les deux idéaux suivants sont des idéaux de Galois :*

1. *L'idéal de $K_2[x_1, \ldots, x_n]$ engendré par I. Cet idéal est obtenu par extension des scalaires et s'exprime sous la forme du produit tensoriel $K_2 \otimes_{K_1} I$.*
2. *L'idéal $K_1[x_1, \ldots, x_n] \cap J$ trace de J dans $K_1[x_1, \ldots, x_n]$.*

Définition 3.4. L'*injecteur* $\mathrm{Inj}(J, J')$ d'un idéal J dans un idéal J' est l'ensemble des permutations σ de S_n qui vérifient $\sigma.J \subset J'$.
L'*injecteur de I relatif à $\underline{\alpha}$* est l'injecteur de I dans $\mathfrak{M}$, noté aussi $\mathrm{Inj}(I, \underline{\alpha})$.

La variété $V(I)$ est donnée par :

$$V(I) = \{\sigma.\underline{\alpha} \mid \sigma \in \mathrm{Inj}(I, \mathfrak{M})\} \quad (= \mathrm{Inj}(I, \mathfrak{M}).\underline{\alpha}) \tag{3.1}$$

et comme le polynôme f est séparable,

$$\mathrm{Card}(\mathrm{Inj}(I, \mathfrak{M})) = \mathrm{Card}(V(I)) \quad . \tag{3.2}$$

En remarquant que $Id_K(\sigma.\underline{\alpha}) = \sigma^{-1}.\mathfrak{M}$, nous avons donc :

$$I = \bigcap_{\sigma \in \mathrm{Inj}(I, \mathfrak{M})} \sigma^{-1}.\mathfrak{M} = \bigcap_{\sigma \in L} \sigma^{-1}.\mathfrak{M} \tag{3.3}$$

et l'ensemble $\mathcal{M}(I)$ des idéaux maximaux contenant I est

$$\mathcal{M}(I) = \{\sigma^{-1}.\mathfrak{M} \mid \sigma \in \mathrm{Inj}(I, \mathfrak{M})\} = \{\sigma^{-1}.\mathfrak{M} \mid \sigma \in L\} \quad . \tag{3.4}$$

Les injecteurs de l'idéal de Galois I sont tous reliés par la proposition suivante :

Proposition 3.5. *Si $\sigma \in S_n$ alors* $\mathrm{Inj}(I, \sigma.\mathfrak{M}) = \sigma\,\mathrm{Inj}(I, \mathfrak{M})$.

Démonstration. Car pour tout $R \in I$, et $\tau \in \mathrm{Inj}(I, \sigma.\mathfrak{M})$, nous avons $\tau.R \in \sigma.\mathfrak{M}$ si et seulement si $\sigma^{-1}\tau.R \in \mathfrak{M}$; i.e. $\tau \in \sigma\,\mathrm{Inj}(I, \mathfrak{M})$.

Remarque 3.6. L'identité (3.1) fait apparaître que l'idéal I est entièrement déterminé par un n-uplet de $\overline{k}$ sur lequel il s'annule et par son injecteur relatif à ce n-uplet. Ainsi, l'injecteur de I relatif à $\underline{\alpha}$ est de nature géométrique. En effet, pour toute extension algébrique K' de K, nous avons :

$$\mathrm{Inj}(I, Id_K(\underline{\alpha})) = \mathrm{Inj}(K' \otimes_K I, Id_{K'}(\underline{\alpha}))$$

qui s'écrit plus simplement

$$\mathrm{Inj}(I, \underline{\alpha}) = \mathrm{Inj}(K' \otimes_K I, \underline{\alpha})\,. \tag{3.5}$$

Exprimons I sous la forme d'une décomposition de I en idéaux deux-à-deux comaximaux :

$$I = \bigcap_{i=1}^{m} \mathcal{N}_i \, .$$

La variété de I s'écrit alors comme l'union disjointe des variétés $V(\mathcal{N}_i)$ et l'égalité 3.1 permet d'exprimer l'injecteur de I relatif à $\mathfrak{M}$ comme l'union disjointe suivante :

$$\mathrm{Inj}(I, \mathfrak{M}) = \mathrm{Inj}(\mathcal{N}_1, \mathfrak{M}) + \mathrm{Inj}(\mathcal{N}_2, \mathfrak{M}) + \ldots + \mathrm{Inj}(\mathcal{N}_m, \mathfrak{M}) \, . \tag{3.6}$$

Proposition 3.7. *Soit E une partie de S_n. Les deux assertions suivantes sont équivalentes :*

(1) *il existe $\mathfrak{N} \in \mathcal{M}(I)$ tel que $E \subset \mathrm{Inj}(I, \mathfrak{N})$;*
(2) *l'idéal $\langle I \cup E.I \rangle_{k[x_1,\ldots,x_n]}$ est de Galois (i.e. distinct de $k[x_1, \ldots, x_n]$).*

Démonstration. L'idéal J de $k[x_1, \ldots, x_n]$ engendré par $I \cup E.I$ est un idéal de Galois si et seulement s'il est un idéal propre de $k[x_1, \ldots, x_n]$ (voir Proposition 3.2). De l'égalité 3.3, nous déduisons que :

$$\begin{aligned} J \neq k[x_1, \ldots, x_n] \quad \text{ssi} \quad & \bigcap_{\mathfrak{N} \in \mathcal{M}(I)} \langle \mathfrak{N} \cup E.I \rangle_{k[x_1,\ldots,x_n]} \neq k[x_1, \ldots, x_n] \\ \text{ssi} \quad & \exists \mathfrak{N} \in \mathcal{M}(I), \ \langle \mathfrak{N} \cup E.I \rangle_{k[x_1,\ldots,x_n]} \neq k[x_1, \ldots, x_n] \\ \text{ssi} \quad & \exists \mathfrak{N} \in \mathcal{M}(I), \ E.I \subset \mathfrak{N} \end{aligned}$$

car $\mathfrak{N}$ est maximal. □

Un injecteur peut être un groupe ; c'est le cas, particulier et important en théorie de Galois, de l'injecteur de tout idéal dans lui même :

Définition 3.8. L'injecteur de I dans I est le *groupe de décomposition* $\mathrm{Dec}(I)$ de I.

Définition 3.9. Le *groupe de Galois* $\mathrm{Gal}_K(\underline{\alpha})$ *de* $\underline{\alpha}$ *sur* K est le groupe de décomposition de $Id_K(\{\underline{\alpha}\})$; i.e. c'est $\mathrm{Dec}(\mathfrak{M})$.

Notations 3.10. Le groupe de Galois $\mathrm{Gal}_K(\underline{\alpha})$ est isomorphe au groupe des K-automorphismes de $K(\underline{\alpha})$ par l'application qui à tout élément τ de $\mathrm{Gal}_k(\underline{\alpha})$ associe $\overline{\tau}$ dans $Aut_K(K(\underline{\alpha}))$ défini par $\overline{\tau}(\alpha_i) = \alpha_{\tau(i)}$. L'action de $Aut_K(K(\underline{\alpha}))$ sur $K(\underline{\alpha})$ est étendue naturellement à $K(\underline{\alpha})[x_1, \ldots, x_n]$ par action sur les coefficients des polynômes.
Nous convenons que $\mathrm{Gal}_K(f)$ désigne un conjugué de $\mathrm{Gal}_K(\underline{\alpha})$ dans S_n.

Remarque 3.11. Pour tout $\tau \in \mathrm{Gal}_k(\underline{\alpha})$ et tout $g \in k(\underline{\alpha})[x_1, \ldots, x_n]$, nous avons donc deux notations distinctes :

- $\overline{\tau}(g)$ désignant le polynôme obtenu par l'action de τ sur les coefficients de g et
- $\tau.g$ désignant le polynôme $g(x_{\tau(1)}, \ldots, x_{\tau(n)})$.

Le lemme suivant sera utilisé pour montrer la proposition 7.1.

Lemme 3.12. *Pour tout idéal J de $k(\underline{\alpha})[x_1,\dots,x_n]$ et tout $\tau \in Gal_k(\underline{\alpha})$, nous avons l'identité suivante :*

$$\mathrm{Inj}(\overline{\tau}(J),\underline{\alpha}) \;=\; \tau\,\mathrm{Inj}(J,\underline{\alpha})\;. \tag{3.7}$$

Démonstration. Pour V un sous-ensemble de $S_n.\underline{\alpha}$, montrons que :

$$\overline{\tau}(Id_{k(\underline{\alpha})}(V)) \;=\; Id_{k(\underline{\alpha})}(\tau.V)\;. \tag{3.8}$$

Avec les notations de l'énoncé, nous avons les égalités successives :

$$\begin{aligned}
Id_{k(\underline{\alpha})}(\tau.V) &= \bigcap_{\underline{\beta}\in V} \langle x_1-\beta_{\tau(1)},\dots,x_n-\beta_{\tau(n)}\rangle_{k(\underline{\alpha})[x_1,\dots,x_n]}\\
&= \bigcap_{\underline{\beta}\in V} \langle \overline{\tau}(x_1-\beta_1),\dots,\overline{\tau}(x_n-\beta_n)\rangle_{k(\underline{\alpha})[x_1,\dots,x_n]}\\
&= \bigcap_{\underline{\beta}\in V} \overline{\tau}(\langle x_1-\beta_1,\dots,x_n-\beta_n\rangle_{\overline{\tau}^{-1}(k(\underline{\alpha})[x_1,\dots,x_n])})\\
&= \overline{\tau}(\bigcap_{\underline{\beta}\in V} \langle x_1-\beta_1,\dots,x_n-\beta_n\rangle_{k(\underline{\alpha})[x_1,\dots,x_n]})\\
&= \overline{\tau}(Id_{k(\underline{\alpha})}(V))
\end{aligned}$$

où l'avant dernière égalité est obtenue car $\overline{\tau}$ est k-automorphisme de l'algèbre $k(\underline{\alpha})[x_1,\dots,x_n]$. Montrons maintenant que :

$$\mathrm{Inj}(\overline{\tau}(J),Id_{k(\underline{\alpha})}(\underline{\alpha})) \;=\; \mathrm{Inj}(J,\overline{\tau}^{-1}(\mathrm{Id}_{k(\underline{\alpha})}(\underline{\alpha}))\;. \tag{3.9}$$

Nous avons les égalités suivantes :

$$\begin{aligned}
\mathrm{Inj}(\overline{\tau}(J),Id_{k(\underline{\alpha})}(\underline{\alpha})) &= \{\sigma\in S_n \mid \forall P\in\overline{\tau}(J),\ \sigma.P\in Id_{k(\underline{\alpha})}(\underline{\alpha})\}\\
&= \{\sigma\in S_n \mid \forall P\in J,\ \sigma.\overline{\tau}(P)\in Id_{k(\underline{\alpha})}(\underline{\alpha})\}\\
&= \{\sigma\in S_n \mid \forall P\in J,\ \overline{\tau}(\sigma.P)\in Id_{k(\underline{\alpha})}(\underline{\alpha})\}\\
&= \{\sigma\in S_n \mid \forall P\in J,\ \sigma.J\in\overline{\tau}^{-1}(Id_{k(\underline{\alpha})}(\underline{\alpha}))\},
\end{aligned}$$

d'où le résultat. Pour terminer, les égalités successives suivantes prouvent l'identité (3.7) :

$$\begin{aligned}
\mathrm{Inj}(\overline{\tau}(J),Id_{k(\underline{\alpha})}(\underline{\alpha})) &= \mathrm{Inj}(J,\overline{\tau}^{-1}(Id_{k(\underline{\alpha})}(\underline{\alpha}))),\text{ d'après l'identité (3.9) ,}\\
&= \mathrm{Inj}(J,Id_{k(\underline{\alpha})}(\tau^{-1}.\underline{\alpha})),\text{ d'après l'identité (3.8),}\\
&= \tau\,\mathrm{Inj}(J,Id_{k(\underline{\alpha})}(\underline{\alpha})),\text{ d'après la proposition 3.5.}\qquad\square
\end{aligned}$$

La proposition suivante permet, sous certaines conditions, de déterminer un injecteur de l'idéal I.

Proposition 3.13. *Si $I\subset\mathfrak{M}$ alors $\mathrm{Dec}(I)\subset\mathrm{Inj}(I,\mathfrak{M})$ et*

$$\mathrm{Inj}(I,\mathfrak{M}) = \mathrm{Dec}(\mathfrak{M})L\ \ (=\{\,g\,l\ \mid\ g\in\mathrm{Dec}(\mathfrak{M}),\ l\in L\}\,).$$

Soit e l'entier tel que $\mathrm{Card}(\mathrm{Inj}(I,\mathfrak{M})) = e.\,\mathrm{Card}(\mathrm{Dec}(\mathfrak{M}))$. L'injecteur $\mathrm{Inj}(I,\mathfrak{M})$ s'écrit comme une réunion disjointe de e classes à droite :

$$\mathrm{Inj}(I,\mathfrak{M}) = \mathrm{Dec}(\mathfrak{M})\tau_1 + \mathrm{Dec}(\mathfrak{M})\tau_2 + \cdots + \mathrm{Dec}(\mathfrak{M})\tau_e \tag{3.10}$$

où $\tau_1 = id, \ldots, \tau_e$ sont des permutations de S_n. Ainsi, I se décompose comme intersection d'idéaux maximaux distincts :

$$I = \bigcap_{i=1}^{e} \tau_i^{-1}.\mathfrak{M} \quad . \tag{3.11}$$

Proposition 3.14. *Soit H un sous-groupe de S_n. Le groupe de décomposition de l'idéal $Id_K(H.\underline{\alpha})$ contient H.*

Définition 3.15. (voir [5]) Un idéal de $K[x_1, \ldots, x_n]$ est dit *triangulaire* s'il est engendré par un ensemble triangulaire séparable.

Proposition 3.16. *(Voir [5]) Si $\mathrm{Inj}(I, \mathfrak{M})$ est un groupe alors I est un idéal triangulaire.*

Dans cet article, tous les idéaux considérés seront triangulaires ou bien par construction ou bien par la proposition 3.16. Nous supposerons donc, à partir de maintenant, que I est engendré par l'ensemble triangulaire séparable

$$T = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}.$$

Définition 3.17. Le n-uplet $\mathcal{L}(I)$ défini par

$$\mathcal{L}(I) = (deg_{x_1}(f_1), \ldots, deg_{x_n}(f_n))$$

est appelé *liste des degrés initiaux* de I. Nous noterons $deg_{x_i}(I)$ le $i^{\text{ème}}$ élément de la liste $\mathcal{L}(I)$.

Notations 3.18. Pour tout groupe $H \subset S_n$, dans [5] il est montré comment calculer, à partir de H, une liste identique à $\mathcal{L}(J)$ pour tout idéal de Galois J ayant H comme injecteur. Cette liste est aussi notée $\mathcal{L}(H)$.

Comme l'idéal I est triangulaire, nous pouvons calculer le cardinal des injecteurs de I par la formule suivante (voir Égalité (3.2)) :

$$\mathrm{Card}(V(I)) = \prod_{i=1}^{n} deg_{x_i}(I) = \mathrm{Card}(\mathrm{Inj}(I, \mathfrak{M})). \tag{3.12}$$

La proposition suivante donne des conditions équivalentes pour qu'un injecteur $\mathrm{Inj}(I, \mathfrak{M})$ soit un groupe ainsi qu'un test effectif :

Proposition 3.19. *Les assertions suivantes sont équivalentes :*

1. $\mathrm{Dec}(I) = \mathrm{Inj}(I, \mathfrak{M})$,
2. $\mathrm{Dec}(\mathfrak{M}) \subset \mathrm{Dec}(I)$,
3. $\mathrm{Card}(\mathrm{Dec}(I)) = \prod_{i=1}^{n} deg_{x_i}(I)$,
4. *les injecteurs de I dans les idéaux de $\mathcal{M}(I)$ sont identiques.*

Si l'une de ces assertions est vérifiée, l'idéal I n'admet qu'un seul injecteur : le groupe $\mathrm{Dec}(I)$. Nous parlerons alors de l'injecteur de I.

Il est important de pouvoir tester si $\mathrm{Dec}(I)$ est l'injecteur de I car le groupe de décomposition est rapidement calculable à partir de I (voir [1]) alors que le calcul de $\mathrm{Inj}(I, \mathfrak{M})$ nécessite, a priori, la connaissance de $\mathfrak{M}$. Néanmoins, dans le paragraphe 7, nous verrons qu'il est parfois possible de pré-déterminer de tels injecteurs.

4. Table de rupture

Dans cette partie, nous montrons comment construire les *tables de rupture*. En degré n, la table est pré-calculable car elle ne dépend que de la liste des classes de S_n-conjugaison des sous-groupes transitifs de S_n (un seul représentant par classe suffit). Elle discrimine partiellement ces groupes transitifs en fonction de l'action de leur stabilisateur en 1 sur l'ensemble $\{1, 2, \ldots, n\}$. Cette table sera utilisée suite à la factorisation du polynôme f sur un de ses corps de rupture. Il apparaîtra alors que certains groupes ne peuvent être le groupe de Galois de f sur k. Au paragraphe 7, nous approfondirons l'utilisation de cette table afin de déterminer un injecteur d'un idéal de Galois de f construit à partir de sa factorisation sur un de ses corps de rupture.

Proposition 4.1. *Soient K une extension algébrique de k et $g \in K[x]$ un polynôme séparable de degré d. Notons $\mathrm{Gal}_K(g)$ le groupe de Galois de g sur K et O une orbite de $\{1, \ldots, d\}$ sous l'action de $\mathrm{Gal}_K(g)$. L'application*

$$\varphi : \ \mathrm{Gal}_K(g) \ \longrightarrow \ S_O,$$

induite par l'action de $\mathrm{Gal}_K(g)$ sur O, a pour image le groupe de Galois du facteur irréductible g_1 de g sur K donné par :

$$g_1 = \prod_{i \in O} (x - \beta_i),$$

où les β_i sont des racines de g dans $\overline{k}$.
En particulier, nous avons l'égalité $\mathrm{Card}(O) = deg(g_1)$.

Comme le polynôme f est irréductible, l'anneau quotient $k[x]/\langle f \rangle$ est isomorphe au corps $k(\alpha_1)$ appelé *corps de rupture* de f. Nous pouvons donc appliquer la proposition 4.1 avec $K = k(\alpha_1)$ et $g = \frac{f(x)}{(x-\alpha_1)}$, de groupe de Galois $\mathrm{Gal}_K(g) = \mathrm{Gal}_k(f)_{\{1\}}$.

Notations 4.2. Dans toute la suite, nous utiliserons les notations suivantes :

- $\mathcal{T}(n)$ désignera la liste des représentants des classes de conjugaison des sous-groupes transitifs de S_n du logiciel de calcul symbolique Magma (voir [6]). Pour $n \leq 15$, ces listes sont celles de G. Butler et J. McKay (voir [7]).
- Le groupe nT_i est le i-ième groupe de $\mathcal{T}(n)$ retourné par l'appel à la fonction `TransitiveGroup`(n, i) de Magma.
- La parité du groupe nT_i sera indiquée par un exposant $+$.

Désormais $\mathrm{Gal}_k(f)$ désignera le groupe de $\mathcal{T}(n)$ conjugué à $\mathrm{Gal}_k(\underline{\alpha})$.

À un groupe T de $\mathcal{T}(n)$, nous associons :

- O_T la suite des orbites induites par l'action de $T_{\{1\}}$ sur $\{2, \ldots, n\}$ ordonnées par cardinalité croissante ;
- $\Delta(T)$ la suite croissante des cardinaux des orbites de O_T ;
- $\Gamma(T)$ la suite croissante pour l'ordre $\prec$ des groupes transitifs induits par l'action de $T_{\{1\}}$ sur les orbites de O_T où l'ordre $\prec$ est défini par $n_1T_{i_1} \prec n_2T_{i_2}$

ssi $(n_1, i_1) <_{Lex} (n_2, i_2)$, où $<_{Lex}$ est l'ordre lexicographique sur les couples d'entiers.

Nous adoptons la notation exponentielle pour les suites finies d'entiers et de groupes ; par exemple, la suite finie a, a, a, b, c, c s'écrit a^3, b, c^2.

Définition 4.3. La table qui recense les images par Γ et Δ de tous les groupes de $\mathcal{T}(n)$ sera appelée *la table de rupture en degré n.*

$\Delta(T)$	$\Gamma(T)$	T
1^7	$(1T_1)^7$	$8T_1, 8T_2^+, 8T_3^+, 8T_4^+, 8T_5^+$
$1^3, 2^2$	$(1T_1)^3, (2T_1)^2$	$8T_7, 8T_9^+, 8T_{10}^+, 8T_{11}^+$
$1^3, 4$	$(1T_1)^3, 4T_1$	$8T_{17}$
	$(1T_1)^3, 4T_2^+$	$8T_{18}^+$
$1, 2^3$	$1T_1, (2T_1)^3$	$8T_6, 8T_8, 8T_{16}, 8T_{20}^+, 8T_{21}, 8T_{22}^+, 8T_{27}, 8T_{31}$
$1, 2, 4$	$1T_1, 2T_1, 4T_1$	$8T_{19}^+$
	$1T_1, 2T_1, 4T_2^+$	$8T_{15}$
	$1T_1, 2T_1, 4T_3$	$8T_{26}, 8T_{28}, 8T_{29}^+, 8T_{30}, 8T_{35}$
$1, 3^2$	$1T_1, (3T_1^+)^2$	$8T_{12}^+, 8T_{13}^+, 8T_{14}^+$
	$1T_1, (3T_2)^2$	$8T_{24}^+$
$1, 6$	$1T_1, 6T_2$	$8T_{23}$
	$1T_1, 6T_4^+$	$8T_{32}^+$
	$1T_1, 6T_6$	$8T_{38}$
	$1T_1, 6T_7^+$	$8T_{39}^+$
	$1T_1, 6T_8$	$8T_{40}$
	$1T_1, 6T_{11}$	$8T_{44}$
$3, 4$	$3T_1^+, 4T_4^+$	$8T_{33}^+, 8T_{34}^+, 8T_{42}^+$
	$3T_2, 4T_5$	$8T_{41}^+, 8T_{45}^+, 8T_{46}, 8T_{47}$
7	$7T_1^+$	$8T_{25}^+$
	$7T_3^+$	$8T_{36}^+, 8T_{37}^+$
	$7T_4$	$8T_{43}$
	$7T_5^+$	$8T_{48}^+$
	$7T_6^+$	$8T_{49}^+$
	$7T_7$	$8T_{50}$

TABLE 1. Table de rupture en degré 8.

Nous allons décrire comment exploiter les tables de rupture pour obtenir des informations sur les groupes de Galois des polynômes irréductibles.

Définition 4.4. Les facteurs irréductibles $f_1, \ldots, f_r$ de $f(x)/(x - \alpha_1)$ dans $k(\alpha_1)[x]$ sont appelés *les facteurs de rupture de* f et sont supposés être ordonnés par degrés croissants.

Notations 4.5. Comme nous avons convenu que $\mathrm{Gal}_k(f) \in \mathcal{T}(n)$, nous pouvons noter $\Gamma(f)$ la suite $\Gamma(\mathrm{Gal}_k(f))$ et $\Delta(f)$ la suite $\Delta(\mathrm{Gal}_k(f))$.

La proposition 4.1 montre que :

– $\Gamma(f)$ est, à permutation des facteurs de même degré près, la suite
$$\mathrm{Gal}_{k(\alpha_1)}(f_1), \ldots, \mathrm{Gal}_{k(\alpha_1)}(f_r)$$
– $\Delta(f) = deg(f_1), \ldots, deg(f_r)$.

La table de rupture donne des informations sur le groupe de Galois de f en fonction de $\Delta(f)$ ou $\Gamma(f)$ et vice-versa, comme l'illustrent en degré 8 les exemples ci-après.

Exemple 4.6. Considérons le polynôme irréductible sur $k = \mathbb{Q}$:
$$f := x^8 - 4x^7 + 14x^5 - 8x^4 - 12x^3 + 7x^2 + 2x - 1 \ .$$
En factorisant f dans son corps de rupture, nous obtenons quatre facteurs linéaires et un facteur irréductible de degré 4. Nous avons donc $\Delta(f) = 1^3, 4$. D'après la table TAB. 1, $\mathrm{Gal}_{\mathbb{Q}}(f)$ est un conjugué de $8T_{17}$ ou de $8T_{18}^{+}$. Le discriminant $300416 = 2^{12}41^3$ de f n'étant pas un carré dans $\mathbb{Q}$, $\mathrm{Gal}_{\mathbb{Q}}(f)$ est donc le groupe impair $8T_{17}$. On peut aussi bien tester la parité avec le facteur f_4 qu'avec f.

Exemple 4.7. Si $n = 8$ et $\mathrm{Gal}_k(f) = 8T_{46}$ alors $\Delta(f) = 3, 4$ et la factorisation de f sur $k(\alpha_1)$ s'écrit :
$$f(x) = (x - \alpha_1) f_1(\alpha_1, x) f_2(\alpha_1, x) \ ,$$
où f_1 et f_2 sont les facteurs de rupture de f de groupes de Galois respectifs $3T_2$ et $4T_5$ sur $k(\alpha_1)$.

La factorisation du polynôme f sur $k(\alpha_1)$ étant donnée, deux informations sont alors disponibles. D'une part, la table de rupture en degré n fournit une liste de groupes candidats à être le groupe de Galois. D'autre part, nous disposons des facteurs de rupture de f à partir desquels nous construirons un idéal de Galois de f (voir Section 5). Ces deux informations ne sont pas exploitées dans les algorithmes de factorisation dans les extensions.

5. Idéal de rupture et idéal induit

Posons $K = k(\alpha_1)$ et considérons les facteurs de rupture $f_1, \ldots, f_r$ de f sur $K[x]$ (voir Définition 4.4). Pour tout $i \in [\![1, n]\!]$, notons m_i le degré en la variable x de f_i, posons (avec $m_0 = 1$) :
$$X_i = \{x_{m_0 + \cdots + m_{i-1} + 1}, \ldots, x_{m_0 + \cdots + m_i}\}$$
et notons $T_{f_i}(\alpha_1)$ l'ensemble triangulaire formé par les modules de Cauchy du facteur f_i dans l'anneau de polynômes $K[X_i]$. Nous avons $\{x_2, \ldots, x_n\} = X_1 \cup \cdots \cup X_{m_r}$. Rappelons que $\Delta(f) = m_1, \ldots, m_r$. Dans $K[x_1, \ldots, x_n]$, l'idéal $\mathcal{I}$ engendré par l'ensemble triangulaire
$$\{x_1 - \alpha_1\} \cup T_{f_1}(x_1) \cup \cdots \cup T_{f_r}(x_1)$$
est l'idéal de Galois de f sur le corps K d'injecteur $S_{1,\Delta(f)}$ (voir [18]).

Exemple 5.1. Dans cet exemple, k désigne le corps des rationnels $\mathbb{Q}$. Soit le polynôme $f = x^8 - x^6 - x^4 + x^2 + 1$, irréductible sur k. Il se factorise sur son corps de rupture $k(\alpha_1)$ en :
$$f = (x - \alpha_1)(x + \alpha_1)(x^2 - \alpha_1^6 + \alpha_1^4 + \alpha_1^2 - 1)(x^4 + (\alpha_1^6 - \alpha_1^4)x^2 - 1)$$

et $\Delta(f) = 1, 2, 4$. D'après la table de rupture en degré 8, $\mathrm{Gal}_{\mathbb{Q}}(f)$ est un sous-groupe de $8T_{35}$. Les modules de Cauchy des facteurs de rupture de degré 2 et de degré 4 sont respectivement les deux ensembles de polynômes :

$$\begin{aligned} T_1(\alpha_1) &= \{ \quad x_3^2 - \alpha_1^6 + \alpha_1^4 + \alpha_1^2 - 1, \\ &\qquad x_4 + x_3\} \text{ dans } k(\alpha_1)[x_3, x_4] \text{ et} \\ T_2(\alpha_1) &= \{ \quad x_5^4 + (\alpha_1^6 - \alpha_1^4)x_5^2 - 1, \\ &\qquad x_6^3 + x_5^3 + x_5^2 x_6 + x_5 x_6^2 + (\alpha_1^6 - \alpha_1^4)x_5 + (\alpha_1^6 - \alpha_1^4)x_6, \\ &\qquad x_7^2 + x_5^2 + x_5 x_6 + x_5 x_7 + x_6^2 + x_6 x_7 + \alpha_1^6 - \alpha_1^4, \\ &\qquad x_8 + x_7 + x_6 + x_5\} \text{ dans } k(\alpha_1)[x_5, x_6, x_7, x_8]\,. \end{aligned}$$

L'idéal de Galois de f dur $K[x]$ d'injecteur $S_{1^2,2,4}$ est engendré par l'ensemble triangulaire T :

$$T = \{x_1 - \alpha_1\} \cup \{x_2 + x_1\} \cup T_1(x_1) \cup T_2(x_1)\,.$$

Définition 5.2. Un idéal de Galois de f sur $k(\alpha_1)$ est appelé un *idéal de rupture de* f. L'idéal $\mathcal{I}$ est appelé un *idéal de rupture symétrique de* f.

Remarque 5.3. À partir des facteurs de rupture de f, peuvent être construits autant d'idéaux de rupture symétriques que de permutations de S_r laissant la suite $\Delta(f)$ invariante (l'ordre des facteurs de rupture n'est pas unique dès que deux d'entre eux ont le même degré). Néanmoins, tous admettent $S_{1,\Delta(f)}$ comme injecteur.

Notations 5.4. Dans toute la suite de cet article, I_1 et $\mathfrak{M}_r$ désigneront des idéaux de rupture de f vérifiant :

$$\mathcal{I} \subset I_1 \subset \mathfrak{M}_r \tag{5.1}$$

et $\mathfrak{M}_r = Id_{k(\alpha_1)}(\underline{\alpha}) \in \mathcal{M}(I_1)$. Nous supposons que I_1 possède pour injecteur dans $\mathfrak{M}_r$ son groupe de décomposition que nous notons $\mathrm{Inj}(I_1)$. D'après la proposition 3.16, l'idéal I_1 est engendré par un ensemble triangulaire

$$\{x_1 - \alpha_1, F_2(x_1, x_2), \ldots, F_n(x_1, \ldots, x_n)\}$$

où les polynômes $F_2, \ldots, F_n$ sont à coefficients dans k.

De l'idéal I_1 se déduit naturellement un idéal de Galois de f de l'anneau $k[x_1, \ldots, x_n]$ (voir Corollaire 3.3) :

Définition 5.5. L'*idéal induit de l'idéal* I_1 est l'idéal I de Galois de f sur k défini par :

$$I = I_1 \cap k[x_1, \ldots, x_n]\,.$$

Proposition 5.6. *Posons* $F_1 = f$. *L'idéal* I *induit de* I_1 *est engendré par l'ensemble :*

$$\mathcal{T} = \{F_1(x_1), F_2(x_1, x_2), \ldots, F_n(x_1, \ldots, x_n)\}$$

qui est triangulaire.

Démonstration. Car le polynôme f est irréductible sur k. □

Proposition 5.7. *Pour tout $\mathfrak{M} \in \mathcal{M}(I)$, alors il existe $\mathfrak{N}_r \in \mathcal{M}(\mathcal{I})$ tel que $\mathfrak{M}$ est induit de $\mathfrak{N}_r$ et*

$$\mathcal{M}(I) = \{\sigma.\mathfrak{M} \mid \sigma \in \mathrm{Inj}(I_1)\}.$$

Autrement formulé :

$$\mathcal{M}(I) = \{Id_k(\underline{\beta}) \mid \underline{\beta} \in V(I_1)\} .$$

Démonstration. Le première assertion est évidente. Soit $\mathfrak{N}_r$ l'idéal dont $\mathfrak{M}$ est induit. Nous avons $\mathrm{Inj}(I_1) = \mathrm{Inj}(I_1, \mathfrak{N}_r)$. La proposition est démontrée par la suite d'égalités suivantes.

$$I = I_1 \cap k[x_1, \ldots, x_n] = \bigcap_{\sigma \in \mathrm{Inj}(I_1)} \sigma^{-1}.\mathfrak{N}_r \cap k[x_1, \ldots, x_n] = \bigcap_{\sigma \in \mathrm{Inj}(I_1)} \sigma.\mathfrak{M}$$

car $\mathrm{Inj}(I_1)$ est un groupe. □

Proposition 5.8. *Tout $\mathfrak{M} \in \mathcal{M}(I)$ vérifie :*

(1) $\mathrm{Dec}(\mathfrak{M})_{\{1\}} \subset \mathrm{Inj}(I_1) \subset S_{1,\Delta(f)}$;
(2) $Orb(Dec(\mathfrak{M})_{\{1\}}) = Orb(\mathrm{Inj}(I_1)) = Orb(S_{1,\Delta(f)})$.

Démonstration. Nous pouvons supposer que $\mathfrak{M} = \mathfrak{M}_r \cap k[x_1, \ldots, x_n]$. Nous obtenons les inclusions inverses des injecteurs des idéaux de (5.1) :

$$\mathrm{Dec}(\mathfrak{M}_r) \subset \mathrm{Inj}(I_1) \subset S_{1,\Delta(f)} . \quad (*)$$

Des identités $\mathrm{Dec}(\mathfrak{M}_r) = \mathrm{Dec}(\mathfrak{M})_{\{1\}}$ et $Orb(\mathrm{Dec}(\mathfrak{M})_{\{1\}}) = Orb(S_{1,\Delta(f)})$ (par définition de $\Delta(f)$), nous en déduisons, avec $(*)$, les assertions (1) et (2) de la proposition. □

Nous allons maintenant donner une décomposition de l'idéal I :

Proposition 5.9. *Soit $\mathfrak{M} \in \mathcal{M}(I)$ et soient $\tau_1, \ldots, \tau_n$, des permutations du groupe $\mathrm{Dec}(\mathfrak{M})$ telles que, pour tout $i \in [\![1, n]\!]$, $\tau_i(1) = i$. Nous avons :*

$$k(\underline{\alpha}) \otimes_k I = \bigcap_{i=1}^{n} \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1) .$$

Démonstration. Nous pouvons supposer que $\mathfrak{M} = Id_k(\underline{\alpha})$. Notons $V = Inj(I_1).\underline{\alpha}$ la variété de I_1 et posons $W = \mathrm{Gal}_k(\underline{\alpha}).V$. Comme V est stable par $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha})$ (voir Proposition 3.13) et que $\tau_1, \ldots, \tau_n$ est une transversale à gauche de $\mathrm{Gal}_k(\underline{\alpha})$ modulo $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha})$, nous avons

$$W = \bigcup_{i \in [\![1,n]\!]} \tau_i.V .$$

Par définition, W est la variété de l'idéal de Galois $Id_k(V)$ (voir Proposition 3.13). Ainsi,

$$\mathrm{Id}_k(W) = \mathrm{Id}_k(V) = I_1 \cap k[x_1, \ldots, x_n]$$

et donc, comme W est une variété définie sur k (i.e. son idéal possède un système de générateurs à coefficients dans k)

$$Id_{k(\underline{\alpha})}(W) = k(\underline{\alpha}) \otimes_k (I_1 \cap k[x_1, \ldots, x_n]) .$$

Par définition de I, il vient

$$k(\underline{\alpha}) \otimes_k I = k(\underline{\alpha}) \otimes_k (I_1 \cap k[x_1, \ldots, x_n]) = Id_{k(\underline{\alpha})}(W) = \bigcap_{i \in [\![1,n]\!]} Id_{k(\underline{\alpha})}(\tau_i.V)$$

Or, d'après le lemme 3.12, nous avons les égalités

$$\forall i \in [\![1, n]\!],\ Id_{k(\underline{\alpha})}(\tau_i.V) = \overline{\tau_i}(Id_{k(\underline{\alpha})}(V)) = \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)\,,$$

d'où le résultat. □

Étant donné $L = \mathrm{Inj}(I_1)$, l'objectif est maintenant de calculer un injecteur de l'idéal I induit de I_1 (voir Paragraphe 7) pour le cas où ce n'est pas le groupe de décomposition de I. Pour cela, nous ferons appel aux résultats résultats du paragraphe suivant.

6. Ensemble $\mathcal{A}(L)$, application Ψ et groupes L-conjugués

Dans ce paragraphe, sont présentés les résultats portant uniquement sur les ensembles de permutations.
Considérons un sous-groupe L de $S_{1,n-1}$ (i.e. tel que $\forall \sigma \in L,\ \sigma(1) = 1$).

Définition 6.1. Nous appellerons *groupe admissible* tout sous-groupe transitif H de S_n vérifiant $H_{\{1\}} \subset L$ et tel que $Orb(L) = Orb(H_{\{1\}})$. L'ensemble des groupes admissibles sera noté $\mathcal{A}(L)$.

Remarque 6.2. Notons $1, e$ la suite croissante des cardinaux des éléments de $Orb(L)$. Pour H un sous-groupe transitif de S_n, il est facile de montrer l'équivalence :

$$H \in \mathcal{A}(L) \ \text{ ssi } \ \Delta(H) = 1, e \ \text{ et } \ H_{\{1\}} \subset L.$$

Ainsi, pour obtenir $\mathcal{A}(L)$, il suffit de déterminer les groupes H' de $\mathcal{T}(n)$ tel que $\Delta(H') = 1, e$ (à l'aide de la table de rupture en degré n), puis de calculer les groupes H conjugués de H' vérifiant $H_{\{1\}} \subset L$.

Proposition 6.3. *Soit $H \in \mathcal{A}(L)$ et soient $\{\sigma_1, \ldots, \sigma_s\}$ et $\{\sigma'_1, \ldots, \sigma'_s\}$ deux transversales à droite de L modulo $H_{\{1\}}$. Alors*

$$H\sigma_1 + \cdots + H\sigma_s = H\sigma'_1 + \cdots + H\sigma'_s\,.$$

Démonstration. Puisque $\forall i \in [\![1, n]\!],\ \sigma_i \in L$, il vient $\sigma_i \in H_{\{1\}}\sigma'_1 + \cdots + H_{\{1\}}\sigma'_s$, puis successivement,

$$\forall i \in [\![1, n]\!],\ H\sigma_i \subset H\sigma'_1 + \cdots + H\sigma'_s,$$
$$H\sigma_1 + \cdots + H\sigma_s \subset H\sigma'_1 + \cdots + H\sigma'_s.$$

L'inclusion réciproque se démontre de la même manière. □

Cette proposition montre que l'application Ψ ci-dessous est bien définie.

Notations 6.4. Nous noterons Ψ l'application de $\mathcal{A}(L)$ dans l'ensemble des parties de S_n définie pour tout $H \in \mathcal{A}(L)$ par :

$$\Psi(H) = H\sigma_1 + \cdots + H\sigma_s\,,$$

où $\{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ est une transversale à droite de L modulo $H_{\{1\}}$.

Proposition 6.5. *L'application Ψ possède les propriétés suivantes :*

(1) *Si $H \in \mathcal{A}(L)$ et si $\tau_1 = id, \ldots, \tau_n$ désignent n permutations de H telles que, pour tout $i \in [\![1, n]\!]$ $\tau_i(1) = i$, alors*
$$\Psi(H) = \tau_1 L + \cdots + \tau_n L\,.$$

(2) *Si H et G appartiennent à $\mathcal{A}(L)$ et si $H \cap G$ est un sous-groupe transitif de S_n alors $\Psi(G) = \Psi(H)$.*

Démonstration. Démontrons la première assertion. Puisque le groupe H est transitif, les permutations τ_i existent et $H = \tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}}$. Nous avons alors, pour $\{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ une transversale à droite de L modulo $H_{\{1\}}$:
$$\begin{aligned}\Psi(H) &= (\tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}})\sigma_1 + \cdots + (\tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}})\sigma_s \\ &= \tau_1 L + \cdots + \tau_n L\,.\end{aligned}$$
Pour la seconde assertion, il suffit de prendre $\tau_1, \ldots, \tau_n$ dans l'intersection transitive $H \cap G$ et l'assertion (1) donne $\Psi(H) = \tau_1 L + \cdots + \tau_n L = \Psi(G)$. □

Corollaire 6.6. *Soit $H \in \mathcal{A}(L)$. Alors, le cardinal de $\Psi(H)$ ne dépend que de celui de L :*
$$\mathrm{Card}(\Psi(H)) = s\,\mathrm{Card}(H) = n\,\mathrm{Card}(L)\,.$$

Définition 6.7. Soient deux sous-groupes G et H de S_n. Le groupe G est dit *L-conjugué à H* s'il existe σ dans L tel que $H = G^\sigma = \sigma G \sigma^{-1}$.

Proposition 6.8. *Soient H et G deux groupes L-conjugués appartenant à $\mathcal{A}(L)$. Nous avons les assertions suivantes :*

(1) *si σ désigne une permutation de L telle que $H = G^\sigma$, alors*
$$\Psi(H) = \sigma\,\Psi(G)\,;$$

(2) *si $\{\sigma_1, \ldots, \sigma_s\}$ désigne une transversale à droite de L modulo $H_{\{1\}}$ alors il existe $i \in [\![1, s]\!]$ tel que $H = G^{\sigma_i}$; en particulier, le nombre de groupes L-conjugués à H est majoré par s.*

Démonstration. Montrons l'assertion (1) et reprenons les notations de la Proposition 6.5. Posons, pour tout $i \in [\![1, n]\!]$, $\rho_i = \sigma^{-1}\tau_i\,\sigma$. Les permutations $\rho_1, \ldots, \rho_n$ appartiennent à $G = H^{\sigma^{-1}}$ et nous avons successivement,
$$\begin{aligned}\Psi(H) &= \tau_1 L + \cdots + \tau_n L \\ &= \sigma\,\rho_1\sigma^{-1} L + \cdots + \sigma\,\rho_n\sigma^{-1} L \\ &= \sigma\,\rho_1 L + \cdots + \sigma\,\rho_n L \\ &= \sigma\,\Psi(G),\end{aligned}$$
d'après l'assertion (1) de la proposition 6.5 et le fait que $\{\rho_i(1) \mid i \in [\![1, n]\!]\} = \{1, \ldots, n\}$.

Montrons l'assertion (2). Si G et H sont L-conjugués, il existe $\sigma \in L$ tel que $H = G^\sigma$. L'égalité $L = H_{\{1\}}\sigma_1 + H_{\{1\}}\sigma_2 + \cdots + H_{\{1\}}\sigma_s$ impose à σ d'appartenir à l'un des ensembles $H_{\{1\}}\sigma_i$, pour un entier $i \in [\![1, s]\!]$, et donc de s'écrire $\sigma = h\sigma_i$, où

h désigne une permutation de H. Le résultat se déduit alors des égalités successives : $G = \sigma_i^{-1} h^{-1} H\, h\, \sigma_i = \sigma_i^{-1}\, H\, \sigma_i$. □

Les deux propositions suivantes nous seront utiles pour exprimer l'ensemble des injecteurs d'un idéal induit de I_1 et pour déterminer de manière constructive cet ensemble même lorsqu'il existe plusieurs idéaux de rupture symétriques (voir Remarque 5.3).

Proposition 6.9. *Soit H un groupe appartenant à $\mathcal{A}(L)$. Alors, pour tout $\sigma \in L$, le groupe H^σ appartient à $\mathcal{A}(L)$.*

Démonstration. Pour tout sous-groupe G de S_n et toute permutation $\sigma \in S_n$, nous avons :

$$(G^\sigma)_{\{1\}} = (G_{\{\sigma^{-1}(1)\}})^\sigma \text{ et} \tag{6.1}$$

$$Orb(G^\sigma) = \sigma.Orb(G)\ . \tag{6.2}$$

Il s'ensuit les égalités successives suivantes :

$$\begin{aligned} Orb((H^\sigma)_{\{1\}}) &= Orb((H_{\{1\}})^\sigma), \text{ d'après l'égalité (6.1) et puisque } \sigma(1) = 1, \\ &= \sigma.Orb(H_{\{1\}}), \text{ d'après l'égalité (6.2)}, \\ &= \sigma.Orb(L), \text{ car } H \in \mathcal{A}(L), \\ &= Orb(L), \text{ car } \sigma \in L\ . \end{aligned}$$

Le groupe H^σ étant transitif, H^σ appartient à $\mathcal{A}(L)$. □

7. Calcul des injecteurs d'un idéal induit

L'idéal I_1 de ce paragraphe est celui du paragraphe 5 (voir Notation 5.4). Nous notons L l'injecteur de I_1. Il vérifie $L \subset S_{1,\Delta(f)}$ (voir Proposition 5.8). L'idéal I est induit de I_1 (voir Définition 5.5). Nous cherchons à déterminer les injecteurs de I dans les idéaux de $\mathcal{M}(I)$.

7.1. Formulation des injecteurs de l'idéal induit.

Proposition 7.1. *Pour tout $\mathfrak{M} \in \mathcal{M}(I)$, le groupe de Galois* $\mathrm{Dec}(\mathfrak{M})$ *appartient à $\mathcal{A}(L)$ et*

$$\mathrm{Inj}(I, \mathfrak{M}) = \Psi(Dec(\mathfrak{M}))\ ,$$

où Ψ est l'application définie dans la notation 6.4.

Démonstration. Le groupe $\mathrm{Dec}(\mathfrak{M})$ appartient à $\mathcal{A}(L)$ d'après la proposition 5.8. D'après la proposition 5.7, nous pouvons supposer que $\mathfrak{M} = Id_k(\underline{\alpha})$ avec $\underline{\alpha} \in V(I_1)$; i.e. $\mathrm{Inj}(I, \mathfrak{M}) = \mathrm{Inj}(I, \underline{\alpha})$. Soient n permutations $\tau_1, \ldots, \tau_n$ de $\mathrm{Dec}(\mathfrak{M})$ telles que, pour tout $i \in [\![1, n]\!]$, $\tau_i(1) = i$. D'après la proposition 5.9, nous avons l'égalité :

$$k(\underline{\alpha}) \otimes_k I = \bigcap_{i=1}^{n} \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)\ .$$

L'idéal $\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)$ contient le polynôme $x_1 - \alpha_i$. Puisque les racines $\alpha_1, \ldots, \alpha_n$ sont distinctes, les idéaux $\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)$, pour $i \in [\![1, n]\!]$, sont deux à deux comaximaux. Nous avons les égalités suivantes :

$$\begin{aligned}
\mathrm{Inj}(I, \underline{\alpha}) &= \mathrm{Inj}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I, \underline{\alpha}), \text{ d'après l'égalité (3.5)}, \\
&= \sum_{i=1}^{n} \mathrm{Inj}(\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha}), \text{ d'après l'égalité (3.6)}, \\
&= \sum_{i=1}^{n} \tau_i \, \mathrm{Inj}((k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha}), \text{ d'après le lemme 3.12}, \\
&= \sum_{i=1}^{n} \tau_i \, \mathrm{Inj}(I_1, \underline{\alpha}), \text{ d'après la remarque 3.6}, \\
&= \Psi(Dec(\mathfrak{M})),
\end{aligned}$$

où la dernière égalité est obtenue en appliquant l'assertion (1) de la proposition 6.5 à $L = \mathrm{Inj}(I_1, \underline{\alpha})$. □

Théorème 7.2. *Soit $H \in \mathcal{A}(L)$ et $\mathfrak{M} \in \mathcal{M}(I)$ tels que $H \cap \mathrm{Dec}(\mathfrak{M})$ soit un sous-groupe transitif de S_n. Alors l'ensemble des injecteurs de l'idéal I induit de I_1 dans les idéaux maximaux qui le contiennent est formé des*

$$\mathrm{Inj}(I, \sigma.\mathfrak{M}) = \Psi(H^\sigma)$$

où σ parcourt l'injecteur L de I_1.

Démonstration. D'après les propositions 5.7 et 7.1, l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent est formé des $\mathrm{Inj}(I, \sigma.\mathfrak{M}) = \Psi(Dec(\sigma.\mathfrak{M}))$ où σ parcourt L. Soit $\sigma \in L$. Comme $H \cap \mathrm{Dec}(\mathfrak{M})$ est transitif, le groupe $H^\sigma \cap \mathrm{Dec}(\mathfrak{M})^\sigma = H^\sigma \cap \mathrm{Dec}(\sigma.\mathcal{M})$ est aussi transitif. Selon l'assertion (2) de la proposition 6.5 appliquée à $G = Dec(\sigma.\mathfrak{M})$, nous avons donc $\Psi(H^\sigma) = \Psi(G)$. □

Corollaire 7.3. *Reprenons les hypothèses du théorème 7.2 et notons s l'indice de $H_{\{1\}}$ dans L. Alors*

$$\mathrm{Card}(\mathrm{Inj}(I, \mathfrak{M})) = s.\,\mathrm{Card}(H) = n.\,\mathrm{Card}(L)\ .$$

Démonstration. Ces deux égalités sont des conséquences immédiates du corollaire 6.6 et du théorème 7.2. □

Si un groupe H vérifiant les hypothèses du théorème 7.2 est connu, il est alors possible de calculer un injecteur de I. Il n'est pas toujours immédiat de tester si $H \cap \mathrm{Dec}(\mathfrak{M})$ est transitif pour un idéal $\mathfrak{M} \in \mathcal{M}(I)$; et ce d'autant plus lorsqu'au moins deux des facteurs de rupture de f sont de même degré. C'est à cette question que sont consacrés les deux paragraphes suivants.

7.2. Classes de L-conjugaison associées aux idéaux induits.

Définition 7.4. Un groupe $H \in \mathcal{A}(L)$ est dit *associé à l'idéal* I s'il existe $\mathfrak{M} \in \mathcal{M}(I)$ tel que $H \cap \mathrm{Dec}(\mathfrak{M})$ soit transitif (i.e. si H vérifie les hypothèses du théorème 7.2).

Il s'agit d'étudier à quels idéaux sont associés les différents conjugués dans $\mathcal{A}(L)$ d'un groupe H de $\mathcal{A}(L)$. Les groupes L-conjugués à H appartiennent aussi à $\mathcal{A}(L)$ (voir Proposition 6.9) et si H est associé à I alors tout groupe de sa classe de L-conjugaison $\mathcal{C}$ l'est aussi (voir Démonstration du théorème 7.2). Nous pouvons donc introduire la définition suivante :

Définition 7.5. La classe $\mathcal{C}$ de L-conjugaison d'un groupe $H \in \mathcal{A}(L)$ est dite *associée à l'idéal* I si H est associé à I.

Remarque 7.6. Si la classe $\mathcal{C}$ est associée à l'idéal I alors, d'après le théorème 7.2, $\{\Psi(H') \mid H' \in \mathcal{C}\}$ est l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent.

Nous commençons notre étude par celle plus simple de $\mathcal{A}(S_{1,e})$, avec $e = (e_1, \ldots, e_r) \in \mathbb{N}^r$, un r-uplet d'entiers croissants de somme $n-1$. Les résultats sur $\mathcal{A}(L)$ s'en déduiront aisément.
Soit le sous-groupe de S_n

$$M = \{\sigma \in S_n \,|\, \sigma(1) = 1 \ \text{ et } \ Orb(S_{1,e}) = \sigma.Orb(S_{1,e})\} \ .$$

D'après l'identité (6.2), le groupe M est le normalisateur de $S_{1,e}$ dans $S_{1,n-1}$; en particulier, le groupe $S_{1,e}$ est distingué dans M.
Le groupe M agit sur les $S_{1,e}$-orbites $O_0 = (1), O_1, \ldots, O_r$ de $\{1, \ldots, n\}$ (i.e. sur $Orb(S_{1,e})$) en laissant fixe une orbite (par les permutations de $S_{1,e}$) ou en l'envoyant sur une autre orbite de même cardinal.
Nous supposons que les orbites sont indicées par cardinalité croissante (i.e. $\mathrm{Card}(O_i) = e_i$ pour $i = 1, \ldots, r$). Le groupe $S_{1,e}$ (distingué dans M) est le noyau du morphisme surjectif :

$$\begin{array}{rccl} \phi: & M & \longrightarrow & \mathrm{Stab}_{S_r}(e) \\ & \sigma & \mapsto & \tau : \tau(i) = j \text{ si } \sigma.O_i = O_j (= O_{\tau(i)}) \ i = 1, \ldots, r \ . \end{array}$$

Le cardinal N du stabilisateur $\mathrm{Stab}_{S_r}(e)$ de e dans S_r est aussi l'ordre du groupe $M/S_{1,e}$. Nous considérons $\{\tau_1 = id, \ldots, \tau_N\}$ une transversale à droite de $M \mod S_{1,e}$ (c'est aussi une transversale à gauche).

Lemme 7.7. *Soit $H \in \mathcal{A}(S_{1,e})$. Alors l'ensemble des groupes S_n-conjugués à H appartenant à $\mathcal{A}(S_{1,e})$ est formé des H^σ où σ parcourt M.*

Démonstration. Soit $\sigma \in M$. Nous avons d'une part (voir (6.1)) :

$$(H^\sigma)_{\{1\}} = (H_{\{\sigma^{-1}(1)\}})^\sigma = (H_{\{1\}})^\sigma \subset S_{1,e}^\sigma = S_{1,e}$$

et d'autre part (voir (6.2)) :

$$Orb(H^\sigma) = \sigma.Orb(H) = \sigma.Orb(S_{1,e}) = Orb(S_{1,e}) \ .$$

Donc $H^\sigma \in \mathcal{A}(S_{1,e})$.
Pour l'inclusion inverse, prenons $\tau \in S_n$ tel que $H^\tau \in \mathcal{A}(S_{1,e})$. Puisque H est transitif, il existe $h \in H$ tel que $\tau h(1) = 1$. Posons $\sigma = \tau h$. Nous avons $H^\tau = H^\sigma$. Donc, d'une part, $\sigma(1) = 1$ et, d'autre part, $Orb(S_{1,e}) = \sigma.Orb(S_{1,e})$ puisque $Orb(H^\sigma) = Orb(S_{1,e})$ et que $Orb(H) = Orb(S_{1,e})$. D'où $\sigma \in M$. □

Lemme 7.8. *Soit $H \in \mathcal{A}(S_{1,e})$ et considérons les m classes de conjugaison par $S_{1,e}$ des S_n-conjugués de H appartenant à $\mathcal{A}(S_{1,e})$ (i.e. les H^σ où σ parcourt M). Alors nous avons les assertions suivantes :*
(1) soit $\sigma \in S_{1,e}\tau_i$; la conjugaison par σ induit une bijection entre la classe de H et celle de H^{τ_i} ;
(2) chaque classe est celle d'un groupe H^{τ_i}, où $i \in [\![1, N]\!]$ formé des H^σ où $\sigma \in S_{1,e}\tau_i$.
(3) $m \leq N$.

Démonstration. Pour montrer (1), il suffit de constater que si $l \in S_{1,e}$, alors $(H^l)^\sigma = (H^\sigma)^{\sigma l \sigma^{-1}}$ appartient à la même classe que H^σ puisque $S_{1,e}$ est distingué dans M. Cette orbite est celle de H^{τ_i} puisque $\sigma = \tau\tau_i \in M$ avec $\tau \in S_{1,e}$ et donc $H^\sigma = (H^{\tau_i})^\tau$.
Pour montrer (2), considérons une classe. Elle est celle d'un groupe H^σ où $\sigma \in M$ (voir Lemme 7.7) ; c'est-à-dire qu'il existe $i \in [\![1, N]\!]$ tel que $\sigma \in S_{1,e}\tau_i$. Donc la classe est celle de H^{τ_i}.
Il est évident que le nombre de classes est inférieur à N. □

Ayant étudié les classes de conjugaison par $S_{1,e}$ des conjugués H dans $\mathcal{A}(S_{1,e})$, nous cherchons à savoir à quels idéaux induits des idéaux de rupture symétriques de f elles sont associées lorsque :
- $e = \Delta(f)$ est la suite croissante des degrés des facteurs de rupture $f_1, \ldots, f_r$ (voir Paragraphe 4), que
- H est associé à l'idéal de rupture symétrique $\mathcal{I}$ construit à partir de $f_1, \ldots, f_r$ (voir Paragraphe 5) et que
- I est l'idéal induit de $\mathcal{I}$ (i.e. $I = \mathcal{I} \cap k[x_1, \ldots, x_n]$).

Les facteurs de rupture sont ordonnés en respectant la croissance des degrés. Donc il existe exactement N, le cardinal de $\mathrm{Stab}_{S_r}(e)$, listes de facteurs de ruptures distinctes (car les racines de f le sont) induisant par construction N idéaux de rupture symétriques distincts. Plus précisément, comme $S_{1,e}$ est le noyau du morphisme surjectif ϕ, ces N listes sont les

$$(f_{\phi(\tau_i)(1)}, \ldots, f_{\phi(\tau_i)(r)}) \quad i = 1, \ldots, N$$

respectivement aux origines des constructions des N idéaux de rupture symétriques $\tau_i.\mathcal{I}$, d'idéaux induits respectifs :

$$\tau_1.I, \tau_2.I, \ldots, \tau_N.I \ .$$

Remarque 7.9. Le groupe $S_{1,e}$ étant celui de décomposition de chaque idéal de rupture symétrique, par définition de $\tau_1, \ldots, \tau_N$, l'ensemble $\{\sigma.I \mid \sigma \in M\}$ est l'ensemble des idéaux induits des idéaux de rupture symétriques. Soit $\mathfrak{M} \in \mathcal{M}(I)$. Nous avons

$\mathrm{Dec}(\mathfrak{M}) \in \mathcal{A}(S_{1,e})$ (voir Proposition 5.8). Comme $\mathcal{M}(I) = \{\tau.\mathcal{M} \mid \tau \in S_{1,e}\}$ (voir Proposition 5.7) , l'ensemble des idéaux maximaux contenant un idéal induit est

$$\mathcal{F} = \{\sigma.\mathfrak{M} \mid \sigma \in M\}.$$

L'ensemble des groupes de décomposition des idéaux de $\mathcal{F}$ est formé des $\mathrm{Dec}(\mathfrak{M})^\sigma$ (=$\mathrm{Dec}(\sigma.\mathfrak{M})$) où σ parcourt M ; c'est-à-dire l'ensemble des conjugués de $\mathrm{Gal}_k(f)$ (i.e. de $\mathrm{Dec}(\mathfrak{M})$) appartenant à $\mathcal{A}(S_{1,e})$ (voir Lemme 7.7).

Lemme 7.10. *Soit $\sigma \in M$. Si le groupe H est associé à l'idéal I alors le groupe H^σ est associé à l'idéal $\sigma.I$ induit de $\sigma.\mathcal{I}$.*

Démonstration. Soit $\mathfrak{M} \in \mathcal{M}(I)$ tel que $H \cap \mathrm{Dec}(\mathfrak{M})$ soit un sous-groupe transitif de S_n. Alors $H^\sigma \cap Dec(\sigma.\mathfrak{M})$ est également transitif avec $\sigma.\mathfrak{M} \in \mathcal{M}(\sigma.I)$ (i.e. l'idéal $\sigma.\mathfrak{M}$ est un idéal maximal contenant $\sigma.I$). □

Les résultats précédents permettent d'énoncer le théorème suivant :

Théorème 7.11. *Soit $H \in \mathcal{A}(S_{1,e})$ supposé être associé à l'idéal I induit de $\mathcal{I}$. Alors :*
(1) à chaque idéal $\tau_i.I$ induit de l'idéal de rupture $\tau_i.\mathcal{I}$, $i = 1, \ldots, N$, est associée la classe de $S_{1,e}$-conjugaison du groupe H^{τ_i} ;
(2) tout groupe $H^\sigma \in \mathcal{A}(S_{1,e})$ (i.e. $\sigma \in M$) est associé à l'idéal $\sigma.I$ induit de l'idéal de rupture $\sigma.\mathcal{I}$. Donc toute la classe de $S_{1,e}$-conjugaison de H^σ est associée à $\sigma.I$.

Le corollaire suivant est utilisé dans les pré-calculs :

Corollaire 7.12. *Soient G, un conjugué de $\mathrm{Gal}_k(f)$, et H deux groupes de $\mathcal{A}(S_{1,e})$ tels que $H \cap G$ soit un sous-groupe transitif de S_n. Alors il existe groupe conjugué de H appartenant $\mathcal{A}(S_{1,e})$ qui est associé I (ainsi que sa classe de $S_{1,e}$-conjugaison). En particulier, si les groupes conjugués à H appartenant $\mathcal{A}(S_{1,e})$ sont tous $S_{1,e}$-conjugués alors H est associé à I.*

Remarque 7.13. L'hypothèse du corollaire 7.12 est vérifiée lorsque nous savons que le groupe de Galois $\mathrm{Gal}_k(f)$ appartient à un ensemble et que tout groupe de cet ensemble possède un conjugué dans $\mathcal{A}(S_{1,e})$ d'intersection transitive avec le groupe H.

Remarque 7.14. Plaçons-nous dans le cas où les parts e_i du n-uplet $e = (e_1, \ldots, e_r)$ sont distinctes deux à deux (i.e. $N = 1$, $M = S_{1,e}$ et $\mathrm{Stab}_{S_r}(e)$ est réduit à l'identité). Il n'existe qu'un seul idéal de rupture symétrique de f. Si $H \in \mathcal{A}(S_{1,e})$ alors les conjugués de H dans $\mathcal{A}(S_{1,e})$ sont $S_{1,e}$-conjugués à H (voir Lemme 7.7).

Nous pouvons désormais revenir à I induit de l'idéal de rupture I_1 avec $L = \mathrm{Inj}(I_1)$. Soit $H \in \mathcal{A}(L)$. D'après la proposition 6.9, les S_n-conjugués de H qui appartiennent à $\mathcal{A}(L)$ se répartissent en classes de L-conjugaison.

Corollaire 7.15. *Supposons le groupe H associé à l'idéal I. Alors, pour tout conjugué G de H appartenant à $\mathcal{A}(L)$, il existe $\sigma \in M$ tels que $G = H^\sigma$ et G est associé à l'idéal $\sigma.I$ induit de $\sigma.I_1$.*

Démonstration. Comme $\mathcal{A}(L) \subset \mathcal{A}(S_{1,e})$ (voir Proposition 5.8), il existe $\sigma \in M$ tel que $G = H^\sigma$ (voir Lemme 7.7). L'idéal $\sigma.I_1$ contient l'idéal $\sigma.\mathcal{I}$ qui est de rupture symétrique puisque $\sigma \in M$ (voir Remarque 7.9). En reprenant la démonstration du lemme 7.10, le groupe H^σ est bien associé à l'idéal $\sigma.I$ induit de $\sigma.I_1$. □

Remarque 7.16. Pour tout $\mathfrak{M} \in \mathcal{M}(I)$, $\mathrm{Dec}(\mathfrak{M}) \in \mathcal{A}(L)$ (voir Proposition 5.8) est associé I. Lorsque $\mathrm{Gal}_k(f)$ est déterminé, nous connaissons ses S_n-conjugués appartenant à $\mathcal{A}(L)$. Il s'agit de pouvoir identifier la classe de L-conjugaison de $\mathfrak{M}$.

Nous venons d'étudier les liens entre les classes de $S_{1,e}$-conjugaisons et les idéaux induits d'idéaux de rupture symétriques. Nous n'avons pas résolu le problème d'identification de la classe associée à I. C'est à la résolution de ce problème qu'est consacré le paragraphe suivant.

7.3. **Association d'une classe de L-conjugaison à l'idéal induit I.**

Dans ce paragraphe, I désignera un idéal induit d'un idéal de rupture I_1 et $\mathfrak{C}$ l'ensemble des classes de L-conjugaison de groupes appartenant à $\mathcal{A}(L)$. Nous savons qu'au moins une de ces classes est associée à I (voir Remarque 7.16). Les résultats de ce paragraphe permettent de tester si une classe de L-conjugaison de $\mathfrak{C}$ est associée ou non à l'idéal I.

La proposition suivante permet toujours de déterminer un injecteur de I.

Proposition 7.17. *Un groupe H de $\mathcal{A}(L)$ est associé à I si et seulement si il vérifie*

$$I + \Psi(H).I \neq k[x_1, \ldots, x_n] \ .$$

Démonstration. Cette dernière inégalité est vérifiée si et seulement si il existe $\underline{\beta} \in V(I)$ tel que $\Psi(H) \subset \mathrm{Inj}(I, \underline{\beta})$ (voir Proposition 3.7). Puisque $\mathrm{Card}(\Psi(H))$ est le cardinal de tout injecteur de I (voir Corollaire 6.6 et Corollaire 7.3), $\Psi(H)$ est égal à $\mathrm{Inj}(I, \underline{\beta})$. □

Remarque 7.18. Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux classes de $\mathfrak{C}$. D'après les propositions 6.5 et 6.8, s'il existe deux groupes $H_1 \in \mathcal{C}_1$ et $H_2 \in \mathcal{C}_2$ tels que $H_1 \cap H_2$ soit un sous-groupe transitif de S_n alors

$$\{\Psi(H) \mid H \in \mathcal{C}_1\} = \{\Psi(H) \mid H \in \mathcal{C}_2\} \ .$$

Supposons que $I + \Psi(H_1).I = k[x_1, \ldots, x_n]$. Avec cette hypothèse, la proposition 7.17 prouve qu'aucun des groupes de $\mathcal{C}_1$ et de $\mathcal{C}_2$ ne permet le calcul d'un injecteur de I. Supposons que $I + \Psi(H_1).I \neq k[x_1, \ldots, x_n]$. Avec cette hypothèse, la proposition 7.17 montre que $\Psi(H_1)$ est un injecteur de I et qu'aucune des classes $\mathcal{C}$ telle que $\Psi(H_1) \notin \{\Psi(H) \mid H \in \mathcal{C}\}$ n'est associée à I.

La proposition suivante permet de pré-établir des *critères d'association* entre les classes de $\mathfrak{C}$ et les idéaux induits :

Proposition 7.19. *Si $\mathcal{C} \in \mathfrak{C}$ est associée à l'idéal induit I, alors*

$$I = \bigcap_{H\in\mathcal{C}} H.I \quad \left(= \bigcap_{H\in\mathcal{C}} \{\sigma.R \mid \sigma \in H, \quad R \in I\} \right) .$$

Démonstration. Soit $H \in \mathcal{C}$. Par hypothèse, il existe $\mathfrak{M} \in \mathcal{M}(I)$ tel que $\mathrm{Inj}(I, \mathfrak{M}) = \Psi(H)$ (voir Théorème 7.2). Par définition de Ψ, l'injecteur $\mathrm{Inj}(I, \mathfrak{M})$ s'écrit donc

$$\mathrm{Inj}(I, \mathfrak{M}) = H\sigma_1 + \cdots + H\sigma_s ,$$

où $\{\sigma_1, \ldots, \sigma_s\}$ est une transversale à droite de L modulo $H_{\{1\}}$. Par suite, l'idéal I se décompose comme suit :

$$I = Id_k(\mathrm{Inj}(I, \underline{\alpha}).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k((H\sigma_i).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k(H^{\sigma_i^{-1}}.(\sigma_i.\underline{\alpha})) , \tag{7.1}$$

Soient $H^\sigma \in \mathcal{C}$ où $\sigma \in \{\sigma_1^{-1}, \ldots, \sigma_n^{-1}\} \subset L$ et $R \in I$. D'après l'égalité (7.1), nous avons $R \in Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$ et donc, par la proposition 3.14, il vient $H^\sigma.I \subset Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$. La décomposition (7.1) permet d'en déduire l'inclusion $\bigcap_{H'\in\mathcal{C}} H'.I \subset I$. Or $I \subset \bigcap_{H'\in\mathcal{C}} H'.I$, d'où le résultat. □

La proposition 7.19 s'applique pour établir des *critères d'association* tels ceux présentés dans l'exemple 7.20 qui suit.

Exemple 7.20. Supposons que f soit un polynôme de degré 8 tel que $\Delta(f) = 1^3, 2^2$. L'injecteur de tout idéal de rupture symétrique $\mathcal{I}$ est $L = S_{1^4,2^2}$. Tout idéal I induit par un idéal de rupture symétrique est engendré par un ensemble triangulaire $\mathfrak{T}_I$ de la forme :

$$\begin{aligned} \mathfrak{T}_I \quad = \quad \{&f(x_1),\ x_2 + g_2(x_1),\ x_3 + g_3(x_1),\ x_4 + g_4(x_1),\\ &F_5(x_5, x_1),\ x_6 + g_6(x_5, x_1),\ F_7(x_7, x_1),\ F_8(x_6, x_1)\}, \end{aligned}$$

où les polynômes g_2, g_3, g_4 sont distincts.
Supposons $\mathrm{Gal}_k(f)$ impair, il s'agit alors d'un conjugué de $8T_7$, c'est-à-dire l'un de ses 6 conjugués dans $\mathcal{A}(L)$ qui sont :

$$\begin{aligned} H_1 &= \langle (1,5,3,7,2,6,4,8), \sigma_1 = (1,2)(3,4)\rangle, \quad H_2 = \langle (1,6,3,7,2,5,4,8), \sigma_1\rangle,\\ H_3 &= \langle (1,5,2,7,3,6,4,8), \sigma_2 = (1,3)(2,4)\rangle, \quad H_4 = \langle (1,5,2,8,3,6,4,7), \sigma_2\rangle,\\ H_5 &= \langle (1,5,2,7,4,6,3,8), \sigma_3 = (1,4)(2,3)\rangle, \quad H_6 = \langle (1,5,2,8,4,6,3,7), \sigma_3\rangle. \end{aligned}$$

Ces 6 groupes se répartissent en trois classes de L-conjugaison :

$$\mathcal{C}_1 = \{H_1, H_2\},\ \mathcal{C}_2 = \{H_3, H_4\} \text{ et } \mathcal{C}_3 = \{H_5, H_6\},$$

avec $H_2 = \tau^{-1}H_1\tau$, $H_4 = \tau^{-1}H_3\tau$ et $H_6 = \tau^{-1}H_5\tau$ et $\tau = (5,6) \in L$.
D'après le théorème 7.11, il existe $i \in \{1,2,3\}$ tel que $I = \bigcap_{H\in\mathcal{C}_i} H.I$. La proposition 7.19 permet ensuite de déterminer la classe associée à I sous la forme d'un critère d'association.
À partir du polynôme $R = x_2 + g_2(x_1)$ de $\mathfrak{T}_I$ et des permutations $\sigma_1 = (1,5,3,7,2,6,4,8)$ de H_1 et $\sigma_2 = (1,6,2,5,3,7,4,8)(1,2)(3,4)$ de H_2, nous formons le polynôme $P_1 = \sigma_1.R = \sigma_2.R = x_6 + g_2(x_5)$ qui appartient à $\bigcap_{H\in\mathcal{C}_1} H.I$. De même, nous construisons

le polynôme $P_2 = x_6 + g_3(x_5)$ de $\bigcap_{H\in\mathcal{C}_2} H.I$ et le polynôme $P_3 = x_6 + g_4(x_5)$ de $\bigcap_{H\in\mathcal{C}_3} H.I$.
Les polynômes P_1 et P_2 ne peuvent appartenir simultanément à I car, si tel était le cas, le polynôme $g_2(x_5) - g_3(x_5) = P_1 - P_2$ appartiendrait à I et, étant de degré strictement inférieur à f, il diviserait f sur k. Il en va de même, pour les couples (P_1, P_3) et (P_2, P_3). Nous obtenons ainsi les critères d'association :

i) si $P_1 \in I$ alors la classe $\mathcal{C}_1$ est associée à I;
ii) si $P_2 \in I$ alors la classe $\mathcal{C}_2$ est associée à I;
iii) si $P_3 \in I$ alors la classe $\mathcal{C}_3$ est associée à I.

Supposons que $\mathcal{C}_1$ soit associée à I. Alors I est l'intersection de deux idéaux maximaux (ceux de $\mathcal{M}(I)$): $I = \mathfrak{M}_1 \cap \mathfrak{M}_2$ avec $H_i = Dec(\mathfrak{M}_i)$, $i = 1, 2$. Les ensembles $\Psi(H_1) = H_1 + H_1\tau$ et $\Psi(H_2)$ sont les injecteurs de I dans $\mathfrak{M}_1$ et $\mathfrak{M}_2$, respectivement (voir Théorème 7.2).

Remarque 7.21. Nous constatons sur l'exemple ci-dessus que la proposition 7.19 est utilisable pour pré-établir des critères d'association. Il s'agit d'une conséquence du fait que les variables et les degrés des polynômes intervenant dans l'ensemble triangulaire engendrant l'idéal induit ne dépendent que du groupe de Galois de f.

8. Adjonction de relations à l'idéal induit

Fixons nous un idéal de Galois I et $\mathfrak{M} = Id_k(\underline{\alpha}) \in \mathcal{M}(I)$. Nous cherchons à construire, sans coût supplémentaire, un idéal de Galois contenant strictement I. L'idée est de permuter les relations de I pour en déduire de nouvelles. Nous chercherons à déterminer un injecteur de ce nouvel idéal.

Proposition 8.1. *Soit H un sous-groupe de S_n vérifiant $H \subset \mathrm{Inj}(I, \mathfrak{M})$. Pour tout $\sigma \in H$ et $R \in I$, l'idéal $J = I + \langle \sigma.R \rangle$ est un idéal de Galois contenu dans $Id_k(H.\underline{\alpha})$.*

Démonstration. Montrons l'inclusion $J \subset Id_k(H.\underline{\alpha})$. Puisque $H \subset \mathrm{Inj}(I, \underline{\alpha})$, nous avons $I \subset Id_k(H.\underline{\alpha})$ et il suffit donc de montrer que $\sigma.R$ appartient à $Id_k(H.\underline{\alpha})$.
D'après la proposition 3.14, le groupe H est inclus dans le groupe de décomposition de $Id_k(H.\underline{\alpha})$ et donc $\sigma.R \in Id_k(H.\underline{\alpha})$, d'où l'inclusion.
Ceci implique, en particulier, que J est un idéal propre et, comme il contient les relations symétriques, J est un idéal de Galois. □

Si dans la proposition précédente $\sigma \notin \mathrm{Dec}(I)$, nécessairement il existe $R \in I$ tel que $I \subsetneq J$. C'est ainsi qu'un nouvel idéal pourra être construit rapidement. Le procédé s'éxécute récursivement avec J à la place de I. Par exemple, lorsque $\mathrm{Gal}_k(f)$ est T_{17}, nous trouvons ainsi deux relations linéaires en x_6 et x_7 respectivement qui fournissent sans calcul l'ensemble triangulaire $\mathfrak{T}$ d'un idéal maximal à partir d'un idéal de rupture symétrique (voir Paragraphe 10.3).

Il est bien évident qu'un sous-groupe de H n'apporte rien de plus que H. Donc nous nous limitons aux groupes maximaux inclus dans $\mathrm{Inj}(I, \mathfrak{M})$.

Désormais, supposons I engendré par $\mathfrak{T}_I = \{F_1, F_2, \ldots, F_n\}$ triangulaire séparable.

Une conséquence immédiate de la proposition 8.1 est le corollaire suivant :

Corollaire 8.2. *Reprenons les notations de la proposition 8.1. Si $F = \sigma.R$ est de la forme $x_j^d + g(x_1, \ldots, x_j)$ avec $d > 0$ et $\deg_{x_j}(g) < d$ et si l'ensemble $S = \{F_1, \ldots, F_{j-1}, F, F_{j+1}, \ldots, F_n\}$ engendre un idéal I' contenant I, alors S est triangulaire séparable et $I' = J$.*

Dans le corollaire 8.2, il suffit que F soit un facteur de F_j dans $k[x_1, \ldots x_j]$ pour que l'hypothèse d'inclusion soit vérifiée.
Le résultat suivant montre que cette même hypothèse d'inclusion est vérifiée sous certaines conditions moins contraignantes.

Corollaire 8.3. *Reprenons les notations du corollaire 8.2 et supposons que F soit de la forme $x_j^d + g(x_1, \ldots, x_j)$, avec $d = \deg_{x_j}(Id_k(H.\underline{\alpha}))$ et $\deg_{x_j}(g) < d$. Alors, J est un idéal de Galois de f et il est engendré par l'ensemble S.*

Démonstration. D'après le corollaire 8.2, il suffit de montrer que $F_j \in \langle S \rangle$. D'après la proposition 8.1, nous avons la suite d'inclusions d'idéaux de $k[x_1, \ldots, x_j]$:

$$\langle F_1, \ldots, F_{j-1}, F \rangle \subset \langle F_1, \ldots, F_{j-1}, F, F_j \rangle \subset Id_k(H.\underline{\alpha}) \cap k[x_1, \ldots, x_j].$$

Supposons, sans perte de généralité, l'ensemble $\mathfrak{T}_I$ réduit et F égal à sa forme normale modulo $\mathfrak{T}_I$. Nous avons l'isomorphisme suivant :

$$k[x_1, \ldots, x_j]/\langle F_1, \ldots, F_j, F \rangle \simeq \Big(k[x_1, \ldots, x_{j-1}]/\langle F_1, \ldots, F_{j-1} \rangle\Big)[x_j]/\langle F_j, F \rangle.$$

L'anneau $R = k[x_1, \ldots, x_{j-1}]/\langle F_1, \ldots, F_{j-1} \rangle$ est un produit de corps (voir [4, Théorème 4.4.14]), ainsi nous pouvons considérer le PGCD P de F et F_j en tant que polynôme à coefficients dans R (voir [4, Chapitre 3]). L'idéal $\langle F_j, F \rangle$ de R est donc monogène engendré par P et, en tant qu'idéaux de $k[x_1, \ldots, x_n]$, nous avons l'égalité $\langle F_1, \ldots, F_n, F \rangle = \langle F_1, \ldots, F_{j-1}, P, F_{j+1}, \ldots, F_n \rangle$.
Comme P est de la forme $x_j^k + h(x_1, \ldots, x_j)$ avec $\deg_{x_j}(h) < k$ et qu'il est inclus dans $Id_k(H.\underline{\alpha})$ nous avons $k \geqslant d$. Mais comme P est le PGCD de F et F_j nous avons $k \leqslant d$ et donc $k = d$. Ainsi, nous avons $P = F$ et le corollaire s'ensuit. □

Soit J un idéal de Galois triangulaire obtenu par les permutations d'un groupe H inclus dans $\mathrm{Inj}(I, \mathfrak{M})$. Connaissant une ensemble triangulaire de générateurs de J, nous pouvons calculer le cardinal de sa variété (voir Égalité (3.12)). Si $\mathrm{Card}(V(J)) = \mathrm{Card}(H)$ alors, d'après la proposition 3.19, $J = Id_k(H.\underline{\alpha})$ et H est l'injecteur de J. Dans le cas où H n'est pas l'injecteur de J, nous pouvons, dans certains cas, calculer un injecteur de J.

Supposons que E soit un ensemble de permutations telles que $\mathrm{Inj}(I, \mathfrak{M}) = \sum_{e \in E} He$. Alors

$$J = I + \langle F \rangle = \bigcap_{\tau \in E} Id_k(H\tau.\underline{\alpha}) + \langle F \rangle \, .$$

Soit E_1 l'ensemble des permutations $\tau \in E$ telles que $F \in Id_k(H\tau.\underline{\alpha})$. Comme les idéaux I et $\langle F \rangle$ sont inclus dans $\bigcap_{\tau \in E_1} Id_k(H\tau.\underline{\alpha})$, l'idéal $J = I + \langle F \rangle$ l'est également.

Proposition 8.4. *Supposons que* $\mathrm{Gal}_k(\underline{\alpha}) \subset H$. *Si nous avons l'égalité*

$$\mathrm{Card}(V(J)) = \mathrm{Card}(E_1) \, . \, \mathrm{Card}(H)$$

alors $J = \bigcap_{\tau \in E_1} Id_k(H\tau.\underline{\alpha})$ *et* $Inj(J, \underline{\alpha}) = \sum_{\tau \in E_1} H\tau$.

Ainsi, pour construire un injecteur de l'idéal J nous devons déterminer l'ensemble E_1 de la proposition 8.4.

Proposition 8.5. *Reprenons les notations précédentes. Une permutation* $\tau \in \{\tau_1, \ldots, \tau_s\}$ *appartient à* E_1 *dès qu'elle vérifie la condition suivante :*

$$\exists (R, \sigma) \in I \times H^{\tau^{-1}}, \ F = \sigma.R \, .$$

Démonstration. Montrons la contraposée de cette condition. Supposons donc que la permutation τ n'appartienne pas à E_1, i.e. $F \notin \mathcal{I} = Id_k(H\tau.\underline{\alpha})$. Nous avons donc, par définition du groupe de décomposition et puisque $\sigma.R \in \mathcal{I}$,

$$\forall (R, \sigma) \in \mathcal{I} \times \mathrm{Dec}(\mathcal{I}), \ F \neq \sigma.R \, .$$

Comme $I \subset \mathcal{I}$, d'après la proposition 3.14 nous avons

$$H^{\tau^{-1}} \subset \mathrm{Dec}(Id_k(H^{\tau^{-1}}.\tau\underline{\alpha})) \, (= \mathrm{Dec}(Id_k(H\tau.\underline{\alpha}))) \, .$$

Donc, $\forall (R, \sigma) \in I \times H^{\tau^{-1}}, \ F \neq \sigma.R$. □

Exemple 8.6. Supposons que I soit un idéal induit d'un idéal de rupture d'un polynôme f de degré 8. Supposons que $\Delta(f) = 1^3, 2^2$. À l'aide de la table 1, nous calculons l'ensemble des groupes H vérifiant $H_{\{1\}} \subset S_{1^4,2^2}$ et $\Delta(H) = \Delta(f)$. Tous ces groupes vérifient $\mathcal{L}(H) = (8, 1^3, 2, 1^3)$. En comparant avec $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$, nous en déduisons, qu'en remplaçant le polynôme $F_7(x_1, x_7)$ de $\mathfrak{T}_I$ par une relation $r_7(x_1, x_5, x_7)$ linéaire en x_7, nous obtiendrons un ensemble triangulaire $\mathfrak{T}$ engendrant un idéal de relations $\mathfrak{M}$ de f (voir Paragraphe 10.2 pour la solution).

9. Construction d'un algorithme

9.1. Méthodologie de pré-calculs.

Dans ce paragraphe, nous décrivons une méthodologie à suivre pour établir un algorithme de détermination d'un idéal maximal de relations. Cette méthodologie met en œuvre les résultats théoriques des paragraphes précédents.

Nous allons distinguer plusieurs étapes. La première n'intervient que dans le cadre où le polynôme f est factorisé sur l'un de ses corps de rupture. Ceci permet de déterminer les groupes susceptibles d'être injecteurs des idéaux de rupture symétriques.

À partir de la deuxième étape, nous désignerons par L un groupe qui, lors du calcul du corps de décomposition d'un polynôme f de degré n, est susceptible d'êtres l'injecteur d'un idéal de Galois I_1 de $k(\alpha_1)[x_1, \ldots, x_n]$. Notons $1, e$ la suite croissante des cardinaux des orbites de $\{1, \ldots, n\}$ sous l'action de L (i.e. des éléments de $Orb(L)$).
L'étape 1 est à appliquer chaque fois qu'il sera nécessaire de factoriser dans une extension. Les étapes 2 à 5 ont pour objectif de calculer un idéal de Galois de f sur k contenant strictement un idéal induit ; un injecteur de cet idéal sera aussi à déterminer.
À l'aide de la table de rupture en degré n, est déterminé l'ensemble

$$\mathcal{G} = \{G \in \mathcal{T}(n) \mid \Delta(G) = 1, e\} .$$

Pour les polynômes f tels que $\Delta(f) = 1, e$, le groupe $\mathrm{Gal}_k(f)$ appartient à l'ensemble $\mathcal{G}$ puisque $\Delta(f) = \Delta(\mathrm{Gal}_k(f))$..
Pour décrire ces étapes, nous devons introduire les relations d'équivalence qui y seront utilisées.

Relations d'équivalence.
Pour tout groupe $G \in \mathcal{G}$, nous notons $\mathcal{A}(L, G)$ l'ensemble des S_n-conjugués de G qui appartiennent à $\mathcal{A}(L)$:

$$\mathcal{A}(L, G) = \{G^\sigma \mid \sigma \in S_n\} \cap \mathcal{A}(L) .$$

(Pour la définition de $\mathcal{A}(L)$, voir Définition 6.1.) Nous avons naturellement :

$$\mathcal{A}(L) = \bigcup_{G \in \mathcal{G}} \mathcal{A}(L, G). \tag{9.1}$$

Relation $\sim$ sur les ensembles $\mathcal{A}(L)$ et $\mathcal{A}(L, G)$.
Nous noterons $\sim$ la relation d'équivalence induite par la L-conjugaison sur les ensembles $\mathcal{A}(L)$ et $\mathcal{A}(L, G)$.

Relation $\mathcal{R}$ sur l'ensemble des classes de L-conjugaison $\mathcal{A}(L)/\sim$.
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux classes appartenant à $\mathcal{A}(L)/\sim$. Nous posons

$$\mathcal{C}\ \mathcal{R}\ \mathcal{C}' \text{ s'il existe } H \in \mathcal{C} \text{ et } H' \in \mathcal{C}' \text{ tels que } \Psi(H) = \Psi(H').$$

Relation $\mathcal{R}$ pour les groupes de $\mathcal{G}$.
Soient G et G' deux groupes de $\mathcal{G}$. Nous posons

$$G\ \mathcal{R}\ G' \text{ s'il existe } \mathcal{C} \in \mathcal{A}(L, G)/\sim \text{ et } \mathcal{C}' \in \mathcal{A}(L, G')/\sim \text{ telles que } \mathcal{C}\ \mathcal{R}\ \mathcal{C}'.$$

En cours de calcul, certains groupes peuvent être retirés de l'ensemble $\mathcal{G}$ ou de $\mathcal{A}(L)$. De telles réductions de l'ensemble $\mathcal{A}(L)$ ne modifient pas la méthodologie que nous allons décrire.

Étape 1 : Injecteurs des idéaux de rupture symétriques.
Avec la table de rupture en degré n, nous déterminons l'ensemble E des entiers e tels que $1, e \in \{\Delta(G) \mid G \in \mathcal{T}(n)\}$. Les sous-groupes de S_n susceptibles d'être injecteurs d'idéaux de rupture symétriques sont les $S_{1,e}$ où e parcourt E.

Étape 2 : Calcul de $\mathcal{A}(L)$ et des ensembles $\mathcal{A}(L, G)$.
Avec l'un des systèmes GAP ou Magma, sont calculés les ensembles $\mathcal{A}(L, G)$, pour tout groupe $G \in \mathcal{G}$. L'ensemble $\mathcal{A}(L)$ est obtenu avec l'égalité (9.1).

Étape 3 : Discrimination des classes de L-conjugaison dans $\mathcal{A}(L, G)$.
Dans cette partie, nous considérons C_0 un classe de $\mathcal{R}$-équivalence de $\mathcal{G}$ et avec les résultats du paragraphe 7.3, nous déterminons comment associer les classes de L-conjugaisons aux idéaux induits.
Nous pourrons aussi introduire d'autres critère discriminants tels la parité du groupe de Galois ou critère de Dedekind qui peuvent exclure un groupe de $\mathcal{G}$. Dans le cadre de cet article, en plus des critères classiques, nous testerons parfois si un groupe est le groupe de décomposition de I.

Étape 4 : Construction d'un idéal contenant strictement l'idéal induit.
Nous utilisons les résultats du paragraphe 8 afin de calculer un idéal J contenant I en nous limitant aux groupes H maximaux de $\mathcal{A}(L)$. De plus, comme $H_{(1)} \subset \mathrm{Dec}(I_1) = L$, il serait vain de chercher de nouvelles relations avec les permutations de $H_{(1)}$.

Une fois ces étapes achevées, il s'agit de savoir ce qui doit être fait de l'idéal J : chercher de nouvelles relations par calcul de facteurs dans les extensions ou avancer avec l'algorithme `GaloisIdéal`. Ce dernier algorithme peut aussi être stoppé pour chercher des relations par une autre méthode. Une étude de ce qui serait alors le plus efficace s'impose. Pour illustrer notre travail, nous avons choisi de nous arrêter à l'idéal de rupture symétrique et de terminer avec l'algorithme `GaloisIdéal` que nous décrivons succinctement ci-après.

9.2. Algorithme `GaloisIdéal`.

Soit I un idéal de Galois de f donné par un ensemble triangulaire `T` de générateurs. Nous supposons déterminés un injecteur `Inj` de I et un ensemble $\mathfrak{A}$ de groupes dit *candidats* auquel appartiennent les groupes de Galois $\mathrm{Dec}(\mathfrak{M})$, $\mathfrak{M} \in \mathcal{M}(I)$ (dans le cadre de cet article, $\mathfrak{A}$ est un sous-ensemble de $\mathcal{A}(L)$). L'algorithme

`GaloisIdéal(Inj, T, 𝔄 )`

calcule un idéal (maximal) des relations $\mathfrak{M}$ contenant I ainsi que le groupe de Galois $\mathrm{Dec}(\mathfrak{M})$ (l'algorithme est décrit dans [23] en supposant que `Inj` est un groupe, il a été généralisé à tout injecteur dans [24]). La méthode utilisée pour cet algorithme est celle évoquée dans l'introduction. Il s'agit de construire récursivement une chaîne ascendante d'idéaux de Galois

$$I = I_1 \subset I_2 \subset \cdots \subset I_r = \mathfrak{M},$$

où, pour calculer I_{i+1} à partir de I_i (avec $i \in [\![1, r-1]\!]$), il est nécessaire de connaître un ensemble triangulaire engendrant I_i et un injecteur H de I_i :

$$I_{i+1} = I_i + < R >$$

où $R \in k[x_1, \ldots, x_n]$ est construit à partir d'une résolvante H-relative (voir [5] pour son calcul). Cette même résolvante est exploitée pour réduire la liste des groupes candidats en comparant les groupes de Galois de ses facteurs avec ceux attendus

dans la *matrice des groupes* (voir [22]). En particulier, les groupes pairs et impairs sont discriminés en testant si le discriminant de f est ou non un carré dans k.

Dans [9], L. Ducos propose une méthode analogue à `GaloisIdéal`. Cette méthode ne s'appliquant qu'aux idéaux de Galois dont les injecteurs sont des groupes, elle ne pourra pas être utilisée dans le cadre plus général de notre étude.

10. Étude en degré 8

Pour illustrer la méthodologie d'élaboration d'un algorithme de calcul de l'ensemble triangulaire $\mathfrak{T}$ engendrant un idéal maximal $\mathfrak{M}$, nous avons choisi d'étudier le degré $n = 8$. Nous nous contentons de suivre les étapes 1 à 4 du paragraphe 9.1 avec chaque groupe $L = S_{1,\Delta(T)}$, $T \in \mathcal{T}(8)$, et de terminer avec l'algorithme `GaloisIdéal`. Même sur cette étude restreinte, nous ne cherchons pas la meilleure stratégie mais seulement à mettre en évidence les différentes situations qui peuvent se présenter. Malgré cette utilisation réduite de nos résultats, nous en constaterons l'efficacité.

L'idéal I est donc supposé être induit d'un idéal de rupture symétrique de f dans $k(\alpha_1)[x_1, \ldots, x_n]$ et

$$\mathfrak{T}_I = \{F_1(x_1), \ldots, F_8(x_1, \ldots, x_8)\}$$

est l'ensemble triangulaire l'engendrant donné dans la proposition 5.6. Lorsqu'un facteur de rupture f_i de f est linéaire ($i \in [\![1, r]\!]$), nous notons g_i le polynôme tel que

$$f_i = x + g_i(\alpha_1) \quad .$$

Chaque groupe $8T_i$ de $\mathcal{T}(8)$ est noté T_i et le groupe noté G_i en est un conjugué.

10.1. $\Delta(f) = 1^7$; i.e. $L = S_{1^8}$ et $\mathcal{L}(I) = (8, 1^7)$.

$\mathcal{G}/\mathcal{R} = \{\{T_1\}, \{T_2^+\}, \{T_3^+\}, \{T_4^+\}, \{T_5^+\}\}$ et $I = \mathfrak{M}$.

Exemple 10.1. Sur $k(\alpha_1)$, le polynôme irréductible $f = x^8 + 8x^6 + 20x^4 + 16x^2 + 2$ se factorise en :

$$(x - \alpha_1)(x + \alpha_1)(x - \alpha_1^3 - 3\alpha_1)(x + \alpha_1^3 + 3\alpha_1)(x - \alpha_1^5 - 5\alpha_1^3 - 5\alpha_1)$$
$$(x + \alpha_1^5 + 5\alpha_1^3 + 5\alpha_1)(x - \alpha_1^7 - 7\alpha_1^5 - 14\alpha_1^3 - 7\alpha_1)(x + \alpha_1^7 + 7\alpha_1^5 + 14\alpha_1^3 + 7\alpha_1).$$

Nous avons $\mathrm{Dec}(\mathfrak{M}) = T_1^\sigma$ avec $\sigma = (2, 3, 7, 8, 5)(4, 6)$ et

$$\begin{aligned}\mathfrak{T} \;=\; & \{f(x_1),\ x_2 + x_1,\ x_3 - x_1^3 - 3x_1, x_4 + x_1^3 + 3x_1,\ x_5 - x_1^5 - 5x_1^3 - 5x_1,\\ & x_6 + x_1^5 + 5x_1^3 + 5x_1, x_7 - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1,\ x_8 + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1\}\ .\end{aligned}$$

10.2. $\Delta(f) = 1^3, 2^2$; i.e. $L = S_{1^4,2^2}$ et $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$.

$\mathcal{G}/\mathcal{R} = \{\{T_7\}, \{T_9^+\}, \{T_{10}^+\}, \{T_{11}^+\}\}$.
Critère d'association : $x_6 + g_1(x_5) \in I$

$$\mathfrak{T} = \mathfrak{T}_I \cup \{x_7 + g_2(x_5)\} \backslash \{F_7\}$$

et $\mathrm{Dec}(\mathfrak{M})$ est l'un des groupes

$$\begin{aligned} G_7 &= \langle (1,5,3,7,2,6,4,8),(1,2)(3,4)9\rangle, \\ G_9^+ &= \langle (1,2)(3,4)(5,6)(7,8),(1,4)(2,3)(5,8)(6,7),(1,5)(2,6)(3,7)(4,8),(5,6)(7,8)\rangle, \\ G_{10}^+ &= \langle (1,2)(3,4),(1,5,3,7)(2,6,4,8)\rangle \text{ et} \\ G_{11}^+ &= \langle (1,2)(3,4),(1,3,2,4)(5,7,6,8),(1,7,2,8)(3,6,4,5)\rangle \quad . \end{aligned}$$

10.3. $\underline{\Delta(f) = 1^3,4}$ **; i.e.** $L = S_{1^4,4}$ **et** $\mathcal{L}(I) = (8,1^3,4,3,2,1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{17}\},\{T_{18}^+\}\}$.
Les groupes de $\mathcal{A}(L,T_{18}^+)$ sont L-conjugués et $\mathcal{A}(L,T_{17})$ possède 3 classes de L-conjugaison. Soient les deux groupes :

$$\begin{aligned} G_{17} &= \langle (1,2,3,4),(1,5)(2,7)(3,8)(4,6)\rangle \text{ et} \\ G_{18}^+ &= \langle (1,4)(2,3)(5,6)(7,8),(1,3)(2,4)(5,8)(6,7), \\ &\quad (1,5)(2,7)(3,8)(4,6),(5,6)(7,8),(5,8)(6,7)\rangle \quad . \end{aligned}$$

Critère d'association pour G_{17} : $x_1 + g_3(x_2) \in I$

$$\mathfrak{T} = \mathfrak{T}_I \cup \{x_6 + g_3(x_5), x_7 + g_1(x_5)\}\backslash\{F_6,F_7\}$$

et $\mathrm{Dec}(\mathfrak{M})$ est G_{17} ou G_{18}^+.

10.4. $\underline{\Delta(f) = 1,2^3}$ **; i.e.** $L = S_{1^2,2^3}$ **et** $\mathcal{L}(I) = (8,1,2,1,2,1,2,1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{27},T_{16},T_{20}^+\},\{T_{31},T_{21},T_{22}^+\},\{T_6\},\{T_8\}\}$.
Comme $\mathrm{Card}(V(I)) = 64 = \mathrm{Card}(T_{27}) = \mathrm{Card}(T_{31})$, le calcul du groupe de décomposition $\mathrm{Dec}(I)$ permet de distinguer trois cas :
Cas A. $\mathrm{Dec}(I) \in \mathcal{A}(L,T_{27})$ (i.e. $\mathrm{Dec}(I)$ est conjugué à T_{27}).
On a $\mathrm{Card}(\mathcal{A}(L,T_{27})) = 3$. Soit $\mathfrak{A}$ l'ensemble des sous-groupes de $\mathrm{Dec}(I)$ conjugués à T_{16} et T_{20}^+. Le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal(}\mathrm{Dec}(I)\texttt{, }\mathfrak{T}_I\texttt{, }\mathfrak{A}\texttt{)} \quad .$$

Cas B. $\mathrm{Dec}(I) = G_{31} = \langle (7,8)(1,8)(2,7)(3,5)(4,6)(1,5)(2,6)(3,8)(4,7)\rangle$
car $\mathcal{A}(L,T_{31}) = \{G_{31}\}$. Soit $\mathfrak{A}$ l'ensemble des sous-groupes de G_{31} conjugués à T_{21} et T_{22}^+. Le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal(}G_{31}\texttt{, }\mathfrak{T}_I\texttt{, }\mathfrak{A}\texttt{)} \quad .$$

où G_{21} et G_{22} sont les sous-groupes de G_{31} conjugués respectifs de T_{21} et T_{22}^+.
Cas C. $\mathrm{Dec}(I) \notin \mathcal{A}(L,T_{27})$ et $\mathrm{Dec}(I) \neq G_{31}$
Nous avons nécessairement $\mathrm{Gal}_k(f) \in \{T_6,T_8\}$ et $\mathcal{L}(\mathfrak{M}) = (8,1,2,1^5)$.
Deux facteurs linéaires $r_5 = x + h_5(\alpha_1,\alpha_3)$ et $r_7 = x + h_7(\alpha_1,\alpha_3)$ de f sur $k(\alpha_1,\alpha_3) = k(\underline{\alpha})$ sont à déterminer. Soient les groupes

$$\begin{aligned} G_6 &= \langle (1,3,5,8,2,7,6,4),(1,7)(2,3)(4,6)(5,8)\rangle \quad \text{et} \\ G_8 &= \langle (1,7,5,8,2,3,6,4),(1,5)(2,6)(3,7),(1,3,5,4,2,7,6,8)\rangle. \end{aligned}$$

Critère d'association de G_6 et G_8 : $x_6 + g_1(x_5) \in I$

$$\mathfrak{T}_J = \mathfrak{T}_I \cup \{x_7 + g_1(x_3)\}\backslash\{F_7\}$$

L'idéal $J = \langle \mathfrak{T}_J \rangle$ est l'intersection de deux idéaux des relations (voir Égalités (3.2) et 3.1). Le calcul d'un idéal des relations $\mathfrak{M}$ peut alors être réalisé par l'appel

$$\texttt{GaloisIdéal}(L_i, \mathfrak{T}_J, \{G_i\})$$

où $L_i = G_i + G_i(5,6)$ $(i = 6, 8)$ est l'injecteur de J dans $\mathfrak{M}$ selon que le groupe de Galois est T_6 ou T_8. Le calcul de L_i est donné par le théorème 7.2 et la proposition 7.17 permet d'identifier le groupe de Galois en déterminant lequel des ensembles L_6 ou L_8 est un injecteur de J. Notons qu'ici la relation $x_5 + h_5(x_1, x_3)$ avec $deg_{x_i}(h_5) < deg_{x_i}(F_i)$ est aussi calculable par la méthode linéaire de Yokoyama évoquée dans l'introduction où, comme elle linéaire en x_5, par la méthode interpolatrice de McKay et Stauduhar (voir resp. [26] et [14]).

10.5. $\underline{\Delta(f) = 1, 2, 4}$ **; i.e.** $L_0 = S_{1^2,2,4}$ **et** $\mathcal{L}(I) = (8, 1, 2, 1, 4, 3, 2, 1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{15}, T_{19}^+, T_{26}, T_{28}, T_{30}, T_{29}^+, T_{30}, T_{35}\}\}$ avec $\mathcal{L}(G_{35}) = (8, 1, 2, 1, 4, 1, 2, 1)$.

$$\mathfrak{T}_J = \mathfrak{T}_I \cup \{x_6 + g_1(x_5)\} \backslash \{F_6\} \quad .$$

L'idéal $J = \langle \mathfrak{T}_J \rangle$ est d'injecteur $G_{35} = \langle (7,8), (1,3)(2,4), (1,5,3,8)(2,6,4,7) \rangle$. Soit $\mathfrak{A}$ l'ensemble des sous-groupes de G_{35} conjugués aux groupes de $\mathcal{G}$ (T_{35} mis à part). Le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal}(G_{35}, \mathfrak{T}_J, \mathfrak{A}) \quad .$$

Note Le groupe de Galois sur $k(\alpha_1)$ du facteur de rupture $f_4(\alpha_1, x) = x^4 + g_4(\alpha_1, x)$ de f départage T_{19}^+ et T_{29}^+ ; de plus, la parité de ce groupe de Galois détermine si $\mathrm{Gal}_k(f)$ est ou non T_{15} (voir Table 1).

10.6. $\underline{\Delta(f) = 1, 3^2}$ **; i.e.** $L = S_{1^2,3^2}$ **et** $\mathcal{L}(I) = (8, 1, 3, 2, 1, 3, 2, 1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{13}^+, T_{14}^+, T_{24}^+\}, \{T_{12}^+\}\}$.
Bien que l'ensemble $\mathcal{A}(L, T_{24})$ possède plusieurs classes de L-conjugaison et que $\mathcal{G}$ possède deux classes de $\mathcal{R}$-équivalence, l'étape 4 s'applique dès le départ. Soit J l'idéal engendré par

$$\mathfrak{T}_J = \mathfrak{T}_I \cup \{x_6 + g_1(x_3), x_7 + g_1(x_4)\} \backslash \{F_6, F_7\} \quad .$$

$Card(V(J)) = \mathrm{Card}(T_{24}) = 48$. Soient les deux conjugués de T_{24} :

$$\begin{aligned} G_{24} &= \langle (1,5)(2,8)(3,4)(6,7), (1,3)(2,6)(4,5)(7,8), (1,7)(2,4)(3,8)(5,6), (1,4,3)(2,7,6), (3,4)(6,7) \rangle \text{ et} \\ H_{24} &= \langle (1,8)(2,5)(3,4)(6,7), (1,6)(2,3)(4,5)(7,8), (1,4)(2,7)(3,8)(5,6), (1,7,6)(2,4,3), (3,4)(6,7) \rangle \quad . \end{aligned}$$

Critère d'association : Soit $F_5(x_1, x_3, x_4, x_5)$, la relation linéaire en x_5 dans $\mathfrak{T}_I$. Si $F_5(x_5, x_4, x_3, x_1) \in J$ alors $\mathrm{Dec}(I) = G_{24}$ sinon si $F_5(x_8, x_4, x_3, x_2) \in J$ alors $\mathrm{Dec}(I) = H_{24}$ sinon

$$\mathfrak{M} = J + \langle F_5(x_7, x_8, x_1, x_3) \rangle$$

avec $G_{12} = \mathrm{Dec}(\mathfrak{M}) = \langle (1,7,2,4)(3,8,6,5), (1,7,5)(2,4,8) \rangle$ et $\mathcal{L}(G_{12}) = (8, 1, 3, 1^5)$.

Lorsque G_{24} est associé à I, le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal}(G_{24}, \mathfrak{T}_I, \mathfrak{A})$$

où $\mathfrak{A}$ est l'ensemble des sous-groupes de G_{24} conjugués à T_{13}^+ et T_{14}^+.

Note 1. Si le groupe de Galois d'un des facteurs de rupture de degré 3 est S_3 alors $\mathrm{Gal}_k(f) = T_{24}^+$ (voir Table 1).

Note 2. Ici nous avons choisi un critère d'association plutôt que le test du groupe de décomposition. La recherche d'un critère est la méthode la plus efficace.
Note 3. Pour illustrer une situation particulière, nous n'avons pas donné le meilleur conjugué de T_{12} qui permettrait d'obtenir $\mathfrak{T}$ en remplaçant F_4 par une relation linéaire en x_4 déduite uniquement par permutation.

10.7. $\underline{\Delta(f) = 1, 6}$ **; i.e.** $L = S_{1^2,6}$ **et** $\mathcal{L}(I) = (8, 1, 6, 5, 4, 3, 2, 1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{23}, T_{24}^+, T_{32}^+, T_{38}, T_{39}^+, T_{40}, T_{44}\}\}$ avec $\mathcal{L}(G_{44}) = (8, 1, 6, 1, 4, 1, 2, 1)$.

$$\mathfrak{T}_J = \mathfrak{T}_I \cup \{x_4 + g_1(x_3), x_6 + g_1(x_5)\}\backslash\{F_4, F_6\} \quad .$$

L'idéal $J = \langle \mathfrak{T}_J \rangle$ est d'injecteur $G_{44} = \langle (1,3)(2,4)(1,5,8,3)(2,6,7,4) \rangle$. Soit $\mathfrak{A}$ l'ensemble des sous-groupes de G_{44} conjugués aux groupes de $\mathcal{G}$ (T_{44} mis à part). Le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal}(G_{44}\texttt{,}\ \mathfrak{T}_J\texttt{,}\ \mathfrak{A}) \quad .$$

10.8. $\underline{\Delta(f) = 3, 4}$ **; i.e.** $L = S_{1,3,4}$ **et** $\mathcal{L}(I) = (8, 3, 2, 1, 4, 3, 2, 1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{8T_{33}^+, 8T_{34}^+, 8T_{41}^+, 8T_{42}^+, 8T_{45}^+, 8T_{46}, 8T_{47}\}\}$. L'idéal I possède pour injecteur le groupe $G_{47} = \langle (1,2,3,4), (2,3), (1,5)(2,6)(3,7)(4,8)(4,8) \rangle$. Soit $\mathfrak{A}$ l'ensemble des sous-groupes de G_{47} conjugués aux groupes de $\mathcal{G}$ (T_{47} mis à part). Le calcul de $\mathfrak{M}$ est réalisé avec

$$\texttt{GaloisIdéal}(G_{47}\texttt{,}\ \mathfrak{T}_I\texttt{,}\ \mathfrak{A}) \quad .$$

10.9. $\underline{\Delta(f) = 7}$ **; i.e.** $L = S_{1,7}$ **et** $\mathcal{L}(I) = (8, 7, 6, 5, 4, 3, 2, 1)$**.**

$\mathcal{G}/\mathcal{R} = \{\{T_{25}^+, 8T_{36}^+, 8T_{37}^+, 8T_{43}, 8T_{48}^+, 8T_{49}^+, 8T_{50}\}\}$. Le groupe de Galois est 2-transitif et $I = \mathcal{S}$.

11. Implantation et résultats expérimentaux

Nous appellerons `FEGI` (algorithme de Factorisation dans la première extension puis algorithme `GaloisIdéal`) l'algorithme découlant de notre étude partielle en degré $n = 8$ (voir Paragraphe 10). Nous allons le comparer à celui de [2] que nous appellerons `FE`.
Nous avons implanté les deux algorithmes dans le système de calcul formel Magma. Nous avons choisi ce logiciel car il permet de travailler avec toutes les structures mathématiques dont nous avons besoin (groupes symétriques, polynômes univariés et multivariés, algèbres affines ...).
Nous avons rencontré un problème pour la factorisation de polynômes à coefficients dans un corps de nombres. Nous avons donc implanté l'algorithme de factorisation donné dans [2], version améliorée de celui de Trager (voir [21]).
Les temps de calcul, en "cpu-seconde", sont recensés dans le tableau 2. Pour chaque ligne, la première colonne contient le polynôme considéré, la seconde son groupe de Galois sur $\mathbb{Q}$, la suivante l'ordre de ce groupe, et les deux dernières donnent respectivement le temps de calcul des algorithmes `FE` et `FEGI`. Tous ces tests ont été effectués sur Giulia4 [10]. Remarquons que l'implantation de l'algorithme `FE` faite dans le

logiciel RISA/ASIR [19] (interfacé avec PARI [17] version 2.2.5 pour la factorisation des polynômes à coefficients rationnels) nous a donné des temps équivalents à ceux de notre implantation en MAGMA. Les temps de calcul de la factorisation dans les extensions peuvent aussi être améliorés en employant l'algorithme de factorisation de van Hoeij (voir [25]) adapté aux polynômes à coefficients dans une tour d'extensions algébriques ; une telle factorisation existe dans le système PARI version 2.2.5 dans le cas où les coefficients appartiennent à une extension simple de $\mathbb{Q}$.

f	$\mathrm{Gal}(f)$	$\lvert\mathrm{Gal}(f)\rvert$	`FE`	`FEGI`
$x^8-x^7-7x^6+5x^5+15x^4-7x^3-10x^2+2x+1$	$8T_{47}$	1152	3732.05	0.21
$x^8+7x^7-10x^6-131x^5-200x^4+131x^3+382x^2-191$	$8T_{46}$	576	8400.61	519.29
$x^8+x^7-14x^6-3x^5+62x^4-25x^3-63x^2+24x+16$	$8T_{45}$	576	6040.89	179.55
$x^8-x^5-x^4-x^3+1$	$8T_{44}$	384	66.35	0.19
$x^8+x^4-4x^2+1$	$8T_{39}$	192	10.54	0.17
$x^8+2x^6-12x^4-3x^2+11$	$8T_{35}$	128	3.53	0.32
$x^8+12x^6+48x^4+72x^2+31$	$8T_{31}$	64	0.66	0.26
$x^8-x^6-x^4+x^2+1$	$8T_{29}$	64	2.03	0.65
$x^8-5x^5-3x^4-5x^3+1$	$8T_{26}$	64	1.8	1.44
$x^8+x^6+2x^2+4$	$8T_{19}$	32	0.63	0.82

TABLE 2. Temps de calcul.

12. CONCLUSION

Nous avons supposé que le polynôme f est irréductible sur k, mais notre méthode est généralisable aux polynômes réductibles en l'appliquant à chacun de ses facteurs et en utilisant les résultats de l'article [16].

Comme le montre le tableau 2, notre méthode de calcul d'un corps de décomposition s'avère comparativement d'autant plus efficace que son degré sur le corps de base est élevé.
Lorsque l'algorithme `FEGI` est plus lent que l'algorithme `FE`, cela ne signifie pas que ce que nous proposons est moins efficace mais seulement qu'il est préférable de calculer certaines relations de $\mathfrak{T}$ autrement qu'avec `GaloisIdéal`. C'est l'étude complète dans toutes les extensions $k(\alpha_1), k(\alpha_1,\alpha_2),\ldots,k(\underline{\alpha})$ qui déterminera la meilleure stratégie. Cette meilleure stratégie pourra parfois se révéler être celle qui consiste à déterminer a priori partiellement ou complètement le groupe de Galois pour pouvoir appliquer partiellement ou complètement la méthode linéaire de Yokoyama ou, lorsque la relation cherchée est linéaire en sa variable principale, la méthode interpolatrice de McKay et Stauduhar (voir Cas C. Paragraphe 10.4).

Comme nous l'avions annoncé dans l'introduction, nous pouvons désormais mixer toutes les méthodes connues tout en apportant à chacune des améliorations substantielles.

REMERCIEMENT

Nous tenons à remercier le rapporteur pour toutes ses critiques constructives et judicieuses.

References

[1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *Appl. Algebra Engrg. Comm. Comput.*, 15(3-4):279–294, 2004.

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

[3] J.M. Arnaudiès and A. Valibouze. Résolvantes de lagrange. Technical Report 93.61, LITP, 1993.

[4] P. Aubry. Ensembles triangulaires de polynômes et résolution de systèmes algébriques. *PhD thesis, Université Paris 6*, 1999.

[5] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6):635–651, 2000. Algorithmic methods in Galois theory.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[7] G. Butler and J. McKay. The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8):863–911, 1983.

[8] A. Cauchy. Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée. *Oeuvres*, **5**:473 Extrait 108, 1840.

[9] L. Ducos. Construction de corps de décomposition grâce aux facteurs de résolvantes. *Comm. Algebra*, 28(2):903–924, 2000.

[10] Giulia. UMS MEDICIS. Intel - Pentium III 2 x 933 Mhz, 1024 Mo, Linux 2.4.1, http://www.medicis.polytechnique.fr.

[11] J. Klüners and G. Malle. A database for polynomials over the rationals. http://www.mathematik.uni-kassel.de/ klueners/minimum/.

[12] J. Klüners and G. Malle. Explicit Galois realization of transitive groups of degree up to 15. *J. Symbolic Comput.*, 30(6):675–716, 2000. Algorithmic methods in Galois theory.

[13] S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1):184–195, 1985.

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

[15] M. Noro and K. Yokoyama. Factoring polynomials over algebraic extension fields. *Josai Information Science Researches*, **9**:11–33, 1997.

[16] Sébastien Orange, Guenaël Renault, and Annick Valibouze. Note sur les relations entre les racines d'un polynôme réductible. *Theor. Inform. Appl.*, 39(4):651–659, 2005.

[17] *PARI/GP, version* `2.2.5`, 2003. http://www.parigp-home.de.

[18] N. Rennert and A. Valibouze. Calcul de résolvantes avec les modules de Cauchy. *Experiment. Math.*, 8(4):351–366, 1999.
[19] *Risa/Asir, version 2003/05/07*. http://www.asir.org.
[20] N. Tchebotarev. *Gründzüge des Galois'shen Theorie*. P. Noordhoff, 1950.
[21] B. Trager. Algebraic factoring and rational functiun integration. In *Proceedings of SYMSAC'76*, pages 219–226, 1976.
[22] A. Valibouze. Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 456–468. Springer, Berlin, 1995.
[23] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4):507–535, 1999. Version longue du rapport LIP6 du 10/09/1997 : http://www.lip6.fr/fr/production/publications-rapports.php.
[24] Annick Valibouze. Dépendance algébrique des zéros de polynômes et groupes de Galois. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 48(96)(1):73–96, 2005.
[25] M. van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2):167–189, 2002.
[26] K. Yokoyama. A modular method to compute the splitting field of a polynomial. 1999. Communication privée.

L.I.P.6, Université Pierre et Marie Curie, 4, place Jussieu, F-75252 Paris Cedex 05
E-mail address: *name*@upmc.fr