



**HAL**  
open science

## Calcul efficace de corps de décomposition

Sébastien Orange, Guénaël Renault, Annick Valibouze

► **To cite this version:**

Sébastien Orange, Guénaël Renault, Annick Valibouze. Calcul efficace de corps de décomposition. [Rapport de recherche] lip6.2003.005, LIP6. 2003. hal-02545653v1

**HAL Id: hal-02545653**

**<https://hal.science/hal-02545653v1>**

Submitted on 17 Apr 2020 (v1), last revised 10 Sep 2024 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# CALCUL EFFICACE DE CORPS DE DÉCOMPOSITION.

S. ORANGE, G. RENAULT, A. VALIBOUZE

## Résumé

Dans cet article, nous proposons une nouvelle méthode pour le calcul du corps de décomposition d'un polynôme d'une variable sur un corps parfait. Cette méthode rend compatibles deux algorithmes connus (factorisation dans les extensions algébriques et calcul d'un idéal de Galois maximal) afin de compenser leurs faiblesses respectives.

## Abstract

In this paper, we propose a new method for the computation of the splitting field of an univariate polynomial over a perfect field. This method mixes two known algorithms (factorizations in algebraic extensions and computation of a maximal Galois ideal) in a faster one by avoiding their respective drawbacks.

## 1. INTRODUCTION.

Dans cet article, nous fixons un corps  $k$  supposé parfait et un polynôme  $f$  irréductible sur  $k$  et de degré  $n$ . Sous ces hypothèses, les racines  $\alpha_1, \alpha_2, \dots, \alpha_n$  de  $f$  dans une clôture algébrique  $\bar{k}$  de  $k$  sont nécessairement distinctes et le groupe de Galois  $Gal_k(f)$  de  $f$  sur  $k$  est transitif.

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

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

Le but de cet article est de proposer un algorithme efficace pour le calcul de l'idéal  $\mathcal{M}$ , c'est-à-dire celui de l'ensemble triangulaire  $T$ .

---

*Date:* 26 mai 2003.

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

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

L'ensemble  $T$  est calculable par factorisations successives du polynôme  $f$  dans les extensions algébriques  $k(\alpha_1), k(\alpha_1, \alpha_2), \dots, k(\alpha_1, \alpha_2, \dots, \alpha_n)$  (voir [15], [9],[2], [11]). C'est dans l'exécution de ses dernières étapes que cette méthode peut s'avérer très coûteuse (voire infaisable) lorsque l'ordre du groupe de Galois est élevé.

Une autre méthode est proposée avec l'algorithme **GaloisIdéal** (voir Paragraphe 9.2 et [17]) qui construit récursivement une chaîne strictement ascendante d'idéaux (triangulaires) dits de *Galois* :

$$I_1 \subset I_2 \subset \dots \subset I_r = \mathcal{M}$$

Il est toujours possible de prendre pour  $I_1$  l'idéal  $\mathcal{S}$  des relations symétriques entre les racines du polynôme  $f$  qui peut, à l'instar de  $f$ , être considéré comme la donnée du problème.

Pour chaque  $j \in \{1, \dots, r-1\}$ , le temps calcul de l'idéal  $I_{j+1}$  décroît avec le cardinal  $c_j$  de la  $k$ -variété affine de  $I_j$ . Nous avons donc la suite d'inégalités  $c_1 \leq c_2 \leq \dots \leq c_r = \text{Card}(\text{Gal}_k(f))$ . Dans le cas où  $I_1 = \mathcal{S}$ , nous avons  $c_1 = n!$  et l'algorithme est fortement ralenti lors des premières étapes.

Dans cet article, nous montrons comment calculer rapidement un idéal de Galois  $J$  à partir des premières étapes de l'algorithme de factorisation dans les extensions.

Nous expliquerons notre démarche en utilisant la première étape de la première méthode (i.e. la factorisation de  $f$  sur  $k(\alpha_1)$ ). Les deux idées de base sont les suivantes :

1) Les degrés et les groupes de Galois des facteurs (irréductibles)  $f_1 = x - \alpha_1, f_2, \dots, f_s$  de  $f$  dans  $k(\alpha_1)[x]$  ne dépendent que du groupe de Galois  $\text{Gal}_k(f)$  ; ainsi, nous définissons une table dite *de première rupture* qui, à une factorisation type (degrés et groupes de Galois sur  $k(\alpha_1)$  des polynômes  $f_1, \dots, f_s$ ), associe les groupes candidats à être le groupe de Galois  $\text{Gal}_k(f)$  (voir Paragraphe 4 et la table TAB 1 pour le degré 8). Des informations sur les degrés initiaux des polynômes de l'ensemble triangulaire  $T$  cherché se déduisent de cette table (voir paragraphe 9.1).

2) Les facteurs  $f_1, f_2, \dots, f_s$  de degrés respectifs  $n_1 = 1, n_2, \dots, n_s$  peuvent permettre de calculer un idéal de Galois  $I$  dit de *départ* dont chaque variété est de cardinal  $n_1!n_2! \dots n_s!$ . Cet idéal contient strictement l'idéal  $\mathcal{S}$  lorsque le groupe de Galois  $\text{Gal}_k(f)$  n'est pas 2-transitif, sinon  $I = \mathcal{S}$  (voir Paragraphes 6 et 5).

Notre objectif sera alors d'utiliser l'algorithme **GaloisIdéal** pour calculer l'idéal  $\mathcal{M}$  à partir de  $I_1 = I$  avec  $c_1 = n_1!n_2! \dots n_s!$  et donc de calculer un de ses stabilisateurs  $L$  indispensable pour cet algorithme (voir Paragraphe 3 et Définition 3.3). Nous verrons que la principale difficulté se pose lorsque plusieurs degrés parmi  $n_2, \dots, n_s$  sont égaux

puisqu'alors l'ordre des polynômes  $f_2, \dots, f_s$  ne peut être déterminé de manière unique à partir des degrés (voir Paragraphe 5).

Il sera parfois possible de déduire de  $I$  et de son stabilisateur  $L$  un nouvel idéal  $J$  contenant strictement  $I$  ainsi qu'un de ses stabilisateurs (voir Paragraphe 8). L'algorithme `GaloisIdéal` démarrera alors avec  $I_1 = J$ .

Au paragraphe 9 est décrit comment construire un algorithme de calcul de corps de décomposition. A titre d'illustration, nous étudierons le degré 8 (voir Paragraphe 10). Ce degré offre un panel complet des situations diverses qu'il sera possible de rencontrer. Nous avons exclus le cas des groupes 2-transitifs. Ce cas s'inscrit dans une étude globale des extensions supérieures qui s'appuie sur les résultats fondamentaux de cet article. Le paragraphe 11 est dédié à l'implantation et l'expérimentation de notre nouvelle méthode.

Les polynômes que nous utiliserons à titre d'illustration sont extraits de la base de données de G. Malle et J. Klüners (voir [7] et [8]).

## 2. NOTATIONS.

Nous utiliserons les notations suivantes :

- $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \bar{k}^n$  désignera un  $n$ -uplet des  $n$  racines distinctes de  $f$  ;
- Pour tout idéal  $I$  de  $k[x_1, \dots, x_n]$ ,  $V(I)$  sera la variété affine de  $I$  dans  $\bar{k}^n$  ;
- Soit  $E$  un ensemble fini ; l'ensemble des permutations de  $E$  (resp. de  $\{1, \dots, n\}$ ) sera noté  $S_E$  (resp.  $S_n$ ) ;
- Si  $L$  un sous-ensemble de  $S_E$ , le stabilisateur d'un élément  $e \in E$ , considéré comme un sous-groupe de  $S_{E \setminus \{e\}}$ , sera noté  $L_{\{e\}}$  ;
- Les actions naturelles de  $S_n$  sur  $P \in k[x_1, \dots, x_n]$  et  $\underline{\alpha}$  seront notées  $\sigma.P$  et  $\sigma.\underline{\alpha}$  ;
- Le produit direct de groupes symétriques  $S_{n_1} \times \dots \times S_{n_m}$  sera noté  $S_{n_1, \dots, n_m}$  ;
- $\mathcal{T}(n)$  désignera un ensemble fini  $\{nT_1, nT_2, \dots\}$  de représentants de chacune des classes de conjugaison des groupes transitifs de degré  $n$  ;
- lorsque  $n \leq 15$  chaque représentant  $nT_i$  suivra la numérotation du logiciel MAGMA (voir [4]) donnée par la fonction `TransitiveGroup(n, i)` ;
- Pour  $H$  un groupe de permutations et  $\sigma$  un élément d'un de ses sur-groupes, nous noterons  $H^\sigma$  la conjugaison  $\sigma H \sigma^{-1}$  ;
- Nous utiliserons la notation exponentielle pour les suites finies d'un ensemble quelconque ; par exemple, la suite finie  $a, a, a, b, c, c$  s'écrira  $a^3, b, c^2$ .

## 3. IDÉAUX DE GALOIS.

Tout ce qui est décrit dans ce paragraphe reste valable lorsque  $f$  est réductible sur  $k$ . Nous reprenons les définitions et les résultats de [17] et [3].

**Définition 3.1.** Soit  $L$  un sous-ensemble de  $S_n$ . L'idéal des  $\underline{\alpha}$ -relations invariantes par  $L$  défini par :

$$I_{\underline{\alpha}}^L := \{R \in k[x_1, \dots, x_n] \mid \forall l \in L, l.R(\underline{\alpha}) = 0\},$$

est appelé *idéal de Galois de  $f$* .

En particulier, l'idéal  $I_{\underline{\alpha}} = I_{\underline{\alpha}}^{\{Id\}}$  (respectivement,  $I_{\underline{\alpha}}^{S_n}$ ) est appelé l'*idéal des  $\underline{\alpha}$ -relations* (respectivement, *idéal des relations symétriques*).

La proposition suivante donne une caractérisation des idéaux de Galois.

**Proposition 3.2.** *Un idéal  $I$  de  $k[x_1, \dots, x_n]$  est un idéal de Galois de  $f$  ssi il vérifie les deux assertions suivantes :*

- (1)  *$I$  est radical,*
- (2) *il existe  $\underline{\alpha} \in \bar{k}^n$  un  $n$ -uplet des racines de  $f$  tel que  $V(I)$  soit une sous-variété de  $S_n.\underline{\alpha}$ .*

*Démonstration.* Supposons que  $I$  vérifie ces deux assertions. d'après 2), il existe un sous ensemble  $L$  de  $S_n$  tel que  $V(I) = L.\underline{\alpha}$ , et donc,

$$\sqrt{I} = \{P \in k[x_1, \dots, x_n] \mid \forall \sigma \in L, P(\sigma.\underline{\alpha}) = 0\} = I_{\underline{\alpha}}^L.$$

L'assertion 1) donne alors l'égalité  $I = I_{\underline{\alpha}}^L$ .

La réciproque découle de la définition des idéaux de Galois.  $\square$

Fixons  $I$  un idéal de Galois de  $f$  et  $\underline{\alpha} \in V(I)$ .

**Définition 3.3.** Le *stabilisateur de  $I$  relatif à  $\underline{\alpha}$*  noté  $Stab(I, \underline{\alpha})$  est défini par :

$$Stab(I, \underline{\alpha}) = \{\tau \in S_n \mid \forall R \in I, \tau.R(\underline{\alpha}) = 0\}.$$

Ainsi nous pouvons décrire la variété  $V(I)$  :

$$V(I) = \{\sigma.\underline{\alpha} \mid \sigma \in Stab(I, \underline{\alpha})\},$$

et, comme  $f$  est séparable,

$$Card(Stab(I, \underline{\alpha})) = Card(V(I)).$$

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

**Proposition 3.4.** *Soit  $\sigma \in Stab(I, \underline{\alpha})$  alors*

$$Stab(I, \sigma.\underline{\alpha}) = \sigma^{-1} Stab(I, \underline{\alpha}).$$

**Démonstration.** Puisque  $\sigma \in \text{Stab}(I, \underline{\alpha})$ , nous avons bien  $\sigma.\underline{\alpha} \in V(I)$  et, par définition du stabilisateur, nous obtenons :

$$\begin{aligned} \text{Stab}(I, \sigma.\underline{\alpha}) &= \{\tau \in S_n \mid \forall R \in I, (\tau.R)(\sigma.\underline{\alpha}) = 0\} \\ &= \{\tau \in S_n \mid \forall R \in I, (\sigma\tau.R)(\underline{\alpha}) = 0\}. \end{aligned}$$

En posant  $\rho = \sigma\tau$ , nous obtenons le résultat :

$$\text{Stab}(I, \sigma.\underline{\alpha}) = \sigma^{-1}\{\rho \in S_n \mid \forall R \in I, (\rho.R)(\underline{\alpha}) = 0\} = \sigma^{-1}\text{Stab}(I, \underline{\alpha}). \quad \square$$

Ainsi, si tous les stabilisateurs de  $I$  relatifs aux éléments de  $V(I)$  sont identiques, ils forment un groupe que nous notons  $\text{Stab}(I)$  et appelons le *stabilisateur de  $I$* . C'est le cas de l'idéal des relations :

**Définition 3.5.** Le *groupe de Galois* de  $\underline{\alpha}$  sur  $k$ , noté  $\text{Gal}_k(\underline{\alpha})$ , est le stabilisateur de l'idéal des relations  $I_{\underline{\alpha}}$ .

*Remarque 3.6.* Le groupe de Galois  $\text{Gal}_k(\underline{\alpha})$  est isomorphe au groupe de Galois  $\text{Gal}_k(f)$  des  $k$  automorphismes de  $k(\underline{\alpha})$ . Ainsi, nous identifierons  $\text{Gal}_k(f)$  au conjugué de  $\text{Gal}_k(\underline{\alpha})$  dans  $\mathcal{T}(n)$ .

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

**Proposition 3.7.** (voir [17]) *Nous avons  $\text{Gal}_k(\underline{\alpha}) \subset \text{Stab}(I, \underline{\alpha})$ . De plus si  $L$  est sous-ensemble  $S_n$  vérifiant  $I = I_{\underline{\alpha}}^L$ , alors  $\text{Stab}(I, \underline{\alpha}) = \text{Gal}_k(\underline{\alpha})L$ . C'est en particulier vrai pour  $L = \text{Stab}(I, \underline{\alpha})$ .*

**Définition 3.8.** Le *groupe de décomposition*  $\text{Gr}(I)$  de  $I$  est défini par :

$$\text{Gr}(I) := \{\sigma \in S_n \mid \forall R \in I, \sigma.R \in I\}.$$

Nous avons alors la proposition suivante :

**Proposition 3.9.** (Voir [17]) *Il y a équivalence entre les assertions suivantes :*

- (1)  $\text{Gal}_k(\underline{\alpha}) \subset \text{Gr}(I)$ ,
- (2)  $\text{Card}(\text{Stab}(I, \underline{\alpha})) = \text{Card}(\text{Gr}(I))$ ,
- (3)  $\text{Gr}(I) = \text{Stab}(I, \underline{\alpha})$ ,
- (4) *les stabilisateurs de  $I$  relatifs aux éléments de  $V(I)$  sont identiques.*

*De plus si l'une de ces assertions est satisfaite alors  $\text{Stab}(I) = \text{Gr}(I)$ .*

Il est important de pouvoir tester si  $\text{Gr}(I)$  est le stabilisateur de  $I$  car le groupe de décomposition est rapidement calculable à partir de  $I$  (voir [1]) alors que le calcul de  $\text{Stab}(I, \underline{\alpha})$  nécessite de connaître l'idéal des  $\underline{\alpha}$ -relations  $I_{\underline{\alpha}}$ .

**Définition 3.10.** Un idéal de  $k[x_1, \dots, x_n]$  est dit *triangulaire* s'il est engendré par un ensemble triangulaire séparable (voir [3] pour la définition).

**Proposition 3.11.** (Voir [3]) *Si  $Gr(I)$  est le stabilisateur de  $I$ , alors  $I$  est un idéal triangulaire.*

*Remarque 3.12.* D'après [5], l'idéal des relations symétriques est engendré par l'ensemble triangulaire formé par les *modules de Cauchy* du polynôme  $f$ .

Dans cet article, tous les idéaux de Galois considérés seront triangulaires ou bien par construction ou bien par la proposition 3.11. Nous supposons donc à partir de maintenant que  $I$  est engendré par l'ensemble triangulaire séparable  $T = \{f_1(x_1), f(x_1, x_2) \cdots, f_n(x_1, \dots, x_n)\}$ .

**Définition 3.13.** Le  $n$ -uplet  $\mathcal{L}(I)$  défini par

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

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

Ce sont les degrés initiaux de  $I$  qui vont nous permettre de calculer le cardinal de  $V(I)$  et donc celui de  $\text{Stab}(I, \underline{\alpha})$ . En effet, comme  $I$  est triangulaire nous avons :

$$\text{Card}(V(I)) = \prod_{i=1}^n deg_{x_i}(I) = \text{Card}(\text{Stab}(I, \underline{\alpha})).$$

Nous en déduisons le test cherché :

**Proposition 3.14.** *Si  $Gr(I)$  vérifie :*

$$\text{Card}(Gr(I)) = \prod_{i=1}^n deg_{x_i}(I),$$

*alors  $Gr(I)$  est le stabilisateur de  $I$ .*

*Démonstration.* Découle de la proposition 3.9. □

Soit  $G$  un sous-groupe de  $S_n$ . Il est possible de calculer a priori  $\mathcal{L}(J)$  pour tout idéal de Galois  $J$  dont  $G$  est le stabilisateur. Nous notons  $\mathcal{L}(G)$  la liste  $\mathcal{L}(J)$  d'un tel idéal  $J$ . Cette liste se calcule avec la fonction Magma `InitDeg(G,n)` suivante qui transcrit un résultat de l'article [3] :

```

InitDeg:= fonction(G,n);
  L:=[]; L[1]:=G; Degr:=[];
  for i:=1 to n do
    L[i+1]:= Stabilizer(G,i) meet L[i];
    Degr[i]:=Order(L[i])/Order(L[i+1]);
  end for;
  return Degr;
end fonction;

```

C'est l'idéal  $I_{\underline{\alpha}}$  qui à partir de maintenant joue le rôle de l'idéal  $\mathcal{M}$  de l'introduction.

#### 4. LA TABLE DE PREMIÈRE RUPTURE.

Dans cette partie nous montrons comment construire l'objet central de notre article : la *table de première rupture*. Pour ce faire, nous allons étudier le lien entre le groupe de Galois  $Gal_k(f)$  et le groupe de Galois de chacun des facteurs irréductibles de  $f$  sur un de ses corps de rupture.

##### 4.1. Groupes de Galois des facteurs irréductibles d'un polynôme.

Soit  $K$  un corps parfait. Considérons  $g \in K[x]$  un polynôme séparable de degré  $d$ . La théorie classique de Galois lie, par la proposition suivante,  $Gal_K(g)$  aux groupes de Galois sur  $K$  de chacun de ses facteurs irréductibles dans  $K[x]$ .

**Proposition 4.1.** *Soit  $O$  une orbite de l'action de  $Gal_K(g)$  sur  $\{1, \dots, d\}$ . L'injection canonique*

$$\varphi_O : Gal_K(g) \longrightarrow S_O,$$

*induit par l'action de  $Gal_K(g)$  sur  $O$ , a pour image le groupe de Galois du facteur irréductible  $g_1$  de  $g$  sur  $k$  donné par :*

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

*En particulier  $Card(O) = Deg(g_1)$ .*

Dans la suite de ce paragraphe, nous noterons  $O_G$  l'ensemble des orbites de l'action sur  $\{1, \dots, d\}$  d'un sous-groupe  $G$  de  $S_d$ .

Soit  $\mathcal{T} := \cup_{n \in \mathbb{N}} \mathcal{T}(n)$  l'ensemble des représentants des classes de conjugaison des groupes transitifs. Ordonnons  $\mathcal{T}$  à l'aide de l'ordre lexicographique  $\prec$  : soient  $mT_i$  et  $nT_j$  deux éléments de  $\mathcal{T}$ ,

$$mT_i \prec nT_j \text{ si } (m, i) <_{lex} (n, j).$$

Pour  $T$  un groupe de permutations transitif quelconque, nous noterons  $\iota(T)$  le représentant dans  $\mathcal{T}$  de sa classe de conjugaison.

Soit  $(E, <)$  un ensemble ordonné, on notera  $S(E, <)$  l'ensemble des suites finies d'éléments de  $E$  croissantes selon  $<$ .

Définissons les applications  $\gamma$  et  $\delta$  de  $\mathcal{G}$ , l'ensemble des groupes de permutations, dans respectivement  $S(\mathcal{T}, \prec)$  et  $S(\mathbb{N}, \leq)$  :



$$\begin{aligned}
\gamma : \mathcal{G} &\longrightarrow S(\mathcal{T}, \prec) \\
G &\longmapsto (\iota(\varphi_O(G)))_{O \in O_G} \\
\delta : \mathcal{G} &\longrightarrow S(\mathbb{N}, \leq) \\
G &\longmapsto (\text{Card}(O))_{O \in O_G}
\end{aligned}$$

L'algorithme suivant calcule les images par  $\gamma$  et  $\delta$  d'un groupe  $G$  de permutations :

*Algorithme 4.2.*

---

**FactGaloisGroups**( $G$ )

**Entrée** :  $G$  un sous-groupe de  $S_d$

**Sorties** :  $\delta(G), \gamma(G)$

$j := 1$  ;

**Pour**  $O \in O_G$  **Faire**

$\text{Deg}[j] := \text{Card}(O)$  ;

$\text{Group}[j] := \iota(\varphi_O(G))$  ;

$j := j + 1$  ;

**Fin Pour** ;

**Retourne**  $\text{Ordonne}(\text{Deg}, \leq)$ ,  $\text{Ordonne}(\text{Group}, \prec)$  ;

**Fin FactGaloisGroups** ;

---

*Commentaires 4.3.*

- La fonction  $\text{Ordonne}(L, \prec)$  ordonne les éléments d'une liste  $L$  selon l'ordre  $\prec$  croissant.
- Les fonctions MAGMA  $\text{TransitifGroupIdentification}(H)$  et  $\text{OrbiteImage}(G, O)$  implantent respectivement les applications  $\iota(H)$  et  $\varphi_O(G)$ .

Nous allons maintenant utiliser ce résultat pour construire la table de première rupture.

#### 4.2. Construction de la table de première rupture.

Comme le polynôme  $f$  est irréductible, l'anneau quotient  $k[x]/\langle f \rangle$  est un corps appelé ici *corps de première rupture* pour  $f$ . Ce corps est isomorphe à  $k(\alpha_1)$ . 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  $\text{Gal}_K(g) = \text{Gal}_k(f)_{\{1\}}$ .

**Notations 4.4.** Soit  $T$  un groupe transitif de  $\mathcal{T}$ ,  $\Gamma(T)$  désignera la suite  $\gamma(T_{\{1\}})$  et  $\Delta(T)$  la suite  $\delta(T_{\{1\}})$ .

La table qui recense les images, par  $\Gamma$  et  $\Delta$ , de tous les groupes de  $\mathcal{T}_n$  sera appelée *la table de première rupture en degré  $n$* . Par exemple, celle en degré 8 est la suivante :

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

TAB. 1. Table de première rupture en degré 8.

Nous allons maintenant exploiter la table de première rupture pour obtenir des informations sur le Groupe de Galois des polynômes irréductibles.

**Définition 4.5.** Les facteurs irréductibles  $f_1, \dots, f_r$  de  $f(x)/(x - \alpha_1)$  dans  $k(\alpha_1)[x]$  sont appelés *les facteurs de première rupture de  $f$*  et sont supposés ordonnés par degrés croissants.

**Notations 4.6.** Rappelons qu'ici  $f$  est irréductible, ainsi nous pouvons noter  $\Gamma(f)$  la suite  $\Gamma(\text{Gal}_k(f))$  et  $\Delta(f)$  la suite  $\Delta(\text{Gal}_k(f))$ .

La Proposition 4.1 montre que  $\Gamma(f)$  est, à permutation des facteurs de même degré près, la suite  $\text{Gal}_{k(\alpha_1)}(f_1), \dots, \text{Gal}_{k(\alpha_1)}(f_r)$  et que  $\Delta(f)$  est la suite  $\text{deg}(f_1), \dots, \text{deg}(f_r)$ . La table de première 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 les exemples ci-après.

*Exemple 4.7.* Soit le polynôme irréductible  $f := x^8 - 4x^7 + 14x^5 - 8x^4 - 12x^3 + 7x^2 + 2x - 1$ . En factorisant  $f$  dans sa première extension,

nous obtenons quatre facteurs linéaires et un facteur irréductible de degré 4, donc  $\Delta_8(f) = 1^3, 4$ . Ainsi, d'après la table TAB. 1, les groupes candidats à être le groupe de Galois de  $f$  sur  $\mathbb{Q}$  sont  $8T_{17}$  et  $8T_{18}^+$ . Le discriminant de  $f$  étant égal à  $300416 = 2^{12}41^3$ , qui n'est pas un carré dans  $\mathbb{Q}$ , le groupe de Galois de  $f$  est donc le groupe impair  $8T_{17}$ .

*Exemple 4.8.* Si un polynôme  $f$  de degré 8 admet pour groupe de Galois sur  $k$  le groupe  $8T_{46}$  alors, comme  $\Delta_8(f) = (3, 4)$ , la factorisation de  $f$  sur  $k(\alpha_1)$  est de la forme :

$$f(x) = (x - \alpha_1)g_1(x)g_2(x) ,$$

où les facteurs  $g_1$  de degré 3 et  $g_2$  de degré 4 sont les facteurs de première rupture de  $f$ . Les groupes de Galois sur  $k(\alpha_1)$  de  $g_1(x)$  et  $g_2(x)$  sont alors respectivement  $3T_2$  et  $4T_5$ .

La table de première rupture ne donne apparemment que des informations sur le groupe de Galois des polynômes. De plus, même en l'étendant aux extensions algébriques supérieures (la théorie étant la même), elle n'est pas toujours suffisante pour déterminer le groupe de Galois d'un polynôme irréductible à partir de ses facteurs de rupture (la première ligne de la table permet de s'en convaincre). Pourtant, elle fait faire un grand pas vers le calcul simultané du groupe de Galois et d'un idéal des relations. C'est ce que nous allons développer dans la suite de cet article.

## 5. IDÉAL DE PREMIÈRE RUPTURE.

Supposons que  $f$  possède trois facteurs irréductibles sur  $k(\alpha_1)$  :

$$f(x) = (x - \alpha_1).g(\alpha_1, x).h(\alpha_1, x).$$

Soit  $m$  le degré de  $g$  et  $p$  celui de  $h$ . Soit  $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \bar{k}^n$  un  $n$ -uplet de racines de  $f$  ordonné de telle sorte que  $\underline{\beta} = (\alpha_2, \dots, \alpha_{m+1})$  soit un  $m$ -uplet de racines de  $g$  et que  $\underline{\gamma} = (\alpha_{m+2}, \dots, \alpha_n)$  soit un  $p$ -uplet de racines de  $h$ .

L'idéal de Galois  $I_{\underline{\beta}}^{S^m}$  (resp.  $I_{\underline{\gamma}}^{S^p}$ ) est supposé appartenir au corps  $k(\alpha_1)[x_2, \dots, x_m]$  (resp.  $k(\alpha_1)[x_{m+2}, \dots, x_n]$ ).

Notons  $T_g(\alpha_1)$  (resp.  $T_h(\alpha_1)$ ) l'ensemble triangulaire formé par les modules de Cauchy de  $g$  (resp.  $h$ ) (voir Remarque 3.12).

Alors dans  $A_0 = k(\alpha_1)[x_1, \dots, x_n]$  nous avons :

$$(5.1) \quad I_{\underline{\alpha}}^{S^{1,m,p}} = (x_1 - \alpha_1)A_0 + I_{\underline{\beta}}^{S^m} A_0 + I_{\underline{\gamma}}^{S^p} A_0 \quad .$$

L'idéal  $I_{\underline{\alpha}}^{S^{1,m,p}}$  de  $A_0$  est engendré par l'ensemble triangulaire séparable  $\{x_1 - \alpha_1\} \cup T_g(x_1) \cup T_h(x_1)$  et a pour stabilisateur  $S_{1,m,p}$ .

Par induction, la construction précédente se généralise à toute factorisation de  $f$  dans  $k(\alpha_1)[x]$ . Soient  $f_1, f_2, \dots, f_r$  les facteurs de première

ruptures (voir Définition 4.5) et les ensembles triangulaires  $T_{f_i}(\alpha_1)$  formés par les modules de Cauchy de chacun des facteurs de première rupture  $f_i$  pour  $i = 1, \dots, n$ .

L'idéal de Galois  $I_{\underline{\alpha}}^{S_{1,\Delta(f)}}$  de  $k(\alpha_1)[x_1, \dots, x_n]$  sera appelé un *idéal de première rupture de  $f$* . Il admet pour stabilisateur le groupe  $S_{1,\Delta(f)}$  et pour système générateur l'ensemble triangulaire

$$\{x_1 - \alpha_1\} \cup T_{f_1}(x_1) \cup \dots \cup T_{f_r}(x_1).$$

*Remarque 5.1.* Il existe autant d'idéaux de première rupture que de permutations de  $S_r$  qui laissent  $\Delta(f)$  invariant. Chacun a néanmoins  $S_{1,\Delta(f)}$  comme stabilisateur.

Dans le paragraphe 6, nous verrons que l'idéal  $I$ , dit de départ, engendré par  $\{f(x_1)\} \cup T_{f_1}(x_1) \cup \dots \cup T_{f_r}(x_1)$  est un idéal de Galois de  $f$  dans  $k[x_1, x_2, \dots, x_n]$  dont nous chercherons à calculer un stabilisateur à partir du stabilisateur  $S_{1,\Delta(f)}$  des idéaux de première rupture.

*Remarque 5.2.* Si le groupe de Galois de  $f$  est 2-transitif alors il n'y a qu'un facteur de première rupture  $f_1$  (de degré  $n-1$ ), l'idéal  $I$  est l'idéal des relations symétriques entre les racines de  $f$  et  $\{f(x_1)\} \cup T_{f_1}(x_1)$  est l'ensemble des modules de Cauchy de  $f$ . Il faudra donc appliquer nos résultats pour les factorisations dans les extension  $k(\alpha_1, \alpha_2, \dots, \alpha_i)$  avec  $1 < i < n$ .

*Exemple 5.3.* Soit le polynôme  $f = x^8 - x^6 - x^4 + x^2 + 1$ , irréductible sur  $\mathbb{Q}$  et de groupe de Galois  $8T_{29}^+$ . Il se factorise sur un corps de première rupture en :

$$f = (x - \alpha_1)(x + \alpha_1)(x^2 - \alpha_1^6 + \alpha_1^4 + \alpha_1^2 - 1)(x^4 + (\alpha_1^6 - \alpha_1^4)x^2 - 1) \quad ,$$

avec  $\Delta(f) = 1, 2, 4$ . D'après la Table de première rupture 1, son groupe de Galois est un sous-groupe de  $8T_{35}$ . Les modules de Cauchy des facteurs de première rupture de degré 2 et de degré 4 sont respectivement les deux ensembles de polynômes :

$$\begin{aligned} T_1(\alpha_1) &= \{ x_3^2 - \alpha_1^6 + \alpha_1^4 + \alpha_1^2 - 1, \\ &\quad x_4 + x_3 \} \\ T_2(\alpha_1) &= \{ x_5^4 + (\alpha_1^6 - \alpha_1^4)x_5^2 - 1, \\ &\quad x_6^3 + x_5^3 + x_5^2x_6 + x_5x_6^2 + (\alpha_1^6 - \alpha_1^4)x_5 + (\alpha_1^6 - \alpha_1^4)x_6, \\ &\quad x_7^2 + x_5^2 + x_5x_6 + x_5x_7 + x_6^2 + x_6x_7 + \alpha_1^6 - \alpha_1^4, \\ &\quad x_8 + x_7 + x_6 + x_5 \}. \end{aligned}$$

L'idéal de première rupture  $I_{\underline{\alpha}}^{S_{12,2,4}}$  de  $f$  est donc engendré par l'ensemble triangulaire  $T$  suivant :

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

## 6. IDÉAL DE DÉPART

Dans ce paragraphe, nous fixons  $I_0$  un idéal de Galois de  $f$  sur  $k(\alpha_1)$  engendré par l'ensemble triangulaire suivant :

$$\{x_1 - \alpha_1, f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)\}$$

avec  $f_i \in k[x_1, \dots, x_n]$ . Nous allons donner les moyens théoriques pour que s'en déduise un idéal de Galois  $I$  de  $f$  sur  $k[x_1, \dots, x_n]$  dont nous chercherons à calculer un stabilisateur. En dehors de  $I_0$ , tous les idéaux seront dans  $k[x_1, x_2, \dots, x_n]$ .

Fixons  $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in V(I_0)$  et notons  $L_0$  le stabilisateur de  $I_0$  relatif à  $\underline{\alpha}$ . Nous avons  $V(I_0) = \{\sigma.\underline{\alpha} \mid \sigma \in L_0\}$  et, d'après la proposition 3.7,

$$\text{Stab}(\text{Gal}_k(\underline{\alpha}), 1) = \text{Gal}_{k(\alpha_1)}(\underline{\alpha}) \subset \text{Stab}(I_0, \underline{\alpha}) = L_0 \quad .$$

**Définition 6.1.** Posons  $f_1 = f$ . L'idéal de départ est l'idéal, noté  $I$ , de  $k[x_1, \dots, x_n]$  engendré par l'ensemble triangulaire suivant :

$$\{f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)\}.$$

**Proposition 6.2.** L'idéal de départ  $I$  est un idéal de Galois de  $f$ .

*Démonstration.* Par construction, la variété de  $I$  est un sous-ensemble de  $S_n.\underline{\alpha}$ . Les racines de  $f$  étant distinctes et l'idéal  $I_0$  étant triangulaire, il en est de même pour  $I$ . À fortiori  $I$  est radical, par conséquent, d'après la proposition 3.2, l'idéal  $I$  est un idéal de Galois.  $\square$

## 6.1. Décomposition de la variété de l'idéal de départ.

Pour tout  $i \in \{1, \dots, n\}$ , notons  $V(I)_{\{i\}}$  le sous-ensemble de  $V(I)$  défini par :

$$V(I)_{\{i\}} := \{\tau.\underline{\alpha} \in \bar{k}^n \mid \tau \in S_n \text{ et } \tau(1) = i\} \cap V(I).$$

Ces nouveaux ensembles permettent de décomposer la variété  $V(I)$  en l'union disjointe :

$$(6.1) \quad V(I) = \bigcup_{i=1}^n V(I)_{\{i\}}.$$

**Lemme 6.3.** Soient  $\sigma_1, \dots, \sigma_n$  des permutations de  $\text{Gal}_k(\underline{\alpha})$ , telles que  $\sigma_i(1) = i$ , alors nous avons :

$$(6.2) \quad V(I)_{\{i\}} = \sigma_i.V(I)_{\{1\}} = \sigma_i.V(I_0) \quad \text{et}$$

$$(6.3) \quad V(I) = \bigcup_{i=1}^n \sigma_i.V(I_0) \quad .$$

*Démonstration.* Soit  $\sigma_i \in \text{Gal}_k(\underline{\alpha})$  telle que  $\sigma_i(1) = i$ , nous avons,

$$\sigma_i.V(I)_{\{1\}} = \sigma_i.\{\tau.\underline{\alpha} \in \bar{k}^n \mid \tau \in S_n \text{ et } \tau(1) = 1\} \cap \sigma_i.V(I).$$

Comme  $V(I) = \text{Stab}(I, \underline{\alpha}).\underline{\alpha}$  et que  $\text{Gal}_k(\underline{\alpha})\text{Stab}(I, \underline{\alpha}) = \text{Stab}(I, \underline{\alpha}) =$  (voir Proposition 3.7), nous avons  $\sigma_i.V(I) = V(I)$  et il s'en suit les égalités suivantes :

$$\begin{aligned} \sigma_i.V(I)_{\{1\}} &= \sigma_i.\{\tau.\underline{\alpha} \mid \tau \in S_n \text{ et } \tau(1) = 1\} \cap V(I) \\ &= \{\tau.\underline{\alpha} \mid \tau \in S_n \text{ et } \tau(1) = i\} \cap V(I) \\ &= V(I)_{\{i\}}. \end{aligned}$$

L'égalité  $V(I)_{\{1\}} = V(I_0)$  permet de conclure.  $\square$

## 6.2. Calcul d'un stabilisateur de $I$ .

### 6.2.1. Théorème fondamental.

**Lemme 6.4.** *Soient  $\sigma_1, \dots, \sigma_n \in \text{Gal}_k(\underline{\alpha})$  vérifiant  $\sigma_i(1) = i$  pour  $i \in \{1, \dots, n\}$ . Alors*

$$\text{Stab}(I, \underline{\alpha}) = \sigma_1\text{Stab}(I_0, \underline{\alpha}) + \dots + \sigma_n\text{Stab}(I_0, \underline{\alpha}).$$

**Démonstration.** Puisque  $V(I_0) = \{\tau.\underline{\alpha} \mid \tau \in L_0\}$  où  $L_0 = \text{Stab}(I_0, \underline{\alpha})$ , l'égalité 6.3 du lemme 6.3 entraîne :

$$\text{Stab}(I, \underline{\alpha}) = \sigma_1 L_0 + \dots + \sigma_n L_0$$

L'application du lemme 6.4 nécessite de connaître au moins un sous-groupe transitif de  $\text{Gal}_k(\underline{\alpha})$ . Nous allons en déduire un théorème moins contraignant pour calculer ce stabilisateur.

Définissons l'ensemble, noté  $\mathcal{A}(L_0)$ , des sous-groupes transitifs  $H$  de  $S_n$  tels qu'ils existent  $\tau_1 = id, \dots, \tau_s \in L_0$  vérifiant :

$$L_0 = H_{\{1\}}\tau_1 + \dots + H_{\{1\}}\tau_s.$$

D'après la proposition 3.7, nous avons  $\text{Gal}_k(\underline{\alpha}) \in \mathcal{A}(L_0)$ .

*Remarque 6.5.* Si  $L_0$  est un groupe (comme pour  $I_0$  un idéal de première rupture) alors

$$\mathcal{A}(L_0) = \{H \text{ sous-groupe transitif de } S_n \mid H_{\{1\}} \subset L_0\};$$

de plus, pour tout  $\underline{\beta} \in V(I_0)$ , nous avons :

$$\text{Stab}(\text{Gal}_k(\underline{\beta}), 1) = \text{Gal}_{k(\alpha_1)}(\underline{\beta}) \subset \text{Stab}(I_0, \underline{\beta}) = L_0.$$

**Proposition 6.6.** *L'application  $\Psi_{L_0}$  qui à tout  $H$  dans  $\mathcal{A}(L_0)$  fait correspondre le sous-ensemble  $H\tau_1 + \dots + H\tau_s$  de  $S_n$ , où  $\tau_1 = id, \dots, \tau_s$  sont des éléments de  $L_0$  tels que  $L_0 = H_{\{1\}}\tau_1 + \dots + H_{\{1\}}\tau_s$ , est bien définie.*

*Démonstration.* Il suffit de montrer que  $\Psi_{L_0}(H) = H\tau_1 + \dots + H\tau_s$  ne dépend pas de la transversale à droite,  $\tau_1, \dots, \tau_s$  de  $L_0$  modulo  $H_{\{1\}}$ . Soit  $\tau'_1, \dots, \tau'_s$  une autre transversale de  $L_0$  modulo  $H_{\{1\}}$ . De  $\tau_1 \in L_0$ , il vient  $\tau_1 \in H_{\{1\}}\tau'_1 + \dots + H_{\{1\}}\tau'_s$ , puis successivement,

$$H\tau_1 \subset H\tau'_1 + \dots + H\tau'_s \text{ et}$$

$$H\tau_1 + \dots + H\tau_s \subset H\tau'_1 + \dots + H\tau'_s.$$

De la même manière se prouve l'inclusion réciproque. Par conséquent,  $H\tau_1 + \dots + H\tau_s = H\tau'_1 + \dots + H\tau'_s$  ce qui termine la preuve.  $\square$

Nous définissons ainsi une application  $\Psi_{L_0}$  de  $\mathcal{A}(L_0)$  dans les parties de  $S_n$ . Pour la suite, nous fixons  $L_0$  et notons  $\Psi = \Psi_{L_0}$ .

**Lemme 6.7.** *Soit  $H$  un groupe de  $\mathcal{A}(L_0)$ . Si  $\sigma_1 = id, \dots, \sigma_n \in H$  vérifient  $\sigma_i(1) = i$  pour  $i \in \{1, \dots, n\}$ , alors  $\Psi(H) = \sigma_1 L_0 + \dots + \sigma_n L_0$ .*

**Démonstration.** Comme  $H$  est transitif, les  $\sigma_i$  existent et  $H = \sigma_1 H_{\{1\}} + \dots + \sigma_n H_{\{1\}}$ . Nous avons alors

$$\begin{aligned} \Psi(H) &= (\sigma_1 H_{\{1\}} + \dots + \sigma_n H_{\{1\}})\tau_1 + \dots + (\sigma_1 H_{\{1\}} + \dots + \sigma_n H_{\{1\}})\tau_s \\ &= \sigma_1 L_0 + \dots + \sigma_n L_0 \quad \square \end{aligned}$$

**Lemme 6.8.** *Soient  $G$  et  $H$  deux groupes de  $\mathcal{A}(L_0)$ . Si  $G \cap H$  est transitif alors  $\Psi(G) = \Psi(H)$ .*

*Démonstration.* C'est évident en prenant les  $\sigma_i$  du lemme 6.7 dans  $G \cap H$ .  $\square$

**Théorème 6.9.** *Soit  $H$  un élément de  $\mathcal{A}(L_0)$  tel que  $H \cap Gal_k(\underline{\alpha})$  soit un sous-groupe transitif de  $S_n$ . Soient  $\sigma_1 = id, \dots, \sigma_n \in H$  vérifiant  $\sigma_i(1) = i$  pour  $i \in \{1, \dots, n\}$ . Alors*

$$\begin{aligned} Stab(I, \underline{\alpha}) = \Psi(H) &= H\tau_1 + \dots + H\tau_s \\ &= \sigma_1 Stab(I_0, \underline{\alpha}) + \dots + \sigma_n Stab(I_0, \underline{\alpha}). \end{aligned}$$

*En particulier, en posant  $m_i = deg_{x_i}(I_0)$  pour  $i \in \{1, \dots, n\}$ ,*

$$Card(Stab(I, \underline{\alpha})) = s.Card(H) = n.Card(Stab(I_0, \underline{\alpha})) = n.m_2 \dots m_n.$$

*Démonstration.* Comme  $Gal_k(\underline{\alpha}) \in \mathcal{A}(L_0)$  donc, d'après le lemme 6.8,  $\Psi(H) = \Psi(Gal_k(\underline{\alpha}))$ . Comme, d'après le lemme 6.4,  $\Psi(Gal_k(\underline{\alpha})) = Stab(I, \underline{\alpha})$ , la démonstration est terminée.  $\square$

Avec le Lemme suivant, nous pouvons prendre  $\underline{\alpha}$  dans  $V(I)$  aussi bien que dans  $V(I_0)$ .

**Lemme 6.10.** *Soit  $\underline{\beta} \in V(I)$  alors il existe  $\underline{\gamma} \in V(I_0)$  tel que  $I_{\underline{\gamma}} = I_{\underline{\beta}}$ ,  $Gal_k(\underline{\beta}) = Gal_k(\underline{\gamma})$  et  $Stab(I, \underline{\beta}) = Stab(I, \underline{\gamma})$ .*

*Démonstration.* Si  $\underline{\beta} \in V(I)$  alors, comme  $\underline{\alpha} \in V(I_0) \subset V(I)$ , il existe  $\sigma \in \text{Stab}(I, \underline{\alpha})$  tel que  $\underline{\beta} = \sigma.\underline{\alpha}$ . Comme  $\sigma \in \text{Stab}(I, \underline{\alpha})$ , d'après le lemme 6.4,  $\sigma = \sigma_i l_0$  avec  $\sigma_i \in \text{Gal}_k(\underline{\alpha})$  et  $l_0 \in L_0$ . Comme  $\sigma_i \in \text{Gal}_k(\underline{\alpha})$ , nous avons l'identité  $I_{\underline{\beta}} = I_{\sigma_i l_0.\underline{\alpha}} = I_{l_0.\underline{\alpha}}$  et donc  $\text{Gal}_k(\underline{\beta}) = \text{Gal}_k(l_0.\underline{\alpha})$ . En posant  $\underline{\gamma} = l_0.\underline{\alpha}$ , comme  $L_0 = \text{Stab}(I_0, \underline{\alpha})$ , nous avons  $\underline{\gamma} \in V(I_0)$ . De plus,  $\text{Stab}(I, \underline{\beta}) = l_0^{-1} \sigma_i^{-1} \text{Stab}(I, \underline{\alpha}) = l_0^{-1} \text{Stab}(I, \underline{\alpha})$  car  $\sigma_i \in \text{Gal}_k(\underline{\alpha})$ . Nous obtenons ainsi  $\text{Stab}(I, \underline{\beta}) = \text{Stab}(I, l_0.\underline{\alpha}) = \text{Stab}(I, \underline{\gamma})$ .  $\square$

### 6.2.2. Stabilisateurs de $I$ et classes de $L_0$ -conjugaison.

Dans le théorème 6.9, il s'agit de tester si  $H \cap \text{Gal}_k(\underline{\alpha})$  est transitif pour  $\underline{\alpha} \in V(I_0)$  quelconque afin de pouvoir calculer un stabilisateur de  $I$ . Mais il apparaît comme impossible de réaliser directement ce test sans connaître  $\text{Gal}_k(\underline{\alpha})$ . En revanche, à partir d'informations obtenues sur le groupe de Galois de  $f$ , il est parfois possible de tester si  $H' \cap \text{Gal}_k(f)$  est transitif pour un conjugué quelconque  $H'$  de  $H$ . La proposition 6.12 permettra de tester si  $H \cap \text{Gal}_k(\underline{\alpha})$  est transitif, c'est à dire si  $\Psi(H)$  est un stabilisateur de  $I$  (celui relatif à  $\underline{\alpha}$ ).

**Lemme 6.11.** *Soit  $G$  un sous-groupe de  $S_n$ . Il existe  $\sigma \in L_0$  tel que  $\text{Gal}_k(\underline{\alpha}) = G^\sigma$  si et seulement si il existe  $\underline{\beta} \in V(I_0)$  tel que  $G = \text{Gal}_k(\underline{\beta})$ .*

*Démonstration.* Supposons qu'il existe  $\sigma \in L_0$  tel que  $\text{Gal}_k(\underline{\alpha}) = \sigma G \sigma^{-1}$ , alors  $G = \text{Gal}_k(\sigma.\underline{\alpha})$  et  $\sigma.\underline{\alpha} \in V(I_0)$  puisque  $\sigma \in L_0$ . Réciproquement, on a nécessairement  $\underline{\beta} = \sigma.\underline{\alpha}$  avec  $\sigma \in L_0$  et  $G = \text{Gal}_k(\underline{\beta}) = \text{Gal}_k(\sigma.\underline{\alpha}) = \sigma^{-1} \text{Gal}_k(\underline{\alpha}) \sigma$ .  $\square$

**Proposition 6.12.** *Supposons que  $H \cap \text{Gal}_k(\underline{\alpha})$  soit transitif. Alors*  
 1) *Pour tout  $\sigma \in L_0$  il existe  $\underline{\beta} \in V(I_0)$  tel que  $H^{\sigma^{-1}} \cap \text{Gal}_k(\underline{\beta})$  soit transitif avec  $\underline{\beta} = \sigma.\underline{\alpha}$  ;*  
 2) *pour tout  $\underline{\beta} \in V(I)$ , il existe  $\sigma \in L_0$  tel que  $H^{\sigma^{-1}} \cap \text{Gal}_k(\underline{\beta})$  soit transitif avec  $\text{Gal}_k(\underline{\beta}) = \text{Gal}_k(\sigma.\underline{\alpha})$ .*

*Démonstration.* Rappelons que  $\text{Gal}_k(\sigma.\underline{\alpha}) = \sigma^{-1} \text{Gal}_k(\underline{\alpha}) \sigma$ . Montrons tout d'abord l'assertion 1). Soit  $\sigma \in L_0$ , posons  $\underline{\beta} = \sigma.\underline{\alpha} \in V(I_0)$ , alors le groupe  $H^{\sigma^{-1}} \cap \text{Gal}_k(\underline{\beta}) = \sigma^{-1} (H \cap \text{Gal}_k(\underline{\alpha})) \sigma$  transitif. Pour l'assertion 2), si  $\underline{\beta} \in V(I)$  alors, d'après le lemme 6.10,  $\text{Gal}_k(\underline{\beta}) = \text{Gal}_k(\underline{\gamma})$  où  $\underline{\gamma} = \sigma.\underline{\alpha}$  avec  $\sigma \in L_0$ .  $\square$

**Proposition 6.13.** *Supposons que  $H \cap \text{Gal}_k(\underline{\alpha})$  soit transitif. Alors les stabilisateurs de l'idéal  $I$  sont les ensembles :*

$$\text{Stab}(I, \sigma.\underline{\alpha}) = \Psi_{\sigma^{-1}L_0}(H^{\sigma^{-1}}) = \sigma^{-1} \Psi(H)$$

*où  $\sigma$  parcourt  $L_0$ . Si, de plus,  $L_0$  est un groupe alors les stabilisateurs de  $I$  sont les  $\text{Stab}(I, \sigma.\underline{\alpha}) = \Psi(H^{\sigma^{-1}})$  où  $\sigma$  parcourt  $L_0$ .*



*Démonstration.* D'après le lemme 6.10, les stabilisateurs de  $I$  sont les stabilisateurs relatifs aux  $\sigma.\underline{\alpha}$ , où  $\sigma$  parcourt  $L_0$ . Soit  $\sigma \in L_0$ , d'après la proposition 6.12,  $H^{\sigma^{-1}} \cap \text{Gal}_k(\sigma.\underline{\alpha})$  est transitif avec  $\sigma.\underline{\alpha} \in V(I_0)$ . Alors, puisque  $H^{\sigma^{-1}} \in \mathcal{A}(\sigma^{-1}L_0)$ , il est possible d'appliquer le théorème 6.9 avec  $H^{\sigma^{-1}}$  à la place de  $H$  et  $\sigma.\underline{\alpha}$  à la place de  $\underline{\alpha}$  pour obtenir :

$$\text{Stab}(I, \sigma.\underline{\alpha}) = \Psi_{\sigma^{-1}L_0}(H^{\sigma^{-1}})$$

et par ailleurs :  $\text{Stab}(I, \sigma.\underline{\alpha}) = \sigma^{-1}\text{Stab}(I, \underline{\alpha}) = \sigma^{-1}\Psi(H)$ . Si  $L_0$  est un groupe, alors  $\Psi_{\sigma^{-1}L_0} = \Psi$ .  $\square$

**Définition 6.14.** Un groupe  $G$  est dit  $L_0$ -conjugué à  $H$  s'il existe  $\sigma$  dans  $L_0$  tel que  $H = G^\sigma$ .

**Proposition 6.15.** Un groupe  $G$  est  $L_0$ -conjugué à  $H$  si et seulement si il existe  $i \in [1, s]$  tel que  $H = G^{\tau_i}$ . De plus, le cardinal de l'ensemble des groupes  $L_0$ -conjugués au groupe  $H$  est majoré par  $s$ .

*Démonstration.* Si  $G$  et  $H$  sont  $L_0$ -conjugués, il existe  $\tau \in L_0$  tel que  $H = G^\tau$ . L'égalité  $L_0 = H_{\{1\}}\tau_1 + H_{\{1\}}\tau_2 + \cdots + H_{\{1\}}\tau_s$  impose à  $\tau$  d'appartenir à l'un des ensembles  $H_{\{1\}}\tau_i$ , pour un entier  $i \in [1, s]$ , et donc de s'écrire  $\tau = h\tau_i$ , où  $h$  désigne une permutation de  $H$ . Le résultat se déduit alors des égalités successives :  $G = \tau_i^{-1}h^{-1}Hh\tau_i = \tau_i^{-1}H\tau_i$ . La réciproque est évidente. La seconde assertion est une conséquence directe de la première.  $\square$

**Définition 6.16.** L'idéal de départ  $I$  (resp. l'idéal  $I_0$ ) de  $f$  est dit *associé* à l'ensemble des groupes  $L_0$ -conjugués à un groupe  $G$  s'il existe  $\underline{\beta} \in V(I_0)$  tel que  $G \cap \text{Gal}_k(\underline{\beta})$  soit transitif avec  $G \in \mathcal{A}(\text{Stab}(I_0, \underline{\beta}))$ .

*Remarque 6.17.* Si  $L_0$  est un groupe la propriété d'être  $L_0$ -conjugué à un groupe est la conjugaison classique. Dans ce cas l'ensemble des groupes  $L_0$ -conjugués à un groupe  $G$  est une classe d'équivalence et son cardinal est divisible par  $s$  (voir 6.15).

*Exemple 6.18.* Poursuivons notre exemple 5.3 avec le polynôme  $f = x^8 - x^6 - x^4 + x^2 + 1$  de groupe de Galois  $8T_{29}^+$ . Il a été construit un idéal de première rupture  $I_0$  de stabilisateur  $L_0 = S_{1^2, 2, 4}$  dont nous déduisons l'idéal de départ  $I_{29}$  engendré par l'ensemble triangulaire suivant :

$$\{f(x_1), x_2 + x_1\} \cup T_1(x_1) \cup T_2(x_1).$$

La variété  $V(I_{29})$  est de cardinal  $384 = 6 \cdot \text{Card}(8T_{29})$ . (Donc  $I$  contient 6 idéaux des relations.) Comme  $L_0$  est un groupe, l'ensemble  $\mathcal{A}(L_0)$  est composé des groupes transitifs  $H$  tels que  $H_{\{1\}} \subset L_0$ . Posons  $C(L_0) = \{H \in \mathcal{A}(L_0) \mid \Delta(H) = 1, 2, 4\}$ , c'est-à-dire les groupes pouvant être le groupe de Galois de  $f$ . En utilisant la table de première rupture en degré 8, nous constatons que dans  $C(L_0)$  deux groupes  $S_n$ -conjugués sont toujours  $L_0$ -conjugués. De plus, le groupe de Galois

sur  $k$  de  $f$  est un sous-groupe du groupe  $8T_{35}$  de cardinal 128. Prenons  $H = G_{35} = \langle (7, 8), (1, 3)(2, 4), (1, 5, 3, 8)(2, 6, 4, 7) \rangle$ , un des 3 conjugués de  $8T_{35}$  dans  $C(L_0)$ . Il existe un conjugué  $G$  du groupe de Galois de  $f$  inclus dans  $G_{35}$  et donc aussi dans  $C(L_0)$ . Choisissons  $\underline{\alpha}$  tel que  $G = \text{Gal}_k(\underline{\alpha})$ . On a nécessairement  $\underline{\alpha} \in V(I)$  puisque  $I$  est associé à la classe de  $L_0$ -conjugaison de  $G$ , la seule dans  $C(L_0)$  pour les groupes  $S_n$ -conjugués à  $G$ . L'idéal  $I$  est donc associé à la classe de  $L_0$ -conjugaison de  $G_{35}$  et d'après le théorème 6.9,  $\text{Stab}(I, \underline{\alpha}) = \Psi(H) = H\tau_1 + H\tau_2 + H\tau_3$  avec  $\tau_1 = id$ ,  $\tau_2 = (6, 7, 8)$  et  $\tau_3 = (6, 7)$ . Calculons maintenant ce même stabilisateur avec le lemme 6.4. Le discriminant de  $f$  étant un carré dans  $k$ , son groupe de Galois est pair, c'est donc  $8T_{19}^+$  ou  $8T_{29}^+$ . Prenons  $G_{19} = t8T_{19}t^{-1}$  avec  $t = (2, 3)(4, 8, 7, 5)$  un conjugué de  $8T_{19}$  inclus dans  $G_{35}$  et  $\underline{\alpha} \in V(I_0)$  tel que  $G_{19} \subset \text{Gal}_k(\underline{\alpha}) \subset G_{35}$  (c'est possible car le groupe de Galois est ou bien  $8T_{29}$  ou bien son sous-groupe  $8T_{19}$ ). Soit  $\{\sigma_1, \dots, \sigma_8\}$  une transversale à gauche de  $G_{19}_{\{1\}}$  dans  $L_0$ , alors  $\text{Stab}(I, \underline{\alpha}) = \sigma_1 L_0 + \dots + \sigma_8 L_0$ . Le calcul montre que nous trouvons bien le même résultat avec les deux formules.

Dans l'exemple 6.18, avec  $L_0 = S_{1,2,4}$ , il n'y a qu'une classe de  $L_0$ -conjugaison pour  $G_{35}$  (et donc aussi ses sous-groupes) dans  $\mathcal{A}(L_0)$ . Ceci provient du fait que les entiers 1,2,4 sont distincts et relève d'un résultat général que nous énonçons dans la proposition 6.22 du paragraphe suivant.

### 6.2.3. Application à $I_0$ un idéal de première rupture.

Nous supposons désormais que  $I_0$  est un idéal de première rupture avec  $\Delta(f) = e$ . Nous avons donc  $\text{Stab}(I_0) = L_0 = S_{1,e}$  qui est un groupe. Considérons l'ensemble :

$$C(L_0) = \{G \in \mathcal{A}(L_0) \mid \Delta(G) = e\}$$

que nous appelons l'ensemble des groupes compatibles avec  $L_0$ . Prenons  $T$  un sous-groupe transitif de  $S_n$  vérifiant  $\Delta(T) = e$  et définissons l'ensemble

$$C(L_0, T) = \{G \in C(L_0) \mid G \text{ est conjugué à } T\}.$$

En particulier nous avons le lemme suivant

**Lemme 6.19.** *Pour tout  $\underline{\alpha} \in V(I)$  nous avons :*

$$\text{Gal}_k(\underline{\alpha}) \in C(L_0).$$

*Exemple 6.20.* Pour  $L_0 = S_{1^4,4}$ ,  $\text{Card}(C(L_0, 8T_{17})) = 18$  et  $\text{Card}(C(L_0, 8T_{18}^+)) = 6$ . Il n'y a qu'une classe de  $L_0$ -conjugaison dans  $C(L_0, 8T_{18}^+)$ , donc les stabilisateurs de  $I$  sont calculables avec le théorème 6.9 et la proposition 6.13 si  $\text{Gal}_k(f) = 8T_{18}$ . Pour  $8T_{17}$ , il y a plusieurs classes de  $L_0$ -conjugaison. Nous devons savoir déterminer laquelle comporte un groupe  $H$  tel que  $H \cap \text{Gal}_k(\underline{\alpha})$  soit transitif.

*Exemple 6.21.* Pour  $L_0 = S_{1^2,2,4}$ , l'ensemble des groupes compatibles avec  $L_0$  sont des conjugués des groupes  $8T_{15}$ ,  $8T_{19}^+$ ,  $8T_{26}$ ,  $8T_{28}$ ,  $8T_{29}^+$ ,  $8T_{30}$  et  $8T_{35}$ . Pour chaque groupe  $G \in C(L_0)$ . Il n'y a qu'une classe de  $L_0$ -conjugaison dans  $C(L_0, G)$ .

**Proposition 6.22.** *Soit  $e$  la suite  $m_1, \dots, m_r$  des degrés de première rupture du polynôme  $f$  (i.e.  $\Delta(f) = e$  et  $L_0 = S_{1,e}$ ). Soit  $N$ , le nombre de permutations de  $S_r$  laissant  $e$  invariant. Nous avons :*

- (1)  $N$  idéaux de première rupture distincts,
- (2) et au plus  $N$  classes de  $L_0$ -conjugaison dans  $C(L_0, H)$  pour tout groupe  $H$  de  $C(L_0)$ .

*En particulier, si les parts de  $e$  sont distinctes (i.e. les cardinaux des  $H_{\{1\}}$ -orbites de  $\{2, \dots, n\}$  sont distincts) alors  $C(L_0, H)$  n'a qu'une classe de  $L_0$ -conjugaison pour tout groupe  $H$  de  $C(L_0)$ .*

*Démonstration.* L'assertion 1 est vraie car le nombre d'idéaux de première rupture est le nombre de façons d'ordonner les facteurs de première rupture de telle sorte que la croissance de leur degré soit respectée.

Pour l'assertion 2. Les  $H_{\{1\}}$ -orbites de  $\{2, \dots, n\}$  sont les  $L_0$ -orbites de  $\{2, \dots, n\}$ . Ainsi, une permutation  $\tau$  telle que  $H^\tau \in C(L_0)$  conserve ces orbites. Elle ne peut qu'échanger des orbites de même cardinal ou, si  $\tau \in L_0$ , les laisser inchangées. Il ne peut donc exister plus de  $N$  classes de  $L_0$ -conjugaison.  $\square$

Cette proposition montre pourquoi dans les exemples 6.18 et 6.21 il n'y a qu'une classe de  $L_0$ -conjugaison. Dans l'exemple 6.20, pour  $8T_{18}$ , il n'y a qu'une classe de  $L_0$ -conjugaison et plusieurs idéaux de départ distincts qui lui sont associés.

Lorsque l'on sait associer un idéal de départ  $I$ , ou ce qui revient au même l'idéal de première rupture dont il émane (voir lemme 6.10), à une classe de  $L_0$ -conjugaison  $C$  alors ses stabilisateurs  $I$  sont les  $\Psi(G)$ , où  $G$  est dans  $C$  (voir Proposition 6.13).

Nous savons que pour tout  $\underline{\alpha} \in V(I)$ ,  $\text{Gal}_k(\underline{\alpha}) \in C(L_0)$ . Le lemme suivant s'intéresse à la réciproque :

**Lemme 6.23.** *Soit  $G$  un conjugué de  $\text{Gal}_k(f)$  contenu dans  $C(L_0)$ . Alors il existe un élément  $\underline{\beta}$  dans une variété associée à un idéal de première rupture de  $f$  tel que  $G = \text{Gal}_k(\underline{\beta})$ .*

*Démonstration.* Soit  $e$  la suite  $m_1, m_2, \dots, m_r$  des facteurs de première rupture du polynôme  $f$ . Par hypothèse, il existe  $\underline{\beta}$ , un  $n$ -uplet des racines de  $f$  tel que  $G = \text{Gal}_k(\underline{\beta})$  et  $G_{\{1\}} \subset C(L_0)$ . Comme  $G$  est transitif, on peut décider que  $\beta_1 = \alpha_1$  et donc  $G_{\{1\}} = \text{Gal}_{k(\alpha_1)}(\underline{\beta}) \subset L_0$ . Montrons que  $\underline{\beta}$  est dans la variété d'un idéal de première rupture.

Comme  $\text{Gal}_{k(\alpha_1)}(\underline{\beta}) \subset L_0 = S_{1,e}$ , sur  $k(\alpha_1)$ , le polynôme  $f$  se factorise en  $r + 1$  polynômes  $(x - \alpha_1)g_1 \cdots g_r$  de degrés respectifs  $1, m_1, \dots, m_r$  avec  $\beta_2, \dots, \beta_{m_1+1}$  racines de  $g_1$ ,  $\beta_{m_1+2}, \dots, \beta_{m_1+m_2+1}$  racines de  $g_2, \dots$ . Comme les degrés des facteurs  $g_i$  sont ceux de première rupture du polynôme  $f$ , ce sont les facteurs de première rupture de  $f$ . Donc l'idéal de Galois  $I_{\underline{\beta}}^{L_0}$  dans  $k(\alpha_1)[x_1, x_2, \dots, x_n]$  est un idéal de première rupture de  $f$  avec  $\underline{\beta} \in V(I_{\underline{\beta}}^{L_0})$ .  $\square$

Soit  $T$  un sous-groupe transitif de  $S_n$  tel que  $\Delta(T) = e$ . Nous cherchons une condition suffisante pour qu'à chaque classe de  $L_0$ -conjugaison dans  $C(L_0, T)$  corresponde un idéal de première rupture à laquelle il est associé.

**Lemme 6.24.** *Soient  $G, H \in C(L_0)$ , tels que  $H^\sigma \cap G^\rho$  soit transitif avec  $\sigma, \rho \in S_n$ . Alors il existe  $\tau \in S_n$  tel que  $G^\tau \in C(L_0)$  et  $H \cap G^\tau$  transitif.*

*Démonstration.* Soit  $M$  un sous-groupe de  $S_n$  tel que  $M^\sigma = H^\sigma \cap G^\rho$ . Alors  $M \subset H$  et  $M_{\{1\}} \subset L_0$ . Il existe  $\tau \in S_n$  tel que  $M \subset G^\tau$  et donc, en posant  $L = M^{\tau^{-1}}$ , il vient  $L_{\{1\}} \subset G_{\{1\}} \subset L_0$ . Nous avons  $M = H \cap G^\tau$  transitif. Montrons que  $G^\tau \in C(L_0)$ . (Si  $\tau \in L_0$ , c'est évident). Comme  $L_{\{1\}}$  et  $M_{\{1\}} = L_{\{1\}}^\tau$  sont dans  $L_0$ , les  $L_0$ -orbites de  $\{2, \dots, n\}$  sont conservées par  $\tau$ . Comme ces  $L_0$ -orbites sont identiques aux  $G_{\{1\}}$ -orbites, nous avons  $G_{\{1\}}^\tau \in L_0$  et donc  $G^\tau \in C(L_0)$ .  $\square$

**Proposition 6.25.** *Soit  $H \in C(L_0)$ . S'il existe un conjugué  $T$  de  $H$  vérifiant  $T \cap \text{Gal}_k(f)$  transitif alors il existe un idéal de première rupture de  $f$  associé à la classe de  $L_0$ -conjugaison de  $H$ .*

*Démonstration.* D'après le lemme 6.24, il existe  $G$  un conjugué de  $\text{Gal}_k(f)$  dans  $C(L_0)$  tel que  $G \cap H$  soit transitif car il existe des conjugués du groupe de Galois de  $f$  dans  $C(L_0)$ . Et finalement, comme d'après le lemme 6.23, il existe un  $\underline{\beta}$  dans la variété d'un idéal de première rupture de  $f$  tel que  $G = \text{Gal}_k(\underline{\beta})$ , cet idéal est associé à la classe de  $L_0$ -conjugaison de  $H$ .  $\square$

*Exemple 6.26.* Soit  $I_0$  un idéal de première rupture du polynôme  $f$  tel que  $\Delta(f) = 1^3, 2^2$ . Nous avons  $\text{Stab}(I_0) = L_0 = S_{1^4, 2^2}$ . Supposons que le groupe de Galois de  $f$  sur  $k$  soit impair. Dans ce cas il s'agit de  $8T_7$  et l'ensemble  $C(L_0, 8T_7)$  est constitué des 6 conjugués de  $8T_7$  suivants :

$$\begin{aligned} G_1 &= \langle (1, 5, 3, 7, 2, 6, 4, 8), \sigma_1 = (1, 2)(3, 4) \rangle, & G_2 &= \langle (1, 6, 3, 7, 2, 5, 4, 8), \sigma_1 \rangle, \\ G_3 &= \langle (1, 5, 2, 7, 3, 6, 4, 8), \sigma_2 = (1, 3)(2, 4) \rangle, & G_4 &= \langle (1, 5, 2, 8, 3, 6, 4, 7), \sigma_2 \rangle, \\ G_5 &= \langle (1, 5, 2, 7, 4, 6, 3, 8), \sigma_3 = (1, 4)(2, 3) \rangle, & G_6 &= \langle (1, 5, 2, 8, 4, 6, 3, 7), \sigma_3 \rangle. \end{aligned}$$

Soit  $\underline{\alpha} \in V(I)$ ,  $G = \text{Gal}_k(\underline{\alpha})$  et  $\tau \in L_0$  tel que  $L_0 = G_{\{1\}} + G_{\{1\}}\tau$  (car  $\text{Card}(L_0) = 2 \cdot \text{Card}(G_{\{1\}})$ ). Alors, d'après le théorème 6.9,  $\text{Stab}(I, \underline{\alpha}) =$

$G + G\tau$  et donc (voir Paragraphe 7) :

$$(6.4) \quad I = I_{\underline{\alpha}}^G \cap I_{\tau, \underline{\alpha}}^{\tau^{-1}G\tau} = I_{\underline{\alpha}} \cap I_{\tau, \underline{\alpha}} \quad .$$

En notant  $N_i$  le stabilisateur de 1 sous l'action de  $G_i$  et  $\tau$  la permutation (5, 6) de  $L_0$ , nous avons :

$$L_0 = N_1 + N_1\tau = N_3 + N_3.\tau = N_5 + N_5\tau$$

avec  $G_2 = \tau^{-1}G_1\tau$ ,  $G_4 = \tau^{-1}G_3\tau$  et  $G_6 = \tau^{-1}G_5\tau$ . Il y a 3 classes de  $L_0$ -conjugaison  $C_1 = \{G_1, G_2\}$ ,  $C_2 = \{G_3, G_4\}$  et  $C_3 = \{G_5, G_6\}$  auxquelles sont associés les  $2.3! = 12$  idéaux de rupture distincts. Dans le paragraphe 6.3, nous montrerons comment il est possible d'associer un idéal de départ à une classe de  $L_0$ -conjugaison dans  $C(L_0, 8T_7)$  pour pouvoir calculer un stabilisateur de  $I$ . C'est ce que nous appellerons un critère d'association.

### 6.3. Critère d'association d'un idéal de première rupture.

Supposons comme dans le paragraphe précédent que  $I_0$  soit un idéal de première rupture de stabilisateur  $L_0 = S_{1,e}$  (i.e.  $\Delta_n(f) = e$ ).

Le problème est de pouvoir calculer un stabilisateur de  $I$ . S'il n'existe qu'une seule classe de  $L_0$ -conjugaison pour un groupe  $T$  tel que  $\Delta(T) = e$  et que  $T \cap Gal_k(f)$  soit transitif, il suffit d'appliquer les résultats du paragraphe 6.2. Si  $I$  n'a qu'un stabilisateur, c'est-à-dire son groupe de décomposition, alors il suffit de le calculer (voir Exemple 6.27). Pour les autres cas, nous établissons la proposition 6.28 utilisée pour trouver un critère, dit *critère d'association*, associant un idéal de départ  $I$  à sa classe de  $L_0$ -conjugaison. Si un tel critère est trouvé alors il devient possible de calculer un stabilisateur de  $I$ .

*Exemple 6.27.* Soit  $f$  un polynôme irréductible de degré 8 tel que  $\Delta_8(f) = (1, 2^3)$ . Nous construisons un idéal de départ  $I$  à partir d'un de ses 6 idéaux de première rupture.

Nous avons  $\text{Card}(V(I)) = 64 = \text{Card}(8T_{27})$  avec  $\Delta_8(f) = \Delta_8(8T_{27})$  (voir Table 1). Il y a 3 classes de  $L_0$ -conjugaison dans  $C(L, 8T_{27})$ . Le groupe de décomposition de  $I$  est un groupe de  $C(L_0, 8T_{27})$  si et seulement si, pour tout  $\underline{\alpha} \in V(I)$ , le groupe de Galois  $Gal_k(\underline{\alpha})$  est un sous-groupe d'un groupe de  $C(L_0, 8T_{27})$ . Les sous-groupes de  $8T_{27}$  dans  $C(L_0)$  sont des conjugués à  $8T_{20}^+$  ou  $8T_{16}$ . Ainsi, si  $Gr(I)$  est un conjugué de  $8T_{27}$ , l'idéal  $I$  est associé à la classe de  $L_0$ -conjugaison de  $Gr(I)$  et à celle de ses sous-groupes conjugués à  $8T_{20}^+$  ou  $8T_{16}$ . (Voir Paragraphe 10.1.4 pour plus de détails.)

**Proposition 6.28.** *Soit  $A$  une classe de  $L_0$ -conjugaison dans  $C(L_0)$ . Posons  $E(A, I) = \bigcap_{G \in A} E(G, I)$  avec*

$$E(G, I) = \{\sigma.R(x_1, \dots, x_n) \mid R \in I, \sigma \in G\} \quad .$$

*Si  $A$  est associé à  $I$ , de telle sorte qu'il existe  $\underline{\alpha} \in V(I)$  et  $G_0 \in A$  tels que  $G_0 \subset Gal_k(\underline{\alpha})$  ou bien  $Gal_k(\underline{\alpha}) \subset G_0$ , alors  $E(A, I) = I$ .*

*Démonstration.* Sous les hypothèses de la proposition 6.28, pour tout  $G$  dans  $A$ , il existe  $\underline{\alpha}_G \in V(I)$  tel que  $G \subset G_{\underline{\alpha}_G}$  ou bien  $G_{\underline{\alpha}_G} \subset G$  puisque  $V(I) = L_0 \cdot \underline{\alpha}$ . Nous avons alors (voir Paragraphe 7) :

$$I = \bigcap_{G \in A} I_{\underline{\alpha}_G}^G \quad .$$

Soit  $P \in E(A, I)$  et  $R \in I$  tel que  $P = \sigma.R$  avec  $\sigma \in G \in A$ . Nous avons  $R \in I_{\underline{\alpha}_G}^G$  et donc  $P = \sigma.R \in I_{\underline{\alpha}_G}^G$  puisque  $G$  est ou bien le groupe de décomposition de  $I_{\underline{\alpha}_G}^G$  (si  $G_{\underline{\alpha}_G} \subset G$ ) ou bien un de ses sous-groupes (si  $G \subset G_{\underline{\alpha}_G}$  et alors il vient  $I_{\underline{\alpha}_G}^G = I_{\underline{\alpha}_G}$ ). Comme ceci est vrai pour tout  $G$  dans  $A$ , nous avons bien  $P \in I$ .  $\square$

### Utilisation de la proposition 6.28

Supposons qu'il existe  $T$  un sous-groupe transitif de  $S_n$  tel que  $\Delta_n(T) = \Delta_n(f) = e$  et que  $\text{Gal}_k(f)$  soit un sous-groupe de  $T$  (ceci peut être testé sur  $C(L_0)$ ). Supposons, pour simplifier, que  $C(L_0, T)$  se décompose en deux classes de  $L_0$ -conjugaison  $A$  et  $B$ . Nous cherchons deux polynômes  $P_A$  dans  $E(A, I)$  et  $P_B$  dans  $E(B, I)$  qui ne pourraient appartenir simultanément à  $I$ . Le critère d'association de l'idéal de départ  $I$  est alors :

si  $P_A \in I$  alors  $I$  est associé à la classe  $A$   
si  $P_B \in I$  alors  $I$  est associé à la classe  $B$

*Exemple 6.29.* Reprenons l'exemple 6.26 avec  $\text{Gal}_k(f) = 8T_7$ . L'idéal de départ  $I$  est engendré par un ensemble triangulaire  $T$  de la forme :

$$T = \{f(x_1), x_2 + g_2(x_1), x_3 + g_3(x_1), x_4 + g_4(x_1), \\ f_5(x_5, x_1), x_6 + g_6(x_5, x_1), f_7(x_7, x_1), f_8(x_6, x_1)\}.$$

où les polynômes  $g_2, g_3, g_4$  sont distincts (car les racines de  $f$  le sont) et de degrés respectifs en  $x_1$  strictement inférieurs à 8, celui de  $f$ . Les trois classes de  $L_0$ -conjugaison  $C_1, C_2$  et  $C_3$  de  $C(L_0, 8T_7)$ .

Avec les permutations  $\sigma_1 = (1, 5, 3, 7, 2, 6, 4, 8) \in G_1$  et  $\sigma_2 = (1, 6, 2, 5, 3, 7, 4, 8)(1, 2)(3, 4) \in G_2$  et le polynôme  $R = x_2 + g_2(x_1)$  de  $T$ , nous formons le polynôme  $P_1 = \sigma_1.R = x_6 + g_2(x_5)$  qui appartient donc à  $E(C_1, I)$ . De même, nous avons  $P_2 = x_6 + g_3(x_5) \in E(C_2, I)$  et  $P_3 = x_6 + g_4(x_5) \in E(C_3, I)$ . Nous ne pouvons avoir  $P_1$  et  $P_2$  appartenant simultanément à  $I$  car, si c'était le cas, nous aurions  $P_1 - P_2 = g_2(x_5) - g_3(x_5) \in I$ , ce qui est impossible puisque  $g_2 - g_3$  est non nul de degré strictement inférieur à 8 et ne peut donc avoir comme racine une racine de  $f$  irréductible de degré 8. Il en va de même, pour  $(P_1, P_3)$  et pour  $(P_2, P_3)$ . Le critère d'association est donc :

- i) si  $x_6 + g_2(x_5) \in I$  alors  $I$  est associé à la classe  $C_1$  ;
- ii) si  $x_6 + g_3(x_5) \in I$  alors  $I$  est associé à la classe  $C_2$  ;
- iii) si  $x_6 + g_4(x_5) \in I$  alors  $I$  est associé à la classe  $C_3$ .

7. DÉCOMPOSITION DE L'IDÉAL DE DÉPART  $I$ 

Soit  $I$  un idéal de départ construit à partir d'un idéal  $I_0$  de  $k(\alpha_1)[x_1, \dots, x_n]$ . Soit  $\underline{\alpha} \in V(I_0)$  et  $H \in \mathcal{A}(\text{Stab}(I_0, \underline{\alpha}))$  tel que  $H \cap \text{Gal}_k(\underline{\alpha})$  soit transitif. L'idéal  $I$  est donc associé à la classe de  $L_0$ -conjugaison du groupe  $H$  et d'après le théorème 6.9 :

$$\text{Stab}(I, \underline{\alpha}) = \Psi(H) = H\tau_1 + \dots + H\tau_s \quad \text{avec } \tau_1 = id$$

et  $\tau_i \in \text{Stab}(I_0, \underline{\alpha})$ . Nous avons alors la décomposition suivante :

$$(7.1) \quad I = I_{\underline{\alpha}}^{\text{Stab}(I_0, \underline{\alpha})} = I_{\underline{\alpha}}^{\Psi(H)} = \bigcap_{i=1}^s I_{\underline{\alpha}}^{H\tau_i} = \bigcap_{i=1}^s I_{\tau_i \cdot \underline{\alpha}}^{\tau_i^{-1}H\tau_i}.$$

Pour  $i = 1, \dots, s$ , posons  $H_i = \tau_i^{-1}H\tau_i$  et  $J_i = I_{\tau_i \cdot \underline{\alpha}}^{H_i}$ . Nous savons que  $\text{Gal}_k(\tau_i \cdot \underline{\alpha}) = \tau_i^{-1}\text{Gal}_k(\underline{\alpha})\tau_i$ . Nous traitons ci-dessous deux cas particuliers.

**Cas 1**  $\text{Gal}_k(\underline{\alpha}) \subset H$

Alors comme  $\text{Gal}_k(\tau_i \cdot \underline{\alpha}) \subset H_i$ , nous avons  $H_i = \text{Stab}(J_i)$  (voir Proposition 3.9) et les  $J_i$  sont deux-à-deux distincts.

**Cas 2**  $H \subset \text{Gal}_k(\underline{\alpha})$

Alors  $H_i \subset \text{Gal}_k(\tau_i \cdot \underline{\alpha}) = \text{Stab}(J_i)$  avec  $J_i = I_{\tau_i \cdot \underline{\alpha}}$ . L'égalité 7.1 donne la décomposition en idéaux de relations (premiers) :

$$I = \bigcap_{i=1}^s I_{\tau_i \cdot \underline{\alpha}}.$$

Si  $e$  est l'indice de  $H$  dans  $\text{Gal}_k(\underline{\alpha})$ , alors il existe  $e$  idéaux identiques à  $J_i$  dans cette décomposition. Si  $H = \text{Gal}_k(\underline{\alpha})$  alors les  $J_i$  sont distincts 2 à 2.

*Remarque 7.1.* Quel que soit le groupe  $H_i$  choisit dans la classe de  $L_0$ -conjugaison de  $H$  pour calculer un stabilisateur de  $I$ , la décomposition 7.1 reste inchangée.

*Exemple 7.2.* Poursuivons l'exemple 6.18 avec le polynôme  $f = x^8 - x^6 - x^4 + x^2 + 1$  de groupe de Galois  $8T_{29}^+$ . Choisissons  $H = G_{35}$ . En posant, pour  $i \in \{1, 2, 3\}$ ,  $\underline{\beta}_i = \tau_i \cdot \underline{\alpha}$  et  $H_i = \tau_i^{-1}H\tau_i$ ,  $\Psi(H_i) = \tau_i^{-1}\Psi(H)$  est le stabilisateur de  $I_{29}$  relatif à  $\underline{\beta}_i$  (voir Proposition 6.13) et nous obtenons :

$$I_{29} = I_{\underline{\beta}_i}^{\Psi(H_i)} = I_{\underline{\beta}_1}^{H_1} \cap I_{\underline{\beta}_2}^{H_2} \cap I_{\underline{\beta}_3}^{H_3},$$

avec  $V(I_{\underline{\beta}_i}^{H_i}) = \{\sigma \cdot \underline{\beta}_i \mid \sigma \in H_i\}$  puisque  $H_i$  contient le groupe de Galois  $\text{Gal}_k(\underline{\beta}_i) = \tau_i^{-1}\text{Gal}_k(\underline{\alpha})\tau_i$ . La variété de  $I_{29}$  se décompose en 3 variétés disjointes :

$$V(I_{29}) = \bigcup_{i=1}^3 V(I_{\underline{\beta}_i}^{H_i}).$$

## 8. ADJONCTION DE RELATIONS À L'IDÉAL DE DÉPART

Les résultats de ce paragraphe seront utilisés pour construire sans coût un nouvel idéal de Galois pouvant contenir strictement l'idéal de départ  $I$  construit à partir d'un idéal triangulaire  $I_0$ . Nous chercherons, comme pour  $I$ , à calculer un stabilisateur de ce nouvel idéal. Nous supposons que l'idéal  $I$  est engendré par un ensemble triangulaire séparable  $T = \{f_1, \dots, f_n\}$ .

Nous fixons  $\underline{\alpha} \in V(I_0)$ ,  $L_0 = \text{Stab}(I_0, \underline{\alpha})$ , un groupe  $H \in \mathcal{A}(L_0)$  tel que  $\text{Gal}_k(\underline{\alpha}) \subset H \subset \text{Stab}(I, \underline{\alpha})$  et  $\tau_1 = \text{id}, \dots, \tau_s \in L_0$  tels que

$$\text{Stab}(I, \underline{\alpha}) = \Psi(H) = H\tau_1 + \dots + H\tau_s \quad .$$

**Lemme 8.1.** *Pour tout  $(\sigma, R)$  dans  $H \times I$ ,  $I + \langle \sigma.R \rangle \subset I_{\underline{\alpha}}^H$ .*

*Démonstration.* Puisque  $H \subset L = \text{Stab}(I, \underline{\alpha})$ , nous avons  $I = I_{\underline{\alpha}}^L \subset I_{\underline{\alpha}}^H$ . De plus, d'après la proposition 3.9,  $H = \text{Stab}(I_{\underline{\alpha}}^H)$  car  $H$  contient le groupe de Galois  $\text{Gal}_k(\underline{\alpha})$ . Donc  $H$  est le groupe de décomposition de  $I_{\underline{\alpha}}^H$  et la proposition découle alors de la définition du groupe de décomposition.  $\square$

Supposons qu'il existe  $(\sigma, R) \in H \times I$  tel que  $J = I + \langle \sigma.R \rangle$  contienne strictement  $I$ , notons  $F = \sigma.R$ . D'après la proposition 3.2, comme l'idéal  $J$  contient  $I$ ,  $J$  est un idéal de Galois de  $f$  ssi il est radical. La proposition suivante nous donne des conditions suffisantes pour qu'il en soit ainsi.

**Proposition 8.2.** *Supposons que  $F = x_j^k + g(x_1, \dots, x_{j-1})$  avec  $k > 0$  et que l'ensemble  $S = \{f_1, \dots, f_{j-1}, F, f_{j+1}, \dots, f_n\}$  engendre un idéal  $I'$  contenant  $I$ . Alors  $S$  est triangulaire séparable et  $I' = J$  est un idéal de Galois de  $f$ .*

**Démonstration.** L'ensemble  $S$  est triangulaire et comme nous venons de le voir il suffit de montrer qu'il est séparable pour que  $I'$  soit de Galois.

Comme  $I \subset I'$ , nous avons  $f_j \in \langle f_1, \dots, f_{j-1}, F \rangle$  et il existe  $\lambda_1, \dots, \lambda_j$  des éléments de  $k[x_1, \dots, x_n]$  tels que

$$f_j = \lambda_1 f_1 + \dots + \lambda_{j-1} f_{j-1} + \lambda_j F,$$

avec  $\lambda_j \neq 0$ .

$\forall \underline{\beta} \in V(\langle f_1, \dots, f_{j-1} \rangle)$  on a :

$$\begin{aligned} f_j(\underline{\beta}, x_j) &= (\lambda_1 f_1 + \dots + \lambda_{j-1} f_{j-1})(\underline{\beta}) + (\lambda_j F)(\underline{\beta}, x_j) \\ &= (\lambda_j F)(\underline{\beta}, x_j). \end{aligned}$$

Comme  $f_j(\underline{\beta}, x_j)$  est séparable il en est de même pour  $F(\underline{\beta}, x_j)$ .

Pour finir il suffit de voir que  $\forall i \in \{j+1, \dots, n\}$  :

$$V(\langle f_1, \dots, f_{j-1}, F, f_{j+1}, \dots, f_i \rangle) \subset V(\langle f_1, \dots, f_i \rangle) \quad \square$$



Si  $F$  est un facteur de  $f_j$  dans  $k[x_1, \dots, x_j]$  alors les hypothèses de la proposition 8.2 sont vérifiées. Ceci est illustré dans l'exemple suivant.

*Exemple 8.3.* Poursuivons notre exemple 7.2 avec le polynôme  $f$  de groupe de Galois  $8T_{29}^+$ . En prenant  $\sigma = (1, 5, 3, 8)(2, 6, 4, 7)$  dans  $H = G_{35}$  et  $R = x_4 + x_3$  dans  $I_{29}$ , nous obtenons  $F = \sigma.R = x_6 + x_5$  qui est un facteur dans  $k[x_1, \dots, x_6]$  de  $f_6$ . L'idéal de Galois  $J = I_{29} + \langle \sigma.R \rangle$  est inclus dans  $I_{\underline{\alpha}}^H$  est alors engendré par l'ensemble triangulaire suivant :

$$T_J = \{ f(x_1), x_2 + x_1, x_3^2 - x_1^6 + x_1^4 + x_1^2 - 1, x_4 + x_3, \\ x_5^4 + (x_1^6 - x_1^4)x_5^2 - 1, x_6 + x_5, x_7^2 + x_5^2 + x_1^6 - x_1^4, x_8 + x_7 \} .$$

Comme  $\text{Card}(G_{35}) = 128 = \prod_{i=1}^n \text{deg}_{x_i}(I)$ , d'après 3.14, le groupe  $G_{35}$  est le stabilisateur de  $J$ . Soit  $G_{29}$  un conjugué de  $8T_{29}$  inclus dans  $G_{35}$ . Nous avons la décomposition  $G_{35} = G_{29} + G_{29}\tau$ , avec  $\tau = (3, 4)$  et  $G_{29} = \tau^{-1}G_{29}\tau$ , qui induit que pour tout  $\underline{\alpha} \in V(J)$  :

$$J = I_{\underline{\alpha}}^{G_{35}} = I_{\underline{\alpha}}^{G_{29}} \cap I_{\tau.\underline{\alpha}}^{G_{29}} .$$

Nous obtiendrions le même résultat si le groupe de Galois était  $8T_{19}$ . Comme ici le groupe de Galois est  $8T_{29}$ , nous avons de plus :

$$J = I_{\underline{\alpha}} \cap I_{\tau.\underline{\alpha}} .$$

La liste des degrés initiaux de  $I_{\underline{\alpha}}^{G_{29}}$  est  $\mathcal{L}(G_{29}) = (8, 1, 2, 1, 4, 1, 1, 1)$ . Donc pour trouver un système triangulaire engendrant cet idéal, il reste à calculer une relation linéaire en  $x_7$ , les autres relations étant prises dans l'ensemble  $T_J$ . Le calcul d'une  $G_{29}$ -résolvante  $G_{35}$ -relative de degré 2 suivi d'un calcul rapide d'ensemble triangulaire permet de trouver la relation  $x_7 + x_5^3x_3x_1 + x_5x_3x_1^7 - x_5x_3x_1^5$  que nous cherchons (voir l'algorithme `GaloisIdéal` de [17]). Ceci termine notre exemple.

Le résultat suivant nous permet d'éviter de tester si la nouvelle relation est un facteur d'une des relations de  $I$ .

**Corollaire 8.4.** *Si  $F$  est de la forme  $x_j^k + g(x_1, \dots, x_{j-1})$  avec*

$$k = \text{deg}_{x_j}(I_{\underline{\alpha}}^H)$$

*et que l'idéal  $I$  vérifie*

$$\text{deg}_{x_i}(I) = \text{deg}_{x_i}(I_{\underline{\alpha}}^H) \quad i \in \{1, \dots, j-1\}.$$

*Alors  $J$  est un idéal de Galois de  $f$  et est engendré par l'ensemble  $S = \{f_1, \dots, f_{j-1}, F, f_{j+1}, \dots, f_n\}$ .*

*Démonstration.* D'après la proposition 8.2 il suffit de montrer que  $f_j \in \langle S \rangle$ .

D'après le lemme 8.1, nous avons la suite d'inclusions d'idéaux de  $k[x_1, \dots, x_j]$  :

$$\langle f_1, \dots, f_{j-1}, F \rangle \subset \langle f_1, \dots, f_{j-1}, F, f_j \rangle \subset I_{\underline{\alpha}}^H \cap k[x_1, \dots, x_j].$$

Les hypothèses faites sur les degrés des monômes initiaux de ces idéaux transforment ces inclusions en égalités et le résultat suit.  $\square$

Supposons désormais que l'idéal  $J$  est de Galois. Nous devons connaître un stabilisateur de  $J$ . Si, comme dans l'exemple 8.3,  $\text{card}(V(J)) = \text{card}(H)$  alors  $J = I_{\underline{\alpha}}^H$  avec  $H = \text{Stab}(J)$ . Dans le cas contraire, nous pouvons utiliser la proposition suivante :

**Proposition 8.5.** *Soit  $\mathcal{I}$  l'ensemble d'entiers défini par :*

$$\mathcal{I} := \{i \in \{1, \dots, s\} \mid \exists(\tau, P) \in \tau_i^{-1} H \tau_i \times I, J = I + \langle \tau.P \rangle\}.$$

*Si  $\text{Card}(V(J)) = \text{Card}(\mathcal{I}).\text{Card}(H)$  alors le stabilisateur de  $J$  relatif à  $\underline{\alpha}$  est  $\sum_{i \in \mathcal{I}} H \tau_i$ .*

*Démonstration.* Posons  $L = \sum_{i \in \mathcal{I}} H \tau_i$ . Tout d'abord, comme  $\text{Gal}_k(\underline{\alpha}) \subset H$ , alors  $L = \text{Gal}_k(\underline{\alpha})L$ . Donc  $L = \text{Stab}(I_{\underline{\alpha}}^L, \underline{\alpha})$  et en utilisant l'hypothèse, il vient :

$$\text{Card}(L) = \text{Card}(V(I_{\underline{\alpha}}^L)) = \text{Card}(\mathcal{I}).\text{Card}(H) = \text{Card}(V(J)).$$

Comme les idéaux sont radicaux, nous avons juste à montrer que  $I_{\underline{\alpha}}^L \supset J$ . Soit  $i \in \{1, \dots, n\}$ , de l'égalité  $\text{Gal}_k(\tau_i \underline{\alpha}) = \text{Gal}_k(\underline{\alpha})^{\tau_i^{-1}} \subset H^{\tau_i^{-1}}$  et de l'inclusion  $H \tau_i \subset \text{Stab}(I, \underline{\alpha})$ , il vient  $H^{\tau_i^{-1}} \subset \tau_i^{-1} \text{Stab}(I, \underline{\alpha}) = \text{Stab}(I, \tau_i \underline{\alpha})$ . Nous pouvons alors appliquer le lemme 8.1 avec  $\tau_i \underline{\alpha}$  et  $H^{\tau_i^{-1}}$ . Donc, pour tout  $i \in \mathcal{I}$ ,  $J \subset I_{\tau_i \underline{\alpha}}^{H^{\tau_i^{-1}}} = I_{\underline{\alpha}}^{H \tau_i}$ , d'où  $J \subset I_{\underline{\alpha}}^L$ .  $\square$

## 9. CONSTRUCTION D'UN IDÉAL DES RELATIONS

Pour calculer un idéal des relations du polynôme  $f$ , nous utiliserons les résultats des paragraphes 6 et 8 afin déterminer un ensemble triangulaire générateur et un stabilisateur d'un idéal de Galois  $J$  de  $f$  qui contiendra l'idéal des relations symétriques du polynôme. Nous montrons dans le paragraphe 9.1 comment utiliser les résultats du paragraphe 8. Si  $J$  n'est pas l'idéal des relations, il est ensuite possible d'utiliser l'algorithme `GaloisIdéal` décrit dans 9.2 pour calculer un idéal des relations de cet idéal avec  $I_1 = J$ . Nous décrirons dans le paragraphe 9.3 la méthodologie à suivre pour construire un algorithme de calcul d'un idéal des relations en degré fixé.

C'est cette méthodologie qui est illustrée à travers l'étude du degré 8 (voir Paragraphe 10).

### 9.1. Utilisation des degrés initiaux d'un idéal de Galois.

Si  $J$  est un idéal de Galois de stabilisateur un groupe  $G$ , la liste  $\mathcal{L}(J)$  des degrés initiaux de  $J$  sont calculables avec la fonction `InitDeg(G, n)` du paragraphe 3. Notons  $\mathcal{L}(G)$ , la liste calculée par `InitDeg(G, n)`.

Supposons que pour un idéal de Galois  $I$ , nous sachions calculer un ensemble triangulaire  $T$  l'engendrant et qu'il existe  $\underline{\alpha} \in V(I)$  tel que  $Gal_k(\underline{\alpha}) \subset G \subset Stab(I, \underline{\alpha})$ . Alors nous connaissons avec  $\mathcal{L}(G)$  les degrés des polynômes de tout ensemble triangulaire  $T_J$  engendrant l'idéal  $J = I_{\underline{\alpha}}^G$  de stabilisateur  $G$  et en particulier les polynômes de  $T$  qui appartiennent à  $T_G$ . C'est en comparant  $\mathcal{L}(G)$  et  $\mathcal{L}(I)$  que nous recherchons de nouvelles relations comme expliqué au paragraphe 8 afin de calculer un ensemble triangulaire engendrant un idéal de Galois  $J$  contenant l'idéal  $I$ .

*Exemple 9.1.* Soit  $I$  un idéal de départ calculé à partir de l'idéal de première rupture d'un polynôme  $f$  de degré 8 tel que  $\Delta(f) = 1^3, 2^2$ . Alors  $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$ . Notons  $f_7(x_1, x_7)$  le 7-ième polynôme de  $T_I$ . D'après la table 1, nous calculons l'ensemble  $C(L_0)$  des groupes  $L_0$ -compatibles avec  $L_0 = S_{1^4, 2^2}$ . Pour chacun des groupes  $G$  de  $C(L_0)$ , nous avons  $\mathcal{L}(G) = (8, 1^3, 2, 1^3)$ . Ainsi, si  $G$  est le groupe de Galois, pour calculer  $T_G$  (et donc ici un idéal des relations), il suffit de chercher une relation  $r_7(x_1, x_5, x_7)$  linéaire en  $x_7$ . L'ensemble  $T_G$  est alors l'ensemble  $T_I$  dans lequel  $f_7$  est remplacé par  $r_7$ .

## 9.2. L'algorithme GaloisIdéal.

### 9.2.1. L'algorithme.

Dans [17], l'algorithme `GaloisIdéal(G, T, Liste)` a pour paramètres :

- $T$  un ensemble triangulaire engendrant un idéal de Galois  $I$ ,
- le stabilisateur  $G$  de  $I$  qui est supposé être un groupe,
- Une liste `Liste` de groupes candidats à être le groupe de Galois à conjugaison près dans  $G$ .

Cet algorithme calcule un idéal des relations  $I_{\underline{\alpha}}$  contenant  $I$  (avec  $\underline{\alpha} \in V(I)$ ) et le groupe de Galois  $Gal_k(\underline{\alpha})$  qui est le groupe de décomposition et le stabilisateur de  $I_{\underline{\alpha}}$ .

Avec les résultats de [18], cet algorithme est généralisable au cas où les stabilisateurs de  $I$  ne sont pas des groupes.

La méthode utilisée est celle évoquée dans l'introduction. Il s'agit de construire récursivement une chaîne ascendante d'idéaux de Galois

$$I = I_1 \subset I_2 \subset \cdots \subset I_r = I_{\underline{\alpha}}$$

où pour calculer  $I_{i+1}$  à partir de  $I_i$  (avec  $i \in \{1, \dots, r-1\}$ ), il est nécessaire de connaître un ensemble triangulaire engendrant  $I_i$  et un stabilisateur de  $I_i$ .

*Exemple 9.2.* Au Paragraphe 10.1.4 Cas A., supposons que  $Gal_k(f)$  est  $8T_{27}$  ou  $8T_{16}$  (information inconnue a priori). La factorisation de  $f$  dans  $k(\alpha_1)$  permet de calculer un ensemble triangulaire de générateurs

de  $I = I_{\underline{\alpha}}^{G_{27}}$  et de savoir que  $Gal_k(\underline{\alpha})$  est ou bien  $G_{27}$  ou bien  $G_{16}$  des conjugués respectifs de  $8T_{27}$  et  $8T_{16}$  dans  $S_8$ . Le calcul de  $I_{\underline{\alpha}}$  et de son groupe de décomposition  $Gal_k(\underline{\alpha})$  se fera alors par l'appel : `GaloisIdéal( $G_{27}$ ,  $T$ , [ $G_{16}$ ])`.

Comme  $Card(V(I))$  est au plus le double du cardinal de  $V(I_{\underline{\alpha}})$  ce calcul sera très rapide.

### 9.3. Construction de l'algorithme.

La première étape consiste à calculer un ensemble triangulaire  $T_I$  d'un idéal de départ  $I$  construit à partir d'un idéal de première rupture  $I_0$  et à déterminer ensuite un stabilisateur de  $I$  connaissant le stabilisateur  $L_0$  de  $I_0$ .

Nous dirons qu'un groupe est candidat s'il appartient à  $C(L_0)$  et s'il vérifie d'éventuelles conditions, comme un critère de parité ou celui de Dedekind.

Dans l'algorithme ci-dessous, nous procédons par cas : **Cas i** ou **Cas i.j**. Si l'hypothèse (en italique) du **Cas i** (resp. **Cas i.j**) n'est pas vérifiée, il faut passer au **Cas i+1** (resp. **Cas i.j+1**). Lorsque l'algorithme renvoie à un cas particulier, c'est que l'hypothèse de celui-ci est vérifiée.

**Cas 1** *Un des groupes candidats  $G$  vérifie  $Card(G) = Card(V(I))$ .*

Il existe  $\underline{\alpha} \in V(I)$  tel que  $Gal_k(\underline{\alpha}) \subset G$  si et seulement si  $Stab(I) = G$  (voir Proposition 3.9). Il suffit de calculer  $Gr(I)$ .

Si  $G \neq Gr(I)$  alors on retire  $G$  et tous ses sous-groupes de la liste des candidats et on recommence à tester le Cas 1.

Si  $G = Gr(I)$  Alors

**Cas 1.1**  *$G$  est le groupe de Galois.*

Dans ce cas  $I = I_{\underline{\alpha}}$  et  $G = Gal_k(\underline{\alpha})$ .

**Cas 1.2**  *$G$  n'est pas le groupe de Galois.*

Notant  $L$  la liste des groupes candidats inclus dans  $G$ , l'algorithme se termine avec

$$\text{GaloisIdéal}(G, T_I, L).$$

**Cas 2** *Il n'existe qu'une classe de  $L_0$ -conjugaison par groupe candidat.*

**Cas 2.1** *L'idéal  $I$  est associable à une classe de  $L_0$ -conjugaison.*

Soit  $G$  un groupe de cette classe. (Le cas  $G = Stab(I)$  relève des Cas 1.1. ou 1.2.) D'après le Théorème 6.9, il existe  $\underline{\alpha} \in V(I)$  tel que

$$Stab(I, \underline{\alpha}) = \Psi(G) \quad .$$

Nous comparons  $\mathcal{L}(I)$  et  $\mathcal{L}(G)$  pour trouver des relations nouvelles avec les résultats du paragraphe 8. Soit  $J$ , l'idéal de Galois ainsi obtenu et

$T_J$  un ensemble triangulaire l'engendrant. Un stabilisateur  $S$  de  $J$  se déduit de  $\Psi(G)$  celui de  $I$ . Si aucune relation n'est trouvée alors  $J = I$ . On peut se retrouver avec un seul candidat  $G$  avec  $G = S$ , c'est-à-dire dans le Cas 1.1. avec  $J$  à la place de  $I$ . Sinon l'algorithme se termine avec

GaloisIdéal( $S, T_J, L$ )

où  $L$  est la liste des groupes candidats de laquelle on a retiré les groupes non inclus dans  $S$ .

**Cas 2.2** *Tous les groupes candidats permettent de rajouter les mêmes relations.*

Nous reprenons les notations du Cas 2.1. Il y a plusieurs stabilisateurs possibles pour  $J$  selon le groupe de Galois. La liste des groupes candidats est réduite aux groupes pouvant être inclus dans l'un de ces stabilisateurs. Si  $\text{Card}(V(J))$  est identique au cardinal de tous les candidats, alors on se retrouve dans le Cas 1.1. avec  $J$  à la place de  $I$ .

**Cas 2.3** *On obtient de nouvelles informations sur le groupe de Galois.* Ces informations peuvent être trouvées en étudiant le comportement des *résolvantes  $S$ -relatives* en fonction des différents stabilisateurs  $S$  possibles de  $J$ . On recommence l'algorithme au Cas 1 avec  $J$  à la place de  $I$ .

**Cas 2.4** C'est le cas par défaut. Il est nécessaire de factoriser dans des extensions supérieures pour calculer de nouvelles relations ou encore de terminer avec la décomposition de  $I$  en idéaux premiers. Il peut être judicieux de calculer le groupe de Galois de  $f$  en parallèle. Le calcul du stabilisateur de l'idéal  $J$  est alors possible et celui d'un idéal des relations sera alors plus efficace qu'avec une décomposition en idéaux premiers ou une factorisation dans une extension supérieure.

**Cas 3** *Des groupes candidats  $S_n$ -conjugués ne sont pas  $L_0$ -conjugués.* Cela se produit lorsque les degrés des facteurs de rupture ne sont pas distincts deux à deux. Nous avons écarté de la liste des candidats les groupes  $G$  vérifiant  $\text{Card}(G) = \text{Card}(V(I))$  (Cas 1.). Nous cherchons un critère d'association entre  $I$  et les classes de  $L_0$ -conjugaison.

**Cas 3.1** *Un critère d'association est trouvé.*

Nous savons a priori comment ordonner les facteurs de rupture de  $f$  pour que l'idéal de départ  $I$  soit associé à une classe de  $L_0$ -conjugaison donnée. Nous retirons de la liste des groupes candidats les groupes appartenant aux classes de  $L_0$ -conjugaison auxquelles l'idéal  $I$  ne peut être associé. Nous nous retrouvons alors dans le Cas 2.

**Cas 3.2** *Nous pouvons rajouter des relations quelque soit le groupe de Galois.*

Soit  $J$  l'idéal obtenu. Nous recommençons l'algorithme au Cas 1 avec l'idéal  $J$  à la place de l'idéal  $I$ .

**Cas 3.3** C'est le cas par défaut. Il faut agir comme pour le Cas 2.4.

*Remarque 9.3.* Concernant le Cas 2.1. Soit  $G$  un groupe candidat tel que  $C(L_0, G)$  ne contienne qu'une classe de  $L_0$ -conjugaison. D'après la proposition 6.25, pour que  $I$  soit associé à la classe de  $L_0$ -conjugaison de  $G$ , il faut et il suffit qu'il existe  $\sigma \in S_n$  tel que  $\text{Gal}_k(f) \cap G^\sigma$  soit transitif. Lorsqu'il existe plusieurs classes de  $L_0$ -conjugaisons dans  $C(L_0, G)$  et que par un critère d'association nous passons du Cas 3. au Cas 2., il faut alors procéder à un autre test pour s'assurer que nous sommes dans le Cas 2.1. L'idéal  $I$  sera associé à la classe de  $L_0$ -conjugaison de  $G$  si tout groupe candidat possède un  $L_0$ -conjugué  $H$  tel que  $G \cap H$  soit transitif (voir, par exemple, Cas C. Paragraphe 10.1.4).

### 10. ÉTUDE EN DEGRÉ 8

Pour illustrer cet article, nous avons choisi le degré  $n = 8$ . L'objectif est l'élaboration d'un algorithme calculant un idéal des relations  $I_{\underline{\alpha}}$  où  $\underline{\alpha}$  est un 8-uplet des racines de  $f$  ainsi que son groupe de décomposition  $\text{Gal}_k(\underline{\alpha})$ . Nous excluons le cas où  $\Delta(f) = (7)$ , c'est-à-dire celui où le groupe de Galois de  $f$  est 2-transitif.

Nous supposons que  $I$  est un idéal de départ construit à partir d'un idéal de première rupture  $I_0$  de  $f$  et engendré par un ensemble triangulaire  $T_I = \{f_1(x_1), \dots, f_8(x_1, \dots, x_8)\}$ . Lorsque  $\Delta(f) = e$ ,  $L_0 = S_{1,e}$  est le stabilisateur de  $I_0$ .

Les groupes  $8T_i$  de l'ensemble  $\mathcal{T}(8)$  seront notés  $T_i$ . Lorsque nous évoquerons le groupe de Galois d'un polynôme, ce sera, à conjugaison près un des groupes  $T_i$ . Nous utiliserons des groupes conjugués  $G_i = T_i^\sigma$  des groupes  $T_i$  qui appartiendront aux ensembles  $C(L_0)$  considérés. Les permutations  $\sigma_i$  sont données ci-dessous :

i	7	8	9	10	11	12	14
$\sigma_i$	(2, 7, 3, 4, 5)(6, 8)	$ba^{-1}$	db(5, 7)	(2,7)c(6,8)	(2, 8, 6, 7)c	(2, 7, 6, 4, 5)	(2, 4, 6, 7, 8, 3, 5)
i	17	18	19	29	39	31	32
$t_i$	(2, 3, 4, 5, 6, 8)	(1, 5)(2, 7)(3, 8)(4, 6)	d(4, 7, 6, 8)	d(4, 5, 8)	(2, 6)(7, 8)	(2, 7, 6, 8, 3, 5)	(2, 6)

où  $a = \sigma_6 = (2, 7, 6, 3, 5)$ ,  $b = t_{47} = (4, 8)$ ,  $c = (4, 5)$   $d = (2, 3)$ ,  $e = \sigma_{13} = \sigma_{24} = (2, 4, 6)(5, 7, 8)$  et pour  $i = 15, 23, 26, 28, 30, 35, 38, 40, 44$ ,  $\sigma_i = (2, 5)(4, 7)$ .

#### 10.1. Étude détaillée.

C'est en fonction de  $L_0$  que les différents cas sont distingués en étudiant l'ensemble  $C(L_0)$ . Nous nous référerons aux différents cas de l'algorithme du paragraphe 9.3 et nous utilisons la table de première rupture en degré 8 (voir Paragraphe 4.2).

10.1.1.  $\Delta(f) = (1^8)$ ,  $L_0 = S_{1^8}$  et  $\mathcal{L}(I) = (8, 1^7)$ .

Nous sommes dans le Cas 1.1. Par exemple, le polynôme  $f := x^8 + 8x^6 + 20x^4 + 16x^2 + 2$  se factorise en  $(x - x_1)(x + x_1)(x - x_1^3 - 3x_1)(x + x_1^3 + 3x_1)(x - x_1^5 - 5x_1^3 - 5x_1)(x + x_1^5 + 5x_1^3 + 5x_1)(x - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1)(x + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1)$  dans  $k[x_1]/f(x_1)$ . Nous en déduisons l'idéal des relations :

$$I_{\underline{\alpha}} = \langle f(x_1), x_2 + x_1, x_3 - x_1^3 - 3x_1, x_4 + x_1^3 + 3x_1, x_5 - x_1^5 - 5x_1^3 - 5x_1, \\ x_6 + x_1^5 + 5x_1^3 + 5x_1, x_7 - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1, x_8 + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1 \rangle$$

de groupe de décomposition  $Gal_k(\underline{\alpha}) = T_1^\sigma$  avec  $\sigma = (2, 3, 7, 8, 5)(4, 6)$ .

10.1.2.  $\Delta(f) = (1^3, 2^2)$ ,  $L_0 = S_{1^4, 2^2}$  et  $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$ .

Pour tout  $G \in C(L_0)$ , nous avons  $\mathcal{L}(G) = (8, 1^3, 2, 1^3)$ . En comparant avec  $\mathcal{L}(I)$ , nous savons que nous cherchons une relation de la forme  $r_7 = x_7 + h_7(x_1, \dots, x_6)$  pour obtenir un ensemble triangulaire  $\{f_1, \dots, f_6, r_7, f_8\}$  engendrant un idéal des relations  $I_{\underline{\alpha}}$ . Les polynômes  $f_2$  et  $f_3$  de  $T_I$  sont respectivement de la forme  $x_2 + g_2(x_1)$  et  $x_3 + g_3(x_1)$ .

**Cas A** Le groupe de Galois de  $f$  est le groupe impair  $T_7$ .

Ce cas relève du Cas 3.1. puis du Cas 2.1. puis du Cas 1.1. Un critère d'association est donné dans l'exemple 6.29. Ordonnons les facteurs de rupture de telle sorte que  $x_6 + g_2(x_5) \in I$ . Nous trouvons la relation  $r_7 = x_7 + g_3(x_5)$  avec  $Gal_k(\underline{\alpha}) = G_7$ .

**Cas B** Le groupe de Galois de  $f$  est pair.

Ce cas relève du Cas 3.1. puis du Cas 2.1. puis du Cas 1.1. Il y a 3 classes de  $L_0$ -conjugaison pour chaque groupe candidat : pour  $i = 1, 2, 3$ , notons  $A_i$  celles de  $C(L_0, T_9)$ ,  $B_i$  celles de  $C(L_0, T_{10})$  et  $C_i$  celles de  $C(L_0, T_{11})$ . (Chacune des classes comporte 2 groupes.) Le critère d'association est :

- 1) si  $x_6 + g_2(x_5) \in I$  alors  $I$  est associé à  $A_2$ , ou à  $B_2$  ou à  $C_2$  ;
- 2) si  $x_6 + g_3(x_5) \in I$  alors  $I$  est associé à  $A_3$  ou à  $B_3$  ou à  $C_3$  ;
- 3) si  $x_6 + g_4(x_5) \in I$  alors  $I$  est associé à  $A_1$  ou à  $B_1$  ou à  $C_1$ .

Optons pour l'idéal de départ  $I$  associé à  $A_1, B_1$  ou  $C_1$ . Nous trouvons  $r_7 = x_7 + g_2(x_5)$  avec  $Gal_k(\underline{\alpha}) \in \{G_9, G_{10}, G_{11}\}$  déterminé par le calcul du groupe de décomposition de  $I_{\underline{\alpha}}$ .

10.1.3.  $\Delta(f) = (1^3, 4)$ ,  $L_0 = S_{1^4, 4}$  et  $\mathcal{L}(I) = (8, 1^3, 4, 3, 2, 1)$ .

Pour tout groupe  $G$  de  $C(L_0)$ ,  $\mathcal{L}(G) = (8, 1^3, 4, 1^3)$ . Nous recherchons donc deux relations linéaires  $r_6 = x_6 + h_6(x_1, \dots, x_5)$  et  $r_7 = x_7 + h_7(x_1, \dots, x_6)$ . Les polynômes  $f_2, f_3$  et  $f_4$  de l'ensemble triangulaire  $T_I$  sont de la forme :  $f_2 = x_2 + g_2(x_1)$ ,  $f_3 = x_3 + g_3(x_1)$  et  $f_4 = x_4 + g_4(x_1)$ .

Supposons que  $Gal_k(f)$  soit le groupe pair  $T_{18}$ . L'ensemble  $C(L_0, T_{18})$  n'a qu'une classe de  $L_0$ -conjugaison (Cas 2.1). Avec  $Gal_k(\underline{\alpha}) = G_{18}$ , nous trouvons  $r_6 = x_6 + g_4(x_5)$  et  $r_7 = x_7 + g_2(x_5)$ .

Supposons que  $Gal_k(f)$  soit le groupe impair  $T_{17}$ . Ce cas relève du Cas 3.1. puis du Cas 2.1. puis du Cas 1.1. L'ensemble  $C(L_0, T_{17})$  comporte 18 groupes qui se répartissent en 3 classes  $A_1, A_2$  et  $A_3$  de  $L_0$ -conjugaison avec le critère d'association suivant :

- 1) si  $x_1 + g_4(x_2) \in I$  alors  $I$  est associé à  $A_1$  ;
- 2) si  $x_1 + g_3(x_2) \in I$  alors  $I$  est associé à  $A_2$  ;
- 3) si  $x_1 + g_2(x_2) \in I$  alors  $I$  est associé à  $A_3$ .

Supposons l'idéal de départ  $I$  associé à la classe  $A_2$ . Avec  $Gal_k(\underline{\alpha}) = G_{17}$  dans  $A_2$ , nous trouvons  $r_6 = x_6 + g_3(x_5)$  et  $r_7 = x_7 + g_2(x_5)$ .

10.1.4.  $\Delta(f) = (1, 2^3)$ ,  $L_0 = S_{1^2, 2^3}$  et  $\mathcal{L}(I) = (8, 1, 2, 1, 2, 1, 2, 1)$ .

Comme  $card(V(I)) = 64 = card(T_{31}) = card(T_{27})$ , c'est le Cas 1. L'ensemble  $C(L_0, T_{27})$  comporte 3-classes de  $L_0$  conjugaison et  $C(L_0, T_{31}) = \{G_{31}\}$ .

**Cas A.**  $Gr(I) = T_{27}^\sigma$  avec  $\sigma \in S_n$  (Cas 1.2).

L'idéal  $I$  est associé à la classe de  $L_0$ -conjugaison de  $H_{27} = T_{27}^\sigma$  réduite à ce groupe. Selon la parité du groupe de Galois, le calcul se termine avec  $\text{GaloisIdéal}(H_{27}, T_I, [H_{20}^+])$  ou bien avec  $\text{GaloisIdéal}(H_{27}, T_I, [H_{16}])$ , où  $H_{16}$  et  $H_{20}$  sont des sous-groupes de  $H_{27}$  conjugués respectifs de  $T_{16}$  et  $T_{20}^+$ .

**Cas B.**  $Gr(I) = G_{31}$  (Cas 1.2).

Selon la parité du groupe de Galois, le calcul se termine avec  $\text{GaloisIdéal}(G_{27}, T_I, [G_{22}^+])$  ou bien avec  $\text{GaloisIdéal}(G_{27}, T_I, [G_{21}])$ .

**Cas C.** Le groupe de Galois est  $T_6$  ou  $T_8$ .

C'est le cas lorsque les Cas A. et B. ne sont pas vérifiés et que dans la liste des groupes candidats il ne reste que les groupes de  $C(L_0)$  conjugués à  $T_6$  ou à  $T_8$ . Comme pour tout groupe  $G$  candidat  $\mathcal{L}(G) = (8, 1, 2, 1^5)$ , en comparant avec  $\mathcal{L}(I)$ , nous savons que nous cherchons deux relations linéaires  $r_5 = x_5 + h_5(x_1, x_3)$  et  $r_7 = x_7 + h_7(x_1, x_3)$ .

Nous sommes dans le Cas 3.2. Il y a 3 classes  $A_1, A_2$  et  $A_3$  (resp.  $B_1, B_2$  et  $B_3$ ) de  $L_0$ -conjugaison pour les groupes conjugués à  $T_6$  (resp.  $T_8$ ). Nous avons le critère d'association suivant :

- 1) si  $x_4 + g_2(x_3) \in I$  alors  $I$  est associé à  $A_1$  ou à  $B_1$ ,
- 2) si  $x_6 + g_2(x_5) \in I$  alors  $I$  est associé à  $A_2$  ou à  $B_2$ ,
- 3) si  $x_8 + g_2(x_7) \in I$  alors  $I$  est associé à  $A_3$  ou à  $B_3$ .

Supposons l'idéal de départ  $I$  associé à  $A_2$  ou  $B_2$ . Nous passons du Cas 3.2. au Cas 2.2. Avec le groupe  $G_6$  dans  $A_2$  et le groupe  $G_8$  dans  $B_2$ , nous obtenons la relation linéaire  $r_7 = x_7 + g_2(x_3)$  et l'idéal  $J = I + \langle r_7 \rangle$  est l'intersection de deux idéaux de relations. Les autres groupes des classes  $A_2$  et  $B_2$  permettant de rajouter cette relation sont



respectivement  $H_i = G_i^\sigma$  avec  $\sigma = (5, 6)$  pour  $i = 6, 8$ . Le stabilisateur de  $J$  est l'un des  $L_i = G_i + G_i(5, 6)$ ,  $i = 6, 8$ , selon que le groupe de Galois est  $G_6$  ou  $G_8$  (voir Théorème 6.9 et Proposition 8.5). Bien que  $T_6 \cap T_8 = T_1$  transitif, pour tout groupe  $L$  de  $A_2$  et  $M$  de  $B_2$ ,  $L \cap M$  est non transitif. C'est pour cette raison que les deux ensembles  $L_6$  et  $L_8$  sont distincts. Ils engendrent dans  $S_8$  le même groupe  $T_{35}^\sigma$  avec  $\sigma = (2, 3, 5)(6, 7)$ . Si le groupe de Galois est connu, il est possible de terminer avec  $\text{GaloisIdéal}(L_i, T_J, [G_i])$  où  $G_i$  est conjugué à  $\text{Gal}_k(f)$ . Sinon, nous sommes dans le Cas 2.4. L'étude des résolvantes  $L_i$ -relatives pour  $i = 6, 8$  n'apporte rien. La décomposition en idéaux premiers est peu coûteuse. Il ne restera qu'à tester lequel des 4 groupes  $G_i, H_i$  avec  $i = 6, 8$  est le groupe de décomposition  $\text{Gal}_k(\underline{\alpha})$  de  $I_{\underline{\alpha}}$  choisi dans la décomposition en idéaux premiers. Il est aussi possible de factoriser  $f_5$  de la forme  $x_5^2 + g_5(x_1, x_5)$  en deux facteurs linéaires sur le corps  $k[x_1, x_3] / \langle f_1(x_1), f_3(x_1, x_3) \rangle$  isomorphe à  $k(\alpha_1, \dots, \alpha_4)$  de degré 16 sur  $k$ . L'un des facteurs donnera  $r_5$  et l'autre est  $f_6$  modulo  $r_5$ .

*Exemple 10.1.* Avec le polynôme  $f = x^8 - 3x^5 - x^4 + 3x^3 + 1$ , de groupe de Galois  $T_6$ , la décomposition de  $J$  en deux idéaux premiers  $I_{\underline{\alpha}}$  et  $I_{(5,6)\underline{\alpha}}$  ( $\underline{\alpha} \in V(J)$ ) se instantanément. Il en va de même avec le polynôme  $f = x^8 + 24x^6 + 126x^4 + 216x^2 + 117$ , de groupe de Galois  $T_8$ .

10.1.5.  $\Delta(f) = (1, 2, 4)$ ,  $L_0 = S_{1^2, 2, 4}$  et  $\mathcal{L}(I) = (8, 1, 2, 1, 4, 3, 2, 1)$ .

Le polynôme  $f_2$  est de la forme  $x_2 + g_2(x_1)$ . Nous sommes dans le Cas 2.1. car tout groupe candidat possède un  $L_0$ -conjugué  $H$  inclus dans  $G_{35}$ . Il existe donc  $\underline{\alpha} \in V(I)$  tel que  $\text{Gal}_k(\underline{\alpha}) \subset G_{35}$ . En comparant  $\mathcal{L}(G_{35}) = (8, 1, 2, 1, 4, 1, 2, 1)$  à  $\mathcal{L}(I)$ , nous trouvons l'idéal  $J$  de stabilisateur  $G_{35}$  et engendré par

$$T_J = \{f_1, \dots, f_5, x_6 + g_2(x_5), f_7, f_8\}.$$

Selon la parité de  $\text{Gal}_k(f)$ , on termine avec

$\text{GaloisIdéal}(G_{35}, T_J, [G_{29}^+, G_{19}^+, H_{19}^+])$  où  $H_{19} = T_{19}^\sigma$  avec

$\sigma = (2, 3)(4, 8)(6, 7)$ ; ou avec

$\text{GaloisIdéal}(G_{35}, T_J, [G_{26}, G_{28}, G_{30}, G_{15}, H_{15}])$  où  $H_{15} = T_{15}^\sigma$  avec  $\sigma = (2, 8, 6, 7, 4, 5)$ .

Soit  $g(\alpha_1, x) = x^4 + g_5(\alpha_1)$  un facteur de première rupture de  $f$ . On peut utiliser son groupe de Galois sur  $k(\alpha_1)$  pour départager  $T_{19}$  et  $T_{29}$  et la parité de ce groupe de Galois pour déterminer si  $\text{Gal}_k(f)$  est ou non  $T_{15}$  (voir Table 1).

10.1.6.  $\Delta(f) = (1, 3^3)$ ,  $L_0 = S_{1^2, 3^2}$  et  $\mathcal{L}(I) = (8, 1, 3, 2, 1, 3, 2, 1)$ .

La relation  $f_2$  de  $T_I$  est de la forme  $x_2 + g_2(x_1)$ . Nous sommes dans le Cas 3. et la situation sera celle du Cas 3.2. Pour tout groupe candidat, il existe un groupe  $G$  dans sa classe de  $L_0$ -conjugaison tel que  $r_6 =$

$x_6 + g_2(x_3)$  et  $r_7 = x_7 + g_2(x_4)$  appartiennent à  $I_{\underline{\alpha}}^G$  si  $G$  contient  $\text{Gal}_k(\underline{\alpha})$ . L'ensemble triangulaire  $T_J = \{f_1, \dots, f_5, r_6, r_7, f_8\}$  engendre un idéal de Galois  $J$  dont le cardinal de la variété est 48, celui de  $8T_{24}$ . C'est le Cas 1.

**Cas A**  $\text{Gr}(J)$  est un conjugué de  $8T_{24}$

Le groupe de Galois est  $8T_{24}$  ou l'un de des deux sous-groupes  $T_{13}$  et  $T_{14}$ . Il y a 2 classes de  $L_0$ -conjugaison  $C_1$  et  $C_2$  dans  $C(L_0, T_{24})$  et il en est donc de même pour les deux sous-groupes  $T_{13}$  et  $T_{14}$  de  $T_{24}$ . Le groupe de décomposition est soit le groupe  $G_{24}$  dans  $C_1$ , soit le groupe  $H_{24} = T_{24}^\sigma$  avec  $\sigma = (2, 8, 6)(3, 7)$  dans  $C_2$ . En ordonnant les facteurs de première rupture de  $f$  de telle sorte que  $J$  ait  $G_{24}$  comme groupe de décomposition, le calcul se termine avec  $\text{GaloisIdéal}(G_{24}, T_J, [G_{13}, G_{14}])$ .

**Cas B**  $\text{Gr}(J)$  n'est pas conjugué à  $8T_{24}$

Le groupe de Galois est donc  $8T_{12}$  et  $C(L_0, T_{12})$  n'a qu'une seule classe de  $L_0$ -conjugaison (Cas 2.1 de l'algorithme). D'après la proposition 8.5, il existe  $\underline{\alpha} \in V(J)$  tel que  $\text{Stab}(J, \underline{\alpha}) = G_{12} + G_{12}(3, 4)(6, 7)$ . Le groupe engendrant  $\text{Stab}(J, \underline{\alpha})$  est  $T_{39}^\sigma$  avec  $\sigma = (2, 3, 4, 7, 5, 6)$  (ce groupe est utile à l'algorithme  $\text{GaloisIdéal}$ ). Nous terminons avec  $\text{GaloisIdéal}(L, T_J, [G_{12}])$ .

*Remarque 10.2.* Si le groupe de Galois d'un quelconque des facteurs de rupture de degré 3 est  $3T_2$  (i.e.  $S_3$ ) alors  $\text{Gal}_k(f) = T_{24}$  (voir Table 1).

10.1.7.  $\Delta(f) = (1, 6)$ ,  $L_0 = S_{12,6}$  et  $\mathcal{L}(I) = (8, 1, 6, 5, 4, 3, 2, 1)$ .

Le groupe de Galois est un sous-groupe de  $T_{44}$ . Nous sommes dans le Cas 2.1. Soit  $f_2 = x_2 + g_2(x_1)$ . Avec  $\mathcal{L}(G_{44}) = (8, 1, 6, 1, 4, 1, 2, 1)$ , nous trouvons l'ensemble triangulaire  $T_J = \{f_1, f_2, f_3, x_4 + g_2(x_3), f_5, x_6 + g_2(x_5), f_7, f_8\}$  tel que  $G_{44} = \text{Stab}(J)$ .

Les calculs se terminent avec  $\text{GaloisIdéal}(G_{44}, T_J, [G_{39}^+, G_{19}^+])$  ou avec  $\text{GaloisIdéal}(G_{44}, T_J, [G_{40}, G_{38}, G_{23}])$  selon la parité de  $\text{Gal}_k(f)$ .

10.1.8.  $\Delta(f) = (3, 4)$ ,  $L_0 = S_{1,3,4}$  et  $\mathcal{L}(I) = (8, 3, 2, 1, 4, 3, 2, 1)$ .

Pour chaque groupe il n'y a qu'une classe de  $L_0$ -conjugaison. Tous les groupes de  $C(L_0)$  sont des sous-groupes de  $G_{47}$  (Cas 2.1.) et  $\text{Card}(V(I))$  est égal à  $\text{Card}(G_{47})$ , donc  $\text{Stab}(I) = G_{47}$ .

Nous terminons avec  $\text{GaloisIdéal}(G_{47}, T_I, [G_{46}])$  ou avec  $\text{GaloisIdéal}(G_{47}, T_I, [G_{45}^+, G_{42}^+, G_{41}^+, G_{34}^+, G_{33}^+])$ , selon la parité du groupe de Galois de  $f$ .

## 11. IMPLANTATION ET RÉSULTATS EXPÉRIMENTAUX

L'implantation de notre algorithme pour le degré 8 est réalisée (et toujours en cours d'amélioration) à l'aide du système de calcul formel MAGMA [4]. Nous avons choisi ce logiciel car il nous a permis de

travailler avec toutes les structures mathématiques dont nous avons besoin (groupes, polynômes univariés et multivariés, algèbre affine...). Lors de nos tests nous avons rencontré un problème pour la factorisations de polynômes à coefficients dans un corps de nombres (D’après [14], ce problème sera corrigé dans quelques semaines). Nous avons donc réimplanté une factorisation récursive basée sur l’algorithme de [16]. Ceci nous a permis de faire nos tests en comparant l’algorithme de calcul de l’idéal des relations donné dans [2] au nôtre. Pour faire ces tests, nous avons utilisé des polynômes de la base de données de G. Malle et J. Kluners (voir [7]). Les temps de calculs, en “cpu-seconde”, sont recensés dans le tableau 2. La première colonne donne le polynôme utilisé, la seconde le groupe de Galois de ce dernier, la suivante l’ordre de ce groupe, et les deux dernières donnent respectivement le temps de calcul de la méthode de [2] et celui de notre méthode. Tous ces tests ont été effectués sur GIULIA4 [6].

$f$	$Gal_{\mathbb{Q}}(f)$	$ Gal_{\mathbb{Q}}(f) $	Méth. 1	Méth. 2
$x^8 - x^7 - 7x^6 + 5x^5 + 15x^4 - 7x^3 - 10x^2 + 2x + 1$	$8T_{47}$	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	519.291
$x^8 + x^7 - 14x^6 - 3x^5 + 62x^4 - 25x^3 - 63x^2 + 24x + 16$	$8T_{45}$	576	6040.889	179.551
$x^8 - x^5 - x^4 - x^3 + 1$	$8T_{44}$	384	66.349	0.199
$x^8 + x^4 - 4x^2 + 1$	$8T_{39}$	192	10.54	0.17
$x^8 + 2x^6 - 12x^4 - 3x^2 + 11$	$8T_{35}$	128	3.529	0.32
$x^8 + 12x^6 + 48x^4 + 72x^2 + 31$	$8T_{31}$	64	0.66	0.259
$x^8 - x^6 - x^4 + x^2 + 1$	$8T_{29}$	64	2.03	0.649
$x^8 - 5x^5 - 3x^4 - 5x^3 + 1$	$8T_{26}$	64	1.8	1.439
$x^8 + x^6 + 2x^2 + 4$	$8T_{19}$	32	0.631	0.82

TAB. 2. Temps de calcul.

Les temps de ces deux méthodes peuvent être améliorés en employant pour la première, la factorisation de Van Hoeij (voir [19]) adaptée aux polynômes à coefficients dans une extension relative (une telle factorisation existe dans le système PARI [13] dans le cas où les coefficients sont dans un corps de nombres absolu), et pour la seconde des méthodes  $p$ -adiques (voir [20]).

## 12. CONCLUSION

Comme le montre le tableau Tab 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 le groupe de Galois est connu, cette méthode peut être éventuellement améliorée en utilisant des méthodes d’interpolations pour recherché les relations de degré 1 (voir [10]).

Nous avons supposé tout au long de cet article que le polynôme  $f$  est irréductible sur  $K$ , mais notre méthode est généralisable aux polyôme réductible en l’appliquant à chacun de ses facteurs et en utilisant le

résultat suivant (voir [12]) :

Soit  $g$  et  $h$  deux facteurs de  $f$  sur  $k$  et  $m$  le degré de  $g$ . Soit  $I_1$  (resp.  $I_2$ ) un idéal de Galois de  $g$  (resp.  $h$ ) sur  $k$ . Alors l'idéal

$$I = I_1k[x_1, \dots, x_n] + I_2k[x_1, \dots, x_n]$$

est un idéal de Galois de  $f$  sur  $k$  et

$$\text{Stab}(I, \underline{\alpha}) = \text{Stab}(I_1, (\alpha_1, \dots, \alpha_m)) \times \text{Stab}(I_2, (\alpha_{m+1}, \dots, \alpha_n)).$$

C'est ainsi que cette méthode peut être inductivement utilisée dans les extensions supérieures. C'est pour mettre en pratique cette généralisation que, dans la définition de l'ensemble  $A(L_0)$  du paragraphe 6.2, nous n'avons pas supposé que le stabilisateur  $L_0$  est un groupe. Elle est donc, en particulier, applicable pour les polynômes dont le groupe de Galois est 2-transitif.

## RÉFÉRENCES

- [1] I. Abdeljaouad, S. Orange, G. Renault, and A. Valibouze, 'Calcul du groupe de décomposition d'un idéal triangulaire', *Manuscrit* (2002).
- [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)*, in *Progr. Math.* **143**, pp. 29–50 (Birkhäuser, Basel, 1996).
- [3] P. Aubry and A. Valibouze, 'Using Galois ideals for computing relative resolvents', *J. Symbolic Comput.* **30** (2000), no. 6, 635–651. Algorithmic methods in Galois theory.
- [4] W. Bosma, J. Cannon, and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).
- [5] A. Cauchy, 'Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée', *Oeuvres* **5** (1840), 473 Extrait 108.
- [6] Giulia, *UMS MEDICIS*. Intel - Pentium III 2 x 933 Mhz, 1024 Mo, Linux 2.4.1.
- [7] J. Klüners and G. Malle, *A database for polynomials over the rationals*. <http://www.iwr.uni-heidelberg.de/groups/compalg/minimum/minimum.html>.
- [8] J. Klüners and G. Malle, 'Explicit Galois realization of transitive groups of degree up to 15', *J. Symbolic Comput.* **30** (2000), no. 6, 675–716. Algorithmic methods in Galois theory.
- [9] S. Landau, 'Factoring polynomials over algebraic number fields', *SIAM J. Comput.* **14** (1985), no. 1, 184–195.
- [10] 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)* (ACM, New York, 1997), 75–77 (electronic).
- [11] M. Noro and K. Yokoyama, 'Factoring polynomials over algebraic extension fields', *Josai Information Science Researches* **9** (1997), 11–33.
- [12] S. Orange, G. Renault, and A. Valibouze, 'Calcul du corps de décomposition d'un polynôme réductible', *Manuscrit* (2003).

- [13] *PARI/GP*, version 2.2.4 (2003). <http://www.parigp-home.de>.
- [14] A. Steel, *Communication privée* (Jan. 2003).
- [15] N. Tchebotarev, *Gründzüge des galois'shen theorie* (P. Noordhoff, 1950).
- [16] B. Trager, 'Algebraic factoring and rational function integration', in *Proceedings of SYMSAC'76* (1976), 219–226.
- [17] A. Valibouze, 'Étude des relations algébriques entre les racines d'un polynôme d'une variable', *Bull. Belg. Math. Soc. Simon Stevin* **6** (1999), no. 4, 507–535.
- [18] A. Valibouze, 'Calcul du corps de décomposition à partir d'un idéal de galois quelconque', *manuscrit* (2002).
- [19] M. van Hoeij, 'Factoring polynomials and the knapsack problem', *J. Number Theory* **95** (2002), no. 2, 167–189.
- [20] K. Yokoyama, 'A modular method for computing the Galois groups of polynomials', *J. Pure Appl. Algebra* **117/118** (1997), 617–636. Algorithms for algebra (Eindhoven, 1996).

ÉQUIPE CALFOR - LIP6, 8 RUE DU CAPITAINE SCOTT, 75015 PARIS.

*E-mail address:* `name@calfor.lip6.fr`