Corps de décomposition d'un polynôme réductible

Sébastien Orange, Guénaël Renault, Annick Valibouze

CORPS DE DÉCOMPOSITION D'UN POLYNÔME RÉDUCTIBLE

S. ORANGE, G. RENAULT, A. VALIBOUZE

Résumé

Dans cet article, nous exploitons la reductibilité d'un polynôme d'une variable pour calculer efficacement son corps de décomposition.

Abstract

In this paper, we use reducibility of an univariate polynomial in order to compute efficiently its splitting field.

Introduction

Dans [4], l'auteur calcule le centre du groupe de Galois d'un polynôme de $\mathbb{Z}[x]$ afin de déterminer s'il est abélien. Dans le cas où le polynôme est réductible et où le groupe de Galois de chacun de ses facteurs est abélien, l'auteur calcule alors son corps de décomposition avec efficacité. Dans cet article, est décrite une méthode générale pour calculer efficacement le corps de décomposition d'un polynôme réductible quelconque dont les coefficients appartiennent à un corps parfait.

L'algorithme `GaloisIdéal` de [8] calcule le corps de décomposition K d'un polynôme d'une variable f à coefficients dans un corps parfait k. Le polynôme f est supposé séparable et de degré n. Plus précisément, l'algorithme `GaloisIdéal` retourne un ensemble triangulaire engendrant un idéal maximal $\mathcal{M}$ de $k[x_1, \ldots, x_n]$, appelé *idéal des relations*. Le corps K est isomorphe à l'anneau quotient $k[x_1, \ldots, x_n]/\mathcal{M}$ (où $x_1, \ldots, x_n$ sont des variables algébriquement indépendantes).

La méthode utilisée par l'algorithme `GaloisIdéal` consiste à de construire une chaîne ascendante d'idéaux triangulaires, appelés *idéaux de Galois du polynôme* f, :

$$I_1 \subset I_2 \subset \cdots \subset I_s = \mathcal{M} \tag{1}$$

où I_1 est par défaut l'*idéal des relations symétriques* engendré par l'ensemble triangulaire formé par les *modules de Cauchy* (voir [3] ou [7]). Le calcul d'un idéal I_{i+1} à partir de I_i impose de connaître un ensemble triangulaire engendrant I_i et un stabilisateur L_i de I_i qui est un sous-ensemble du groupe

Date: 20 mai 2003.

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

Key words and phrases. Galois group, Galois ideal , reducible univariate polynomial, splitting field.

symétrique S_n (le stabilisateur de $\mathcal{M}$ est un groupe isomorphe au groupe de Galois de K sur k). La complexité de ce calcul dépend du cardinal de L_i égal à celui de la variété affine $V(I_i)$ de l'idéal I_i. Lorsque I_1 est l'idéal des relations symétriques son stabilisateur est le groupe S_n, de cardinal $n!$.

C'est le calcul coûteux du début de la chaîne (1) que nous pourrons éviter lorsque le polynôme f se factorise sur k en $s > 1$ facteurs de degrés respectifs $d_1, \ldots, d_s$. En effet, avec le Théorème 2.4, il est possible de prendre pour I_1 un idéal de Galois dont le stabilisateur est de cardinal compris entre $m_1!\, m_2! \ldots m_s!$ et $d_1!\, d_2! \ldots d_s!$ où m_i est le cardinal du groupe de Galois sur k du i-ième facteur sur k du polynôme f.

Les paragraphes 1 comporte des rappels des articles [8] et [2] concernant les idéaux de Galois. Le paragraphe 2 comporte le Théorème principal que nous illustrerons par des exemples. Le paragraphe 3 donnera une application du théorème 2.4.

1. Rappels sur les idéaux de Galois

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

Notons $\hat{k}$ une clôture algébrique du corps k. Posons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \hat{k}^n$, un n-uplet des racines supposées distinctes du polynôme f.

Dans $k[x_1, \ldots, x_n]$, l'*idéal des $\underline{\alpha}$-relations*

$$\mathcal{M} = \{R \in k[x_1, \ldots, x_n] \ \mid \ R(\alpha_1, \ldots, \alpha_n) = 0\}$$

est engendré par un ensemble triangulaire de polynômes appelés *modules fondamentaux* dans [7]. Le corps de décomposition $K = k(\alpha_1, \ldots, \alpha_n)$ de f est isomorphe à l'anneau quotient $k[x_1, \ldots, x_n]/\mathcal{M}$. Le calcul des modules fondamentaux revient donc à calculer le corps K. Le groupe

$$\mathrm{Gal}_k(\underline{\alpha}) = \{\sigma \in S_n \ \mid \ (\forall R \in \mathcal{M}) \ \ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\}$$

est appelé le *groupe de Galois de $\underline{\alpha}$ sur k* ; il est isormorphe à $\mathrm{Gal}_k(K)$, le groupe de Galois de K sur k.

1.2. **Idéaux de Galois, Stabilisateurs et variétés.**
Soit L une partie de S_n contenant l'identité. L'idéal radical I définit par :

$$I = \{R \in k[x_1, \ldots, x_n] \mid (\forall \sigma \in L)\ \ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\}$$

est appelé l'$(\underline{\alpha}, L)$-*idéal de Galois* (sur k) ou, de manière plus générale, un *idéal de Galois du polynôme* f (sur k). L'$(\underline{\alpha}, S_n)$-idéal de Galois est appelé l'*idéal des relations symétriques* (entre les racines de f) et l'idéal des $\underline{\alpha}$-relations $\mathcal{M}$ est l' $(\underline{\alpha}, I_n)$-idéal de Galois que nous noterons aussi $I_{\underline{\alpha}}$.

Le *stabilisateur de* I *relatif à* $\underline{\alpha}$ est l'ensemble :

$$\mathrm{Stab}(I, \underline{\alpha}) = \{\sigma \in S_n \mid (\forall R \in I)\ \ R(\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(n)}) = 0\} \quad .$$

Puisque l'idéal I est aussi l'$(\underline{\alpha}, \mathrm{Stab}(I, \underline{\alpha}))$-idéal de Galois, nous pouvons l'appeler l' $\underline{\alpha}$-*idéal de Galois de stabilisateur* $Stab(I, \underline{\alpha})$ (relatif à $\underline{\alpha}$). Ce stabilisateur se déduit de l'ensemble L par la formule suivante :

$$(2) \qquad \mathrm{Stab}(I, \underline{\alpha}) \ = \ \mathrm{Gal}_k(\underline{\alpha})\, L = \{gl \mid g \in \mathrm{Gal}_k(\underline{\alpha})\ ,\ l \in L\} \quad .$$

En particulier, $L \subset \mathrm{Stab}(I, \underline{\alpha})$, $\mathrm{Gal}_k(\underline{\alpha}) \subset \mathrm{Stab}(I, \underline{\alpha})$ et

$$(3) \qquad \mathrm{Stab}(I, \underline{\alpha}) \ = \ \mathrm{Gal}_k(\underline{\alpha})\, \mathrm{Stab}(I, \underline{\alpha}) \quad .$$

Lorsque $\mathrm{Stab}(I, \underline{\alpha})$ est un groupe, il est indépendant du choix de $\underline{\alpha}$ dans la variété de I. Nous l'appelons le *stabilisateur de* I.

Remarque 1. L' idéal des $\underline{\alpha}$-relations est l'$\underline{\alpha}$-idéal de Galois de stabilisateur le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$ et l' idéal des relations symétriques entre les racines de f est l'$\underline{\alpha}$-idéal de Galois de stabilisateur le groupe symétrique S_n.

La variété affine $V(I) = \{\underline{\beta} \in \hat{k}^n \mid (\forall R \in I)\ \ R(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\}$ de I dans $\hat{k}^n$ est donnée par :

$$(4) \qquad V(I) = \{(\alpha_{\tau(1)}, \ldots \alpha_{\tau(n)}) \mid \tau \in \mathrm{Stab}(I, \underline{\alpha})\} \quad .$$

1.3. **Idéaux de Galois triangulaires.**
Un sous-ensemble T de n polynômes de $k[x_1, \ldots, x_n]$ est dit *triangulaire* si $T = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ où le i-ième polynôme f_i est unitaire en tant que polynôme en x_i avec $\deg(f_i, x_i) > 0$. Cet ensemble triangulaire est dit *séparable* si chaque polynôme f_i de T vérifie la condition suivante :

$\forall (\beta_1, \ldots, \beta_n) \in \hat{k}^n$ tel que $\forall j \in [1, n]$, $f_j(\beta_1, \ldots, \beta_n) = 0$, le polynôme d'une variable $f_i(\beta_1, \ldots, \beta_{i-1}, x)$ n'a pas de racine multiple dans $\hat{k}$.

Si un idéal est engendré par un ensemble triangulaire séparable, il est dit *triangulaire*.

Lorsque le stabilisateur d'un idéal de Galois est un groupe, cet idéal est alors triangulaire (voir [2]). Tous les idéaux de Galois construits par des méthodes effectives sont triangulaires (voir [5] ou Théorème 2.4 de cet article). Aucun théorème n'a encore attesté que tout idéal de Galois est nécessairement engendré par un ensemble triangulaire mais si c'est le cas il est nécessairement séparable puisque l'idéal est radical.

2. Idéal de Galois de stabilisateur un groupe produit

Lorsque le polynôme f est réductible sur k, son groupe de Galois sur k est un sous-groupe du produit direct des groupes de Galois sur k de ses facteurs sur k. Nous allons montrer que des idéaux de Galois triangulaires de chacun des facteurs de f nous pouvons déduire un idéal de Galois triangulaire J de f (i.e. un ensemble triangulaire l'engendrant ainsi que son stabilisateur) contenant strictement l'idéal des relations symétriques entre les racines de f. L'algorithme `GaloisIdéal` pourra être ensuite utilisé pour calculer l'idéal des $\underline{\alpha}$-relations à partir de $I_1 = J$.

Supposons dans cette partie que le polynôme f se factorise sur k en deux polynômes g et h de degrés respectifs m et $p = n - m$, que $\underline{\beta} = (\alpha_1, \ldots, \alpha_m)$ est un m-uplet des racines de g et que $\underline{\gamma} = (\alpha_{m+1}, \ldots, \alpha_n)$ est un p-uplet des racines de h.

Rappelons le résultat bien connu suivant dont nous donnons une démonstration simple à partir des idéaux de Galois.

Lemme 2.1. *$Gal_k(\underline{\alpha}) \subset Gal_k(\underline{\beta}) \times Gal_k(\underline{\gamma})$.*

Démonstration. Soit $\sigma \in \mathrm{Gal}_k(\underline{\alpha})$.
Nous avons naturellement $I_{\underline{\beta}}k[x_1, \ldots, x_n] \subset I_{\underline{\alpha}}$, c'est-à-dire que toute $\underline{\beta}$-relation est nécessairement une $\underline{\alpha}$-relation. Si $\sigma \notin S_m \times S_p$ alors il existe $i \in [1, m]$ tel que $j = \sigma(i) \in [m+1, n]$. Comme $g(x_i) \in I_{\underline{\alpha}}$, par définition de $\mathrm{Gal}_k(\underline{\alpha})$, $g(\alpha_j) = 0$, ce qui est impossible car α_j est racine de h et f est séparable. Donc $\sigma \in S_m \times S_p$ et $\sigma = \tau\tau'$ avec $\tau \in S_m$ et $\tau' \in S_p$. Par définition de $\mathrm{Gal}_k(\underline{\alpha})$, pour toute $\underline{\alpha}$-relation R nous avons $R(\alpha_{\tau_{\sigma(1)}}, \ldots, \alpha_{\tau(m)}, \alpha_{\tau'(m+1)}, \ldots, \alpha_{\tau'(n)}) = 0$, et donc, en particulier, pour

toute $\underline{\beta}$-relation R nous avons $R(\alpha_{\tau_{\sigma(1)}}, \ldots, \alpha_{\tau_{\sigma(m)}}) = 0$. Donc $\tau \in \mathrm{Gal}_k(\underline{\beta})$, de même $\tau' \in \mathrm{Gal}_k(\underline{\gamma})$, et finalement $\sigma \in \mathrm{Gal}_k(\underline{\beta}) \times \mathrm{Gal}_k(\underline{\gamma})$. □

Lemme 2.2. *Si g et h sont k-irréductibles alors les $Gal_k(\underline{\alpha})$-orbites de $\{1, \ldots, n\}$ sont $\{1, 2, \ldots, m\}$ et $\{m+1, m+2, \ldots, n\}$.*

Démonstration. Les racines $\alpha_1, \alpha_2, \ldots, \alpha_m$ du polynôme g sont les $\alpha_{\sigma(i)}$ où σ parcourt $\mathrm{Gal}_k(\underline{\alpha})$ puisque g est irréductible sur k. Donc $\{1, 2, \ldots, m\}$ est l'orbite de 1 sous l'action $\mathrm{Gal}_k(\underline{\alpha})$. De même $\{m+1, m+2, \ldots, n\}$ est l'orbite de $m+1$ sous l'action $\mathrm{Gal}_k(\underline{\alpha})$. □

Exemple 2.3. Posons $m = 5$ et $p = 2$.
Supposons que $\mathrm{Gal}_k(\underline{\beta})$ soit le groupe cyclique $C_5 =< (1, 3, 2, 4, 5) >$ et que $\mathrm{Gal}_k(\underline{\gamma}) = S_2$. Comme le groupe $C_5 \times S_2$ n'a pas de sous-groupe propre dont l'action sur $\{1, 2, \ldots, 7\}$ ait une orbite de longueur 5=deg(g) et une de longueur 2=deg(h), nous avons nécessairement $\mathrm{Gal}_k(\underline{\alpha}) = C_5 \times S_2$.
Supposons que $\mathrm{Gal}_k(\underline{\beta})$ soit le groupe dihédral $D_5 =< \sigma = (1, 5, 2, 3, 4), \tau = (1, 3)(2, 5) >$ et que $\mathrm{Gal}_k(\underline{\gamma}) = S_2$. Le seul sous-groupe propre de $D_5 \times S_2$ qui ait une orbite de longueur 5 et une de longueur 2 est le groupe $G_2 =< \sigma, \tau(6, 7) >$. Le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$ est donc ou bien $D_5 \times S_2$ ou bien G_2.

Théorème 2.4. *Soit I_1 (resp. I_2) un $\underline{\beta}$-idéal (resp. $\underline{\gamma}$-idéal) de Galois appartenant à $k[x_1, \ldots, x_m]$ (resp. $k[x_{m+1}, \ldots, x_n]$) de stabilisateur G (resp. H) relatif à $\underline{\beta}$ (resp. $\underline{\gamma}$). (nous avons donc $G \subset S_m$ et $H \subset S_p$).*
Supposons que les idéaux I_1 et I_2 soient engendrés respectivement par des ensembles triangulaires séparables T_1 dans $k[x_1, \ldots, x_m]$ et T_2 dans $k[x_{m+1}, \ldots, x_n]$. Alors l'idéal de $k[x_1, x_2, \ldots, x_n]$ engendré par l'ensemble triangulaire $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois de stabilisateur $G \times H$; il vérifie donc :

$$I_{\underline{\alpha}}^{G \times H} = I_1 k[x_1, \ldots, x_n] + I_2 k[x_1, \ldots, x_n] \quad .$$

En particulier,

$$Card(Gal_k(\underline{\beta}))Card(Gal_k(\underline{\gamma})) \leq Card(V(J)) = Card(G).Card(H) \leq m!\, p!.$$

Démonstration. L'idéal I de $k[x_1, \ldots, x_n]$ engendré par l'ensemble triangulaire $T_1 \cup T_2$ est naturellement l'idéal $I_1 k[x_1, \ldots, x_n] + I_2 k[x_1, \ldots, x_n]$.
Puisque G (resp. H) est le stabilisateur de I_1 (resp. I_2), nous avons d'après (4)

$$V(I_1) = G.\underline{\alpha} = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}) \mid \sigma \in G\}$$

(resp. $V(I_2) = H.\underline{\gamma}$). Les éléments de $\hat{k}^n$ annulant T_1 (resp. T_2) sont les $(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}, u_1, \ldots, u_p)$ (resp. $(v_1, \ldots, v_m, \alpha_{\sigma(m+1)}, \ldots, \alpha_{\sigma(n)})$) avec $\sigma \in G$, (resp. $\sigma \in H$) et $u_i, v_j \in \hat{k}$. Les racines de f étant deux à deux distinctes, les éléments de $\hat{k}^n$ annulant $T_1 \cup T_2$ sont les n-uplets distincts $(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ de $\hat{k}^n$ où σ parcourt $G \times H$.

L'idéal I étant engendré par l'ensemble triangulaire $T_1 \cup T_2$, sa variété affine $V(I)$ est l'ensemble des éléments de $\hat{k}^n$ annulant les polynômes de $T_1 \cup T_2$:

$$V(I) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in G \times H\} .$$

L'ensemble triangulaire $T_1 \cup T_2$ étant séparable, l'idéal I est radical et nous avons :

$$I = \{R \in k[x_1, x_2, \ldots, x_n] \mid (\forall \sigma \in G \times H) \ R(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) = 0\} \quad .$$

Les racines α_i étant deux à deux distinctes, l'idéal I est un $\underline{\alpha}$-idéal de Galois de stabilisateur $G \times H$. □

Remarque 2. Par induction, le théorème précédent se généralise au cas où f se factorise en plus de deux facteurs.

Les polynômes des exemples ci-après on été pris dans la base de données de Jürgen Klüners et Gunter Malle disponible sur internet à l'adresse `http://www.iwr.uni-heidelberg.de/groups/compalg/minimum/`.

Exemple 2.5. Soient les polynômes $\mathbb{Q}$ irréductibles $g = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ et $h = x^2 + 1$ et $f = g.h$. En conservant les notations du théorème 2.4, nous calculons les idéaux des relations $I_{\underline{\beta}}$ et $I_{\underline{\gamma}}$. L'ensemble trianguaire

$$\begin{aligned} T_1 \quad = \{ \quad & x_1^5 - x_1^4 - 4x_1^3 + 3x_1^2 + 3x_1 - 1, \\ & x_2 + x_1^2 - 2, \\ & x_3 - x_1^3 + 3x_1, \\ & x_4 - x_1^4 + x_1^3 + 3x_1^2 - 2x_1 - 1, \\ & x_5 + x_1^4 - 4x_1^2 + 2\} \end{aligned}$$

engendre l'idéal $I_{\underline{\beta}}$ des $\underline{\beta}$-relations de stabilisateur le groupe cyclique $C_5 = < (1,3,2,4,5) >$ et $T_2 = \{x_6^2 + 1, x_7 + x_6\}$ engendre l'idéal $I_{\underline{\gamma}}$ des $\underline{\gamma}$-relations de stabilisateur le groupe symétrique S_2. Nous avons $C_5 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\beta})$ et $S_2 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\gamma})$. Les deux ensembles triangulaires T_1 et T_2 se calculent rapidement. D'après le Théorème 2.4, appliqué à $G = C_5$, $I_1 = I_{\underline{\beta}}$, $H = S_2$ et $I_2 = I_{\underline{\gamma}}$, l'idéal engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois de stabilisateur $C_5 \times S_2$ et, comme $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) = C_5 \times S_2$ (voir Exemple 2.3), c'est l'idéal $I_{\underline{\alpha}}$ des $\underline{\alpha}$-relations.

Exemple 2.6. Soient les polynômes $\mathbb{Q}$ irréductibles $g = x^5 - 2x^4 + 2x^3 - x^2 + 1$ et $h = x^2 + 1$ et $f = g.h$. Nous procédons de même que pour l'exemple précédent. L'ensemble triangulaire

$$\begin{aligned} T_1 \quad = \{ \quad & x_1^5 - 2x_1^4 + 2x_1^3 - x_1^2 + 1, \\ & x_2^2 + (-x_1^4 + x_1^3 - x_1^2 + x_1 - 1)x_2 - x_1 + 1, \\ & x_3 + x_2 - x_1^4 + x_1^3 - x_1^2 + x_1 - 1, \\ & x_4 - x_2 x_1^4 + 2x_2 x_1^3 - 2x_2 x_1^2 + x_2 x_1 + x_1^4 - 2x_1^3 + 2x_1^2 - x_1, \\ & x_5 + x_4 + x_1^4 - x_1^3 + x_1^2 - 1\} \end{aligned}$$

engendre l'idéal $I_{\underline{\beta}}$ des $\underline{\beta}$-relations de stabilisateur le groupe dihédral $D_5 =< \sigma = (1,5,2,3,4), \tau = (1,3)(2,5) >$ (on a $\mathrm{Gal}_k(\underline{\beta}) = D_5$) et $T_2 = \{x_6^2+1, x_7+x_6\}$ engendre l'idéal $I_{\underline{\gamma}}$ des $\underline{\gamma}$-relations de stabilisateur le groupe S_2. D'après le Théorème 2.4, l'idéal I engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois de stabilisateur $D_5 \times S_2$.

Montrons comment l'algorithme `GaloisIdéal` calcule l'idéal des $\underline{\alpha}$-relations à partir de l'idéal I. Le groupe de Galois de $\underline{\alpha}$ sur $\mathbb{Q}$ est soit $G_1 = D_5 \times S_2$ soit son sous-groupe $G_2 =< \sigma, \tau(6,7) >$ (voir Exemple 2.3). Le polynôme Θ donné ci-dessous vérifie $G_2 = \{\sigma \in G_1 \mid \sigma.\Theta = \Theta\}$:

$$\begin{aligned}\Theta &= x_1^2x_2x_6 + x_1^2x_3x_7 + x_1x_2^2x_7 + x_1x_3^2x_6 + x_2^2x_4x_6 \\ &\quad + x_2x_4^2x_7 + x_3^2x_5x_7 + x_3x_5^2x_6 + x_4^2x_5x_6 + x_4x_5^2x_7.\end{aligned}$$

Nous avons $G_1 = G_2 + \tau G_2$; le polynôme $R = (x - \Theta(\underline{\alpha}))(x - \tau.\Theta(\underline{\alpha}))$ s'appelle une *résolvante G_1-relative de $\underline{\alpha}$ par Θ*. Si cette résolvante possède un facteur simple, alors le groupe de Galois de $\underline{\alpha}$ sur k est contenu dans G_2 (voir, par exemple, [6]); c'est donc G_2. L'ensemble triangulaire $T_1 \cup T_2$ engendrant l'idéal I permet de calculer cette résolvante (voir [2]) :

$$R = x^2 - 47 \qquad .$$

Comme elle est irréductible sur $\mathbb{Q}$, le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$ est G_1 . L'idéal $I_{\underline{\alpha}}$ des $\underline{\alpha}$-relations est donc l'idéal I.

Remarque 3. Si la résolvante R avait eu un facteur linéaire simple $u(x)$ sur $\mathbb{Q}$ alors on aurait eu $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) = G_2$ et $I_{\underline{\alpha}} = I + u(\Theta)\mathbb{Q}[x_1, \ldots, x_n]$ (voir [8]). Le calcul des modules fondamentaux $f_1, \ldots, f_7$ engendrant l'idéal $I_{\underline{\alpha}}$ aurait été rapide puisque, les degrés de chaque polynôme f_i en x_i sont calculables à partir de G_2 (voir [2]). Nous savons ainsi que si nous avions eu $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) = G_2$ alors aurions $\{f_1, \ldots, f_5\} = T_1$, $f_7 = x_7 + x_6$ et f_6 de degré 1 en x_6.

Exemple 2.7. Soit le polynôme $f(x) = x^6 + x^4 + x^2 + 1$ qui se factorise sur $\mathbb{Q}$ en deux facteurs irréductibles $g = x^4 + 1$ et $h = y^2 + 1$. L'ensemble triangulaire $T_1 = \{x_1^4 + 1, x_2 + x_1, x_3 - x_1^3, x_4 + x_1^3\}$ engendre l'idéal l'idéal $I_{\underline{\beta}}$ des $\underline{\beta}$-relations de stabilisateur le groupe $V_4 =< (1,2)(3,4) >$ (donc $\mathrm{Gal}_{\mathbb{Q}}(\underline{\beta}) = V_4$) et $T_2 = \{x_5^2 + 1, x_6 + x_5\}$ engendre l'idéal $I_{\underline{\gamma}}$ des $\underline{\gamma}$-relations de stabilisateur le groupe S_2. D'après le Théorème 2.4, l'idéal I engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois de stabilisateur $V_4 \times S_2$. En factorisant le polynôme h dans $k(\beta_1)$, nous trouvons que $\gamma_1 - \beta_1^2 = \gamma_2 + \beta_1^2 = 0$. Donc l'idéal des $\underline{\alpha}$-relations est engendré par l'ensemble triangulaire $T_1 \cup \{x_5 - x_1^2, x_6 + x_1^2\}$ et son stabilisateur (de cardinal 4) est le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) =< (1,2)(3,4), (5,6)(1,2)(3,4) >$ qui est le seul sous-groupe propre dans $V_4 \times S_2$ pouvant être le groupe de Galois de $\underline{\alpha}$ (voir Lemme 2.2). Ici, pour simplifier la présentation nous n'avons pas utilisé l'algorithme `GaloisIdéal` pour calculer un idéal maximal des relations. Une factorisation de h dans $k(\beta_1)$ suffit puisque $k(\underline{\beta}) = k(\beta_1)$ et que h est un polynôme de degré 2. Mais c'est un cas particulier. En général, il est plus efficace d'utiliser `GaloisIdéal` que de factoriser dans des extensions algébriques dont les degrés sont d'autant plus élevés que le cardinal du groupe de Galois de f est grand (voir [1]).

3. Application

Dans [5], il est construit des idéaux de Galois triangulaires des facteurs de f dans une extension algébrique K de k. Les stabilisateurs de ces idéaux sont également calculés. Le théorème 2.4 appliqué à ces idéaux permet d'en déduire un idéal de Galois I_0 de f sur K ainsi qu'un de ses stabilisateurs L_0. Dans l'article sus-cité, à partir de l'ensemble triangulaire engendrant I_0, il est déduit un ensemble triangulaire T engendrant un idéal de Galois I de f sur k et de L_0, un stabilisateur L de I. Il est ensuite possible d'appliquer l'algorithme `GaloisIdeal` avec $I_1 = I$ afin de calculer un idéal des relations $\mathcal{M}$.

References

[1] Yokoyama, K. Anai, H., Noro, M. Computation of the splitting fields and the galois groups of polynomials. *Progr. Math.*, 143:29–50, 1996.

[2] Valibouze, A. Aubry, P. Using galois ideals for computing relative resolvents. *JSC*, **30**:635–651, 2000.

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

[4] Gómez Molleda, M. A. *Cálculo del Centro de un Grupo de Galois y Applicationes.* PhD thesis, Universidad de Cantabria, 2002.

[5] Valibouze, A. Orange, S., Renault, G. Calcul efficace de corps de dcomposition. *Manuscrit*, 2002.

[6] Stauduhar, R.P. . *The determination of Galois groups*, volume **27**. Math. Comp., 1973.

[7] N. Tchebotarev. *Gründzüge des Galois'shen Theorie.* P. Noordhoff, 1950.

[8] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Journal of the belgian mathematical society Simon Stevin*, pages 507–535, 1999.

LIP6, Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05
E-mail address: *name*@calfor.lip6.fr