RAIRO-Inf. Theor. Appl. **39** (2005) 651-659
DOI: 10.1051/ita:2005034

NOTE SUR LES RELATIONS ENTRE LES RACINES D'UN POLYNÔME RÉDUCTIBLE

Sébastien Orange[1], Guenaël Renault[1]
et Annick Valibouze[1]

Abstract. In this paper, we use reducibility of an univariate polynomial in order to compute efficiently the ideal of relations between its roots.

Résumé. Dans cet article, nous exploitons la réductibilité d'un polynôme d'une variable pour calculer efficacement l'idéal des relations algébriques entre ses racines.

Classification Mathématique. 12F10, 12Y05.

Introduction

Une des méthodes pour calculer une représentation du corps de décomposition K d'un polynôme séparable f à coefficients dans un corps k, supposé calculable, consiste à calculer un élément primitif de K sur k, c'est-à-dire le polynôme minimal sur k d'un tel élément. En effet, si $F(x)$ est ce polynôme en la variable x, nous avons alors :

$$K \simeq k[x]/\langle F(x)\rangle$$

où $\langle F(x)\rangle$ est l'idéal de $k[x]$ engendré par le polynôme $F(x)$. Le degré de F est l'ordre du groupe de Galois G de f sur k. D'une part, ce degré peut prendre des valeurs très élevées (jusqu'à $n!$, où $n = deg(f)$). D'autre part, la méthode classique décrite par Galois pour obtenir le polynôme minimal F est de le déterminer comme facteur irréductible sur k d'un polynôme de degré $n!$ appelé *résolvante de Galois*; cette résolvante est calculée à partir d'un polynôme Θ de n variables $x_1, x_2, \ldots, x_n$ (voir [6]).

Mots Clés. Groupe de Galois, idéal de Galois, polynôme réductible, corps de décomposition.

[1] LIP6, Université Paris VI, 4 place Jussieu, 75252 Paris Cedex 05, France; avb@ccr.jussieu.fr

© EDP Sciences 2005

Article published by EDP Sciences and available at http://www.edpsciences.org/ita or http://dx.doi.org/10.1051/ita:2005034

Il est donc naturel de chercher à représenter autrement le corps K. Nous adoptons donc le point de vue de N. Tchebotarev (voir [10]). Il existe un idéal maximal $\mathcal{M}$ de l'anneau des polynômes $k[x_1, \ldots, x_n]$ en les variables $x_1, \ldots, x_n$ et à coefficients dans k tel que

$$K \simeq k[x_1, x_2, \ldots, x_n]/\mathcal{M}.$$

Cet idéal est appelé *idéal des relations*. Si

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

désigne un ensemble triangulaire séparable l'engendrant, alors

$$\mathrm{Card}(G) = \deg(f_1, x_1) \deg(f_2, x_2) \cdots \deg(f_n, x_n).$$

Le polynôme minimal F se déduit aisément de cet ensemble comme le polynôme caractéristique de l'endomorphisme multiplicatif de $k[x_1, x_2, \ldots, x_n]/\mathcal{M}$ induit par le polynôme Θ.

L'enjeu est donc de pouvoir calculer efficacement l'idéal $\mathcal{M}$. Dans [10], N. Tchebotarev propose de calculer les polynômes $f_i(x_1, \ldots, x_i)$, pour $1 \leq i \leq n$, en factorisant le polynôme f dans des corps intermédiaires compris entre les corps k et K (voir aussi [1]). Cette méthode générale a été améliorée (voir, par exemple, [8]). Elle peut l'être aussi en exploitant les propriétés du polynôme f considéré.

Par exemple, dans [7], l'auteur calcule le centre du groupe de Galois d'un polynôme de $\mathbb{Z}[x]$ afin de déterminer si ce groupe est abélien. Lorsque le polynôme est réductible et que le groupe de Galois de chacun de ses facteurs est abélien, l'auteur calcule efficacement le corps de décomposition.

Dans le présent article, est exploitée la réductibilité du polynôme f. Il y est proposé une méthode générale pour calculer efficacement le corps de décomposition d'un polynôme réductible séparable (*i.e.* sans racine multiple) sur un corps k quelconque ou tout au moins calculable.

Pour ce faire, nous pouvons utiliser l'algorithme `GaloisIdéal` (voir [11]) qui retourne un ensemble triangulaire engendrant l'idéal $\mathcal{M}$ des relations. La méthode utilisée par l'algorithme consiste à construire une chaîne ascendante d'idéaux, 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* du polynôme f (voir [4] ou [10]). Le calcul d'un idéal I_{i+1} à partir de l'idéal I_i nécessite de connaître un ensemble de polynômes engendrant I_i et un *injecteur* L_i de I_i qui est une partie de S_n, le groupe symétrique de degré n (l'injecteur 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 $V(I_i)$ de l'idéal I_i (*i.e.* l'ensemble de ses zéros dans K^n). Lorsque I_1 est l'idéal des relations symétriques, son injecteur est 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 2.2, il sera possible de prendre pour I_1 un idéal de Galois de f dont l'injecteur est de cardinal compris entre les produits $m_1\, m_2\, \ldots\, m_s$ 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.

Le paragraphe 1 comporte des rappels concernant les idéaux de Galois. Le paragraphe 2 présente le résultat principal de cet article (voir Th. 2.2) que nous illustrerons par des exemples.

1. Rappels sur les idéaux de Galois

Notons $\hat{k}$ une clôture algébrique du corps k et posons $\mathcal{A} = k[x_1, \ldots, x_n]$. Posons également $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \hat{k}^n$, un n-uplet des racines distinctes du polynôme f. Les résultats non démontrés de ce paragraphe émanent de [11].

1.1. Idéal des relations et groupe de Galois

Dans $\mathcal{A}$, l'*idéal des $\underline{\alpha}$-relations*

$$\mathcal{M} = \{R \in \mathcal{A} \mid R(\alpha_1, \ldots, \alpha_n) = 0\}$$

est engendré par un ensemble triangulaire de polynômes (voir [2, 10]). Le *groupe de Galois de $\underline{\alpha}$ sur k* est le groupe

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

Le groupe $\mathrm{Gal}_k(\underline{\alpha})$ est isomorphe au groupe des k-automorphismes de K.

1.2. Idéaux de Galois

Pour toute la suite du paragraphe 1, nous fixons L une partie du groupe symétrique S_n. Dans $\mathcal{A}$, l'idéal radical

$$\mathrm{Id}_{\mathcal{A}}(L.\underline{\alpha}) = \{R \in \mathcal{A} \mid (\forall \sigma \in L)\ R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0\}$$

s'annulant sur l'ensemble $L.\underline{\alpha} = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in L\}$ de K est appelé l'$(\underline{\alpha}, L)$-*idéal de Galois* (de l'anneau $\mathcal{A}$) ou, de manière plus générale, un *idéal de Galois du polynôme f* (de l'anneau $\mathcal{A}$).

L'idéal de Galois $\mathrm{Id}_{\mathcal{A}}(S_n.\underline{\alpha})$ est appelé l'*idéal des relations symétriques* (entre les racines de f). En adoptant la notation simplifiée $\mathrm{Id}_{\mathcal{A}}(\underline{\alpha}) = \mathrm{Id}_{\mathcal{A}}(\{\underline{\alpha}\})$, nous avons :

$$\mathcal{M} = \mathrm{Id}_{\mathcal{A}}(\underline{\alpha}) = \mathrm{Id}_{\mathcal{A}}(Gal_k(\underline{\alpha}).\underline{\alpha}).$$

Les idéaux de Galois vérifient le critère de radicalité suivant :

Proposition 1.1. *Si I est un idéal de Galois (donc de dimension 0) de $\mathcal{A}$, alors il vérifie le critère de Seidenberg :*

$$\forall i \in [\![1,n]\!],\ \exists g_i(x_i) \in I \text{ avec } g_i(x_i) \text{ séparable.}$$

Démonstration. L'idéal I contient l'idéal des relations symétriques S qui lui même vérifie le critère de Seidenberg. En effet, l'idéal S contient, pour tout entier i dans $[\![1,n]\!]$, le polynôme $f(x_i)$ qui, par hypothèse, est séparable. □

1.3. Injecteurs

Pour toute la suite du paragraphe 1, nous posons $I = \mathrm{Id}_{\mathcal{A}}(L.\underline{\alpha})$. La partie de S_n

$$\mathrm{Inj}(I,\mathcal{M}) = \{\sigma \in S_n \mid \sigma.I \subset \mathcal{M}\},$$

où $\sigma.I = \{R(x_{\sigma(1)},\ldots,x_{\sigma(n)}) \mid R \in I\}$, est appelée l'*injecteur de I dans $\mathcal{M}$* ou encore l'*injecteur de I relatif à $\underline{\alpha}$* et est alors notée $\mathrm{Inj}(I,\underline{\alpha})$.

L'idéal I est l'*$\underline{\alpha}$-idéal de Galois d'injecteur* $\mathrm{Inj}(I,\underline{\alpha})$ *relatif à* $\underline{\alpha}$. Cet injecteur se déduit de la partie L de S_n par la formule suivante :

$$\mathrm{Inj}(I,\underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})L\ (= \{\, g\, l \mid g \in \mathrm{Gal}_k(\underline{\alpha})\,,\ l \in L\}). \tag{2}$$

Dans le cas particulier de $L = \mathrm{Inj}(I,\underline{\alpha})$, cette dernière égalité donne

$$\mathrm{Inj}(I,\underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})\,\mathrm{Inj}(I,\underline{\alpha}). \tag{3}$$

1.4. Variétés

La variété $V(I) = \{\underline{\beta} \in \hat{k}^n \mid (\forall R \in I)\ \ R(\beta_1,\beta_2,\ldots,\beta_n) = 0\}$ de I dans $\hat{k}^n$ est donnée par :

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

Remarquons que si l'ensemble L ne contient pas l'identité alors $\underline{\alpha}$ n'appartient pas nécessairement à la variété de I. Comme le polynôme f est séparable,

$$\mathrm{Card}(V(I)) = \mathrm{Card}(\mathrm{Inj}(I,\underline{\alpha})). \tag{5}$$

Lorsque, pour tout $\underline{\beta}$ dans la variété de I, l'injecteur $\mathrm{Inj}(I,\underline{\beta})$ est un groupe, il est indépendant du choix de $\underline{\beta}$ dans la variété de I. Nous appelons alors ce groupe l'*injecteur de I* et nous le notons $\mathrm{Inj}(I)$ (dans ce cas, $\mathrm{Inj}(I) = \mathrm{Inj}(I,\mathcal{M}) = \mathrm{Inj}(I,I)$).

Remarque 1. Le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$ est l'injecteur de l'idéal $\mathcal{M}$ des $\underline{\alpha}$-relations et le groupe symétrique S_n est celui de l'idéal des relations symétriques.

2. Idéaux de Galois de polynômes réductibles

Dans ce paragraphe, f sera supposé réductible et nous conviendrons que la donnée d'un idéal de Galois consiste en sa base de Gröbner réduite et de l'un de ses injecteurs. À partir d'idéaux de Galois de chacun des facteurs de f, nous pouvons déduire un idéal de Galois I de f contenant l'idéal des relations symétriques entre les racines de f. Un injecteur et une base de Gröbner de l'idéal I étant connus, l'algorithme `GaloisIdéal` pourra être utilisé pour calculer l'idéal des $\underline{\alpha}$-relations (en prenant $I_1 = I$ comme premier terme de la suite d'idéaux (1)).

Supposons, dans cette partie, que le polynôme f se factorise sur k en deux polynômes g et h de degrés respectifs m et $p = n - m$. Ordonnons le n-uplet $\underline{\alpha}$ des racines de f de telle sorte que $\underline{\beta} = (\alpha_1, \ldots, \alpha_m)$ soit un m-uplet des racines de g et que $\underline{\gamma} = (\alpha_{m+1}, \ldots, \alpha_n)$ soit un p-uplet des racines de h. Posons $\mathcal{B} = k[x_1, \ldots, x_m]$ et $\mathcal{C} = k[x_{m+1}, \ldots, x_n]$ et munissons les anneaux $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ de l'ordre lexicographique induit par $x_1 < x_2 < \ldots < x_m < x_{m+1} < \ldots < x_n$. Dans la suite de cet article, les bases de Gröbner considérées le seront toujours relativement à cet ordre.

Nous avons le résultat bien connu suivant :

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

Dans cette partie, nous allons démontrer le résultat plus général suivant :

Théorème 2.2. *Soient G une partie de S_m et H une partie de S_p. Si G (resp. H) est l'injecteur de l'idéal $\mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})$ (resp. $\mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})$) relativement à $\underline{\beta}$ (resp. $\underline{\gamma}$) alors l'$\underline{\alpha}$-idéal de Galois $\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$ possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$ et il vérifie :*

$$\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha}) = \mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})\,\mathcal{A} + \mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})\,\mathcal{A}. \tag{6}$$

De plus, si $\mathcal{G}_1$ et $\mathcal{G}_2$ sont des bases de Gröbner respectives des idéaux $\mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})$ et $\mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})$ alors $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ est une base de Gröbner de l'idéal $\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$.

Démonstration. Posons $I_1 = \mathrm{Id}_{\mathcal{B}}(G.\underline{\beta})$, $I_2 = \mathrm{Id}_{\mathcal{C}}(H.\underline{\gamma})$ et $J = I_1\mathcal{A} + I_2\mathcal{A}$. Montrons que $J = \mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$.

Puisque G (resp. H) est l'injecteur de I_1 (resp. I_2) relatif à $\underline{\beta}$ (resp. $\underline{\gamma}$), nous avons, d'après (4),

$$V(I_1) = G.\underline{\beta} = \{(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(m)}) \mid \sigma \in G\}, \text{ (resp. } V(I_2) = H.\underline{\gamma}).$$

Donc $V(I_1\mathcal{A}) = \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}, u_1, \ldots, u_p) \mid \sigma \in G,\ u_i \in \hat{k}\}$ et $V(I_2\mathcal{A}) = \{(v_1, \ldots, v_m, \alpha_{\tau(m+1)}, \ldots, \alpha_{\tau(n)}) \mid \tau \in H,\ v_i \in \hat{k}\}$. Ainsi,

$$V(J) = V(I_1\mathcal{A} + I_2\mathcal{A}) = V(I_1\mathcal{A}) \cap V(I_2\mathcal{A}) = (G \times H).\underline{\alpha}. \tag{7}$$

Le radical de l'idéal J est donc l'idéal de Galois $\mathrm{Id}_{\mathcal{A}}((G \times H).\underline{\alpha})$ qui, d'après les identités (4) et (7), possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$. Il reste donc à

démontrer que l'idéal J, de dimension 0, est radical. Pour ce faire, nous allons montrer qu'il vérifie le critère de radicalité de Seidenberg (voir, par exemple, Lem. 8.13 dans [3]).

D'après la proposition 1.1, les idéaux de Galois I_1 et I_2 vérifient le critère de Seidenberg dans, respectivement, $\mathcal{B}$ et $\mathcal{C}$. Ainsi, pour tout entier i dans $[\![1, m]\!]$ (resp. $[\![m+1, n]\!]$), il existe un polynôme séparable $g_i(x_i)$ dans I_1 (resp. I_2) et donc dans J. Ainsi, l'idéal J vérifie le critère de Seidenberg.

Montrons que $\mathcal{G}_1 \cup \mathcal{G}_2$ est une base de Gröbner de J. Rappelons que, puisque $\mathcal{G}_1$ est une base de Gröbner de I_1, idéal radical, nous avons :

$$\mathrm{Dim}(\mathcal{B}/I_1) = \mathrm{Card}(V(I_1)) = \mathrm{Card}(\{\underline{x}^{\underline{a}} \in \mathcal{B} \,|\, \underline{a} \notin \mathrm{In}(\mathcal{G}_1) + \mathbb{N}^m\}), \tag{8}$$

où $\underline{x}^{\underline{a}} = x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}$ et $\mathrm{In}(\mathcal{G}_1)$ est l'ensemble des exposants des monômes initiaux (pour l'ordre lexicographique) de $\mathcal{G}_1$. Il en va de même pour I_2 et de toute base de Gröbner de J.

De plus, d'après l'égalité (5), nous avons $\mathrm{Card}(G) = \mathrm{Card}(V(I_1))$, de même pour I_2 et H, ainsi que pour J et $G \times H$. D'après l'égalité (8), il vient alors :

$$\mathrm{Card}(G \times H) = \mathrm{Card}(G)\,\mathrm{Card}(H) = \mathrm{Card}(\{\underline{x}^{\underline{a}} \in \mathcal{A} \,|\, \underline{a} \notin \mathrm{In}(\mathcal{G}_1 \cup \mathcal{G}_2) + \mathbb{N}^n\})\,.$$

Si $\mathcal{G}_1 \cup \mathcal{G}_2$, qui engendre J, n'était pas une base de Gröbner de J, nous aurions nécessairement la contradiction :

$$\mathrm{Card}(G \times H) = \mathrm{Card}(\{\underline{x}^{\underline{a}} \in \mathcal{A} \,|\, \underline{a} \notin \mathrm{In}(\mathcal{G}_1 \cup \mathcal{G}_2) + \mathbb{N}^n\})$$

$$> \mathrm{Dim}(\mathcal{A}/J) = \mathrm{Card}(V(J)) = \mathrm{Card}(G \times H)\,.$$

Par conséquent, $\mathcal{G}_1 \cup \mathcal{G}_2$ est une base de Gröbner de J. □

D'après ce théorème, des idéaux de Galois de chacun des facteurs du polynôme f, se déduit un idéal de Galois I de f vérifiant :

$$\mathrm{Card}(\mathrm{Gal}_k(\underline{\beta}))\,\mathrm{Card}(\mathrm{Gal}_k(\underline{\gamma})) \leq \mathrm{Card}(V(I)) \leq m!\,p!.$$

À partir de cet idéal, pourra être construit l'idéal maximal $\mathcal{M}$.

Définition 2.3. Un sous-ensemble T de $k[x_1, \dots, x_n]$ est dit *triangulaire* si T est constitué de n polynômes $f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, x_2, \dots, x_n)$ tels que le plus grand monôme de f_i pour l'ordre lexicographique soit de la forme $x_i^{d_i}$ où $d_i \in \mathbb{N}^*$.

Remarquons que, si un ensemble de générateurs d'un idéal de $k[x_1, \dots, x_n]$ est triangulaire, il constitue une base de Gröbner de cet idéal.

Remarque 2.

- Par induction, le théorème 2.2 se généralise au cas où f se factorise en plus de deux facteurs.

- Lorsque $\mathcal{G}_1$ et $\mathcal{G}_2$ sont des ensembles triangulaires, l'union $\mathcal{G}_1 \cup \mathcal{G}_2$ l'est également car les monômes initiaux sont premiers deux-à-deux ; elle constitue donc une base de Gröbner de l'idéal J.
- Le théorème 2.2 généralise le résultat d'A. Colin qui établit l'identité (6) lorsque $G = \mathrm{Gal}_k(\underline{\beta})$, $H = \mathrm{Gal}_k(\underline{\gamma})$ et $G \times H = \mathrm{Gal}_k(\underline{\alpha})$ (voir [5]).

Nous présentons maintenant quelques exemples.

2.1. Exemples

Les polynômes des exemples ci-après ont 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/`. Le lemme suivant est utilisé dans les exemples de ce paragraphe ; nous l'utilisons sans y faire référence.

Lemme 2.4. *Si g et h sont k-irréductibles alors les $Gal_k(\underline{\alpha})$-orbites de $\{1,\dots,n\}$ sont $\{1,2,\dots,m\}$ et $\{m+1,m+2,\dots,n\}$.*

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

Pour la suite, posons $m = 5$ et $p = 2$.

Exemple 2.5. Soient les polynômes $\mathbb{Q}$-irréductibles $g = x^5-x^4-4x^3+3x^2+3x-1$, $h = x^2+1$ et $f = gh$. L'ensemble

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

engendre l'idéal $\mathrm{Id}_{\mathcal{B}}(\underline{\beta})$ des $\underline{\beta}$-relations dont l'injecteur $\mathrm{Gal}_{\mathbb{Q}}(\underline{\beta})$ est le groupe cyclique $C_5 = \langle(1,3,2,4,5)\rangle$. L'ensemble $T_2 = \{x_6^2+1, x_7+x_6\}$ engendre l'idéal $\mathrm{Id}_{\mathcal{C}}(\underline{\gamma})$ des $\underline{\gamma}$-relations d'injecteur le groupe symétrique $S_2 = \mathrm{Gal}_{\mathbb{Q}}(\underline{\gamma})$. L'ensemble triangulaire T_1 se calcule rapidement en factorisant le polynôme g dans son corps de rupture de degré 5.

Comme le groupe $C_5 \times S_2$ n'a pas de sous-groupe propre dont l'action sur $\{1,2,\dots,7\}$ ait une orbite de longueur 5(=deg(g)) et une de longueur 2(=deg(h)), nous avons nécessairement $\mathrm{Gal}_k(\underline{\alpha}) = C_5 \times S_2$ (voir Lems. 2.1 et 2.4). D'après le théorème 2.2, appliqué à $G = C_5$ et $H = S_2$, l'idéal I de $\mathcal{A}$ engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois d'injecteur $C_5 \times S_2$. Comme $C_5 \times S_2$ est le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$, l'idéal I est celui des $\underline{\alpha}$-relations $\mathcal{M}$.

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

$$\begin{aligned} T_1 = \{&x_1^5 - 2x_1^4 + 2x_1^3 - x_1^2 + 1,\\ &x_2^2 + (-x_1^4 + x_1^3 - x_1^2 + x_1 - 1)x_2 - x_1 + 1,\\ &x_3 + x_2 - x_1^4 + x_1^3 - x_1^2 + x_1 - 1,\\ &x_4 - x_2x_1^4 + 2x_2x_1^3 - 2x_2x_1^2 + x_2x_1 + x_1^4 - 2x_1^3 + 2x_1^2 - x_1,\\ &x_5 + x_4 + x_1^4 - x_1^3 + x_1^2 - 1\} \end{aligned}$$

engendre l'idéal I_1 des $\underline{\beta}$-relations d'injecteur le groupe dihédral $D_5 = \langle \sigma = (1,5,2,3,4),\ \tau = (1,3)(2,5)\rangle$ et $T_2 = \{x_6^2 + 1, x_7 + x_6\}$ engendre l'idéal I_2 des $\underline{\gamma}$-relations d'injecteur le groupe S_2.

Le seul sous-groupe propre de $D_5 \times S_2$ qui admette une orbite de longueur 5 et une de longueur 2 est le groupe $G_2 = \langle \sigma, \tau(6,7)\rangle$. Le groupe de Galois $\mathrm{Gal}_k(\underline{\alpha})$ est donc ou bien $G_1 = D_5 \times S_2$ ou bien G_2.

L'idéal I engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois d'injecteur $D_5 \times S_2$ (voir Théor. 2.2). Montrons comment, à partir de I, l'algorithme `GaloisIdéal` calcule l'idéal des $\underline{\alpha}$-relations. Le polynôme Θ donné ci-dessous vérifie $G_2 = \{\sigma \in G_1 \mid \sigma.\Theta = \Theta\}$:

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

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 linéaire simple sur $\mathbb{Q}$ alors le groupe de Galois de $\underline{\alpha}$ sur k est contenu dans G_2 (c'est un résultat anciennement connu : par exemple, dans [9], l'auteur l'utilise pour déterminer le groupe de Galois) ; il s'agit donc de G_2. L'ensemble triangulaire $T_1 \cup T_2$ qui engendre l'idéal I est utilisé pour calculer cette résolvante (voir [2]) :

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

Comme le polynôme R est irréductible sur $\mathbb{Q}$, le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$ est G_1 et l'idéal $\mathcal{M}$ est donc l'idéal I.

3. Application

Dans [8], sont construits des idéaux de Galois des facteurs de f dans une extension algébrique K de k. Les injecteurs de ces idéaux sont également calculés. Le théorème 2.2 appliqué à ces idéaux permet d'en déduire un idéal de Galois I_0 de f sur K ainsi qu'un de ses injecteurs L_0. Dans l'article sus-cité, à partir de l'ensemble engendrant I_0, il est déduit un ensemble T engendrant un idéal de Galois I de f

sur k et de l'injecteur L_0 est déduit un injecteur L de I. Il est ensuite possible d'appliquer l'algorithme `GaloisIdéal` à l'idéal $I_1 = I$ afin de calculer un idéal des relations $\mathcal{M}$.

Remerciements. Nous remercions le rapporteur anonyme pour ses remarques qui nous ont permis d'améliorer le contenu de cet article.

Références

[1] 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)*. Birkhäuser, Basel, *Progr. Math.* **143** (1996) 29–50.

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

[3] T. Becker and V. Weispfenning, *Gröbner bases*, Springer-Verlag, New York, A computational approach to commutative algebra, in cooperation with H. Kredel, *Grad. Texts in Math.* **141** (1993).

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

[5] A. Colin, *Théorie des invariants effective. Application à la théorie de Galois et à la résolution de système Algébrique. Implantation en AXIOM*. Ph.D. Thesis, École Polytechnique (1997).

[6] É. Galois, *Œuvres mathématiques*. Gauthier-Villars, Paris (1897).

[7] M.A. Gomez-Molleda, *Cálculo del Centro de un Grupo de Galois y Applicationes*. Ph.D. Thesis, Universidad de Cantabria (2002).

[8] S. Orange, G. Renault and A. Valibouze, Calcul efficace d'un corps de décomposition. Publication interne LIP6 2003.005, LIP6, Laboratoire d'Informatique de Paris 6, 2003. `http ://www.lip6.fr/reports/lip6.2003.005.html`

[9] R. Stauduhar, The determination of Galois groups. *Math. Comp.* **27** (1973) 981–996.

[10] N. Tchebotarev, *Gründzüge des Galois'shen Theorie*, edited by P. Noordhoff (1950).

[11] A. Valibouze, Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin* **6** (1999) 507–535.

Communiqué par C. Choffrut.
Reçu le 4 mars, 2004. Accepté le 1er novembre, 2004.