Gröbner base of the alternated galoisian ideal

Annick Valibouze

Dépôt HAL le 20 Février 2009
Equipe APR- Laboratoire LIP6 - UPMC
corrections de coquilles : 21/02/09

BASE DE GRÖBNER DE L'IDÉAL GALOISIEN DU GROUPE ALTERNÉ

ANNICK VALIBOUZE

1. Introduction

Cet article propose une méthode algébrique efficace et simple pour obtenir une base de Gröbner engendrant l'idéal galoisien des relations alternées d'un polynôme univarié séparable de groupe de Galois pair. Dès que le degré du polynôme s'élève, les méthodes algébriques utilisées pour les autres groupes que le groupe alterné deviennent impraticables (voir Paragraphe 6.2). En revanche, dans le cas du polynôme non séparable x^n, nous disposons d'une formule pour l'idéal alors appelé idéal de Hilbert du groupe alterné (voir [8]).

Nous fixons un polynôme univarié f unitaire, de degré n, sans racine multiple et à coefficients dans un corps k. Nous posons $a = (a_1, a_2, \ldots, a_n)$, un n-uplet formé des n racines distinctes de f. Nous fixons $x_1, \ldots, x_n$ des variables algébriquement indépendantes sur k.

2. Le groupe de Galois et l'idéal des relations

L'ensemble

$$\mathfrak{M} = \{r \in k[x_1, \ldots, x_n] \mid r(a) = 0\}$$

s'appelle l'*idéal des a-relations*. C'est un idéal maximal, noyau du morphisme d'évaluation entre $k[x_1, \ldots, x_n]$ et le corps $k(a_1, \ldots, a_n)$ des racines de f qui à x_i associe a_i. Le corps $k(a_1, \ldots, a_n)$ est donc isomorphe à $k[x_1, \ldots, x_n]/\mathfrak{M}$.

Date: February 23, 2009.
[0]*AMS Subject Classification 2000:* 12F10 12Y05 11Y40.
Keywords: Galois group, galoisian ideal, triangular ideal, splitting field, alternating group.

Le groupe symétrique S_n de degré n agit naturellement sur $k[x_1,\ldots,x_n]$ par permutation sur les indices : pour $s \in S_n$ et $p \in k[x_1,\ldots,x_n]$, cette action est notée $s.p$. Soit L un sous-ensemble de S_n, la notation $L.p$ désigne l'orbite de p sous l'action de L. Soit $E \in k[x_1,\ldots,x_n]$, la notation $s.E$ désigne l'ensemble des $s.e$ où e parcourt E.

Le *groupe de Galois* G de a sur k est le groupe laissant globalement $\mathfrak{M}$ invariant :

$$G = \{s \in S_n \mid s.\mathfrak{M} = \mathfrak{M}\} \quad .$$

3. Idéaux galoisiens

Un idéal I de $k[x_1,\ldots,x_n]$ est dit *galoisien* associé à f s'il s'exprime sous la forme :

$$I \;=\; \{r \in k[x_1,\ldots,x_n] \mid L.r \subset \mathfrak{M}\}$$

où L est un sous-ensemble de S_n. On dit que L *défini* I (cette définition dépend du choix de l'idéal maximal $\mathfrak{M}$). Le *groupe de décomposition* $Gr(I)$ de I est l'ensemble des permutations envoyant globalement I dans I :

$$Gr(I) = \{s \in S_n \mid \; s.I \subset I\} \quad ;$$

il contient le groupe de Galois G à la condition nécessaire et suffisante qu'il définisse l'idéal I qui est alors dit *pur* (voir [7]). Par exemple, l'idéal $\mathfrak{M}$ est pur de groupe de décomposition G.

Definissons la suite $L_{(0)} = L$ et pour $i = 1,\ldots,n$

$$L_{(i)} = \{s \in L_{(i-1)} \mid s(i) = i\} \quad .$$

Nous avons la proposition suivante :

Proposition 3.1. *(voir* [1]*) Soit I un idéal galoisien pur. Alors il est engendré par un ensemble triangulaire séparable $f_1(x_1), f_2(x_1,x_2), \ldots, f_n(x_1,x_2,\ldots,x_n)$ formant une base de Gröbner pour l'ordre lexicographique avec l'ordre $x_1 < x_2 < \cdots < x_n$ sur les variables. Pour tout $a = (a_1,\ldots,a_n)$ dans la variété de I, les racines de $f_i(a_1,\ldots,a_{i-1},x)$ sont les $a_{\tau(i)}$ où τ parcourt $L_{(i-1)}/L_{(i)}$. Les degrés initiaux de la base de Gröbner sont*

$$deg_{x_i} f_i = \frac{card(L_{(i-1)})}{card(L_{(i)})} \quad . \tag{1}$$

4. L'idéal des relations symétriques

L'*idéal $\mathcal{S}$ des relations symétriques* est l'idéal galoisien défini par le groupe symétrique S_n:

$$\mathcal{S} = \{r \in k[x_1, \ldots, x_n] \mid r(a_{s(1)}, \ldots, a_{s(n)}) = 0 \quad \forall s \in S_n\} \quad ;$$

c'est un idéal galoisien pur de groupe de décomposition S_n ; il ne dépend pas du choix de $\mathfrak{M}$. Comme pour $i = 1, \ldots, n$ $card((S_n)_{(i)}) = (n-i)!$, cet l'idéal est engendré par un ensemble triangulaire séparable dont les degrés initiaux sont respectivement $n, n-1, \ldots, 2, 1$.

Définissons les *modules de Cauchy* de f (voir [2]) : le premier module de Cauchy de f est le polynôme $C_1(x_1) = f(x_1)$ et, par induction, pour $r = 1, \ldots, n-1$, son $(r+1)$-ième module de Cauchy est le polynôme

$$C_{r+1} = C_{r+1}(x_1, \ldots, x_{r+1}) = \frac{C_r(x_1, \ldots, x_{r-1}, x_{r+1}) - C_r(x_1, \ldots, x_{r-1}, x_r)}{x_{r+1} - x_r} \quad .$$

Pour tout entiers i et j, nous notons a_i le coefficient de x^i dans f et $h_i(x_1, \ldots, x_j)$ la somme des monômes de degré total i en $x_1, \ldots, x_j$. Sur $k[x_1, \ldots, x_n]$, les modules de Cauchy s'expriment sous la forme

$$C_{r+1} = \sum_{i=r}^{n} a_i h_{r-i}(x_1, x_2, \ldots, x_{r+1}) \quad r = 0, \ldots, n-1 \quad ; \tag{2}$$

ils forment un ensemble triangulaire séparable engendrant $\mathcal{S}$ (voir [5]) ; effectivement, ils forment un ensemble triangulaire séparable de polynômes appartenant à $\mathcal{S}$ tels que

$$deg_{x_1} C_1 = n \quad , deg_{x_2} C_2 = n-2 \quad , \ldots , deg_{x_n} C_n = 1 \quad . \tag{3}$$

L'idéal des relations symétriques se décompose avec des idéaux galoisiens conjugués. En effet, soit L un groupe contenant le groupe G, définissant un idéal galoisien I et $\tau_1, \ldots, \tau_e$ une transversale à droite de S_n modulo L. Alors

$$\mathcal{S} = \bigcap_{i=1}^{e} \tau_i^{-1}.I \quad . \tag{4}$$

Pour toute permutation σ, le groupe de décomposition de $\sigma.I$ est le groupe $\sigma L \sigma^{-1}$ contenant le groupe de Galois $\sigma G \sigma^{-1}$ de $(a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)})$.

Remarque 1. Supposons qu'un idéal galoisien soit défini par A_n, le groupe alterné de degré n, et que le groupe de Galois G ne soit pas pair. Dans ce cas, puisque $S_n = GA_n$ et que GA_n définit également l'idéal, il s'identifie à $\mathcal{S}$.

5. Idéal des relations alternées

Définition 5.1. L'*idéal des relations alternées* est l'idéal galoisien pur associé à un polynôme de groupe de Galois pair dont le groupe de décomposition est le groupe alterné.

Pour toute la suite, nous supposons que le groupe de Galois de f sur k est pair, c'est-à-dire un sous-groupe du groupe alterné A_n. Nous supposons que I est l'idéal des relations alternées.

D'après l'identité (4), nous avons

$$\mathcal{S} = I \cap \tau.I$$

où $\tau = (n, n-1) = \tau^{-1}$ et le groupe de décomposition de $\tau.I$ est $A_n = \tau A_n \tau^{-1}$.

Il existe donc deux idéaux galoisiens alternés ; celui que nous considérons est fixé par le choix $I \subset \mathfrak{M}$.

Nous avons $(A_n)_{(i)} = (S_n)_{(i)}$ pour $i = 0 \dots n-3$ et $(A_n)_{(n-2)}$ est le groupe identité. D'après les identité (1) et (3), les degrés initiaux de I et de $\tau.I$ sont

$$n, n-1, \dots, 3, 1, 1.$$

Par conséquent, il existe sur k un polynôme $G = G(x_1, \dots, x_{n-1})$ (resp. $H(x_1, \dots, x_{n-1})$) de degré 1 en x_{n-1} tel que l'idéal I (resp. $\tau.I$) soit engendré par l'ensemble triangulaire

$$C_1, C_2, \dots, C_{n-2}, G, C_n$$

(resp. $C_1, C_2, \dots, C_{n-2}, H, C_n$). Puisque les modules de Cauchy sont donnés par la formule (2), l'objectif que nous poursuivons est celui du calcul du polynôme G.

Soit a dans la variété de I. Le $(n-2)$-uplet $(a_1, \dots, a_{n-2})$ appartenant à la variété de l'idéal $< C_1, \dots, C_{n-2} >$, il peut s'agir de tout $(n-2)$-uplet de racines disctinctes de f.

Posons

$$g = G(a_1, \dots, a_{n-2}, x) \quad \text{et } h = H(a_1, \dots, a_{n-2}, x) \quad .$$

D'après la proposition 3.1, nous avons $g = x - a_{n-1}$, $h = x - a_n$ et

$$C_{n-1}(a_1, \dots, a_{n-2}, x) = g.h \quad .$$

Nous allons chercher à obtenir a_{n-1} sous la forme d'une expression polynomiale en $a_1, \dots, a_{n-2}$ sur k.

6. Calcul d'une base de Gröbner de l'idéal des relations alternées

6.1. **Le Vandermonde.**

Considérons le (déterminant de) *Vandermonde* :

$$V(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \quad .$$

Le groupe alterné A_n est le stabilisateur du Vandermonde dans S_n ; en d'autres termes, V est un invariant absolu de A_n. Le *Vandermonde associé à un polynôme* $F = \lambda \prod_{1 \leq i \leq n}(x - b_j)$ est donné par :

$$v(F) = V(b_1, b_2, \ldots, b_n)$$

et le discriminant du polynôme F s'identifie à

$$\lambda^{2(n-1)} v(F)^2 \quad .$$

Ayant supposé f unitaire, son discriminant est $v(f)^2$.

Rappelons cette proposition bien connue :

Proposition 6.1. *Le groupe de Galois sur le corps k d'un polynôme univarié sur k sans racine multiple est pair si et seulement si son discriminant est un carré dans k ou, autrement dit, si son Vandermonde appartient à k.*

Remarque 2. Cette proposition est aussi un corollaire du théorème disant que la spécialisation d'un invariant absolu séparable d'un groupe H en les racines $a_1, \ldots, a_n$ de f appartient au corps k si et seulement si le groupe Galois G de a sur k est un sous-groupe de H (voir [6]). Comme les racines de f sont distinctes, le Vandermonde $v(f)$ est toujours séparable.

6.2. **Méthodes connues.**

Factorisation dans une extension :
Lorsque $G = A_n$, le corps $K = k(a_1, \ldots, a_{n-2})$ est isomorphe à l'anneau quotient

$$k[x_1, \ldots, x_{n-2}] / < C_1, \ldots, C_{n-2} > \quad .$$

Au delà d'un certain degré, il est vain de pouvoir calculer g en factorisant $c_{n-1}(x)$ dans K puisque ce corps est de degré $n!/2 = card(A_n)$ sur k.
Lorsque $G \neq A_n$, le corps K n'est pas connu et la base de Gröbner de l'idéal I intervient dans son calcul (voir l'algorithme GaloisIdeal dans [7]).

Algorithme général de calcul de base de Gröbner
Il s'agit d'appliquer le théorème 3.27 de [7] :

$$I = \mathcal{S} + < V - v(f) > \quad ;$$

les générateurs de I sont donc $V - v(f)$ et les modules de Cauchy de f ; l'importance du polynôme V qui comporte $n!/2$ monômes fait renoncer à déduire une base de Gröbner à partir de ces générateurs.

Autres
Il reste les méthodes numériques et p-adiques (voir [10] ou bien [9]) ou encore interpolatrices (voir [4] et [3]) mais non applicables lorsque les coefficients de f sont non numériques.

6.3. **La descente des Vandermondes.**

Pour $r = 1, \ldots, n-1$, posons

$$c_r(x) = C_r(a_1, \ldots, a_{r-1}, x)$$

et notons v_r le Vandermonde associé au polynôme c_r. Puisque f est unitaire, nous avons (voir Proposition 3.1) :

$$c_r(x) = \prod_{i \le j \le n} (x - a_j) \quad \text{et} \tag{5}$$

$$v_r = \prod_{r \le i < j \le n} (a_i - a_j) \quad ; \tag{6}$$

le discriminant de c_r est v_r^2.

Le théorème suivant généralise la proposition 6.1 :

Théorème 6.2. *Soient $C_1, \ldots, C_n$ les modules de Cauchy d'un polynôme f de $k[x]$, de degré n, de groupe de Galois pair et de racines $a_1, \ldots, a_n$ deux-à-deux distinctes. Alors, pour $r = 1, \ldots, n-1$, le discriminant de $c_r(x) = C_r(a_1, \ldots, a_{r-1}, x)$ est un carré dans $k(a_1, \ldots, a_{r-1})$ ($= k$ pour $r = 1$).*

Le théorème découle du lemme suivant :

Lemme 6.3. *Sous les hypothèses du théorème, pour $r = 2, \ldots, n-1$, nous avons*

$$v_r = \frac{v_1}{c_2(a_1) c_3(a_2) \cdots c_r(a_{r-1})} \quad . \tag{7}$$

Démonstration. Puisque les racines $a_1, \ldots, a_n$ de f sont deux-à-deux distinctes et d'après la formule (5), nous avons

$$c_r(a_{r-1}) = \prod_{r \le j \le n} (a_{r-1} - a_j) \neq 0 \quad .$$

Et avec l'identité (6), nous obtenons la formule suivante d'où découle le résultat :

$$v_{r-1} = v_r . \prod_{r \le j \le n} (a_{r-1} - a_j) = v_r . c_r(a_{r-1}) \quad . \tag{8}$$

□

Démonstration. (Théorème 6.2) Soit $r \in [2, \ldots, n-1]$. Montrons que $v_r \in k(a_1, \ldots, a_{r-1})$. Comme le groupe de Galois de f $(= c_1(x))$ est pair, son discriminant, le carré de $v(f)$ $(=v_1)$, appartient à k. D'après (7), v_r appartient donc au corps $k(a_1, \ldots, a_{r-1})$. □

Nous sommes donc en mesure de calculer v_{n-1} sur $k(a_1, \ldots, a_{n-2})$ avec (7) pour $r = n-1$ ou, ce qui revient au même, en utilisant la formule récurrente suivante (voir 8):

$$v_r = \frac{v_{r-1}}{c_r(a_{r-1})} \quad r = 2, \ldots, n-1 \tag{9}$$

qui donne son nom *descente des Vandermonde* à la méthode proposée ici. Nous préférons concevoir la méthode reposant sur les calculs successifs de $v_1, v_2, \ldots, v_{n-1}$ qui présente l'avantage de décomposer les calculs et de fournir les Vandermondes associés aux polynômes $c_2, \ldots c_{n-1}$.

Nous connaissons la somme $a_{n-1} + a_n =$-coeff(c_{n-1}, x) comme expression polynomiale en $a_1, \ldots, a_{n-2}$ sur k et la différence $a_{n-1} - a_n = v_{n-1}$ sur $k(a_1, \ldots, a_{n-2})$. Donc

$$a_{n-1} = \frac{v_{n-1} - \text{coeff}(c_{n-1}, x)}{2} \quad .$$

Ainsi, pour calculer a_{n-1} comme expression polynomiale en $a_1, \ldots, a_{n-2}$ sur k, il ne reste qu'à calculer les inverses des $c_r(a_{r-1})$ dans $k(a_1, \ldots, a_{r-2})$. C'est à cette question qu'est consacré le paragraphe suivant.

6.4. **Inversion dans $k[x_1, \ldots, x_n]/\mathcal{S}$.**

Nous cherchons à inverser $c_{r+1}(a_r)$ pour un certain $r \in [1, n-2]$. Le procédé est classique dés lors que certaines conditions sont satisfaites. Ce paragraphe décrit le procédé tout en vérifiant à chaque étape les contraintes nécessaires à son fonctionnement.

Nous aurons à calculer dans l'anneau quotient

$$K = k[x_1, \ldots, x_r]/ < C_1, \ldots, C_r > \quad .$$

Proposition 6.4. *Pour tout $a \in V(\mathcal{S})$ et tout $r = 1, \ldots, n-2$, nous avons*

$$pgcd(C_{r+1}(a_1, \ldots, a_{r-1}, x_r, x_r), C_r, x_r) = 1 \tag{10}$$

et il existe des polynômes $U, U_1, \ldots, U_r$ dans $k[x_1, \ldots, x_r]$ tels que

$$UC_{r+1}(x_1, \ldots, x_r, x_r) + \sum_{i=1}^{r} U_i C_i(x_i) = 1 \quad . \tag{11}$$

Démonstration. Rappelons que pour tout s l'ensemble des solutions de $C_1, \ldots, C_s$ est constitué de tout s-uplet de racines distinctes de f. Le polynôme $C_{r+1}(x_1, \ldots, x_r, x_r)$ est la dérivée en x_r du module de Cauchy C_r. Comme $C_1, C_2, \ldots, C_r$ est un ensemble triangulaire séparable, le polynôme $C_r(a_1, \ldots, a_{r-1}, x_r)$ et sa dérivée n'ont aucune racine en commun pour tout $(r-1)$-uplet $(a_1, \ldots, a_{r-1})$ de racines distinctes de f. Donc, non seulement la première identité est vérifiée mais aussi, l'idéal $< C_{r+1}(x_1, \ldots, x_r, x_r), C_1, \ldots, C_r >$ ne possédant aucune solution, nous obtenons la deuxième identité par le Nullstellenstatz de Hilbert. □

Nous cherchons le polynôme U de l'identité (11) puisque, dans K, nous avons

$$UC_{r+1}(x_1, \ldots, x_r, x_r) = 1 \quad ;$$

soit pour tout $a \in V(\mathcal{S})$, $\frac{1}{c_{r+1}(a_r)}$ s'exprime comme une expression polynomiale en $a_1, \ldots, a_r$ avec

$$\frac{1}{c_{r+1}(a_r)} = U(a_1, \ldots, a_r) \quad .$$

Afin d'alléger les notations, dans toute la suite, nous noterons \$ toute fraction rationnelle dans $k(x_1, \ldots, x_r)$ dont la valeur et le nom ne nous importe pas et, pour tout $s \in [1, n]$, pour tout n-uplet $(a_1, \ldots, a_n)$ fixé dans $V(\mathcal{S})$ et tout polynôme $Q \in k[x_1, \ldots, x_s]$, nous posons

$$q(x_s) = Q(a_1, \ldots, a_{s-1}, x_s) \quad .$$

Théorème 6.5. *Pour tout $r = 1, \ldots, n-2$, en posant*

$$P_r = C_{r+1}(x_1, \ldots, x_{r-1}, x_r, x_r) \quad ,$$

il est possible de construire trois suites finies $(P_r, \ldots, P_1, P_0 = 1)$, $(N_r, \ldots, N_1)$, $(D_r = P_r, D_{r-1}, \ldots, D_1, D_0 = 1)$ selon le processus inductif suivant : pour tout $i \in [1, r]$ et pour tout $a \in V(\mathcal{S})$

- $P_i, N_i, D_i \in k[x_1, \ldots, x_i]$;
- $pgcd_{x_i}(P_i(a_1, \ldots, a_{i-1}, x_i), C_i(a_1, \ldots, a_{i-1}, x_i)) = 1 \quad ;$
- $N_i P_i(x_1, \ldots, x_i) + \$C_i(x_1, \ldots, x_i) = D_{i-1} \quad ;$
- *le degré en x_i de N_i est strictement inférieur à celui de C_i ;*
- $N_i(a_1, \ldots, a_i) \neq 0$ *et* $P_i(a_1, \ldots, a_i) = D_i(a_1, \ldots, a_i) \neq 0 \quad ;$
- *si $i > 1$ alors P_{i-1} est défini comme la réduction de D_{i-1} modulo $< C_1, \ldots, C_{i-1} >$.*

Démonstration. Montrons d'abord que les propriétés du théorème sont satisfaites pour $i = r$. En accord avec la proposition 6.4, par l'algorithme d'Euclide étendu appliqué à P_r et C_r

en x_r, nous considérons $N_r \in k[x_1, \ldots, x_{r-1}, x_r]$ de telle sorte que $\deg_{x_r}(N_r) < \deg_{x_r}(C_r)$ et $D_{r-1} \in k[x_1, \ldots, x_{r-1}]$ tels que

$$\frac{N_r}{D_{r-1}} P_r + \$C_r = 1 \quad .$$

Soit

$$N_r P_r + D_{r-1} \$C_r = D_{r-1} \quad . \tag{12}$$

Fixons $a \in V(\mathcal{S})$ et supposons par l'absurde que $d_{r-1}(a_{r-1}) = 0$; l'ensemble des racines de $c_r(x)$ est constitué des racines de f distinctes de $a_1, \ldots, a_{r-1}$. Soit b une racine de $c_r(x)$. Puisque $p_r(b) \neq 0$ (voir Identité (10)), avec l'identité (12), nous aboutissons nécessairement à l'identité $n_r(b) = 0$; ce qui est impossible puisque les racines de c_r sont distinctes et que le degré de n_r est strictement inférieur à celui de c_r. Donc pour tout $a \in V(\mathcal{S})$

$$p_{r-1}(a_{r-1}) = d_{r-1}(a_{r-1}) \neq 0$$

et $pgcd(p_{r-1}(x_{r-1}), c_{r-1}(x_{r-1})) = 1$. De plus, comme $d_{r-1}(a_{r-1}) \neq 0$, nous avons

$$n_r(a_r) \neq 0 \quad .$$

Si, par récurrence, nous supposons avoir construit $N_r, \ldots, N_{i-1}$, $P_r, \ldots, P_i$ vérifiant les différentes propriétés inductives du théorème alors, en remplaçant r par i dans ce qui précède, nous obtenons les propriétés pour $i-1$. Ainsi, le théorème est démontré. □

Corollaire 6.6. *Avec les notations du théorème 6.5, pour tout $r \in [1, n-2]$, nous avons l'identité suivante*

$$N_1 \cdots N_r C_{r+1}(x_1, \ldots x_{r-1}, x_r, x_r) = 1 \quad \textit{modulo} < C_1, \ldots, C_r > \quad ;$$

soit pour tout $a \in V(\mathcal{S})$

$$\frac{1}{c_{r+1}(a_r)} = N_1(a_1) N_2(a_1, a_2) \cdots N_r(a_1, \ldots, a_r) \quad . \tag{13}$$

7. EXEMPLE

Nous prenons ici un exemple simple illustratif avec le polynôme $f = x^4 - 2x^3 + 2x^2 + 2$. Ses modules de Cauchy sont

$$\begin{aligned}
C_1(x_1) &= x_1^4 - 2x_1^3 + 2x_1^2 + 2 \\
C_2(x_1, x_2) &= x_2^3 - 2(x_2^2 + x_1 x_2 + x_1^2) + x_1 x_2^2 + 2(x_2 + x_1) + x_1^2 x_2 + x_1^3 \\
C_3(x_1, x_2, x_3) &= x_3^2 + x_3(x_1 + x_2 - 2) - 2(x_2 + x_1) + x_2^2 + x_1 x_2 + x_1^2 + 2 \\
C_4(x_1, x_2, x_3, x_4) &= x_4 + x_3 + x_2 + x_1 - 2 \quad .
\end{aligned}$$

Le discriminant de f est $3136 = 56^2$; donc son groupe de Galois est pair et

$$v_1 = v(f) = 56 \quad .$$

Nous avons

$$C_2(x_1, x_1) = 4x_1^3 - 6x_1^2 + 4x_1 \quad .$$

Nous calculons $N = \frac{x_1^2-4x_1+2}{28}$ tel que :

$$NC_2(x_1,x_1) + \$C_1(x_1) = 1 \quad .$$

Comme $c_1(a_1) = 0$ et $c_2(a_1) = C_2(a_1,a_1) \neq 0$, nous avons

$$\frac{1}{c_2(a_1)} = N(a_1) \quad .$$

D'où

$$v_2 = \frac{v_1}{c_2(a_1)} = 56.N(a_1) = 2(a_1^2 - 4a_1 + 2) \quad .$$

On vérifie facilement que $4(x_1^2 - 4x_1 + 2)^2$ est identique au discriminant de $C_2(x_1,x_2)$ en x_2 dans $k[x_1]/ < C_1 >$. Poursuivons la descente en calculant

$$v_3 = \frac{v_2}{c_3(a_2)} \quad . \tag{14}$$

Nous avons

$$\begin{aligned} P_2 &= C_3(x_1,x_2,x_2) = 3x_2^2 - 2(2x_2+x_1) + 2x_1x_2 + x_1^2 + 2 \quad , \\ N_2 &= 2x_1^2 - 2x_1 + 2)x_2^2 + (-2x_1^3 + x_1^2 - 6)x_2 + x_1^3 - 2x_1 + 4 \quad , \\ D_1 &= 8x_1^6 - 24x_1^5 + 38x_1^4 - 16x_1^3 - 8x_1^2 + 16x_1 + 8 \end{aligned}$$

tels que

$$N_2P_2 + \$C_2(x_1,x_2) = D_1 \quad .$$

Le polynôme $P_1 = 12x_1^3 - 36x_1^2 + 32x_1 - 4$ est la réduction de D_1 modulo C_1. En calculant les coefficients de Bézout de P_1 et C_1, nous obtenons $N_1 = \frac{x_1^3+3x_1^2-4x_1+1}{196}$ tel que $N_1P_1 = 1$ modulo C_1. Soit

$$N_1N_2P_2 = 1 \text{ modulo } < C_1, C_2 > \quad .$$

D'où pour tout $a \in V(\mathcal{S})$

$$v_3 = \frac{v_2}{c_3(a_2)} = 56N(a_1)N_2(a_1,a_2)N_1(a_1) \quad .$$

Le résultat de la réduction de $N(x_1)N_2(x_1,x_2)N_1(x_1)$ modulo $< C_1, C_2 >$ est le polynôme

$$V_3 = -(x_1^3(x_2^2 - 4x_2 + 2) + 2x_2^2 + x_1(-2x_2^2 - 6x_2 + 3) + x_1^2(-3x_2^2 + 12x_2 - 6) - x_2 + 4)$$

tel que $v_3 = V_3(a_1,a_2)$ pour tout $a \in V(\mathcal{S})$. Comme $v_3 = a_3 - a_4$, nous en déduisons

$$\begin{aligned} a_3 - a_4 &= V_3(a_1,a_2) \quad \text{et} \\ a_3 + a_4 &= 2 - a_2 - a_1 \end{aligned}$$

l'opposé du coefficient sous-dominant de $c_3(x)$. Ce qui donne

$$a_3 = G_1(a_1,a_2) \text{ et } a_4 = H_1(a_1,a_2)$$

où

$$\begin{aligned} 7G_1(x_1,x_2) &= \frac{-x_1^3x_2^2}{2}+\frac{3}{2}x_1^2x_2^2+x_1x_2^2-x2^2+2x_1^3x_2-6x_1^2x_2+3x_1x_2-3x_2 \\ &\quad -x_1^3+3x_1^2-5x_1+5 \quad \text{et} \\ 7H_1(x_1,x_2) &= \frac{x_1^3x_2^2}{2}-\frac{3}{2}x_1^2x_2^2-x_1x_2^2+x_2^2-2x_1^3x_2+6x_1^2x_2-3x_1x_2 \\ &\quad -4x_2+x_1^3-3x_1^2-2x_1+9 \quad . \end{aligned}$$

Les deux facteurs linéaires de $c_3(x)$ appartenant à $k[a_1,a_2]$ sont $g = x - G_1(a_1,a_2)$ et $h = x - H_1(a_1,a_2)$; autrement dit, nous avons $G = x_3 - G_1$ et $H = x_3 - H_1$.

Dans cet exemple, le groupe de Galois de f est A_4. Nous avons calculé un ensemble triangulaire engendrant l'idéal maximal $\mathfrak{M}$. Lorsque le groupe de Galois est pair et distinct de A_n, pour calculer $\mathfrak{M}$, il faut poursuivre les calculs avec, par exemple, l'algorithme GaloisIdeal.

References

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

[2] 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.

[3] M. Lederer. Explicit constructions in splitting fields of polynomials. *Riv. Mat. Univ. Parma (7)*, 3*:233–244, 2004.

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

[5] N. Rennert and A. Valibouze. Calculs de résolvantes avec les modules de Cauchy. *Experiment. Math.*, 8(4):351–366, 1999.

[6] R.P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

[7] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4):507–535, 1999. (Version longue du rapport LIP6 1997/014).

[8] Takashi Wada and Hidefumi Ohsugi. Gröbner bases of Hilbert ideals of alternating groups. *J. Symbolic Comput.*, 41(8):905–908, 2006.

[9] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118:617–636, 1997. Algorithms for algebra (Eindhoven, 1996).

[10] K. Yokoyama. A modular method to compute the splitting field of a polynomial. *Communication privée*, 1999.

UPMC, 4, place Jussieu, 75252 Paris Cedex 05

E-mail address: annick.valibouze@upmc.fr www-spiral.lip6.fr/~avb/