Prépublication du Laboratoire LSTA ; Soumis le 03/05/06 manuscrit

A. Valibouze

Sur les relations entre les racines d'un polynôme

3 mai 2006

Résumé Cet article s'intéresse à la description, aux utilisations et au calcul des modules fondamentaux d'un polynôme d'une variable. Il est possible de déterminer simultanément le groupe de Galois. Les modules fondamentaux engendrent l'idéal de Galois maximal triangulaire formé par les relations entre les racines du polynôme. De ce fait, ils déterminent une base du corps de ces racines.

Abstract In this paper, we show how to use and compute efficiently the fundamental moduli of an univariate polynomial. Actually, it is possible to compute the Galois group simultaneously. Fundamental moduli generate the maximal Galois ideal of relations between roots of the univariate polynomial. By this fact, they describe the decomposition field of this polynomial.

1 Introduction

Pour tout cet article, nous nous donnons un polynôme f d'une variable sur un corps parfait k et nous fixons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ un n-uplet formé des n racines de f supposées distinctes (avec $n > 0$). Le corps $k(\underline{\alpha}) = k[\underline{\alpha}]$ est celui des racines de f (i.e. son corps de décomposition).

Pouvoir réaliser des calculs algébriques avec les racines d'un polynôme d'une variable est un problème antique. Tout d'abord, il s'est agi d'exprimer les racines sous forme de radicaux pour les polynômes de degré 2 (plus de 2000 ans avant JC) puis 3 (certaines équations particulières furent résolues dans l'antiquité jusqu'à la solution à $x^3 + px - q$ de Scipione del Ferro en 1500, puis Tartaglia en 1535 et Cardan en 1545) et 4 (Ferrari en 1540) jusqu'à Lagrange ([20]) qui, en introduisant la résolvante, émit le doute que ce soit systématiquement possible au delà de ce degré. Ce fut Abel qui, en 1824, démontra finalement l'impossibilité pour l'équation générale du degré 5 ([2]). Dans le cas où l'équation est résoluble par radicaux, le degré 5 a été résolu en 1991 par Dummit ([8]) et le degré 6 en 2000 par Hagedorn ([15]). La manipulation des radicaux est quasiment inutilisable lorsque le degré du polynôme s'élève. Pour pouvoir traiter tous les cas (résoluble ou non) et réaliser des calculs algébriques dans le corps des racines, il existe trois autres possibilités :

– la méthode numérique consistant à approximer les racines mais induisant les problèmes d'erreurs de calculs qu'il s'agit de pouvoir contrôler ;
– le calcul du polynôme minimal d'un élément k-primitif du corps des racines du polynôme f donné ; le degré D de ce polynôme minimal est identique à celui de l'extension (i.e. l'ordre du groupe de Galois) pouvant atteindre la factorielle du degré n de f ; c'est à la *résolvante de Galois* qu'il faut recourir ([9]) ;

Mathematics Subject Classification (2000) Primary 12F10 · Secondary 12Y05 ; 11Y40

Keywords Splitting fi eld, Galois ideal, Galois group

– le calcul d'un ensemble triangulaire $\mathfrak{T}$ (si les racines de f sont distinctes deux-à-deux) de polynômes sur k en n indéterminées $x_1,\ldots,x_n$:

$$\begin{aligned} F_1 &= x_1^{m_1} + u_1(x_1),\\ F_2 &= x_2^{m_2} + u_2(x_1,x_2),\\ &\vdots\\ F_n &= x_n^{m_n} + u_n(x_1,x_2,\ldots,x_n) \end{aligned}$$

tels que chaque polynôme F_i de degré m_i en x_i satisfait $F_i(\underline{\alpha}) = 0$ et tels que $D = m_1 m_2 \cdots m_n$; ce sont les *modules fondamentaux* de Tchebotarev ([28]).

Cette dernière possibilité offre des avantages multiples dont le plus évident est de répartir sur n polynômes multivariés le caractère exponentiel de l'ordre D du groupe de Galois de f sur k. Tout γ de $k(\underline{\alpha})$ possède une représentation polynomiale unique modulo $F_1,\ldots,F_n$ et cette représentation appartient à k si et seulement si γ lui appartient également (i.e. les modules fondamentaux rendent effectif le théorème de Galois). De plus, une fois ces polynômes calculés, l'obtention du polynôme minimal d'un élément k-primitif de tout sous-corps du corps des racines est aisée.
Plusieurs auteurs ont travaillé sur le calcul de relations entre les racines d'un polynôme. Nous évoquons ci-après les travaux que l'auteur du présent article estime être les plus marquants et représentatifs. K. Girstmair a publié de nombreux résultats sur les relations linéaires ([11,13]). Dans [24], J. McKay et R.P. Stauduhar établissent une formule interpolatrice calculant l'expression d'une racine α_i du polynôme en fonction de celles définissant le corps de décomposition (i.e. quand $m_i = 1$). Dans son travail de thèse, M. L. Gómez-Molleda traite le cas du groupe diédral ([14]). Intéressons-nous aux algorithmes généraux dont le travail présenté ici améliore considérablement les performances. Dans [3], l'algorithme applique la démarche de Tchebotarev en factorisant "à l'aveugle" f dans les extensions $k(\alpha_1,\alpha_2,\ldots,\alpha_i)$. Les idéaux de Galois introduits dans [32] constituent un outil algébrique aboutissant à l'algorithme `GaloisIdéal` (voir ici Paragraphe 6). Dans [38], supposant le groupe de Galois donné et utilisant par ce fait la pré-détermination des degrés m_i (voir Paragraphe 4), l'auteur propose une méthode calculant les coefficients des F_i par l'algèbre linéaire et des approximations p-adiques des racines de f. Cette méthode est à ce jour la plus efficace dans le cas particulier où le groupe de Galois est le groupe alterné A_n (voir Note 5 Paragraphe 6.1) . La méthode exposée dans [26] utilise les *modules de Cauchy* des *facteurs fondamentaux* $F_i(x,\alpha_1,\ldots,\alpha_i)$ et les permutations de relations (voir ici les propositions 63 et 67 qui en sont inspirées) pour obtenir rapidement des relations. Notre méthode mixe toutes les autres tout en les améliorant individuellement. En particulier, pour la méthode entièrement p-adique, les pré-études se décomplexifient puisque le groupe de Galois est supposé donné.

Ce travail est un prolongement de [33], [34] et [26]. Il fait aussi suite à l'article [38] que m'avait remis amicalement K. Yokoyama en 1999. Je lui avais alors fait remarqué qu'il calculait inutilement des coefficients a priori nuls ou identiques qu'il devait être possible d'éviter en étudiant certaines orbites de $\{1,2,\ldots,n\}$. Cet article répond à la question sous-jacente à cette remarque : lesquels ? Sans que cela y soit explicitement écrit, le contenu de [26] peut y répondre également.
C'est à la description (Paragraphe 4), aux intérêts (Paragraphe 5) et au calcul efficace des modules fondamentaux (Paragraphe 6) qu'est consacré cet article. Nous rappellerons la définition du groupe de Galois (Paragraphe 2), celle de la matrice des groupes qui pré-détermine les groupes de Galois des facteurs des résolvantes (Paragraphe 3) et nous terminerons sur des exemples qui illustrent l'efficacité de notre méthode (Paragraphe 7).

2 Le groupe de Galois du polynôme

Fixons tout d'abord des notations qui seront valables tout au long de l'article. Soit E un ensemble non vide. Nous notons S_E le groupe symétrique agissant sur E. Pour $E = \{1,\ldots,m\}$, S_E est aussi noté S_m, le groupe symétrique de degré m. Lorsque $E = \{e_1,\ldots,e_m\} \subset \{1,2,\ldots,n\}$, le groupe S_E agit naturellement sur les polynômes p de $k[x_{e_1},\ldots,x_{e_m}]$ et sur tout m-uplet $\underline{u} = (u_{e_1},\ldots,u_{e_m})$ par permutations des indices et nous avons $\sigma.p(\underline{u}) = p(\sigma.\underline{u})$ pour tout $\sigma \in S_E$.

Le *groupe de Galois* G de $\underline{\alpha}$ sur k est le sous-groupe de S_n formé des permutations σ vérifiant que pour tout polynôme p de $k[x_1,\ldots,x_n]$ tel que $p(\underline{\alpha}) = 0$ alors $\sigma.p(\underline{\alpha}) = 0$.

Le groupe de Galois G est le plus grand sous-ensemble de S_n pour lequel une action sur le corps $k(\underline{\alpha})$ est définissable (à conjugaison près, c'est-à-dire à une numérotation des racines près). Il est isomorphe au groupe des k-automorphismes de $k(\underline{\alpha})$. Ainsi, pour une permutation σ de G et pour θ appartenant à $k(\underline{\alpha})$, il n'y a aucune ambiguïté à noter θ^σ (l'ordre des racines étant fixé). Plus précisément, si $\theta = p(\underline{\alpha}) = q(\underline{\alpha})$ avec $p,q \in k[x_1,\ldots,x_n]$ alors

$$\theta^\sigma = p(\sigma.\underline{\alpha}) = q(\sigma.\underline{\alpha}) \quad .$$

Par la théorie de Galois classique, le polynôme minimal de θ sur k est donné par :

$$\min_{\theta,k} = \prod_{\gamma \in G.\theta} (x-\gamma) \tag{1}$$

où $G.\theta = \{\theta^\sigma \mid \sigma \in G\} = \{\sigma.p(\underline{\alpha}) \mid \sigma \in G\}$ est la *G-orbite de θ* dont le cardinal est identique au degré du corps $k(\theta)$ sur le corps k (i.e. sa dimension en tant que k-espace vectoriel).

Lorsque que le groupe de Galois sera évoqué à conjugaison près (i.e. à une permutation près des racines), nous parlerons du groupe de Galois de f.

3 Groupes de Galois des facteurs d'une résolvante

Fixons L et H deux sous-groupes de S_n tels que H et G soient des sous-groupes de L. Le groupe de Galois (sur k) d'une *H-résolvante L-relative* séparable de $\underline{\alpha}$ sur k est représentable par l'action à gauche de G sur les classes à gauche de L modulo H (voir [4] et [31]). Nous allons décrire précisément cette représentation et ses représentations équivalentes afin de les appliquer au calcul des modules fondamentaux et à la détermination du groupe de Galois.

3.1 Matrices de groupes et de partitions

Donnons-nous un polynôme Θ de $k[x_1,\ldots,x_n]$ tel que $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$. Un tel polynôme Θ est appelé un *H-invariant L-primitif*. À chaque G-orbite

$$\overline{\mathfrak{O}} = \{\sigma_{i_1}H,\ldots,\sigma_{i_m}H\}$$

de L modulo H correspond la G-orbite

$$\mathfrak{O} = \{\sigma_{i_1}.\Theta,\ldots,\sigma_{i_m}.\Theta\}$$

de $L.\Theta$ au sens où la représentation de G par action à gauche sur $\overline{\mathfrak{O}}$ est équivalente à celle de G sur $\mathfrak{O}$. Cette dernière représentation de G est naturellement équivalente à une représentation symétrique dans $S_\mathfrak{O}$ que nous notons

$$\phi(G,\mathfrak{O}) \quad .$$

La représentation symétrique naturelle de $\phi(G,\mathfrak{O})$ dans $S_{\#\mathfrak{O}} = S_m$ sera quant à elle notée

$$\psi(G,\mathfrak{O}) \quad .$$

Fixons l'ordre total $x_1 < \cdots < x_n$ sur les variables et étendons-le aux monômes (par l'ordre lexicographique, par exemple) puis aux polynômes (en comparant les plus grands monômes de chaque polynôme). Munis d'un tel ordre $<$ sur les polynômes, ordonnons les G-orbites $\mathfrak{O}_1,\ldots,\mathfrak{O}_r$ de $L.\Theta$ de telle sorte que

$$\inf(\mathfrak{O}_1) < \inf(\mathfrak{O}_2) < \cdots < \inf(\mathfrak{O}_r) \quad .$$

Définissons alors les applications ϕ de S_n dans S_n et d de S_n dans l'ensemble les partitions de n comme suit :

$$\phi(G) = \phi(G,\mathfrak{O}_1) \times \cdots \times \phi(G,\mathfrak{O}_r) \quad \text{et} \tag{2}$$

$$d(G) = (\#\mathfrak{O}_1, \#\mathfrak{O}_2, \ldots, \#\mathfrak{O}_r) \quad . \tag{3}$$

Nous avons $\phi(G) \subset S_{\mathfrak{O}_1} \times \cdots \times S_{\mathfrak{O}_r}$. Posons encore

$$\psi(G) = (\psi(G,\mathfrak{O}_1),\ldots,\psi(G,\mathfrak{O}_r)) \subset (S_{\#\mathfrak{O}_1},\ldots,S_{\#\mathfrak{O}_r}) \quad .$$

Si G' est L-conjugué à G et que H est remplacé par un de ses L-conjugués quelconque alors $\psi(G) = \psi(G')$. La matrice des $\psi(G,H)$ où G et H parcourent l'ensemble des sous-groupes de L (un groupe par classe de L-conjugaison suffit) est appelée la *matrice des groupes relative à L*. On peut remplacer ψ par d pour obtenir la *matrice des partitions relative à L*.

Lemme 31 *([4]) Les lignes de la matrice de partitions sont distinctes deux-à-deux.*

3.2 Résolvantes

Faisons maintenant le lien avec le polynôme f et continuons à supposer que G et H sont deux sous-groupes de L. La *résolvante L-relative de* $\underline{\alpha}$ *par* Θ est, par définition, le polynôme

$$R = \prod_{\Psi \in L.\Theta} (x - \Psi(\underline{\alpha}))$$

appartenant à $k[x]$ puisque ses coefficients sont invariants par le groupe de Galois G de $\underline{\alpha}$ sur k. Lorsque $L = S_n$, la résolvante ne dépendant pas de la numérotation des racines de f, elle est dite *absolue* et appelée *résolvante de* f *par* Θ. Le degré de R est l'indice de H dans L. Supposons R sans racine multiple (il existe une infinité de polynômes Θ dans ce cas). La résolvante R se factorise alors en r (le nombre de G-orbites) facteurs irréductibles (simples) sur k dont, à une permutation près, $d(G)$ est le r-uplet des degrés respectifs et $\psi(G)$ celui des groupes de Galois respectifs sur k. Plus précisément, l'action de G sur une G-orbite $\mathfrak{O}$ de $L.\Theta$ est équivalente à celle de G sur $\mathfrak{O}(\underline{\alpha})$, l'évaluation de la G-orbite en $\underline{\alpha}$. Le polynôme

$$h = \prod_{\Psi \in \mathfrak{O}(\underline{\alpha})} (x - \psi)$$

de $k[x]$ est irréductible sur k car, d'après l'identité (1) et puisqu'il est sans racine multiple, il est le polynôme minimal sur k de chacune de ses racines. Nous avons $m = \#\mathfrak{O} = \deg(h)$. Si l'orbite $\mathfrak{O}$ est ordonnée (avec l'ordre $<$) et que $\underline{\beta}$ est le m-uplet des racines de h correspondant à cet ordre (i.e. $\beta_i = \sigma.\Theta(\underline{\alpha})$ si $\sigma.\Theta$ est le i-ième élément de $\mathfrak{O}$) alors $\phi(G,\mathfrak{O})$ est le groupe de Galois de $\underline{\beta}$ sur k en tant que sous-groupe de $S_{\mathfrak{O}}$ et $\psi(G,\mathfrak{O})$ est le groupe de Galois de $\underline{\beta}$ sur k en tant que sous-groupe de S_m. D'après le lemme 31, nous avons donc :

Théorème 32 *([4]) La matrice des partitions relative à L permet de déterminer le groupe de Galois de f sur k lorsqu'il est un sous-groupe de L.*

En application du théorème précédent, la matrice des groupes offre un moyen plus efficace que celle des partitions pour l'identification du groupe de Galois.

La résolvante de Tchirnhaus

Choisissons maintenant $H = S_1 \times S_{n-1}$ et $L = S_n$. Nous sommes alors dans le cas particulier de la résolvante dite de *Tchirnhaus* s'identifiant au polynôme f lorsque $\Theta = x_1$, ce que nous supposons jusqu'à la fin de ce paragraphe. Comme $L.\Theta = \{x_1, \ldots, x_n\}$, dans ce cas particulier, chaque variable x_i sera représentée par son indice i. L'ordre $<$ devient l'ordre sur les entiers. Les facteurs irréductibles de f sur k sont donc les r polynômes

$$h_s = \min_{\alpha_{j_s},k} = \prod_{i \in \mathfrak{O}_s} (x - \alpha_i) \quad \text{où } j_s = \inf(\mathfrak{O}_s) \text{ et } s \in [\![1, r]\!]. \tag{4}$$

Le groupe $\psi(G)$ est formé des permutations résultantes de l'opération qui consiste à remplacer simultanément chaque i_j par j dans $\phi(G,\mathfrak{O})$ pour $j \in [\![1, m]\!]$.

3.3 Outils logiciels de calculs

Pour calculer des résolvantes absolues, il existe de nombreuses méthodes. Une bonne partie d'entre elles sont implantées dans le module SYM ([30]) du calcul formel Maxima ([27]). Le calcul de résolvantes relatives est basé uniquement sur celui des résultants ([5]). Tout système de calcul formel généraliste convient.

Concernant la factorisation des polynômes d'une variable, tous les systèmes de calcul formel offrent cette fonctionnalité (dans les extensions y compris). Dans le cas particulier des résolvantes, il serait souhaitable qu'y soient implantés des factorisateurs spécifiques (voir [21] pour $k = Q$).

Le logiciel libre GAP ([10]) et le logiciel MAGMA ([6]) contiennent toutes les fonctionnalités nécessaires aux calculs des représentations $\phi(G,\mathfrak{O})$ et $\psi(G,\mathfrak{O})$ à partir des groupes L, H et G.

En GAP3, le programme `PrimitiveInvariant` écrit par I. Abdeljaouad calcule des invariants primitifs ([1]). Ce travail est encore améliorable avec le travail de K. Girstmair sur l'utilisation des caractères ([12], Section 2).

Pour les groupes transitifs, nous adoptons la nomenclature de G. Butler et J. McKay ([7]) jusqu'au degré 11 et celle d'A. Hulpke ([16]) jusqu'au degré 30 : le groupe jT_i est le i-ième groupe transitif de S_j. Sous GAP et MAGMA, nous disposons de la librairie avec la commande

```
TranstiveGroup(j,i) ;
```

Dans nos exemples, nous choisirons des conjugués qui simplifient la présentation.

Pour $j \leq 15$, des polynômes de groupe de Galois jT_i sont disponibles dans la base de données de G. Malle et J. Klüners ([18,19]). Un de ces polynômes est accessible dans MAGMA avec les commandes :

```
load ''galpols'';
PolynomialWithGaloisGroup(j,i);
```

3.4 Exemple

Choisissons $n = 8$, $\Theta = x_1$ et le sous-groupe

$$G^* = \langle (4,6), (3,7,6)(4,5,8), (4,7,6,8), (7,8) \rangle \tag{5}$$

de S_8 d'ordre 48. Les G^*-orbites de $\{1,2,\ldots,n\}$ sont $\{1\}$, $\{2\}$ et $\mathfrak{O}_3 = \{3,4,5,6,7,8\}$. Nous avons $d(G^*) = (1,1,6)$ et

$$\phi(G^*) = S_{\{1\}} \times S_{\{2\}} \times \phi(G^*, \mathfrak{O}_3) \subset S_{\{1\}} \times S_{\{2\}} \times S_{\mathfrak{O}_3}$$

où $\phi(G^*, \mathfrak{O}_3)$ est engendré dans $S_{\mathfrak{O}_3}$ par les permutations de (5) engendrant G^*. Le sous-groupe $\psi(L, \mathfrak{O}_3)$ de S_6 est le groupe de Galois de $\underline{\beta} = (\alpha_3, \ldots, \alpha_8)$ sur k ; c'est un conjugué de $6T_{11}$. Le calcul montre que parmi les sous-groupes G' de S_n tels que $d(G') = d(G^*)$ (donc les sous-groupes de $S_{d(G^*)}$), les seuls dont $\psi(G', \mathfrak{O}_3)$ et $\psi(G^*, \mathfrak{O}_3)$ soient S_6-conjugués sont des conjugués de G^* dans $S_{d(G^*)}$.
Supposons désormais qu'un polynôme f de degré 8 possède sur k 2 facteurs linéaires et un facteur h de degré 6 possédant $\psi(G^*, \mathfrak{O}_3)$ comme groupe de Galois sur k. Alors G^* est le groupe de Galois de f sur k. Pour déterminer si le groupe de Galois de h est $\psi(G^*, \mathfrak{O}_3)$, il suffit d'utiliser les matrices des groupes en degré 6 sachant a priori que le groupe de Galois de h sur k est un sous-groupe transitif de S_6.

4 Définition des modules et des facteurs fondamentaux

Ce qui est présenté sous forme d'exposé sans preuve relève de résultats communément admis. Le lecteur est invité à consulter, par exemple, l'ouvrage de N. Tchebotarev ou le cours d'A. Machí ([22]). Pour cette étude, le lecteur pourra également se reporter à l'article [5] (bien que les résultats y soient présentés de manière différente et dans un cadre plus général, celui des *idéaux* dit *de Galois*).

Pour chaque $i \in [\![1,n]\!]$, considérons le polynôme

$$f_i(x) = \prod_{\sigma \in G_{(i-1)}/G_{(i)}} (x - \alpha_{\sigma(i)})$$

où $G_{(0)} = G$ et

$$G_{(i)} = \{\sigma \in G_{(i-1)} \mid \sigma(i) = i\} \quad .$$

Ces sous-groupes satisfont la chaîne d'inclusions suivante :

$$G_{(n)} = I_n = G_{(n-1)} < G_{(n-2)} < \cdots < G_{(1)} < G_{(0)} = G \quad .$$

Pour $i \in [\![1,n]\!]$, nous posons $m_i(G) = \#G_{(i-1)}/\#G_{(i)}$ et

$$\underline{m}(G) = (m_1(G), m_2(G), \ldots, m_n(G)) \quad .$$

Remarque 41 *En particulier, $f_n = x - \alpha_n$ et si f est irréductible alors $f = f_1$.*

Le groupe $G_{(i-1)}$ est le groupe de Galois de $\underline{\alpha}$ sur $k(\alpha_1,\ldots,\alpha_{i-1})$. Les coefficients de f_i sont des expressions polynomiales en $\underline{\alpha}$ invariantes par $G_{(i-1)}$. Par la théorie de Galois classique, f_i appartient à $k(\alpha_1,\ldots,\alpha_{i-1})[x]$. Le groupe $G_{(i)}$ stabilisant i dans le groupe de Galois $G_{(i-1)}$, le polynôme f_i de racine α_i est irréductible sur $k(\alpha_1,\ldots,\alpha_{i-1})$. Donc :

$$f_i = \min_{\alpha_i, k(\alpha_1,\ldots,\alpha_{i-1})} \quad . \tag{6}$$

En posant $m_i = \deg(f_i) = m_i(G)$, nous avons l'identité $\#G = m_1 m_2 \cdots m_n$ et la tour d'extensions :

degré de l'extension	corps	polynôme minimal
	$k(\underline{\alpha})^{I_n} = k(\underline{\alpha})$	
$m_{i+1}\cdots m_n = \#G_{(i)}$	$\vert$	
	$k(\underline{\alpha})^{G_{(i)}} = k(\alpha_1,\ldots,\alpha_{i-1},\alpha_i)$	
$m_i = \#G_{(i-1)}/\#G_{(i)}$	$\vert$	f_i
	$k(\underline{\alpha})^{G_{(i-1)}} = k(\alpha_1,\ldots,\alpha_{i-1})$	
$m_1\cdots m_{i-1} = \#G/\#G_{(i-1)}$	$\vert$	
	$k(\underline{\alpha})^{G} = k$.	

Pour chaque $i \in [\![1,n]\!]$, il existe un polynôme $F_i(x_1,\ldots,x_i)$ de $k[x_1,\ldots,x_i]$ tel que

$$f_i(x) = F_i(\alpha_1,\ldots,\alpha_{i-1},x) \quad .$$

Note 1 Le polynôme F_i est unique en le supposant identique à son reste par les divisions euclidiennes successives par F_{i-1} en x_{i-1}, puis par F_{i-2} en x_{i-1} ... puis par F_1 en x_1.

Les polynômes $f_1,\ldots,f_n$ seront appelés les *facteurs fondamentaux* de f sur k (cela ne signifie pas qu'ils sont des facteurs de f sur k mais qu'ils sont définis à partir de k) et les *modules fondamentaux* de f sur k sont les n polynômes de l'ensemble triangulaire :

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

Ils sont bien de la forme donnée dans l'introduction. Ils vérifient, pour $i \in [\![1,n]\!]$, $\deg_{x_i} F_i = m_i$ et, en notant $\langle E\rangle$ l'idéal engendré dans $k[x_1,\ldots,x_n]$ par une de ses parties E, nous avons

$$k[x_1,\ldots,x_i]/\langle F_1,\ldots,F_i\rangle \simeq k(\alpha_1,\ldots,\alpha_i) \quad . \tag{7}$$

En particulier, $k(\underline{\alpha}) \simeq k[x_1,\ldots,x_n]/\langle\mathfrak{T}\rangle$.

Remarque 42 *Le calcul de F_n résulte de la réduction modulo $F_1,\ldots,F_{n-1}$ du polynôme $x_1+x_2+\cdots+x_n+a_1$ où a_1 est le coefficient sous-dominant de f.*

Pour $i \in [\![1,n]\!]$ et pour tous les $\beta_1,\ldots,\beta_{i-1}$ appartenant à $k(\underline{\alpha})$ tels que

$$F_1(\beta_1) = F_2(\beta_1,\beta_2) = \cdots = F_{i-1}(\beta_1,\ldots,\beta_{i-1}) \quad ,$$

le polynôme univarié $F_i(\beta_1,\ldots,\beta_{i-1},x)$ est sans racine multiple. En partant du polynôme $f_i(x) = F_i(\alpha_1,\ldots,\alpha_{i-1},x)$ qui est sans racine multiple, il est facile de le vérifier par la théorie de Galois classique. Un système triangulaire tel $\mathfrak{T}$ est dit *séparable*.

Au regard de la note 1., nous supposons l'ensemble $\mathfrak{T}$ *réduit* ; c'est-à-dire que, pour $i \in [\![1,n]\!]$ et $1 \le j < i$, nous avons :

$$\deg_{x_j} F_i < \deg_{x_j} F_j = m_j \quad .$$

Cette hypothèse n'est pas restrictive puisque, si ce n'est pas le cas, il suffit de remplacer F_i par le reste de sa division entière par F_j en x_j.

5 Intérêts des modules fondamentaux

5.1 Générateurs de l'idéal des relations

L'ensemble $\mathfrak{M}$ des polynômes p de $k[x_1,\ldots,x_n]$ tels que $p(\underline{\alpha})=0$ est appelé l'*idéal des $\underline{\alpha}$-relations*. Il est maximal car noyau du k-morphisme d'évaluation entre l'anneau $k[x_1,\ldots,x_n]$ et le corps $k(\underline{\alpha})$ qui à x_i associe α_i ; c'est-à-dire que le corps $k(\underline{\alpha})$ est isomorphe à l'anneau quotienté par $\mathfrak{M}$:

$$k(\underline{\alpha}) \simeq k[x_1,\ldots,x_n]/\mathfrak{M} \quad .$$

Comme l'ensemble séparable $\mathfrak{T}$ est inclus dans $\mathfrak{M}$, d'après l'isomorphisme (7), nous avons :

$$\mathfrak{M} = \langle \mathfrak{T} \rangle \quad .$$

Ainsi, en tant qu'espace vectoriel sur k, le corps $k(\underline{\alpha})$ possède comme base l'ensemble des

$$\alpha_1^{s_1}, \alpha_2^{s_2}, \ldots, \alpha_n^{s_n}$$

où $0 \leq s_i < m_i$, $i \in [\![1,n]\!]$. Nous retrouvons l'identité $\#G = m_1 \cdots m_n = dim_k(k(\underline{\alpha}))$.

Note 2 Le groupe de Galois G de $\underline{\alpha}$ sur k est le *groupe de décomposition* de l'idéal $\mathfrak{M}$; c'est-à-dire le plus grand sous-groupe de S_n tel que $G.\mathfrak{M} = \mathfrak{M}$.

5.2 Effectivité du théorème de Galois

Lorsqu'un polynôme est symétrique en $x_1,\ldots,x_n$, l'effectivité du théorème fondamental des fonctions symétriques donne sous sa forme effective la valeur dans k de ce polynôme évalué en les racines de f comme polynôme en les coefficients de f. Lorsque le polynôme n'est pas symétrique mais seulement invariant par le groupe de Galois de $\underline{\alpha}$ sur k, le théorème de Galois nous assure que sa valeur en $\underline{\alpha}$ appartient aussi à k. Les modules fondamentaux rendent effectif ce théorème.

Soit p un polynôme de $k[x_1,\ldots,x_n]$. Posons $p = r_{n+1}$ et définissons de manière inductive la suite $r_n, r_{n-1}, \ldots, r_1$ telle que r_j est le reste de la division entière de r_{j+1} par F_j en x_j ($j \in [\![1,n]\!]$). Le reste r_1 sera appelé le *reste de p modulo $\mathfrak{T}$* ou bien le *reste de p modulo $\mathfrak{M}$*. Il satisfait aux propriétés suivantes (facilement vérifiables) :

$$\begin{aligned} &\deg_{x_j} r_1 < m_j \qquad \text{pour tout } \ j \in [\![1,n]\!] \ , \\ &p(\underline{\alpha}) = r_1(\underline{\alpha}) \qquad \text{et surtout} \\ &p(\underline{\alpha}) \in k \qquad \text{si et seulement si} \quad r_1 \in k \quad . \end{aligned}$$

C'est ainsi que les modules fondamentaux rendent effectif le théorème de Galois.

Dans la suite de cet article, lorsque $\gamma \in k(\underline{\alpha}_1)$ sera exprimé sous la forme $\gamma = p(\underline{\alpha}$ avec $p \in k[x_1,x_2,\ldots,x_n]$, il sera sous-entendu que le polynôme p est identique à son reste modulo $\mathfrak{T}$.

5.3 Éléments primitifs et polynômes minimaux

Soit Θ un polynôme de $k[x_1,\ldots,x_n]$ et $\theta = \Theta(\underline{\alpha})$. D'après [32], le polynôme caractéristique χ de l'endomorphisme multiplicatif induit par Θ dans le k-e.v.

$$k[x_1,\ldots,x_n]/\mathfrak{M}$$

est donné par :

$$\chi = \prod_{\sigma \in G} (x - \sigma.\Theta(\underline{\alpha})) \quad . \tag{8}$$

Note 3 Le polynôme χ est aussi le polynôme caractéristique de l'endomorphisme dans le k-e.v. $k(\underline{\alpha})$ qui à γ associe $\theta.\gamma$: $\chi = \prod_{\sigma \in G}(x - \theta^\sigma)$.

Note 4 Sans faire appel aux raisonnements classiques de la théorie de Galois, par l'algèbre linéaire, le polynôme χ est à coefficients dans k.

Le polynôme χ résulte des éliminations (i.e. avec des résultants) successives des variables $x_n, x_{n-1}, \ldots, x_1$ du polynôme $x - \sigma.\Theta$ d'abord avec F_n puis avec F_{n-1} puis ... et enfin avec F_1 (voir [5]).

Nous pouvons ainsi déterminer facilement un élément k-primitif du corps des racines de f en choisissant pour Θ un polynôme tel que $\sigma.\Theta \neq \Theta$ pour tout $\sigma \in G$ et tel que χ soit sans racine multiple (il en existe une infinité). Si tel est le cas, le polynôme χ est le polynôme minimal sur k de l'élément k-primitif $\theta = \Theta(\underline{\alpha})$ de $k(\underline{\alpha})$. À noter les $D = \#G$ modules fondamentaux de χ sur k sont de la forme :

$$\chi(x_1), x_2 + v_2(x_1), x_3 + v_3(x_1), \ldots, x_D + v_D(x_1)$$

où $v_i \in k[x]$.

Soit H un sous-groupe de G. Le calcul d'un élément k-primitif du corps $k(\underline{\alpha})^H$ n'est pas bien différent. Choisissons pour Θ un H-invariant G-primitif. Le polynôme de $k[x]$

$$h = \prod_{\sigma \in G/H} (x - \theta^\sigma)$$

est une racine de χ :

$$\chi = h^{\#H}$$

et s'il est sans racine multiple alors il est le polynôme minimal sur k de θ, élément k-primitif de $k(\underline{\alpha})^H$. Notons que h est en fait la résolvante G-relative de $\underline{\alpha}$ par Θ.

6 Étude et calcul des modules fondamentaux

6.1 Résolvantes et relations

Dans ce paragraphe, nous introduisons les idéaux de Galois et évoquons l'algorithme `GaloisIdéal` calculant $\mathfrak{T}$ en construisant une chaîne croissante d'idéaux dits de Galois (voir [32] et [35]). En terme de coût, la proposition 63 apporte une amélioration importante à cet algorithme. Nous supposons acquises les principales propriétés des idéaux de Galois et nous reprenons également les notations des paragraphes précédents.

Définissons les idéaux de Galois. Soit M un sous-ensemble de S_n contenant l'identité alors l'idéal

$$\mathfrak{I} = \bigcap_{\sigma \in L} \sigma^{-1}.\mathfrak{M} \tag{9}$$

est l'*idéal de Galois défini par M et $\mathfrak{M}$*. Nous notons $\mathscr{M}(\mathfrak{I})$ l'ensemble des idéaux maximaux contenant $\mathfrak{I}$:

$$\mathscr{M}(\mathfrak{I}) = \{\sigma^{-1}.\mathfrak{M} \mid \sigma \in M\} \quad .$$

Le plus grand ensemble de permutations définissant $\mathfrak{I}$ avec $\mathfrak{M}$ est GM.

Pour tout $\sigma \in L$, l'idéal $\mathfrak{I}$ est aussi défini par $\sigma^{-1}.M$ (= M si M est un groupe) et l'idéal $\sigma^{-1}.\mathfrak{M}$ de $\mathscr{M}(\mathfrak{I})$. Ainsi, lorsque nous considérons un idéal de Galois $\mathfrak{I}$ et que nous disons fixer $\mathfrak{M}$, ou ce qui revient au même $\underline{\alpha}$ appartenant à sa variété, $\mathfrak{M}$ désigne en fait un idéal maximal quelconque de $\mathscr{M}(\mathfrak{I})$.

En reprenant les notations du paragraphe 3, supposons que l'idéal $\mathfrak{I}$ soit défini par le groupe L contenant G et l'idéal $\mathfrak{M}$ de groupe de décomposition G (i.e. G est le groupe de Galois de $\underline{\alpha}$ sur k). Le groupe L contenant le groupe de décomposition de $\mathfrak{M}$, il est à la fois le groupe de décomposition de $\mathfrak{I}$ et le plus grand ensemble définissant cet idéal.

Au paragraphe 3, les résolvantes sont exploitées afin de déterminer le groupe de Galois d'un polynôme. Elles fournissent une liste de groupes candidats à être le groupe de Galois. Elles sont également exploitables pour calculer des relations comme le montre le lemme suivant :

Lemme 61 *Pour tout facteur p sur k (simple ou non) de la résolvante R, il existe un idéal $\mathfrak{N}$ de $\mathscr{M}(\mathfrak{I})$ tel que*

$$p(\Theta) \in \mathfrak{N} \quad .$$

Démonstration Car les racines de R sont les $\sigma\Theta(\underline{\alpha}) = \Theta(\sigma.\underline{\alpha})$ où $\underline{\alpha}$ parcourt L et que $\mathfrak{M}$ étant l'idéal des $\underline{\alpha}$-relations, l'idéal $\sigma^{-1}.\mathfrak{M}$ de $\mathscr{M}(\mathfrak{I})$ est celui des $\sigma.\underline{\alpha}$-relations. □

Sans perte de généralité, lorsque le groupe de Galois G de $\underline{\alpha}$ sur k n'est fixé qu'à conjugaison près dans L, nous pouvons toujours supposer que $\Theta(\underline{\alpha})$ est une racine de h. Si G est fixé, et que $\tau.\Theta$ est dans la G-orbite $\mathfrak{O}$ associée à h, il suffit de remplacer, dans ce qui suit, le H-invariant Θ par $\tau.\Theta$ et H par son conjugué $\tau H \tau^{-1}$ qui stabilise $\tau.\Theta$ dans L.

L'algorithme `GaloisIdéal` calculant l'ensemble $\mathfrak{T}$ est basé sur les matrices de groupes et le théorème suivant :

Théorème 62 *Si le polynôme h associé à la G-orbite $\mathfrak{O}$ est sans racine multiple alors l'idéal de Galois*

$$\mathfrak{J} = \mathfrak{I} + \langle h(\Theta)\rangle$$

est défini par H et $\mathfrak{M}$. Le plus grand ensemble définissant $\mathfrak{J}$ avec $\mathfrak{M}$ est

$$GH = \bigcup_{C\in\overline{\mathfrak{O}}} C$$

où $\overline{\mathfrak{O}}$ est la G-orbite de H dans les classes à gauche de L modulo H.
Pour que l'hypothèse de ce théorème soit satisfaite, il est suffisant mais pas nécessaire que h soit un facteur irréductible simple sur k de la résolvante R.

Note 5 Le théorème précédent s'applique également aux idéaux de Hilbert (cas particuliers des idéaux de Galois lorsque $f = x^n$ et $G = I_n$). Les idéaux de Hilbert ne sont pas nécessairement triangulaires. La base de Gröbner de celui défini par le groupe alterné est calculable à la main (voir [36]). Dans le cas des idéaux de Galois, ce calcul est très complexe car le haut degré de transitivité de ce groupe induit à la fois un invariant composé de $n!/2$ monômes difficile à réduire modulo l'idéal défini par S_n et un degré d'extension identique rendant rapidement impossible la factorisation dans les extensions. C'est donc à la méthode linéaire et p-adique de Yokoyama qu'il faut recourir.

La proposition suivante améliore l'algorithme `GaloisIdéal` dans le cas où le groupe de décomposition de $\mathfrak{J}$ ne contient pas le groupe de Galois G :

Proposition 63 *Soit $\mathfrak{J}$ un idéal de Galois tel que $\mathfrak{M} \in \mathscr{M}(\mathfrak{J})$ et M le plus grand ensemble de permutations le définissant avec $\mathfrak{M}$. Alors, considérant G le groupe de décomposition de $\mathfrak{M}$, l'idéal de Galois*

$$G.\mathfrak{J} = \{g.p \mid g \in G \ \ et \ \ p \in \mathfrak{J}\}$$

est défini par $\mathfrak{M}$ et le plus grand sur-groupe D de G contenu dans M.
En particulier, pour tout groupe U intermédiaire entre G et D

$$G.\mathfrak{J} = U.\mathfrak{J} \quad .$$

Démonstration Comme $G.(G.\mathfrak{I}) = G.\mathfrak{I}$, G est un sous-groupe du groupe de décomposition D de l'idéal $G.\mathfrak{J}$. De ce fait, le groupe de décomposition D de $G.\mathfrak{J}$ est aussi le plus grand groupe définissant cet idéal avec $\mathfrak{M}$ (en fait avec tout idéal maximal contenant $G.\mathfrak{J}$). Comme $\mathfrak{J} \subset G.\mathfrak{J}$, nous avons $D = GD \subset GM = M$ (c'est une propriété classique des idéaux de Galois). À partir de là, la maximalité est évidente. La dernière assertion est évidente également puisque D contenant G, il vérifie $D.\mathfrak{J} = DG.\mathfrak{J} = G.\mathfrak{J}$ car D est le groupe de décomposition de $G.\mathfrak{J}$. □

Nous pouvons ainsi déduire des relations en permutant par le groupe de Galois celles déjà obtenues et aboutir ainsi à un nouvel idéal de Galois $\mathfrak{K}$ dont le groupe de décomposition est un sur-groupe de celui de chacun des idéaux maximaux de la décomposition de $\mathfrak{K}$.

Remarques pratiques concernant la proposition 63

Nous supposons que $\mathfrak{J} = \mathfrak{I} + \langle h(\Theta)\rangle$. La plupart des remarques ci-après s'appliquent aussi dans le cadre plus général de la proposition 63.

1. Pour calculer $G.\mathfrak{J}$, il n'est pas nécessaire de permuter tous les polynômes engendrant $\mathfrak{J}$ puisque, D étant un sous-groupe du groupe L de décomposition de $\mathfrak{I}$, nous avons $D.\mathfrak{I} = \mathfrak{I}$.

2. De même, il n'est pas nécessaire de tester toutes les permutations de G puisque H est un sous-groupe du groupe de décomposition de $\mathfrak{J}$ (car $H \subset L$ et $H = \mathrm{Stab}_L(\Theta)$). Ainsi, seules les permutations $\tau_2, \ldots, \tau_m$ telles que
$$GH = \bigcup_{i=1}^{m} \tau_i H$$
sont à considérer (les τ_i sont calculées avec la G-orbite $\overline{\mathfrak{O}}$). De plus, si un groupe U intermédiaire entre D et G est déterminé, il est inutile de tester les permutations n'appartenant pas à $G \cap U$.
3. Dans la pratique, le groupe D est rapidement déterminable à partir de $G.\mathfrak{J}$. Il suffit de tester que $\sigma.p \in G.\mathfrak{J}$ pour tout générateur de D et tout générateur de $\mathfrak{J}$. De plus, l'idéal $G.\mathfrak{J}$ est triangulaire (voir [5]) et $\#D$ est le produit d des degrés initiaux des polynômes de l'ensemble triangulaire l'engendrant. Il suffit donc de chercher D parmi les groupes d'ordre d contenant un groupe candidat. Sachant que D est unique parmi ceux d'ordre d, une vérification modulaire est envisageable.
4. Toujours dans la pratique, le groupe G n'est pas nécessairement déterminé mais, en revanche, l'algorithme `GaloisIdéal` nous assure qu'il fait parti d'une chaîne croissante de groupes candidats contenus dans D (le groupe D a pu éventuellement être éliminé de la liste des candidats). Pour pouvoir appliquer la proposition, il suffit donc de chercher un groupe candidat maximal U tel que $U.\mathfrak{J}$ est un idéal de Galois dont le produit d des degrés initiaux est supérieur ou égal à $\#M$. Si tel est le cas alors $G \subset U \subset D$ et $G.\mathfrak{J} = U.\mathfrak{J} = D.\mathfrak{J}$. Non seulement, $D.\mathfrak{J}$ et D sont calculés, mais, de surcroît, nous pouvons ne conserver que les sous-groupes de D dans la liste des groupes candidats.

Exemple 64 *Choisissons le polynôme $f = x^8 + x^6 + 2x^2 + 4$ de la base de donnée de MAGMA et dont le groupe de Galois sur $k = Q$ est $8T_{19}$. Considérons l'idéal de Galois de f suivant :*

$$\begin{aligned}\mathfrak{J} = \langle\ & g_1 = x_1^8 + x_1^6 + 2x_1^2 + 4, \quad g_2 = x_2 + x_1,\\ & g_3 = x_3^2 + 1/2x_1^6 + 1/2x_1^4 + 1, \quad g_4 = x_3 + x_4,\\ & g_5 = x_5^4 + (-1/2x_1^6 - 1/2x_1^4 + x_1^2)x_5^2 + 2,\\ & g_6 = x_5^3 + x_5^2x_6 + x_5x_6^2 + (-1/2x_1^6 - 1/2x_1^4 + x_1^2)x_5 + x_6^3 + (-1/2x_1^6 - 1/2x_1^4 + x_1^2)x_6,\\ & g_7 = x_5^2 + x_5x_6 + x_5x_7 + x_6^2 + x_6x_7 + x_7^2 + -1/2x_1^6 - 1/2x_1^4 + x_1^2, \quad g_8 = x_7 + x_8\ \rangle\quad .\end{aligned}$$

Les calculs qui nous ont amenés à $\mathfrak{J}$ nous assurent que tous les groupes de la liste des groupes candidats sont inclus dans des conjugués de $8T_{35}$ d'ordre 128. Nous savons également que chaque candidat conjugué de $8T_{35}$ contient un groupe de décomposition d'un idéal de $\mathscr{M}(\mathfrak{J})$. Choisissons parmi les candidats le conjugué

$$D = \langle (7,8), (1,3)(2,4), \sigma = (1,5,3,8)(2,6,4,7) \rangle$$

de $8T_{35}$. Nous constatons que $\sigma.(x_1 + x_2) = x_5 + x_6$ et que l'idéal triangulaire

$$\mathfrak{J} + \langle x_5 + x_6 \rangle$$

a pour produit de ses degrés initiaux l'ordre 128 du groupe D. Donc D est le groupe de décomposition de l'idéal

$$G.\mathfrak{J} = D.\mathfrak{J} = \mathfrak{J} + \langle x_5 + x_6 \rangle = \langle g_1, g_2, g_3, g_4, g_5, x_6 + x_5, 2x_7^2 + 2x_5^2 - x_1^6 - x_1^4 + 2x_1^2, g_8 \rangle \quad .$$

L'algorithme `GaloisIdéal` peut se poursuivre avec $G.\mathfrak{J}$ (la dimension de l'anneau quotient est 128) à la place de $\mathfrak{J}$ (la dimension est 3.128=384).

6.2 Un nouvel algorithme

Nous allons décrire une autre méthodologie simple en partie composée de pré-calculs sur les sous-groupes de S_n afin de calculer efficacement l'ensemble $\mathfrak{T}$ de groupe de décomposition G. Nous reprenons les notations des paragraphes précédents. En particulier, concernant le paragraphe 3, l'invariant Θ est le polynôme x_1 et la résolvante R est donc le polynôme f lui-même de groupe de Galois G sur k.

Afin d'éclairer l'exposé, considérons le polynôme $f=(x-1)(x^2-2)$ et fixons $\underline{\alpha}=(1,\sqrt{2},-\sqrt{2})$. Les modules fondamentaux sont les polynômes $F_1=x_1-1, F_2=x_2^2-2$ et $F_3=x_3+x_2$. Nous voyons que $f_2\in k[x]\subset k(\alpha_1)[x]$ et que $f_3\in k(\alpha_2)[x]\subset k(\alpha_1,\alpha_2)[x]$. Les corps k et $k(\alpha_2)$ sont les corps dit *minimaux* de f_2 et f_3, respectivement.

L'étude de $\mathfrak{T}$ que nous proposons ici commence tout d'abord par distinguer deux étapes auxquelles l'étude générale se ramènera.

Étape 1 Facteurs fondamentaux appartenant à k

Données. f, k et G, le groupe de Galois de $\underline{\alpha}$ sur k.
Supposons que f possède exactement $r\geq 1$ facteurs irréductibles sur k. D'après les identités (4) et (6), ce sont les r facteurs fondamentaux de f sur k appartenant à $k[x]$ suivants :

$$f_{j_1}=h_1, f_{j_2}=h_2,\ldots,f_{j_r}=h_r$$

où, pour $s\in[\![1,r]\!]$, $j_s=\inf(\mathfrak{O}_s)$ et $\phi(G,\mathfrak{O}_s)$ est le groupe de Galois sur k du facteur f_{j_s} en tant que sous-groupe de $S_{\mathfrak{O}_s}$. Naturellement

$$d(G)=(m_{j_1},m_{j_2},\ldots,m_{j_r})\quad .$$

Remarque 65 *Si f est réductible sur k alors nécessairement les degrés*

$$m_{j_1},m_{j_2},\ldots,m_{j_r}$$

de ses modules fondamentaux sont strictement inférieurs à n (on a $n=m_{j_1}+m_{j_2}+\cdots+m_{j_r}$).

Ayant étudié les facteurs fondamentaux appartenant à k par un pré-calcul sur G, il s'agira ensuite de pouvoir les calculer à partir de f sachant que cette étape pourra être appliquée à une extension de k (voir Étape 2.). Il existe plusieurs méthodes. Parmi elles nous avons l'algorithme `GaloisIdéal` (voir l'exemple du groupe $8T_{39}$ du Paragraphe 7), les algorithmes de factorisations dans les extensions (voir, par exemple celui historique de B. Trager [29]) ou une méthode modulaire pour calculer f_i lorsque son degré $m_i=\underline{m_i}(G)$ est déterminé sachant que

$$f_i\in k[x]\subset k(\alpha_1,\alpha_2,\ldots,\alpha_{i-1})[x]$$

pour éviter de calculer des coefficients a priori nuls (voir [25,37,38]). Ici, nous proposons en plus une idée très simple pour calculer efficacement de nombreux modules fondamentaux ; ces calculs sont prévisibles en fonction de G uniquement. Comme nous le constaterons lors de la prochaine étape, certains modules fondamentaux peuvent être déjà déterminés. Supposons que pour $s\in[\![1,r]\!]$ le facteur f_{j_s} soit le seul facteur de f sur $k(\alpha_1)$ non calculé. Il se déduit alors trivialement des autres par :

$$f_{j_s}=\frac{f}{\prod_{i\neq s}f_{j_i}}\quad . \tag{10}$$

Étape 2 f est supposé irréductible sur k

Données. f irréductible sur k et G, le groupe de Galois transitif de $\underline{\alpha}$ sur k.

D'après l'étape 1., $f_1=f$. Donc $F_1=f(x_1)$ est le seul module fondamental appartenant à $k[x_1]$.

Les facteurs fondamentaux de f sur $k(\alpha_1)$ et appartenant à $k(\alpha_1)$ sont obtenus en appliquant l'étape 1. avec les données $f,k(\alpha_1)$ et le groupe $G_{(1)}$. Ces facteurs sont $x-\alpha_1$ et les facteurs fondamentaux $f_{j_2},\ldots,f_{j_r}$ de f sur k et appartenant à $k(\alpha_1)$. Les valeurs $j_2,\ldots,j_r$ sont entièrement déterminées à partir de $G_{(1)}$.

Fixons i appartenant à $\{j_2,\ldots,j_r\}$. Les pré-calculs déterminent les corps minimaux des modules fondamentaux puisque :

$$F_i\in k[x_1,x_i]\quad .$$

Sans être explicitement signalé, ce résultat existe déjà dans [26].

Pour simplifier, pour la suite de cette étape, nous posons $F_i = F_i(x_1, x_i)$. Dans l'esprit de la proposition 63, nous allons pré-déterminer en fonction de G s'il est possible de calculer ou non des facteurs fondamentaux à partir de ceux appartenant à $k(\alpha_1)$.

Lemme 66 *Pour tout $\sigma \in G_{(1)}$, si $\sigma(i) \neq i$ alors $m_{\sigma(i)} < m_i$.*

Démonstration Car, pour tout $\sigma \in G_{(1)}$, le facteur fondamental $f_{\sigma(i)}$ est un facteur fondamental de f_i sur $k(\alpha_1)$; si $\sigma(i) \neq i$ alors $f_{\sigma(i)}$ est un facteur de $f_i/x - \alpha_i$ de degré $m_i - 1$ dans une extension de $k(\alpha_1)$. Par conséquent $m_{\sigma(i)} \leq m_i - 1$. □

D'après ce lemme, les permutations de $G_{(1)}$ n'apportent rien. En revanche, comme le groupe G est un sous-groupe transitif de S_n, nous pourrons appliquer la proposition suivante aux permutations τ de G telles que $\tau(1) \neq 1$:

Proposition 67 *Soit $i \in \{j_2, \ldots, j_r\}$. Si $\tau \in G$ satisfait les conditions suivantes :*

$$m_{\tau(i)} = m_i \quad et \quad \tau(1) < \tau(i)$$

alors $\tau(1) \neq 1$ et le $\tau(i)$-ième facteur fondamental de f sur k est donné par :

$$f_{\tau(i)} = F_i(\alpha_{\tau(1)}, x) \in k[x_{\tau(1)}, x_{\tau(i)}] \quad .$$

Démonstration Nous avons $\tau(1) \neq 1$, d'après le lemme 66. Le reste est évident puisque $F_i \in k[x_1, x_i]$. □

Dans la proposition précédente, le module fondamental $F_{\tau(i)}$ résultera en fait de la réduction de $F_i(x_{\tau(1)}, x_{\tau(i)})$ modulo $\mathfrak{M}$. C'est pour cette raison que nous identifions $f_{\tau(i)}$ et non $F_{\tau(i)}$.

Soient $\tau_1 = id, \ldots, \tau_n$ des permutations du sous-groupe transitif G de S_n telles que $\tau_j(1) = j$ pour $j \in [\![1, n]\!]$. Pour chaque $j \in [\![1, n]\!]$, les r polynômes $f_{\tau_j(i)}$ où i parcourt $\{j_2, \ldots, j_r\}$ sont les facteurs de f sur $k(\alpha_j)$ de groupe de Galois G_j sur $k(\alpha_j)$ (où G_j est le stabilisateur de j dans G). Donc il suffira d'appliquer la proposition 67 aux seules permutations $\tau_2, \ldots, \tau_n$ de G.

Inversement à la proposition 67, s'il existe $l \in [\![1, n]\!]$ et $1 \leq j < l$ tels que f_l soit un facteur irréductible de f sur $k(\alpha_j)$ (i.e. $f_l = P(\alpha_j, x)$ avec $P \in k[y, x]$) alors, par la transitivité de G, $P(\alpha_1, x)$ est aussi un facteur irréductible de f sur $k(\alpha_1)$. Donc nécessairement, la proposition 67 s'applique pour déduire le module F_l d'un des modules $F_{j_2}, \ldots, F_{j_r}$.

Cas général

Pour déterminer les facteurs fondamentaux de f sur k, il faut d'abord appliquer la première étape à f puis appliquer récursivement la deuxième sur chaque facteur irréductible g dans chaque extension $k_{\underline{u}} = k(\alpha_{u_1}, \ldots, \alpha_{u_i})$ considérée. Le polynôme g est un facteur fondamental de f sur k de degré m. Les données de l'étape 2 seront g, k_u et le groupe de de Galois $G_{\underline{u}}$ de $\overline{\beta}$ sur k_u calculé avec la fonction ϕ où $\overline{\beta}$ le m-uplet des racines de g respectant l'ordre induit par la numérotation des racines de f. En particulier, les générateurs de $G_{\underline{u}}$ dans $S_{\underline{u}}$ engendrent un sous-groupe de G dans S_n. Il faudra néanmoins appliquer la proposition 67 au groupe G et non pas uniquement au groupe $G_{\underline{u}}$ comme l'illustrera l'exemple du groupe PSL(2,7) du paragraphe 7.

La plupart des calculs peuvent être menés a priori en utilisant uniquement des considérations groupistiques.

6.3 Application

Dans le paragraphe précédent, nous avons décrit une méthodologie de pré-étude portant sur un groupe G afin de déterminer le canevas d'un algorithme de calcul de $\mathfrak{T}$ lorsque G est son groupe de décomposition. Une fois cette pré-étude réalisée pour tous les groupes d'un même degré n, elle est alors combinable (toujours en pré-étude) avec les matrices de groupes sur k mais aussi sur ses extensions $k_{\underline{u}}$. À tout moment, il est possible d'utiliser l'algorithme `GaloisIdéal` en rajoutant des modules de Cauchy de facteurs fondamentaux déjà calculés (voir [26]). Nous pouvons produire de la sorte un algorithme très efficace pour le calcul simultané de $\mathfrak{T}$ et G en degré n. Si le groupe G est déjà déterminé, la pré-étude précédente suffit.

7 Exemples

Nous allons illustrer la méthode du paragraphe 6 pour calculer $\mathfrak{T}$ à travers 3 exemples caractéristiques. Le premier détaille la méthode à suivre pour la pré-étude sur un groupe fixé. Le second illustre la méthodologie à suivre pour déterminer simultanément le groupe de Galois et l'idéal des relations. Le troisième montre comment bien utiliser la proposition 67.

7.1 Un groupe d'ordre 384 conjugué de $8T_{44}$

Nous supposons que f possède comme groupe de Galois sur k le groupe

$$G = \langle (4,6), (1,6)(2,4), (1,7,3,6)(2,8,5,4) \rangle$$

conjugué de $8T_{44}$, d'ordre 384 et tel que $\underline{m}(G) = (8,1,6,4,1,1,2,1)$. Nous appliquons la première étape qui nous donne

$$f_1 = f \in k[x] \quad .$$

Dans le contexte de la deuxième étape avec f, k et G comme données, nous appliquons la première avec f, $k(\alpha_1)$ et $G_{(1)}$. Le groupe $G_{(1)}$ est le groupe G^* de l'exemple 3.4. Nous avons $j_2 = 2$ et $j_3 = 3$. Comme $d(G_{(1)}) = (1, m_2, m_3) = (1,1,6)$, dans $k(\alpha_1)$, f possède 2 facteurs linéaires $x - \alpha_1$ et f_2 et le facteur f_3 de degré 6 de groupe de Galois $\phi(G^*, \mathfrak{S}_3)$ sur $k(\alpha_1)$. Donc,

$$f_2 \in k(\alpha_1)[x] \quad \text{et, en appliquant (10),}$$
$$f_3 = \frac{f}{(x-\alpha_1) f_2} \in k(\alpha_1)[x] \quad .$$

Comme $m_2 = m_5 = m_6 = m_8 = 1$, nous cherchons à utiliser la proposition 67 avec $i = 2$. Des trois permutations $\tau_4 = (1,4,5,8,2,6,3,7), \tau_3 = (1,3)(2,5)(4,8)(6,7)$ et $\tau_7 = (1,7,3,6)(2,8,5,4)$ de G modulo $G_{(1)}$, nous déduisons les 3 facteurs fondamentaux :

$$f_5 = F_2(\alpha_3, x),\ f_6 = F_2(\alpha_4, x),\ f_8 = F_2(\alpha_7, x) \quad .$$

Il reste à trouver les facteurs fondamentaux f_4 et f_7 de degrés respectifs $m_4 = 4$ et $m_7 = 2$. Comme indiqué dans le cas général, nous appliquons l'étape 2. au polynôme f_3 irréductible sur $k(\alpha_1, \alpha_2) = k(\alpha_1)$ avec $\phi(G^*, \mathfrak{S}_3)$ comme groupe de Galois de $(\alpha_3, \ldots, \alpha_8)$ sur $k(\alpha_1)$ dans $S_{\{3,4,5,6,7,8\}}$ (i.e. agissant sur les indices des α_i). Appliquons l'étape 1. avec f_3 sur $k(\alpha_1)(\alpha_3)$. Le stabilisateur de 3 dans $H = \phi(G^*, \mathfrak{S}_3)$ est le sous-groupe $H^* = \langle (4,6), (4,7,6,8), (7,8) \rangle$ de $S_3 \times S_{\{4,6,7,8\}} \times S_{\{5\}}$ (H^* est engendré par les mêmes générateurs que $G_{(3)}$). Ainsi, avec l'identité (10), dans $k(\alpha_1, \alpha_3)$ nous avons :

$$f_4 = \frac{f_3}{(x-\alpha_3) f_5} \in k(\alpha_1, \alpha_3)[x] \quad .$$

L'étape 2. se poursuit avec f_3. Comme $m_4 \neq m_7$, le facteur f_7 n'est pas déductible de f_4 par permutation. Nous appliquons l'étape 2. à f_4 sur $k(\alpha_1, \alpha_3)$ avec le groupe H^*. Cette étape nous redirige sur l'étape 1. avec le polynôme f_4, le corps $k(\alpha_1, \alpha_3)(\alpha_4)$ et le sous-groupe $S_{\{4\}} \times S_{\{6\}} \times S_{\{7,8\}}$ de $S_{\{4,6,7,8\}}$ (i.e. le stabilisateur de 4 dans H^*). Avec l'identité (10), nous obtenons :

$$f_7 = \frac{f_4}{(x-\alpha_4) f_6} \in k(\alpha_1, \alpha_3, \alpha_4)[x] \quad .$$

Nous savons donc calculer les 8 modules fondamentaux à partir de 2 d'entre eux : $F_1 = f(x_1) \in k[x_1]$ et $F_2 \in k[x_1, x_2]$ linéaire en x_2.

Commentaires. Le gain de notre méthode est extrêmement important. Le module F_2 résulte d'une factorisation partielle de $f/(x-\alpha_1)$ sur $k(\alpha_1)$ (i.e. seul le facteur linéaire est à calculer). Avec la formule (10), nous évitons la factorisation complète de f sur $k(\alpha_1)$. Si nous n'utilisons pas la formule (10) et la proposition 67, pour obtenir f_4 et f_5, nous devons factoriser f_3 de degré 6 sur $k(\alpha_1, \alpha_3, \alpha_4)$ de degré 48 sur k ; c'est-à-dire factoriser sur k un polynôme de degré 288=6.48 (voir [29]). De même, pour obtenir f_6 et f_7 en factorisant f_4 sur $k(\alpha_1, \alpha_3, \alpha_4)$, il est nécessaire de factoriser sur k un polynôme de degré 768=192.4. Cet exemple simple permet donc de mesurer à la fois la simplicité et l'efficacité de la méthode proposée dans cet article.

7.2 Un groupe d'ordre 192 conjugué de $8T_{39}^{+}$

Nous nous plaçons dans le cas plus complexe où le groupe de Galois n'est pas pré-déterminé. Nous appliquons simultanément la détermination du groupe de Galois avec les matrices de groupes et le calcul des facteurs fondamentaux. Pour cet exemple illustratif, ce n'est pas la meilleure stratégie qui est recherchée. L'objectif est d'expliquer comment éviter de lourds calculs dépassant parfois les capacités de la machine. Pour une implantation, afin de déterminer partiellement ou complètement le groupe de Galois, il est possible d'appliquer au préalable le théorème de Dedekind ([7, 23]) ou, en cours de calcul, une des méthodes exposées par A. Hulpke dans [17].

Nous conservons les notations de l'exemple précédent et nous supposons qu'avec la matrice des groupes relative à S_8 nous ayons déterminé que le groupe de Galois de f sur k soit un des groupes $8T_{23}, 8T_{39}^{+}, 8T_{40}$ et $8T_{44}$. Pour cela, il suffit que la résolvante absolue R de f par un invariant primitif de $S_2 \times S_6$ possède sur k un facteur irréductible simple de degré 4 et de groupe de Galois impair (c'est S_4) et un facteur irréductible de degré 24 (voir la sous-matrice des groupes relative à S_8 publiée dans [31]). Nous faisons volontairement l'économie du calcul du discriminant de f pour ne pas discriminer $8T_{39}^{+}$ dès à présent.
Toujours d'après la matrice des groupes, le polynôme f possède alors un facteur linéaire sur $k(\alpha_1)$. De ce facteur linéaire, nous déduisons l'idéal de Galois $\mathfrak{I}$ engendré par les polynômes $F_1, \ldots, F_8$ de l'exemple précédent consacré à $8T_{44}$. Le groupe de décomposition de $\mathfrak{I}$ est le groupe G, conjugué de $8T_{44}$. Avec les polynômes $F_1, \ldots, F_8$, nous sommes en mesure de calculer des résolvantes G-relatives (voir [5]) et donc d'exploiter la matrice de groupes relative à G pour déterminer le groupe de Galois de f sur k. Choisissons le sous-groupe (distingué)

$$H = \langle (1,8)(2,7)(3,4)(5,6), \tau_3, (1,6)(2,4)(3,7)(5,8), (1,4,3)(2,6,5), (1,2)(3,6,5,4) \rangle$$

de G conjugué de $8T_{39}$. En comparant $\underline{m}(H) = (8,1,6,4,1,1,1,1)$ à $\underline{m}(G)$, nous en déduisons, qu'hormis F_7, les polynômes F_i engendrant I sont les modules fondamentaux de $\underline{\alpha}$ sur k si H est son groupe de Galois sur k. Si tel est le cas, H est le groupe de décomposition de $\mathfrak{M}$ et de $(5,6)\mathfrak{M}$ (car H est auto-adjoint dans G) tels que :

$$\mathfrak{I} = \mathfrak{M} \cap (5,6)\mathfrak{M} \quad .$$

Déterminons à la fois le groupe de Galois et $\mathfrak{T}$ (i.e. le module fondamental manquant). Commençons par calculer Θ, un H-invariant G-relatif et réduisons-le à θ modulo $\mathfrak{I}$. Nous calculons (rapidement) R_2, la résolvante G-relative de $\underline{\alpha}$ par θ de degré 2, l'indice de H dans G. Supposons que cette résolvante se factorise en deux facteurs linéaires $(x+a)(x+b)$ distincts. La résolvante R_2 possédant un facteur linéaire simple, le groupe de Galois de $\underline{\alpha}$ sur k est un sous-groupe de H, c'est donc H (c'est un cas particulier d'utilisation de la matrice des groupes qui rejoint un théorème bien connu). D'après le théorème 62, nous avons finalement :

$$\mathfrak{M} = \mathfrak{I} + \langle \theta + a \rangle \quad .$$

Appliquons ce résultat au polynôme irréductible $f = x^8 + x^2 + 1$ calculé par Mattman, McKay et Smith. La résolvante R de f par x_1x_2 possède sur $k = Q$ un facteur irréductible de degré 24 et un de degré 4 de groupe de Galois impair. La parité de f impose que le facteur fondamental simple sur $k(\alpha_1)$ soit :

$$f_2 = F_2(\alpha_1, x) = x + \alpha_1 \quad .$$

Nous en déduisons les générateurs de l'idéal de Galois $\mathfrak{I}$:

$$f_3 = f/(x^2 - \alpha_1^2) = x^6 + \alpha_1^2 x^4 + \alpha_1^4 x^2 + \alpha_1^6 + 1$$

et $F_5 = x_5 + x_3$, $F_6 = x_6 + x_4$ et $F_8 = x_8 + x_7$; autrement dit $f_5 = x + \alpha_3$, $f_6 = x + \alpha_4$ et $f_8 = x + \alpha_7$. Pour finir avec $\mathfrak{I}$, nous avons

$$\begin{aligned} f_4 &= f_3/(x-\alpha_3)(x+\alpha_3) = f_3/(x^2 - \alpha_3^2) = x^4 + x^2\alpha_1^2 + x^2\alpha_3^2 + \alpha_1^4 + \alpha_3^4 + \alpha_3^2\alpha_1^2 \quad \text{et} \\ f_7 &= f_4/(x^2 - \alpha_4^2) = x^2 + \alpha_1^2 + \alpha_3^2 + \alpha_4^2 \quad . \end{aligned}$$

Nous calculons $\theta = x_1x_2x_4x_7 = \Theta$ modulo I et $R_2 = (x-1)(x+1)$. Du calcul

$$g_7 = x_1x_2x_3 f_7(x_7) - x_7(\theta - 1) = x_7 + x_1x_2x_3^3 + x_1x_2^3x_3 + x_1^3x_2x_3$$

nous déduisons

$$\mathfrak{T} = \{F_1, \ldots, F_6, g_7, F_8\} \quad .$$

Commentaires. Cet exemple est assez étonnant car, en dehors du calcul et de la factorisation de la résolvante R, les calculs sont réalisables rapidement "à la main" alors que la fonction `SplittingField` de MAGMA n'en finit pas de calculer sans obtenir de résultat. Pour le calcul de g_7, la factorisation en MAGMA de f_7 dans $k(\alpha_1,\alpha_3,\alpha_4)$ se réalise en plus de 6 secondes sur une machine Intel Pentium 1,60 GHz, 512 MB/Mo. Lorsqu'il ne reste plus qu'à déterminer des facteurs fondamentaux linéaires, pour éviter des factorisations dans les extensions, il est également possible d'appliquer la méthode interpolatrice de J. McKay et R.P. Stauduhar ([24]). Dans cet exemple précis, l'algorithme `GaloisIdéal` pour calculer g_7 est indiscutablement plus rapide. Notons que nous aurions pu exploiter la parité de f pour réduire les calculs de f_3, f_4 et f_7.

7.3 Le groupe $PSL(2,7) = 7T_5$ à 168 éléments

(Voir [34] pour une première étude de ce groupe.)
Soit f un polynôme irréductible sur k de degré $n = 7$ et de groupe de Galois le groupe $PSL(2,7)$ à 168 éléments. Nous avons $f_1 = f$. Fixons le groupe

$$G = \langle (1,4,3,5,6,7,2),(2,5)(3,4)\rangle$$

comme étant le groupe de Galois de $\underline{\alpha}$ sur k. Avec G, nous calculons $\underline{m} = (7,6,1,4,1,1,1)$, le n-uplet des degrés des facteurs fondamentaux de $\underline{\alpha}$ sur k.
Comme $G_{(1)} = \langle (2,5)(3,4)(2,7,4)(3,6,5)\rangle$, d'après la formule (10), dans $k(\alpha_1)$ nous avons :

$$f_2 = \frac{f_1}{(x-\alpha_1)} \in k(\alpha_1)[x] \quad .$$

Puis, comme $G_{(2)} = \langle (4,6)(5,7)(4,5)(6,7)\rangle$, dans $k(\alpha_1,\alpha_2)$, nous avons

$$f_3 \in k(\alpha_1,\alpha_2)[x] \quad \text{et}$$
$$f_4 = \frac{f_2}{(x-\alpha_2)\,f_3} \in k(\alpha_1,\alpha_2)[x]$$

avec $\deg(f_3) = 1 = m_3$ et $\deg(f_4) = 4 = m_4$. Comme $m_3 = m_5 = m_6 = m_7 = 1$, avec $f_3 \in k(\alpha_1)(\alpha_2)$, nous appliquons la proposition 67 à $i = 3$ et aux permutations $\tau_4' = (2,4,7)(3,5,6)$ et $\tau_6' = (2,6)(3,7)$ de $G_{(1)}$ modulo $G_{(2)}$. Donc

$$f_5 = F_3(\alpha_1,\alpha_4,x) \quad \text{et} \quad f_7 = F_3(\alpha_1,\alpha_6,x) \quad .$$

Pour déduire F_6, nous remontons jusqu'à G. Avec la permutation $\tau_3 = (1,3,6,2,4,5,7)$ de G modulo $G_{(1)}$, nous obtenons finalement

$$f_6 = F_3(\alpha_3,\alpha_4,x) \quad .$$

Pour le polynôme $f = x^7 - 7x + 3$ de groupe de Galois $7T_5$, nous obtenons en moins d'une seconde le polynôme :

$$\begin{aligned} 63 f_3 = {} & 63x + (2\alpha_1^5 + 5\alpha_1^4 + \alpha_1^3 + 7\alpha_1^2 - 3\alpha_1 - 6)\alpha_2^5 + (5\alpha_1^5 + 5\alpha_1^3 + 3\alpha_1^2 - 7\alpha_1)\alpha_2^4 \\ & + (\alpha_1^5 + 5\alpha_1^4 - 8\alpha_1^2 - 4\alpha_1 + 24)\alpha_2^3 + (7\alpha_1^5 + 3\alpha_1^4 - 8\alpha_1^3 - 6\alpha_1^2 + 28\alpha_1 - 6)\alpha_2^2 \\ & + (-3\alpha_1^5 - 7\alpha_1^4 - 4\alpha_1^3 + 28\alpha_1^2 - 14\alpha_1 + 45)\alpha_2 + 3(-2\alpha_1^5 + 8\alpha_1^3 - 2\alpha_1^2 + 15\alpha_1 - 4) \quad . \end{aligned}$$

Commentaire. Pour la détermination de $\mathfrak{T}$, avec la formule (10) et la proposition 67, tous les modules fondamentaux se déduisent de $F_1 = f(x_1) \in k[x_1]$ et de $F_3 \in k[x_1,x_2]$ de degré 1 en x_2.

Conclusion

L'étude fine a priori du corps des racines et du groupe de Galois d'un polynôme nous a permis de dégager une méthode algébrique extrêmement efficace pour leur calcul. Les exemples de cet article en apportent une illustration indéniable. Cette méthode est entièrement automatisable et en grande partie composée de pré-calculs.

Remerciements Je remercie mes amis et collaborateurs Jean-Marie Arnaudiès et Antonio Machí pour tous les échanges fructueux que j'ai eu avec eux et qui m'ont aidés dans le cheminement qui m'a amenée à ce travail. Je remercie aussi Carlo Traverso qui m'a invitée au département de Mathématiques de l'université de Pise au printemps 1997. Il m'a fait bénéfi cier de ses compétences en géométrie algébrique. J'ai pu exposer à cette occasion mon premier cours de théorie de Galois avec les idéaux de Galois et l'algorithme `GaloisIdéal`.

Références

[1] I. Abdeljaouad, *Calculs d'invariants primitifs de groupes fi nis*, Theor. Inform. Appl. **33**(1) (1999), 59–77. (http://www-gap.mcs.st-and.ac.uk/Gap3/Contrib3/contrib.html)

[2] N.H. Abel, *Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, In : Oeuvres, vol. **1**, 1824, 28–33

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

[4] J.M. Arnaudiès, A. Valibouze, *Lagrange resolvents*, J. Pure Appl. Algebra **117/118** (1997), 23–40

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

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

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

[8] D.S. Dummit, *Solving solvable quintics*, Math. Comp. **57**(195) (1991), 387–401

[9] E. Galois, *Oeuvres Mathématiques, éditées par la SMF*, Gauthier-Villars, Paris, 1897

[10] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4* 2006. (http://www.gap-system.org)

[11] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. **39**(1) (1982), 81–97

[12] K. Girstmair, *Specht modules and resolvents of algebraic equations*, J. Algebra **137**(1) (1991), 12–43

[13] K. Girstmair, *Linear relations between roots of polynomials*, Acta Arith. **89**(1) (1999), 53–96

[14] M.d.l.A. Gómez-Molleda. *Cálculo del centro de un grupp de Galois y applicationes*. Tesis doctoral, Universidad de Cantabria, Espagne, 1999

[15] T.R. Hagedorn, *General formulas for solving solvable sextic equations*, J. Algebra **233**(2) (2000), 704–757

[16] A. Hulpke, *Konstruction transitiver permutationsgruppen*. Ph.D. thesis, Dissertation of Rheinisch Westfälische Technische Hochschule, Aachen, Germany 1996

[17] A. Hulpke, *Techniques for the computation of Galois groups*, In : Algorithmic algebra and number theory (Heidelberg, 1997). Springer, Berlin, 1999, 65–77

[18] J. Klüners, G. Malle. *A database for polynomials over the rationals*. (http://www.mathematik.uni-kassel.de/~klueners/minimum/)

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

[20] J. Lagrange, *Réflexions sur la résolution algébrique des équations*, Prussian Academy (1770)

[21] F. Lehobey. *Calcul et factorisation interactive de résolvantes de Lagrange en théorie de Galois effective*. Thèse de l'IRMAR, Université de Rennes 1, France,1999

[22] A. Machí, *Dispense di teoria di Galois*. Dipartemento di Matematica, Università degli studi di Roma "La Sapienza". (http://www.mat.uniroma1.it/people/machi/Galois/)

[23] J. McKay, *Some remarks on computing Galois groups*, SIAM J. Comput. **8**(3) (1979), 344–347

[24] J. McKay, 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), 1997, 75–77

[25] M. Noro, K. Yokoyama, *Factoring polynomials over algebraic extension fi elds*, Josai Information Science Researches **9** (1997), 11–33

[26] S. Orange, G. Renault, A. Valibouze, *Calcul effi cace de corps de décomposition*. Publication interne 2003/005, Laboratoire LIP6, Université P. et M. Curie, France 2003. (http://www.lip6.fr/fr/production/publications-rapports.php)

[27] W. Schelter. *Manuel de Maxima* 2001. (http://maxima.sourceforge.net)

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

[29] B. Trager, *Algebraic factoring and rational function integration*, In : Proceedings of the SYMSAC'76, 1976, 219–226

[30] A. Valibouze, *Symbolic computation with symmetric polynomials, an extension to Macsyma*, In : Computers and Mathematics (MIT, USA, June 13-17, 1989). Springer-Verlag, New York Berlin, 1989, 308–320. (Voir "Symmetries" dans http://maxima.sourceforge.net/docs.shtml)

[31] A. Valibouze, *Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems*, In : Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), *Lecture Notes in Comput. Sci.*, vol. 948. Springer, Berlin, 1995, 456–468

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

[33] A. Valibouze, *Galois theory and reducible polynomials*. Publication interne 99.03, Équipe MAX, laboratoire LIX, École Polytechnique, France 1999. (http://www.lix.polytechnique.fr/~max/publications/)

[34] A. Valibouze, *Corps de décomposition de groupe de Galois PSL(2,7)*. Publication interne 2005/001, Laboratoire LIP6, Université P. et M. Curie, France 2005.
(`http://www.lip6.fr/fr/production/publications-rapports.php`)

[35] A. Valibouze, *Dépendance algébrique des zéros de polynômes et groupes de Galois*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **48(96)**(1) (2005), 73–96

[36] T. Wada, H. OhSugi, *Groebner bases of Hilbert ideals of alternating groups*, J. Symbolic Comput. (2005). à paraître

[37] 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)

[38] K. Yokoyama, *A modular method to compute the splitting fi eld of a polynomial*, Communication privée (1999)

A. Valibouze L.S.T.A, Université Pierre et Marie Curie,
4, place Jussieu, F-75252 Paris Cedex 05, France
Tel : +01-45-70-71-94
Page-Web : //www-calfor.lip6.fr/˜avb/ E-mail : annick.valibouze@upmc.fr