ACTA ARITHMETICA
131.1 (2008)

# Sur les relations entre les racines d'un polynôme

par

Annick Valibouze (Paris)

**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 au moins 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]) ;

2000 *Mathematics Subject Classification*: Primary 12F10; Secondary 12Y05, 11Y40, 12F05, 11Y05.

*Key words and phrases*: splitting field, Galois ideal, Galois group, maximal ideal.

 

- 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 $D = m_1 \cdots m_n$ et que, pour chaque $i \in [\![1, n]\!]$, $F_i(\underline{\alpha}) = 0$ et $\deg_{x_j} u_i < m_j$ pour tout $j \in [\![1, i]\!]$ ; ce sont les *modules fondamentaux* de Tchebotarev ([27]). Ils forment une base de Gröbner réduite pour l'ordre lexicographique de l'idéal $\mathfrak{M}$.

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 $k$. L'ensemble $\mathfrak{T}$ étant une base de Gröbner réduite, tout $\gamma$ 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 $\gamma$ 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. Ci-après, sont évoqués ceux qui nous apparaissent comme les plus marquants et représentatifs. K. Girstmair a publié de nombreux résultats sur les relations linéaires ([11, 13]). Dans son travail de thèse, M. Á. 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 $k(\alpha_1, \ldots, \alpha_i)$. Les idéaux de Galois introduits dans [31] constituent un outil algébrique aboutissant à l'algorithme `GaloisIdéal` (paragraphe 6). Dans le cas $k = \mathbb{Q}$, supposant le groupe de Galois donné, K. Yokoyama utilise la pré-détermination des degrés $m_i$ (paragraphe 4) pour calculer les coefficients de chaque $F_i$ par l'algèbre linéaire et des approximations $p$-adiques des racines de $f$ ([36]). Cette méthode est particulièrement efficace lorsque le groupe de Galois est le groupe alterné $A_n$ (paragraphe 6.1, note 5). Dans [21], M. Lederer établit une formule interpolatrice pour le calcul des modules fondamentaux ; de plus, l'idée des approximations $p$-adiques est également utilisée lorsque $k = \mathbb{Q}$. La méthode exposée dans [25] 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 6.4 et 6.8 qui en sont inspirées) pour obtenir rapidement des

relations. Cette méthode, réclamant une pré-étude en chaque degré, mixte toutes les autres tout en les améliorant individuellement. Lorsque le groupe de Galois est supposé donné, la pré-étude se décomplexifie.

Ce travail est un prolongement de [32], [33] et [25]. Il fait aussi suite à un échange avec K. Yokoyama en 1999 concernant le calcul des $F_i$ par sa méthode $p$-adique. Je lui avais alors fait remarquer que des calculs inutiles de coefficients a priori nuls ou identiques étaient évitables en étudiant certaines orbites de $\{1,\ldots,n\}$. Cet article répond à la question sous-jacente à cette remarque : lesquels ? Sans que cela y soit explicitement écrit, l'article [25] y répond 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 classique du groupe de Galois comme groupe de permutations (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 $E=\{e_1,\ldots,e_m\}\subset\{1,\ldots,n\}$, 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 $\sigma$ 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 du corps $k(\underline{\alpha})$. Ainsi, pour une permutation $\sigma$ de $G$ et pour $\theta$ appartenant à $k(\underline{\alpha})$, il n'y a aucune ambiguïté à noter $\theta^\sigma$ (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

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

Par la théorie de Galois classique, le polynôme minimal de $\theta$ 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 $\theta$* 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 le groupe de Galois sera évoqué à conjugaison près (i.e. à une permutation des racines près), 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* (paragraphe 3.2) séparable de $\underline{\alpha}$ sur $k$ est représentable par l'action à gauche de $G$ sur les classes à gauche de $L$ modulo $H$ ([4, 30]). 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 $\Theta$ de $k[x_1, \ldots, x_n]$ tel que $H = \{\sigma \in L \mid \sigma.\Theta = \Theta\}$. Un tel polynôme $\Theta$ est appelé un *$H$-invariant $L$-primitif*. Notons $\{\sigma_1, \ldots, \sigma_e\}$, $e$ étant l'indice de $H$ dans $L$, une transversale à gauche de $L$ modulo $H$. À chaque $G$-orbite

$$\overline{\mathfrak{O}} = \{\sigma_{i_1}H, \ldots, \sigma_{i_m}H\}, \qquad 1 \leq i_1 < \cdots < i_m \leq e,$$

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 $\phi(G, \mathfrak{O})$. Fixons la bijection de $\mathfrak{O}$ dans $\{1, \ldots, m\}$ qui à chaque $\sigma_{i_j}.\Theta$ associe l'entier $j$. Induite par cette bijection, la représentation symétrique naturelle de $\phi(G, \mathfrak{O})$ dans $S_{\#\mathfrak{O}} = S_m$ sera quant à elle notée $\psi(G, \mathfrak{O})$.

Fixons l'ordre total $x_1 < \cdots < x_n$ sur les variables et étendons-le aux monômes par l'ordre lexicographique puis aux polynômes (en comparant les plus grands monômes de chaque polynôme). C'est l'ordre pour lequel $F_1, \ldots, F_n$ forment une base de Gröbner de $\mathfrak{M}$. 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

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

Définissons alors les applications $\phi$ et $d$ qui à tout sous-groupe $G$ de $L$ associent respectivement

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

dans $S_{\mathfrak{O}_1} \times \cdots \times S_{\mathfrak{O}_r}$ et

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

dans l'ensemble des partitions de $n$. Posons encore

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

Si $G'$ est $L$-conjugué à $G$ et que $H$ est remplacé par un de ses $L$-conjugués quelconques 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 $L$*. En remplaçant $\psi$ par $d$, on obtient la *matrice des partitions relative à $L$*.

LEMME 3.1 ([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 $\Theta$* 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 $k$. Une telle résolvante est aussi appelée une *$H$-résolvante $L$-relative*. 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 $\Theta$*. Le degré de $R$ est l'indice $e$ de $H$ dans $L$. Supposons $R$ sans racine multiple (il existe une infinité de polynômes $\Theta$ dans ce cas). La résolvante est alors dite *séparable*. Le corps $k$ étant parfait, la séparabilité se vérifie lors de la factorisation. La résolvante $R$ se factorise 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 $\underline{\beta}$ 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 3.1, nous avons donc :

THÉORÈME 3.2 ([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. Pour s'en convaincre, prenons comme exemple $n = 8$, $L = S_8$ et $H = S_2 \times S_6$. Seuls les trois sous-groupes transitifs $8T_{24}$, $8T_{14}$ et $8T_{13}$ de $S_8$ satisfont $d(8T_i) = (4, 12, 12)$ (voir paragraphe 3.3 pour la notation $jT_i$). La matrice des partitions ne suffit pas à les départager sans le calcul d'une autre résolvante absolue de degré 35 pour l'un d'eux et une autre de degré 112 pour les deux autres. Or on a $\phi(8T_{13}) = A_4 \times U_5 \times U_6$, $\phi(8T_{14}) = S_4 \times U_3^+ \times U_4^-$ et $\phi(8T_{24}) = S_4 \times U_1^+ \times U_2^+$, où les $U_i$ sont des sous-groupes transitifs de $S_{12}$, les exposants $+$ et $-$ précisant s'ils sont ou non sous-groupes du groupe alterné $A_{12}$. Ainsi, si le discriminant du facteur irréductible (simple) de degré 4 est un carré sur $k$ alors $G = 8T_{13}$ ; sinon, si le discriminant d'un des facteurs irréductibles (simple) de degré 12 n'est pas un carré alors $G = 8T_{14}$, sinon $G = 8T_{24}$. La matrice des groupes est également exploitable pour le problème de Galois inverse ([30]).

*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

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

**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 ([29]) du système de calcul formel Maxima ([26]). Le calcul de résolvantes relatives utilise les idéaux de Galois que nous aborderons ultérieurement (paragraphe 6.1, note 6). 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 ([22] pour $k = \mathbb{Q}$). En effet, souvent seules des factorisations partielles sont nécessaires.

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]). Comme expliqué ci-après, K. Girstmair nous propose d'améliorer cet algorithme avec son travail sur les caractères

([12, Section 2]). Soit $M$ un module-gauche sur l'anneau $\mathbb{Q}[S_n]$ ; par exemple, l'espace vectoriel de polynômes $M = \sum_{1\le i<j\le n} \mathbb{Q}x_ix_j$. Soit $H \subset L$ deux sous-groupes de $S_n$. Nous cherchons $w \in \mathrm{Fix}(H)_M = \{v \in M : \forall s \in H : sv = v\}$ qui ne soit pas fixé par $L$. Un tel $w$ n'existe que si $\dim \mathrm{Fix}(L)_M < \dim \mathrm{Fix}(H)_M$. Ces dimensions sont facilement comparables si le $S_n$-caractère $\pi$ de $M$ est connu, car

$$\dim \mathrm{Fix}(H)_M = |H|^{-1} \sum_{s\in H} \pi(s).$$

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

```
TransitiveGroup(j,i);
```

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

Pour $j \le 15$, 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 $\{1,\dots,n\}$ 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 $\underline{\beta} = (\alpha_3, \dots, \alpha_8)$ sur $k$ ; c'est un conjugué de $6T_{11}$. Le calcul montre que parmi les sous-groupes $G'$ de $S_8$ 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 $k$ deux facteurs linéaires et un facteur $h$ de degré 6 ayant $\psi(G^*, \mathfrak{O}_3)$ 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 ([23]). 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* dits *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

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

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

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

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

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

REMARQUE 4.1. 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 $\alpha_i$ est irréductible sur $k(\alpha_1, \ldots, \alpha_{i-1})$. Donc

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

En posant $m_i = \deg f_i = m_i(G)$, nous avons l'identité $\#G = m_1 \cdots m_n$ 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 unique polynôme $F_i(x_1, \ldots, x_i)$ de $k[x_1, \ldots, x_i]$ tel que

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

et $\deg_{x_j} F_i < \deg_{x_j} F_j$ pour tout $j \in [\![1, i-1]\!]$ ; il vérifie $\deg_{x_i} F_i = m_i$.

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 les facteurs de $f$ quand on passe de $k$ à $k(\underline{\alpha})$), et les *modules fondamentaux* de $f$ sur $k$ sont les $n$ polynômes de l'ensemble triangulaire

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

Ils sont bien de la forme donnée dans l'introduction. En notant $\langle E \rangle$ l'idéal engendré dans $k[x_1, \ldots, x_n]$ par une de ses parties $E$, nous avons

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

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

Remarque 4.2. Le calcul du polynôme $F_n$ résulte de la réduction modulo $F_1, \ldots, F_{n-1}$ du polynôme $x_1 + \cdots + x_n + a_1$ 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

$$F_1(\beta_1) = F_2(\beta_1, \beta_2) = \cdots = F_{i-1}(\beta_1, \ldots, \beta_{i-1}) = 0,$$

le polynôme univarié $F_i(\beta_1, \ldots, \beta_{i-1}, x)$ est sans racine multiple. En effet, d'une part, il existe $\tau \in G$ tel que $\beta_1 = \alpha_{\tau(1)}, \ldots, \beta_{i-1} = \alpha_{\tau(i-1)}$ et, d'autre part, $f_i(x) = F_i(\alpha_1, \ldots, \alpha_{i-1}, x)$ est sans racine multiple ; puisque $\tau \in G$, on peut faire agir $\tau$ sur $k(\underline{\alpha})$ ; toute permutation des coefficients de $f_i$ par $\tau$ revenant à permuter ses racines par $\tau$, les racines du polynôme $F_i(\beta_1, \ldots, \beta_{i-1}, x)$ sont bien distinctes. Un système triangulaire tel $\mathfrak{T}$ est dit *séparable* (voir aussi [5]).

L'ensemble triangulaire $\mathfrak{T}$ est *réduit* puisque $\deg_{x_j} F_i < \deg_{x_j} F_j$ pour tout $i \in [\![2, n]\!]$ et tout $j \in [\![1, i-1]\!]$. Ainsi, $\mathfrak{T}$ est une base de Gröbner réduite pour l'ordre lexicographique de l'idéal qu'il engendre.

## 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 $\alpha_i$ ; c'est-à-dire que le corps $k(\underline{\alpha})$ est isomorphe à l'anneau quotienté par $\mathfrak{M}$ :

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

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

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

Ainsi, en tant qu'espace vectoriel sur $k$, le corps $k(\underline{\alpha})$ possède comme base l'ensemble des $\alpha_1^{s_1} \cdots \alpha_n^{s_n}$ 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 1. 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 $x_1, \ldots, x_n$, le théorème fondamental des fonctions symétriques donne sous sa forme effective la valeur dans $k$ de ce polynôme évalué en les racines de $f$ comme expression polynomiale en ses coefficients. 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) :

$$\deg_{x_j} r_1 < m_j \quad \text{pour tout } j \in [\![1, n]\!], \qquad p(\underline{\alpha}) = r_1(\underline{\alpha})$$

et surtout

$$p(\underline{\alpha}) \in k \quad \text{ si et seulement si } \quad r_1 \in k.$$

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

En fait, $\mathfrak{T}$ étant une base de Gröbner pour l'ordre lexicographique, il est possible de diviser $p$ par les éléments de $\mathfrak{T}$ dans n'importe quel ordre pour obtenir sa forme normale $r_1$.

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

**5.3.** *Éléments primitifs et polynômes minimaux.* Soit $\Theta$ un polynôme de $k[x_1, \ldots, x_n]$ et $\theta = \Theta(\underline{\alpha})$. D'après [31], le polynôme caractéristique $\chi$ de l'endomorphisme multiplicatif induit par $\Theta$ dans le $k$-e.v.

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

est donné par

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

NOTE 2. Le polynôme $\chi$ est aussi le polynôme caractéristique de l'endomorphisme dans le $k$-e.v. $k(\underline{\alpha})$ qui à $\gamma$ associe $\theta.\gamma$ : $\chi = \prod_{\sigma \in G}(x - \theta^\sigma)$.

NOTE 3. Sans faire appel aux raisonnements classiques de la théorie de Galois, par l'algèbre linéaire, le polynôme $\chi$ est à coefficients dans $k$.

Le polynôme $\chi$ 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 $F_1$ ([5]).

Nous pouvons ainsi déterminer facilement un élément $k$-primitif du corps des racines de $f$ en choisissant pour $\Theta$ un polynôme tel que $\chi$ soit sans racine multiple (il en existe une infinité). Si tel est le cas, le polynôme $\chi$ est le polynôme minimal sur $k$ de l'élément $k$-primitif $\theta = \Theta(\underline{\alpha})$ de $k(\underline{\alpha})$. Les $D = \#G$ modules fondamentaux de $\chi$ 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 $v_i \in k[x]$. Le groupe de Galois de $\chi$ sur $k$ est une représentation régulière de $G$ dans $S_D$.

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 $\Theta$ un $H$-invariant $G$-primitif. Le polynôme

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

de $k[x]$ est un facteur irréductible de $\chi$ :

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

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

## 6. Étude et calcul des modules fondamentaux

**6.1.** *Résolvantes et idéaux de Galois.* Dans ce paragraphe, nous définissons les idéaux de Galois à la base de l'algorithme `GaloisIdéal` calculant $\mathfrak{T}$ par construction d'une chaîne croissante de tels idéaux ([31, 34]). En terme de coût, la proposition 6.4 apporte une amélioration importante à cet algorithme que nous décrirons sous sa nouvelle forme. Nous supposons acquises les principales propriétés des idéaux de Galois et nous reprenons également les notations des paragraphes précédents. En particulier, $\mathfrak{M}$ est l'idéal (maximal) des $\underline{\alpha}$-relations, et $G$, son groupe de décomposition, est le groupe de Galois de $\underline{\alpha}$ sur $k$.

Définissons les idéaux de Galois. Soit $M$ un sous-ensemble de $S_n$ contenant l'identité ($M$ n'est pas nécessairement un groupe) ; alors l'idéal

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

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

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

Le plus grand ensemble de permutations définissant $\mathfrak{I}$ avec $\mathfrak{M}$ est $GM$. Si $GM$ est un groupe alors c'est le groupe de décomposition de $\mathfrak{I}$ (i.e. celui qui envoie $\mathfrak{I}$ dans $\mathfrak{I}$), et si le groupe de décomposition de $\mathfrak{I}$ contient $G$ alors il s'identifie à $GM$. Dans ce cas, l'idéal $\mathfrak{I}$ est dit *pur*. Un idéal de Galois pur est triangulaire ([5]).

Pour tout $\sigma \in M$, 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 fixons un idéal de Galois $\mathfrak{I}$ et que nous considérons $\mathfrak{M} \in \mathscr{M}(\mathfrak{I})$, ou ce qui revient au même $\underline{\alpha}$ appartenant à la variété de $\mathfrak{M}$, si $M$ n'est pas imposé alors l'idéal $\mathfrak{M}$ peut désigner un idéal quelconque de $\mathscr{M}(\mathfrak{I})$. Cette démarche est donc différente de celle qui consiste à imposer un ordre aux racines comme cela peut se faire dans les méthodes numériques.

En reprenant les notations du paragraphe 3, supposons que l'idéal $\mathfrak{I}$ soit défini par l'idéal $\mathfrak{M}$ et le groupe $L$ contenant $G$ (i.e. l'ensemble de permutations $M$ est le groupe $L$). Le groupe $L$ contenant $G$, le groupe de décomposition le contient également et, par conséquent, l'idéal $\mathfrak{I}$ est pur.

Comme le montre la proposition évidente suivante, l'idéal $\mathfrak{I}$ est un outil algébrique intermédiaire répondant partiellement au problème de l'effectivité du théorème de Galois.

PROPOSITION 6.1. *Soit $p \in k[x_1, \ldots, x_n]$ invariant par $L$ (et donc par $G$). Alors la réduction de $p$ modulo $\mathfrak{I}$ est la valeur de $\Theta(\underline{\alpha})$ sur $k$.*

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 6.2. *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*

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

*Démonstration.* Car les racines de $R$ sont les $\sigma.\Theta(\underline{\alpha}) = \Theta(\sigma.\underline{\alpha})$ où $\sigma$ 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 $h$, le facteur de la résolvante $R$ correspondant à la $G$-orbite $\mathfrak{O}$. Si $G$ est fixé, et que $\tau.\Theta$ appartient à $\mathfrak{O}$, il suffit de remplacer, dans ce qui suit, le $H$-invariant $\Theta$ par $\tau.\Theta$ et $H$ par son conjugué $\tau H \tau^{-1}$ qui stabilise $\tau.\Theta$ dans $L$.

L'algorithme `GaloisIdéal` utilise le théorème fondamental suivant :

THÉORÈME 6.3 ([31]). *Si le polynôme $h$ associé à la $G$-orbite $\mathfrak{O}$ est sans racine multiple, alors l'idéal de Galois*

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

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

*Démonstration.* Idée intuitive de la preuve : comme $\mathfrak{I} \subset \mathfrak{K} \subset \mathfrak{M}$, l'idéal $\mathfrak{K}$ est de Galois ; sa variété est d'intersection vide avec celle de l'idéal de Galois défini par $\bigcup_\tau H^\tau$ où $\tau$ parcourt une transversale à gauche de $L$ modulo $H$ privée des permutations $\sigma$ telles que $h(\sigma.\Theta(\underline{\alpha})) = 0$. Les idéaux de Galois étant radicaux, on prouve que $\mathfrak{K}$ est défini par $H$ et donc que $GH$ est le plus grand ensemble le définissant. Par ailleurs, pour tout $\sigma \in L$, toute classe double $\overline{\sigma}$ de $L$ modulo $G$ et $H$ peut être vue ensemblistement comme $G\sigma H$, soit l'union des classes de la $G$-orbite de $\sigma H$. ∎

NOTE 4. Pour que l'hypothèse du théorème 6.3 soit satisfaite, il est suffisant mais pas nécessaire que $h$ soit un facteur irréductible simple sur $k$ de la résolvante $R$. Le corps $k$ étant parfait lorsqu'un facteur est irréductible, il est sans racine multiple.

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 ([35]). 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 K. Yokoyama qu'il faut recourir.

La proposition suivante améliore l'algorithme `GaloisIdéal` dans le cas où $\mathfrak{K}$ n'est pas pur ou, dit autrement, dans le cas où $M = GH$ n'est pas un groupe :

PROPOSITION 6.4. *Soit $\mathfrak{K}$ un idéal de Galois tel que $\mathfrak{M} \in \mathscr{M}(\mathfrak{K})$ 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*

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

*est un idéal de Galois pur 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 $D$,*

$$G.\mathfrak{K} = U.\mathfrak{K}.$$

*Démonstration.* Comme $G.(G.\mathfrak{I}) = G.\mathfrak{I}$, $G$ est un sous-groupe du groupe de décomposition $D$ de l'idéal $G.\mathfrak{K}$. De ce fait, le groupe de décomposition $D$ de $G.\mathfrak{K}$ est aussi le plus grand groupe définissant cet idéal avec $\mathfrak{M}$ (en fait, avec tout idéal maximal contenant $G.\mathfrak{K}$). Comme $\mathfrak{K} \subset G.\mathfrak{K}$, nous avons $D = GD \subset GM = M$ ([31, Proposition 3.14]). À partir de là, la maximalité est évidente. La dernière assertion est évidente également puisque $D$ contenant $G$, il vérifie $D.\mathfrak{K} = DG.\mathfrak{K} = G.\mathfrak{K}$ car $D$ est le groupe de décomposition de $G.\mathfrak{K}$. ∎

*Utilisation de la proposition 6.4 pour calculer $G.\mathfrak{K}$ et $D$*

1. Si $I$ est un idéal de Galois pur inclus dans $\mathfrak{K}$ et de groupe de décomposition $U$, alors il est inutile de permuter les polynômes de $I$ puisque $D \subset M \subset U$ implique $D.I = U.I = I \subset \mathfrak{K}$. Cela s'applique donc à $I = \mathfrak{I}$ et $U = L$.
2. Si $U$ est un sous-groupe du groupe de décomposition de $\mathfrak{K}$, seules sont utiles les permutations $\tau_2, \ldots, \tau_m$ telles que
$$GU = U + \bigcup_{i=2}^{m} \tau_i U.$$
De plus, si un groupe $U$ intermédiaire entre $D$ et $G$ est déterminé, les permutations de $G \cap U$ sont suffisantes. Cela s'applique au groupe $U = H$ car $H = \mathrm{Stab}_L(\Theta)$ et $\mathfrak{I} \subset H.\mathfrak{I} \subset L.\mathfrak{I} = \mathfrak{I}$ ; les $\tau_i$ sont alors calculées avec la $G$-orbite $\overline{\mathfrak{O}}$.
3. L'algorithme `GaloisIdéal` possède comme paramètre une liste de groupes candidats à être le groupe de Galois. Le groupe $G$ appartient à une chaîne croissante de candidats sous-groupes de $D$. Il existe un groupe candidat $U$ maximal dans la chaîne d'inclusions tel que $U.\mathfrak{K}$ est un idéal de Galois (i.e. $1 \notin U.\mathfrak{K}$) pur. Un tel groupe vérifie $G \subset U \subset D$ et $G.\mathfrak{K} = U.\mathfrak{K} = D.\mathfrak{K}$.
4. Le groupe $D$ est déterminable à partir de l'ensemble triangulaire $\mathfrak{T}'$ engendrant l'idéal pur $G.\mathfrak{K}$ car $\#D$ est le produit $d$ des degrés initiaux des polynômes de $\mathfrak{T}'$. Il suffit de chercher $D$ parmi les groupes d'ordre $d$ contenant un groupe candidat en testant si $\sigma.p \in G.\mathfrak{K}$ pour tout

générateur $\sigma$ de $D$ et tout $p \in \mathfrak{T}'$. Sachant que $D$ est unique parmi ceux d'ordre $d$, une vérification modulaire est envisageable.

*Algorithme* `GaloisIdéal` *amélioré.* L'algorithme `GaloisIdéal`, muni désormais de la proposition 6.4, construit une chaîne croissante d'idéaux de Galois

$$I_1 \subset I_2 \subset \cdots \subset \mathfrak{M}$$

où $I_1$ est un idéal de Galois donné ou, à défaut, l'idéal des relations symétriques entre les racines de $f$. À chaque étape, l'algorithme dispose d'un idéal de Galois pur $\mathfrak{I}$ (i.e. d'un ensemble triangulaire l'engendrant) de groupe de décomposition $L$ et d'une liste de sous-groupes de $L$ candidats à être le groupe de Galois $G$. Un sous-groupe $H$ de $L$ est choisi. Grâce à $\mathfrak{I}$, une $H$-résolvante $L$-relative est calculée (note 6). Avec cette résolvante et la matrice des groupes, la liste des groupes candidats est réduite ; toujours avec cette résolvante, un idéal $\mathfrak{K}$ est calculé (théorème 6.3) ; si $H$ est inclus dans tous les groupes candidats (à conjugaison près) alors $\mathfrak{K} = \mathfrak{M}$ car $GH = G$ (on peut toujours choisir $H = I_n$ lorsque les calculs sont abordables) ; sinon, si $\mathfrak{K}$ n'est pas pur, sont alors calculés l'idéal de Galois pur $G.\mathfrak{K}$ et son groupe de décomposition $D$ (voir les points 1. à 4. ci-dessus). Seuls les candidats sous-groupes de $D$ sont conservés. Ensuite l'algorithme cherche à exploiter les autres facteurs de $R$ pour avancer vers l'idéal maximal (tout dépend des degrés des facteurs qui lorsqu'ils s'élèvent rendent difficiles les calculs de bases de Gröbner). Tant que l'idéal $\mathfrak{M}$ n'est pas atteint, l'algorithme `GaloisIdéal` se poursuit récursivement.

Évidemment, l'algorithme est améliorable dès lors qu'une nouvelle relation (génératrice ou non) est calculable par toute autre méthode. Par exemple, lorsque le degré d'un polynôme $F_i$ est connu (car identique pour tous les groupes candidats) et que la méthode $p$-adique s'avère plus efficace que celle des résolvantes pour calculer $F_i$.

NOTE 6. Chaque résolvante est doublement exploitée : pour déterminer le groupe de Galois et pour calculer de nouvelles relations. Pour calculer des résolvantes $L$-relatives, nous utilisons l'idéal $\mathfrak{I}$. Sont ainsi évités le calcul et la factorisation de résolvantes absolues de degrés élevés (voir exemple 7.2, note 8 pour s'en convaincre). Une résolvante $L$-relative par $\Theta$ est calculable de deux manières : soit avec des résultants éliminant les variables $x_i$ de $x - \Theta$ dans $k[x_1, \ldots, x_n]/\mathfrak{I}$ (voir [5]), soit en réduisant modulo $\mathfrak{I}$ les coefficients de la résolvante générique $\prod_{i=1}^{e}(x - \sigma_i.\Theta)$, puisqu'étant symétriques en les polynômes de la $L$-orbite de $\Theta$, ils sont invariants par $L$ (proposition 6.1).

EXEMPLE 6.5. Choisissons le polynôme $f = x^8 + x^6 + 2x^2 + 4$ de la base de données de MAGMA et dont le groupe de Galois sur $k = \mathbb{Q}$ est $8T_{19}$.

Considérons l'idéal de Galois de $f$ suivant :

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

Les calculs qui nous ont amenés à $\mathfrak{K}$ 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 $\mathscr{M}(\mathfrak{K})$. 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

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

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

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

L'algorithme `GaloisIdéal` peut se poursuivre récursivement avec $G.\mathfrak{K}$ (la dimension de l'anneau quotient est 128) à la place de $\mathfrak{K}$ (la dimension est $3 \cdot 128 = 384$).

**6.2.** *Un nouvel algorithme.* Nous allons décrire une autre méthodologie composée de pré-calculs sur les sous-groupes de $S_n$ afin d'élaborer un algorithme efficace pour le calcul de $\mathfrak{T}$. Par pré-calculs, nous entendons calculs ne dépendant que du groupe $G$ et qui s'appliqueront à tout polynôme de groupe de Galois $G$. Nous reprenons les notations des paragraphes précédents. En particulier, concernant le paragraphe 3, l'invariant $\Theta$ 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 dits *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'algorithme général se ramènera. Ce qui

suit relève de calculs groupistiques et non de calculs sur les polynômes. Il s'agit, par une pré-étude sur $G$, de décrire les modules fondamentaux de tout polynôme de groupe de Galois $G$.

ÉTAPE 1 : Facteurs fondamentaux appartenant à $k[x]$.

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

Supposons que $G$ possède $r \geq 1$ classes de transitivité. Alors $f$ a 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 :

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

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

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

REMARQUE 6.6. Si $f$ est réductible sur $k$ alors nécessairement les degrés $m_{j_1}, \ldots, m_{j_r}$ de ses modules fondamentaux sont strictement inférieurs à $n$ (on a $n = m_{j_1} + \cdots + m_{j_r}$).

Les facteurs fondamentaux de corps minimal $k$ ainsi que leurs groupes de Galois sur $k$ et leurs degrés respectifs ne dépendent que de $j_1, \ldots, j_r$, $\phi(G)$ et $d(G)$ calculés à partir de $G$.

Voici une idée très simple pour calculer efficacement de nombreux modules fondamentaux. 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

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

NOTE 7. Comme nous le constaterons lors de la deuxième étape, il est possible de prévoir par des calculs groupistiques que certains modules fondamentaux parmi $f_{j_1}, \ldots, f_{j_r}$ seront calculables par permutation d'autres facteurs déjà calculés (proposition 6.8). L'utilisation de la formule (10) est elle aussi prévisible en fonction de $G$ uniquement. En effet, il s'agit d'utiliser les indices $j_1, \ldots, j_r$ et éventuellement $d(G)$ car, si un choix doit être fait pour $f_{j_s}$, ce sera le facteur le plus difficile à calculer autrement qu'avec cette formule. Nous verrons dans nos exemples comment cette idée simple en apparence donne des résultats spectaculaires.

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 $x-\alpha_1, f_{j_2}, \ldots, f_{j_r}$ 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 $G_{(1)}$.

Fixons $i$ appartenant à $\{j_2, \ldots, j_r\}$. Le corps minimal $k(\alpha_1)$ de $f_i$ est déterminé :

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

Sans être explicitement signalé, ce résultat existe déjà dans [25].

Pour simplifier, dans la suite de cette étape, nous posons $F_i = F_i(x_1, x_i)$.

Dans l'esprit de la proposition 6.4, nous allons pré-déterminer en fonction de $G$ s'il est possible ou non de calculer des facteurs fondamentaux à partir de ceux appartenant à $k(\alpha_1)$.

LEMME 6.7. *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, aucun permuté de $f_i$ par $G_{(1)}$ n'est un nouveau facteur fondamental $f_j$ de degré $m_j = m_i$. En revanche, comme le groupe $G$ est un sous-groupe transitif de $S_n$, nous pourrons appliquer la proposition suivante aux permutations $\tau$ de $G$ n'appartenant pas à $G_{(1)}$.

PROPOSITION 6.8. *Soit $i \in \{j_2, \ldots, j_r\}$. Si $\tau \in G$ satisfait les conditions*

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

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

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

*Donc $\tau.F_i = F_i(x_{\tau(1)}, x_{\tau(i)}) \in k[x_{\tau(1)}, x_{\tau(i)}]$ et le module fondamental $F_{\tau(i)}$ résulte de la réduction de $\tau.F_i$ modulo $\langle F_1, \ldots, F_{\tau(i)-1}\rangle$.*

*Démonstration.* Nous avons $\tau(1) \neq 1$, d'après le lemme 6.7. Le reste est évident puisque $F_i \in k[x_1, x_i]$. ∎

Soient $\tau_1 = \mathrm{id}, \ldots, \tau_n$ 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 $x - \alpha_j$ et $f_{\tau_j(i)}$ 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 6.8 aux seules permutations $\tau_2, \ldots, \tau_n$ de $G$.

Inversement à la proposition 6.8, 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 6.8 s'applique pour déduire le module $F_l$ d'un des modules $F_{j_2}, \ldots, F_{j_r}$.

*Descriptif de l'algorithme.* Le polynôme $f$ est supposé être un polynôme quelconque de groupe de Galois $G$ sur un corps $k$. Il s'agit d'élaborer un algorithme portant sur $G$ et décrivant les facteurs fondamentaux de $f$. L'écriture de l'algorithme serait illisible. Nous décrivons comment le construire.

Il faut d'abord appliquer la première étape à $G$ avec comme données abstraites le polynôme $f$ et le corps $k$ ; on obtient ainsi $j_1, \ldots, j_r$, $\phi(G)$ et $d(G)$ et nous savons que nous pouvons calculer dans le corps $k(\alpha_{j_1}, \ldots, \alpha_{j_s})$ isomorphe à

$$k[x_{j_1}, \ldots, x_{j_r}]/\langle f_{j_1}, \ldots, f_{j_r}\rangle.$$

Ensuite, à chaque groupe $\phi(G, \mathfrak{O}_s)$, différent de l'identité, agissant transitivement sur $\mathfrak{O}_s$ et obtenu lors de la première étape, est appliquée (à la place de $G$) la deuxième étape avec comme données abstraites $f_{j_s}$ (à la place de $f$) et le corps $k$. Cette deuxième étape renvoie à la première étape. On recommence alors ce que nous venons de décrire. Et ainsi de suite, récursivement, jusqu'à ce que tous les modules fondamentaux soient décrits avec leurs corps minimaux respectifs.

Ainsi, lors d'un appel récursif à la deuxième étape, sera étudié un polynôme $g$ de degré $m$ et irréductible sur une extension $k_{\underline{u}} = k(\alpha_{u_1}, \ldots, \alpha_{u_i})$ ; de plus, les calculs précédents réalisés sur $G$ nous assurent qu'un sous-ensemble $\mathfrak{T}' = \{f_{i_1}, \ldots, f_{i_l}\}$ de $\mathfrak{T}$ est déjà calculable ; cela signifie qu'avec $\mathfrak{T}'$ les calculs algébriques dans le corps $k(\alpha_{i_1}, \ldots, \alpha_{i_l})$ sont possibles. Le polynôme $g$ sera un facteur fondamental de $f$ sur $k$. Les données de l'étape 2 seront $g$, $k_{\underline{u}}$, l'ensemble $\mathfrak{T}'$ (ce sont des données abstraites), et le groupe de Galois $G_{\underline{u}}$ de $\underline{\beta}$ sur $k_{\underline{u}}$ calculé avec la fonction $\phi$, où $\underline{\beta}$ est 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 $S_n$. La première étape est appliquée, en n'oubliant pas la formule (10) qu'il faut utiliser avec $\mathfrak{T}'$ pour déterminer quel facteur $f_{j_s}$ s'en déduira. L'ensemble $\mathfrak{T}'$ est ainsi agrandi et il ne reste qu'à appliquer la proposition 6.8, au groupe $G$, et non pas uniquement au groupe $G_{\underline{u}}$, comme l'illustrera l'exemple du groupe $\mathrm{PSL}(2,7)$ du paragraphe 7. L'algorithme se poursuit ainsi récursivement en cherchant à prédire le calcul et les corps minimaux des modules fondamentaux n'appartenant pas encore à $\mathfrak{T}'$.

*Calcul effectif des modules fondamentaux.* L'algorithme sur le groupe $G$ détermine les facteurs (modules) fondamentaux qui par la proposition 6.8 ou la formule (10) seront déductibles des autres, appelés *principaux*. Pour calculer un facteur fondamental principal $f_i$, nous disposons de plusieurs méthodes, comme : l'algorithme `GaloisIdéal` (voir l'exemple du groupe $8T_{39}$ du paragraphe 7), les algorithmes de factorisation dans les extensions (voir, par exemple, celui historique de B. Trager [28]), la méthode interpolatrice de M. Lederer, la méthode $p$-adique de K. Yokoyama lorsque le degré $m_i =$

$\underline{m_i}(G)$ est déterminable et connaissant le corps minimal de $f_i$ pour éviter le calcul des coefficients a priori nuls.

**6.3.** *Application des résultats dans un cas général.* Dans le paragraphe précédent, nous avons décrit une méthodologie de pré-étude portant sur un groupe $G$ donné 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 $k_{\underline{u}}$. Tant que le groupe de Galois n'est pas déterminé, à tout moment, il est possible d'utiliser l'algorithme `GaloisIdéal` en rajoutant, si nécessaire, des modules de Cauchy de facteurs fondamentaux déjà calculés ([25]). De la sorte, il est possible de produire un algorithme très efficace pour le calcul simultané de $\mathfrak{T}$ et $G$ en degré $n$. Si le groupe $G$ est déjà déterminé, l'algorithme se simplifie. L'utilisation de `GaloisIdéal` est restreinte au calcul de nouvelles relations avec des résolvantes relatives ; il faudra alors comparer au cas par cas son efficacité avec d'autres méthodes (interpolatrice de M. Lederer, $p$-adique de K. Yokoyama, ...).

En fait, l'algorithme idéal de calcul de $\mathfrak{T}$ serait parallèle. En même temps que le groupe de Galois serait déterminé, des relations seraient calculées (avec toute méthode possible), d'autres en seraient déduites par la formule (10) ou l'une des propositions 6.4 et 6.8. Chaque calcul parallèle viendrait enrichir un corps principal qui redistribuerait les informations récoltées et orienterait les calculs en fonction des avancées tout en construisant des idéaux de Galois.

**7. Exemples.** Nous allons illustrer les résultats du paragraphe 6 à travers trois 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 avec l'utilisation de `GaloisIdéal`. Le troisième montre comment utiliser correctement la proposition 6.8.

**7.1.** *Un groupe d'ordre 384 conjugué de* $8T_{44}$. Donnons-nous 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 $\underline{m}(G) = (8,1,6,4,1,1,2,1)$. Pour comprendre les calculs groupistiques, nous supposons qu'un polynôme $f$ ait $G$ comme groupe de Galois sur un corps $k$. Nous commençons par la première étape qui, puisque $G$ est transitif, nous donne le premier facteur principal :

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

Comme $\mathfrak{T}' = \{f_1\}$, il est possible de calculer dans $k(\alpha_1)$ isomorphe à $k[x_1]/f_1$. Dans le contexte de la deuxième étape avec $f_1$, $k$ et $G$ comme données, nous appliquons la première avec $f_1$, $k(\alpha_1)$ et $G_{(1)}$. Le groupe

$G_{(1)}$ est le groupe $G^*$ de l'exemple 3.4. Nous calculons $j_2 = 2$ et $j_3 = 3$, $d(G_{(1)}) = (1, m_2, m_3) = (1, 1, 6)$ et $\phi(G^*)$. Donc, dans $k(\alpha_1)$, $f_1$ a deux facteurs linéaires $x - \alpha_1$ et $f_2$ et le facteur $f_3$ de degré 6 et de groupe de Galois $\phi(G^*, \mathfrak{O}_3)$ sur $k(\alpha_1)$. Ceci nous donne

$$f_2, f_3 \in k(\alpha_1)[x] \quad \text{ou bien} \quad F_2 \in k[x_1, x_2] \text{ et } F_3 \in k[x_1, x_3].$$

Nous décidons que le facteur linéaire $f_2$ (ou bien $F_2$) sera principal ; donc $\mathfrak{T}' = \{f_1, f_2\}$. Le facteur $f_3$ sera obtenu avec la formule (10) :

$$f_3 = \frac{f_1}{(x - \alpha_1) f_2} \in k(\alpha_1)[x]. \tag{11}$$

Désormais $\mathfrak{T}' = \{f_1, f_2, f_3\}$ et nous pouvons calculer dans $k(\alpha_1, \alpha_2, \alpha_3)$. Comme $f_2 \in \mathfrak{T}'$ et $m_2 = m_5 = m_6 = m_8 = 1$, nous cherchons à utiliser la proposition 6.8 avec l'indice $i = 2$ de $m_2$. Des trois permutations $\tau_3 = (1,3)(2,5)(4,8)(6,7)$, $\tau_4 = (1,4,5,8,2,6,3,7)$ et $\tau_7 = (1,7,3,6)(2,8,5,4)$ de $G$ modulo $G_{(1)}$, nous pourrons déduire les trois facteurs fondamentaux :

$$f_5 = F_2(\alpha_3, x), \quad f_6 = F_2(\alpha_4, x), \quad f_8 = F_2(\alpha_7, x). \tag{12}$$

Maintenant $\mathfrak{T}' = \{f_1, f_2, f_3, f_5, f_6, f_8\}$. Il reste à trouver les facteurs fondamentaux $f_4$ et $f_7$ de degrés respectifs $m_4 = 4$ et $m_7 = 2$. Nous appliquons (récursivement) l'étape 2 au polynôme $f_3$ (pas à $f_2$ car ce facteur est linéaire), irréductible sur $k(\alpha_1, \alpha_2) = k(\alpha_1)$ avec $\phi(G^*, \mathfrak{O}_3)$ 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 $\alpha_i$). Appliquons l'étape 1 avec $f_3$ sur $k(\alpha_1)(\alpha_3)$. Le stabilisateur de 3 dans $H = \phi(G^*, \mathfrak{O}_3)$ 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 $G_{(3)}$). Comme $j_1 = 3$, $j_2 = 4$ et $j_3 = 5$ avec $f_3, f_5 \in \mathfrak{T}'$, dans $k(\alpha_1, \alpha_3)[x]$, la formule (10) nous permettra de calculer rapidement $f_4$ :

$$f_4 = \frac{f_3}{(x - \alpha_3) f_5} \in k(\alpha_1, \alpha_3)[x]. \tag{13}$$

Nous avons $\mathfrak{T}' = \{f_1, f_2, f_3, f_4, f_5, f_6, f_8\}$. 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 alors récursivement l'étape 2 au groupe $H^*$, supposé être le groupe de Galois de $f_4$ sur $k(\alpha_1, \alpha_3)$. 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 $H^*$). Ici $j_1 = 4$, $j_2 = 6$ et $j_3 = 7$ avec $f_4, f_6 \in \mathfrak{T}'$. Donc, d'après la formule (10), nous obtenons

$$f_7 = \frac{f_4}{(x - \alpha_4) f_6} \in k(\alpha_1, \alpha_3, \alpha_4)[x]. \tag{14}$$

Nous pourrons donc calculer les 8 modules fondamentaux à partir des deux principaux : $F_1 = f(x_1) \in k[x_1]$ 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 $k(\alpha_1)$. Sans la formule (10) et la proposition 6.8, par la méthode classique de factorisation dans les extensions, pour obtenir $f_4$ et $f_5$, il faut 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 $288 = 6 \cdot 48$ (voir [28]). 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 $768 = 192 \cdot 4$. 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. En suivant l'algorithme `GaloisIdéal`, nous calculons simultanément des facteurs fondamentaux et le groupe de Galois avec les matrices de groupes. 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, 24]) 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 $k$ est l'un des quatre 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 [30]). 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 $8T_{44}$ (exemple 7.1). Avec les polynômes $F_1,\ldots,F_8$, nous sommes en mesure de calculer des résolvantes $G$-relatives ([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)

$$H = \langle (1,8)(2,7)(3,4)(5,6), \tau_3, (1,6)(2,4)(3,7)(5,8), \\ (1,4,3)(2,6,5), (1,2)(3,6,5,4)\rangle \tag{15}$$

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 $\mathfrak{I}$ 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 $(4,6).\mathfrak{M}$ (car $H$ est auto-adjoint dans $G$ et $G = H + H(4,6)$) tels que

$$\mathfrak{I} = \mathfrak{M} \cap (4,6).\mathfrak{M}.$$

Déterminons à la fois le groupe de Galois et $\mathfrak{T}$ (i.e. le module fondamental manquant). Commençons par calculer $\Theta$, un $H$-invariant $G$-relatif, et réduisons-le à $\theta$ modulo $\mathfrak{I}$. Nous calculons (note 6)

$$R_2 = (x - \theta(\underline{\alpha}))(x - (4,6).\theta(\underline{\alpha}))$$

(car $G = H + (4,6)H$), la résolvante $G$-relative de $\underline{\alpha}$ par $\theta$ 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 6.3, nous avons finalement

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

NOTE 8. À travers cet exemple, nous constatons l'intérêt du calcul d'un ensemble triangulaire engendrant l'idéal de Galois $\mathfrak{I}$. Nous avons pu calculer une $H$-résolvante relative (ici $G$-relative) de degré 2 à la place d'une $H$-résolvante absolue de degré $210 = [S_7 : H]$ dont $R_2$ serait un facteur qu'il faudrait identifier. Cette résolvante teste si le groupe de Galois est ou n'est pas $8T_{39}$. De plus, à partir de $\mathfrak{I}$, en utilisant un facteur de $R_2$, nous aboutirons rapidement à l'ensemble triangulaire $\mathfrak{T}$ engendrant $\mathfrak{M}$.

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 $k = \mathbb{Q}$ 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 linéaire sur $k(\alpha_1)$ soit

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

En appliquant les formules (11)–(14) de l'exemple 7.1, nous en déduisons les générateurs de l'idéal de Galois $\mathfrak{I}$ :

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

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

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

Voyons comment avec Maxima nous calculons $f_7$ (avec $x_i$ à la place de $\alpha_i$) :

```
(C10) f7:divide(f4,x^2-x4^2,x);
(D10) [x4^2+x1^2+x3^2+x^2,x4^4+(x1^2+x3^2)*x4^2+x1^4+x3^2*x1^2+x3^4];
```

Vérifions que le reste est nul :

```
(C11) divide(x4^4+(x1^2+x3^2)*x4^2+x1^4+x3^2*x1^2+x3^4,ev(f4,x=x4));
(D11) [1,0];
```

Nous calculons $\theta = x_1x_2x_4x_7 = \Theta$ modulo $\mathfrak{I}$ et, toujours en utilisant l'ensemble triangulaire engendrant $\mathfrak{I}$, nous calculons $R_2 = (x-1)(x+1)$. Ce calcul peut se faire en éliminant $x_1, x_2, x_4, x_7$ dans $x - \theta$ avec des résultants ou en réduisant $x_1x_2x_4x_7 + x_1x_2x_6x_7$ et $x_1x_2x_4x_7.x_1x_2x_6x_7 = x_1^2x_2^2x_4x_6x_7$ modulo $\mathfrak{I}$ (voir note 6). Du calcul (c'est une sysigie intervenant dans les calculs classiques de bases de Gröbner)

$$g_7 = x_1x_2x_3f_7(x_7) - x_7(\theta - 1) = x_7 + x_1x_2x_3^3 + x_1x_2^3x_3 + x_1^3x_2x_3$$

nous déduisons que le groupe $H$ donné en (15) est le groupe de Galois associé (i.e. son groupe de décomposition) à l'idéal maximal $\mathfrak{M}$ engendré par l'ensemble triangulaire

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

*Commentaires.* Cet exemple est assez étonnant car 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. Pour éviter des factorisations dans les extensions, il est également possible d'appliquer la méthode de M. Lederer ou celle de K. Yokoyama. Rappelons que l'algorithme idéal serait parallèle. Ainsi, il faudrait lancer simultanément plusieurs méthodes pour calculer $g_7$. Dans ce cas précis, nous aurions pu exploiter la parité de $f$ pour réduire les calculs de $f_3$, $f_4$ et $f_7$.

**7.3.** *Le groupe* $\mathrm{PSL}(2,7) = 7T_5$ *à 168 éléments.* (Voir [33] 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 $\mathrm{PSL}(2,7)$ 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

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

Puis, en appliquant l'étape 2 à $G_{(1)}$ et $f_2$, nous passons à l'étape 1 avec $G_{(2)} = \langle (4,6)(5,7), (4,5)(6,7)\rangle$ et $f_2$ dans $k(\alpha_1, \alpha_2)$ ; nous avons

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

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 6.8 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

$$f_5 = F_3(\alpha_1, \alpha_4, x), \qquad f_7 = F_3(\alpha_1, \alpha_6, x).$$

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

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

Pour le polynôme $f = x^7 - 7x + 3$ de groupe de Galois $7T_5$, nous avons

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

Ce polynôme est calculable par toutes les méthodes déjà évoquées et, en particulier, en moins d'une seconde par une factorisation partielle de $f$ sur $k(\alpha_1, \alpha_2)$ isomorphe à $k[x_1, x_2]/\langle f_1, f_2\rangle$.

*Commentaire.* Pour la détermination de $\mathfrak{T}$, si le groupe de Galois $7T_5$ est déterminé, avec la formule (10) et la proposition 6.8, tous les modules fondamentaux se calculent à partir des deux principaux $F_1 = f(x_1) \in k[x_1]$ et $F_3 \in k[x_1, x_2, x_3]$, linéaire en $x_3$. Ici encore le gain est remarquable.

**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 son 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 eus avec eux. Ils m'ont aidée dans le cheminement de 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 bénéficier de ses compétences en géométrie algébrique. J'ai pu exposer à cette occasion mon pre-

mier cours de théorie de Galois avec les idéaux de Galois et l'algorithme `GaloisIdéal`. Je n'oublie pas les interventions de Kurt Girstmair, de Francis Touazi et les remarques nombreuses et judicieuses de mon rapporteur anonyme.

## Références


[1] I. Abdeljaouad, *Calculs d'invariants primitifs de groupes finis*, Theor. Inform. Appl. 33 (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*, 1824, dans : Œuvres complètes, vol. 1, Gabay, Sceaux, 1992, 28–33.

[3] H. Anai, M. Noro and K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials*, dans : Algorithms in Algebraic Geometry and Applications (Santander, 1994), Progr. Math. 143, Birkhäuser, Basel, 1996, 29–50.

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

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

[6] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, ibid. 24 (1997), 235–265.

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

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

[9] E. Galois, *Œuvres 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 (1982), 81–97.

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

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

[14] M. Á. Gómez-Molleda, *Cálculo del centro de un grupo de Galois y aplicaciones*, tesis doctoral, Universidad de Cantabria, 1999.

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

[16] A. Hulpke, *Konstruktion transitiver Permutationsgruppen*, thèse Ph.D., Rheinisch Westfälische Technische Hochschule, Aachen, 1996.

[17] —, *Techniques for the computation of Galois groups*, dans : Algorithmic Algebra and Number Theory (Heidelberg, 1997), Springer, Berlin, 1999, 65–77.

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

[19] —, —, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. 30 (2000), 675–716.

[20] J. Lagrange, *Réflexions sur la résolution algébrique des équations*, Nouveaux Mém. Acad. Roy. Sci. Belles-Lett. Berlin 1770, 134–215 (dans : Œuvres, vol. 3).

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

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

[23] A. Machí, *Dispense di teoria di Galois*, Dipartemento di Matematica, Universitá degli Studi di Roma "La Sapienza", http://www.mat.uniroma1.it/people/machi/Galois/.

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

[25] S. Orange, G. Renault et A. Valibouze, *Calcul efficace de corps de décomposition*, en révision à Exp. Math. (2003); issu du rapport 2003/005 du laboratoire LIP6, http://www.lip6.fr/.

[26] W. Schelter, *Manuel de Maxima*, 2001, http://maxima.sourceforge.net.

[27] N. G. Tschebotaröw [N. G. Tchebotarev], *Gründzüge des Galois'schen Theorie*, Noordhoff, Groningen, 1950.

[28] B. Trager, *Algebraic factoring and rational function integration*, dans : Symbolic and Algebraic Computation (Proc. SYMSAC'76, Yorktown Heights, NY), R. D. Jenks (ed.), Assoc. for Computing Machinery, New York, 1976, 219–226.

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

[30] —, *Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems*, dans : Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Paris, 1995), Lecture Notes in Comput. Sci. 948, Springer, Berlin, 1995, 456–468.

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

[32] —, *Galois theory and reducible polynomials*, publication interne 99.03, Équipe MAX, Laboratoire LIX, École Polytechnique, 1999, http://www.lix.polytechnique.fr/~max/publications/.

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

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

[35] T. Wada and H. Ohsugi, *Gröbner bases of Hilbert ideals of alternating groups*, J. Symbolic Comput. 41 (2006), 905–908.

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

L.I.P.6, Université Pierre et Marie Curie
4, place Jussieu
F-75252 Paris Cedex 05, France
E-mail: annick.valibouze@upmc.fr
http://www-calfor.lip6.fr/~avb/

*Reçu le 3.5.2006*
*et révisé le 10.9.2007* (5196)