Calcul efficace de corps de décomposition : version préliminaire avant le rapport LIP6

S. Orange, G. Renault, A. Valibouze

10 Septembre 2002

1 Introduction.

Dans cet article, nous fixons un corps k supposé parfait et un polynôme f irréductible sur k et de degré n. Sous ces hypothèses, les racines $\alpha_1, \alpha_2, \cdots, \alpha_n$ de f dans une clôture algébrique $\overline{k}$ de k sont nécessairement distinctes et le groupe de Galois $Gal_k(f)$ de f sur k est transitif. Nous le noterons G.

Une première méthode pour l'obtention du corps de décomposition K du polynôme f consiste à calculer un ensemble triangulaire séparable T de l'anneau des polynômes $k[x_1, \cdots, x_n]$ engendrant un idéal I, appelé *idéal des relations*. Cet idéal est maximal et le corps K est isomorphe à l'anneau quotient $k[x_1, \cdots, x_n]/I$. Une autre méthode, intrinsèquement exponentielle, consiste à obtenir un polynôme k-primitif F du corps K en calculant une résolvante de Galois du polynôme f car le corps K est isomorphe à $k[x]/ < f(x) >$ (voir [**?**]). Elle est donc à exclure.

Le but de cet article est de proposer un algorithme efficace pour le calcul de l'idéal I, c'est-à-dire celui de l'ensemble triangulaire T.

Dans [Yok97] et dans [Tch50], il est proposé de factoriser successivement le polynôme f dans les extensions algébriques $k(\alpha_1), k(\alpha_1, \alpha_2), \cdots, K = k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ (voir [Yok99] pour une optimisation). Chaque factorisation fait apparaître un ou plusieurs polynômes qui appartiennent à l'ensemble triangulaire T. La factorisation de f dans $k(\alpha_1)$ construit le corps $k(\alpha_1, \alpha_2)$ et ainsi de suite. Mais l'expression algébrique de chaque polynôme apparaissant

après chaque factorisation n'est pas suffisamment exploitée avant de passer à la factorisation suivante. De plus, les groupes de Galois et les degrés des facteurs non linéaires ne sont pas pris en considération pour la construction de l'ensemble T.

Par ailleurs, dans [Val99], l'algorithme `GaloisIdéal` construit récursivement, jusqu'à l'idéal I, une chaîne ascendante :

$$I_1 \subset I_2 \subset \cdots \subset I_r = I \qquad (*)$$

d'idéaux dit de *Galois* à partir d'un idéal I_1 connu (voir paragraphe 6.3.2). Pour chaque $j \in \{2, \cdots, r\}$, le temps calcul de l'idéal I_j est d'autant plus faible que le cardinal de la variété de I_{j-1} est petit. Il est toujours possible de prendre pour I_1 l'idéal I^{S_n} des relations symétriques entre les racines du polynôme f qui peut, à l'instar de f, être considéré comme la donnée du problème. Mais la variété de I^{S_n} a pour cardinal $n!$ (celle de l'idéal I des relations a pour cardinal celui du groupe de Galois G de f sur k). La faiblesse de cet algorithme est donc le temps calcul du début de la chaîne lorsque $I_1 = I^{S_n}$. Ainsi, une méthode calculant plus efficacement que l'algorithme `GaloisIdéal` un idéal J de Galois contenant strictement I^{S_n} améliorera d'autant le temps de calcul de l'idéal I des relations en prenant $I_1 = J$.

Pour parer simultanément aux faiblesses respectives des deux méthodes précédentes, nous cherchons à construire des idéaux de Galois à partir des factorisations dans les extensions algébriques. Afin de simplifier la présentation, nous expliquerons notre démarche sur la première extension $k(\alpha_1)$. Les deux idées de base sont que :

1) Les degrés et les groupes de Galois des facteurs (irréductibles) $f_1 = x - \alpha_1, f_2, \cdots, f_s$ de f dans $k(\alpha_1)[x]$ ne dépendent que du groupe de Galois G de f ; ainsi, nous définissons une table dite *de première rupture* qui, à une factorisation type (degrés et groupes de Galois sur $k(\alpha_1)$ des polynômes $f_1, \cdots, f_s$), associe les groupes candidats à être le groupe de Galois G (voir Paragraphe 4.3 et la table 1 pour le degré 8). Des informations sur les degrés initiaux des polynômes de l'ensemble triangulaire T cherché se déduisent de cette table (voir paragraphe 6.3.1).

2) Les facteurs $f_1, f_2, \cdots, f_s$ de degrés respectifs $n_1 = 1, n_2, \cdots, n_s$ peuvent permettre de calculer un idéal de Galois contenant strictement l'idéal I^{S_n} ; en effet, nous montrons comment déterminer rapidement un idéal de Galois J dit de *départ* dont la variété est de cardinal $n_1!n_2! \cdots n_s!$ (voir Théorème 5.4 et ? ? ? ?) ; l'idéal J contient strictement I^{S_n} lorsque le groupe de Galois G n'est pas 2-transitif.

Notre objectif sera alors d'utiliser l'algorithme `GaloisIdéal` pour calculer l'idéal I à partir de $I_1 = J$ à la place de $I_1 = I^{S_n}$.

Il sera nécessaire de savoir calculer le stabilisateur (appelé aussi le fixateur) de l'idéal J faute de quoi l'algorithme `GaloisIdéal` est inutilisable avec $I_1 = J$. Les résultats que nous obtenons en ce sens (voir corollaire 5.7 et proposition 5.9) sont importants car, pour un idéal de Galois quelconque, le calcul de son stabilisateur n'est réalisable que si l'idéal des relations I est déjà connu.

Nous verrons que nos résultats sont très délicats à appliquer lorsque plusieurs degrés parmi $n_2, \cdots, n_s$ sont égaux puisqu'alors l'ordre des polynômes $f_2, \cdots, f_s$ ne peut être déterminé de manière unique à partir des degrés. Pour répondre à cette difficulté, nous définirons des classes d'équivalences sur les groupes qui permettront d'associer l'idéal de départ J à une telle classe (voir paragraphe 6.2.1).

Il sera parfois possible d'obtenir rapidement un nouvel idéal J' contenant strictement J ainsi que son le stabilisateur (voir Proposition ? ? ? ?). L'algorithme `GaloisIdéal` démarrera alors avec $I_1 = J'$. Ce dernier idéal s'avère parfois être l'idéal des relations I lui-même.

A titre d'illustration, nous étudierons le degré 8. Ce degré offre un panel complet des situations diverses qu'il sera possible de rencontrer. Nous avons exclus le cas des groupes 2-transitifs (voir Paragraphe 4.3). Ce cas s'inscrit dans une étude globale des extensions supérieures qui s'appuie sur les résultats fondamentaux de cet article.

2 Notations.

Dans cet article, nous utiliserons les notations suivantes :
- $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \bar{k}^n$ désignera un n-uplet de racines de f ;
- pour toute racine α de f, $\mathrm{ind}(\alpha)$ désignera l'indice de α dans $\underline{\alpha}$ (par exemple $\mathrm{ind}(\alpha_2) = 2$) ;
- pour tout ensemble fini E, l'ensemble des permutations de E (respectivement, de $\{1, \cdots, n\}$) sera noté S_E (respectivement, S_n) ;
- si E désigne un ensemble fini et G un sous-groupe de S_E , le stabilisateur d'un élément $e \in E$, considéré comme un sous-groupe de $S_{E\setminus\{e\}}$, sera noté $Stab(G, e)$ ou $Stab_G(e)$;

– soit L un sous-ensemble de S_n, le sous-ensemble de L des éléments $l \in L$ tels que $l(1) = i$ sera noté $L_{\{i\}}$;
– la notation exponentielle pour les suites finies d'un ensemble quelconque ; par exemple, la suite finie a, a, a, b, c, c s'écrira a^3, b, c^2 ;
– le i-ième groupe transitif de S_n (à conjugaison près dans S_n) sera le groupe noté nT_i de la nomenclature de MAGMA (voir [McKay]) ;
– $\mathcal{T}(n)$ désignera l'ensemble fini $\{nT_1, \cdots\}$ des représentants des classes des groupes transitifs de degré n.

Notation $\sigma.R.\ L.\sigma.\ S_e$

3 Idéaux de Galois.

Définition 3.1. Soit L un sous-ensemble de S_n. L'*idéal de $\underline{\alpha}$-relations invariantes par L* est défini par :

$$I_{\underline{\alpha}}^L = \{R \in k[x_1, ..., x_n] \mid \forall l \in L,\ l.R(\underline{\alpha}) = 0\}.$$

En particulier, l'idéal $I_{\underline{\alpha}} = I_{\underline{\alpha}}^{\{Id\}}$ (respectivement, $I_{\underline{\alpha}}^{S_n}$) est appelé l'*idéal des $\underline{\alpha}$-relations* (respectivement, *idéal des relations symétriques*).

Définition 3.2. Un idéal I de $k[x_1, ..., x_n]$ est un *idéal de Galois* (relativement au polynôme f) s'il existe $\underline{\alpha} \in \bar{k}^n$ un n-uplet de racines de f et un sous-ensemble L de S_n tel que :

$$I = I_{\underline{\alpha}}^L.$$

L'idéal I est alors appelé un $(\underline{\alpha}, L)$-idéal de Galois.

La proposition suivante donne une caractérisation des idéaux de Galois.

Proposition 3.3. *Un idéal I de $k[x_1, \cdots, x_n]$ est un idéal de de Galois ssi il vérifie les deux assertions suivantes :*

1. *I est un radical,*
2. *il existe $\underline{\alpha} \in \bar{k}^n$ un n-uplet de racines de f tel que $V(I)$ soit une sous-variété de $S_n.\underline{\alpha}$.*

Démonstration. Supposons que I vérifie ces deux assertions. D'après 2), il existe un sous ensemble L de S_n tel que $V(I) = L.\underline{\alpha}$, et donc,

$$\sqrt{I} = \{P \in k[x_1, \cdots, x_n] \mid \forall \sigma \in L,\ P(\sigma.\underline{\alpha}) = 0\} = I^L_{\underline{\alpha}}.$$

L'assertion 1) donne alors le résultat $I = I^L_{\underline{\alpha}}$.
La réciproque découle de la définition des idéaux de Galois. □

Fixons I un $(\underline{\alpha}, L)$-idéal de Galois.

Définition 3.4. L'ensemble $L_{\underline{\alpha}} = \{\tau \in S_n | \tau.\underline{\alpha} \in V(I)\} = \{\tau \in S_n | \forall R \in I, \tau.R(\underline{\alpha}) = 0\}$ est appelé le *stabilisateur de I relatif à $\underline{\alpha}$*.

Les stabilisateurs de l'idéal de Galois I sont reliés par la proposition suivante :

Proposition 3.5. *Soient $\underline{\alpha}$ et $\underline{\beta}$ deux n-uplet de la variété $V(I)$. Alors, il existe $\sigma \in L_{\underline{\alpha}}$ tel que $\underline{\beta} = \sigma.\underline{\alpha}$ et nous avons l'égalité :*

$$L_{\underline{\beta}} = \sigma^{-1} L_{\underline{\alpha}}.$$

Démonstration. D'après la définition 3.2, $\underline{\alpha}$ appartient à la sous-variété $V(I)$ de $S_n.\underline{\beta}$. Il existe donc $\sigma \in S_n$ tel que $\underline{\beta} = \sigma.\underline{\alpha}$. Puisque $\underline{\beta} \in V(I)$, pour tout $R \in I$, nous avons l'égalité $0 = R(\underline{\beta}) = R(\sigma.\underline{\alpha})$ et par suite $\sigma \in L_{\underline{\alpha}}$.
De plus, nous avons :

$$\begin{array}{rcl} \sigma^{-1} L_{\underline{\alpha}} & = & \{\sigma^{-1}\tau \in S_n | \forall R \in I, (\tau.R)(\underline{\alpha}) = 0\} \\ & = & \{\sigma^{-1}\tau \in S_n | \forall R \in I, (\sigma^{-1}\tau.R)(\underline{\beta}) = 0\} \\ & = & L_{\underline{\beta}}. \end{array}$$

□

Remarque 3.6. Si un stabilisateur de I est un groupe alors tous les stabilisateurs de I sont identiques au groupe de décomposition de l'idéal I défini ci-dessous pour un idéal quelconque :

$$Dec(I) = \{\sigma \in S_n | \forall R \in I,\ \sigma.R \in I\}$$

Définition 3.7. Le *groupe de Galois* de $\underline{\alpha}$ sur k, noté $Gal_k(\underline{\alpha})$, est le groupe de décomposition de l'idéal des relations $I_{\underline{\alpha}}$.

?????????????????????????????? Le groupe de Galois $G_k(\underline{\alpha})$ est isomorphe au groupe de Galois $Gal_k(f)$ si $\underline{\alpha}$ est un n-uplet de racine de f.

4 La table des groupes de Galois des facteurs de première rupture.

Dans cette partie nous montrons comment construire l'objet central de notre article : la *table des groupes de Galois des facteurs de première rupture*. Pour ce faire, nous allons considérer le corps de rupture de f obtenu en ajoutant à k une de ses racines, les facteurs de f sur cette extension, et le groupe de Galois de chacun de ces polynômes. Dans un premier temps, nous allons rappeler comment calculer le groupe de Galois de chacun des facteurs d'un polynôme.

4.1 Groupes de Galois des facteurs irréductibles d'un polynôme

La théorie classique de Galois nous donne le moyen de connaître le groupe de Galois de chacun des facteurs irréductibles d'un polynôme à partir du groupe du groupe de Galois de ce dernier :

Proposition 4.1. *Soit $g \in k[x]$ un polynôme de degré d, $\underline{\beta} = (\beta_1, \cdots, \beta_d) \in k$ un d-uplet de racines supposées distinctes de g, et O une orbite de l'action à gauche de $Gal_k(\beta)$ sur $\{1, \cdots, d\}$. L'injection canonique*

$$\psi_O : \quad \mathrm{Gal}_k(\beta) \quad \longrightarrow \quad S_O \ ,$$

induit par l'action de $\mathrm{Gal}_k(\beta)$ sur O, a pour image le groupe de Galois d'un facteur irréductible g_1 de g sur k donné par :

$$g_1 = \prod_{i \in O} (x - \beta_i).$$

Cette proposition est un cas particulier du calcul des groupes de Galois des facteurs d''une résolvante du polynôme g que nous appliquons dans le cas où la résolvante est le polynôme g lui-même.

Démonstration. ???????????????????????????????????? □

Étant donné un groupe G de permutations, la proposition 4.1 permet de calculer les groupes de Galois de chacun des facteurs irréductibles d'un polynôme de groupe de Galois G. Ceci peut se faire à l'aide de l'algorithme suivant :

Algorithme 4.2.

FactGaloisGroups :=Fonction(G)

Entrée : G un sous-groupe de S_n

Sortie : La liste des groupes de Galois des facteurs d'un polynôme de degré n dont le groupe de Galois est G.

$n := Deg(G)$;
Sortie:= [] ;
$j := 1$;
Pour $O \in Orbites(G, \{1, \cdots, n\})$ **Faire**
Sortie$[j] := n_j T_{i_j}$ tel que $n_j T_{i_j} \simeq^1 \psi_O(H)$;
$j := j + 1$;
Fin Pour ;
Retourne Sortie ;
Fin **FactGaloisGroups** ;

Nous allons maintenant utiliser ce résultat pour étudier les groupes de Galois des facteurs irréductibles d'un polynôme sur un de ses corps de rupture.

4.2 Groupes de Galois des facteurs de première rupture.

Définition 4.3. Une extension K de k incluse dans $k(\underline{\alpha})$, isomorphe à l'algèbre quotient

$$k[x]/ < f >,$$

est appelée *extension de première rupture* (ou *corps de première rupture*) pour f.

Un corps de première rupture pour f est donc une extension de k de la forme $k(\alpha)$ avec α racine de f. Le théorème fondamental de la théorie de Galois (voir [Esc97]) nous donne alors :

Proposition 4.4. *Soit $K = k(\alpha_1)$ le corps de première rupture pour f alors :*

$$K = k(\underline{\alpha})^{Stab(Gal_k(\underline{\alpha}), 1)}.$$

[1]Cet isomorphisme peut être implémenté avec la fonction d'identification de Magma TransitiveGroupIdentification

Il s'en déduit alors le résultat suivant :

Corollaire 4.5. *Le groupe de Galois de* $\frac{f}{(x-\alpha_1)}$ *sur* $k(\alpha_1)$ *est* $Stab(Gal_k(\underline{\alpha}), 1)$ *(en tant que sous-groupe de* $S_{\{2,\cdots n\}}$*).*

Rappelons ici que le polynôme f est irréductible et que, par conséquent, pour tout $i \in \{1, \ldots, n\}$, le groupe $Stab(Gal_k(\underline{\alpha}), i)$ est isomorphe au groupe $Stab(Gal_k(f), 1)$.

Nous cherchons maintenant à déterminer le groupe de Galois de chacun des facteurs irréductibles de $\frac{f}{(x-\alpha_1)}$.

Définition 4.6. Les facteurs de $\frac{f}{(x-\alpha_1)}$ sur $k(\alpha_1)$ sont appelés *les facteurs de première rupture de* f.

Soit $\mathcal{O}$ l'ensembles des orbites de l'action de $Gal_k((\alpha_2, \cdots, \alpha_n))$ sur $\{2, \cdots, n\}$. La proposition 4.1 s'applique au cas où $O \in \mathcal{O}$, et $g = \frac{f}{(x-\alpha_1)}$. Le groupe $Gal_k((\alpha_2, \ldots, \alpha_n))$ étant isomorphe au groupe $Stab(Gal_k(f), 1)$, nous pouvons donc déduire de $Gal_k(f)$ les groupes de Galois des facteurs de première rupture. Ci-après, nous fixons les notations pour déterminer les groupes de Galois sur $k(\alpha_1)$ des facteurs de première rupture en fonction du groupe de Galois de f sur k qui est isomorphe à un des groupes de $\mathcal{T}(n)$.

Notons $\mathcal{S}(n)$ l'ensemble des suites finies $n_1T_{i_1}, \cdots, n_sT_{i_r}$ telles que $n_1 + n_2 + \cdots + n_r = n - 1$ ordonnées de sorte que nous ayons :

$$\forall j \in \{1, \cdots, r-1\},\ n_j \leq n_{j+1} \text{ et si } n_j = n_{j+1} \text{ alors } i_j \leq i_{j+1}. \qquad (4.1)$$

La Proposition 4.1 permet alors de définir l'application

$$\Gamma_n : \mathcal{T}(n) \longrightarrow \mathcal{S}(n)$$

qui à un groupe G de $\mathcal{T}(n)$ fait correspondre la suite des groupes de Galois sur $k(\alpha)$ des facteurs de première rupture d'un polynôme irréductible de degré n ayant α comme racine et G comme groupe de Galois (Ces différents groupes étant définis à une conjugaison près).

Notation 4.7. Pour tout polynôme f irréductible sur k de degré n, nous noterons $\Gamma_n(f)$ la suite finie $\Gamma_n(Gal_k(f))$.

A l'aide de l'algorithme 4.2, cette application est facilement implémentable dans un système de calcul formel (GAP ou MAGMA par exemple).

Exemple 4.8. L'exécution de **FactGaloisGroups**($Stab(8T_{46}, 1)$) retourne, à l'ordre près, $\Gamma_8(8T_{46}) = [3T_2, 4T_5]$. Ainsi, si un polynôme f de degré 8 admet pour groupe de Galois sur k le groupe $8T_{46}$ alors, comme $\Delta_8(f) = (3, 4)$, la factorisation de f sur $k(\alpha_1)$ est de la forme :

$$f(x) = (x - \alpha_1)g_1(x)g_2(x) \ ,$$

où les facteurs g_1 de degré 3 et g_2 de degré 4 appartiennent à $k(\alpha_1)[x]$. Les groupes de Galois sur $k(\alpha_1)$ des facteurs $(x - \alpha_1)$, $g_1(x)$ et $g_2(x)$ sont alors respectivement $1T_1$, $3T_2$ et $4T_5$.

Quelque soit le polynôme irréductible f, nous savons, à partir de son groupe de Galois, calculer les groupes de Galois de chacun de ses facteurs de première rupture. La table que nous allons construire dans la prochaine section va recenser les informations obtenues par ce procédé.

4.3 Construction de la table des groupes de Galois des facteurs de première rupture

Étant donné un suite finie s de $\mathcal{S}(n)$, nous voulons savoir quels sont les groupes T de $\mathcal{T}(n)$ vérifiant $\Gamma_n(T) = s$ (i.e. déterminer $\Gamma_n^{-1}(s)$). En effet, si les groupes de Galois des facteurs de première rupture d'un polynôme irréductible f correspondent à la suite s alors le groupe de Galois de f sera isomorphe à l'un des groupes appartenant à $\Gamma_n(T)^{-1}(s)$. Ainsi, nous pouvons obtenir la liste de groupe de Galois candidats pour le polynôme f en ne considérant que les degrés des facteurs de première rupture :

Soit $\mathcal{E}(n)$ l'ensemble des suites finies d'entiers strictement positifs $i_1, i_2, \cdots, i_r$ telles que $i_1+i_2+\cdots+i_r = n-1$ et $\forall j \in \{1, \cdots, r-1\},\ i_j \leq i_{j+1}$. Soit d_n l'application définie par :

$$d_n : \mathcal{S}(n) \longrightarrow \mathcal{E}(n)$$

qui à une suite finie $n_1T_{i_1}, \cdots, n_rT_{i_r}$ de $\mathcal{S}(n)$ fait correspondre la suite finie $n_1, \cdots, n_r$ de $\mathcal{E}(n)$.

Dans la suite de cet article, nous noterons Δ_n l'application définie par :

$$\Delta_n : \mathcal{T}(n) \xrightarrow{d_n \circ \Gamma_n} \mathcal{E}(n).$$

Notation 4.9. Comme nous l'avons fait pour Γ_n, nous noterons $\Delta_n(f)$ la suite finie $\Delta_n(Gal_k(f))$.

Si la suite finie e de $\mathcal{E}(n)$ correspond aux degrés des facteurs de première rupture de f alors le groupe de Galois de f est dans l'image inverse $\Delta_n^{-1}(e)$.

La table des groupes des facteurs de première rupture recense, pour un degré n, les images inverses non vides des éléments de $\mathcal{E}(n)$ et $\mathcal{S}(n)$ par, respectivement, Δ_n et Γ_n. Par exemple, nous avons pour le degré 8 :

$\Delta_8(T)$	$\Gamma_8(T)$	T
1^7	$(1T_1)^7$	$8T_1, 8T_2^+, 8T_3^+, 8T_4^+, 8T_5^+$
$1^3, 2^2$	$(1T_1)^3, (2T_1)^2$	$8T_7, 8T_9^+, 8T_{10}^+, 8T_{11}^+$
$1^3, 4$	$(1T_1)^3, (4T_1)$	$8T_{17}$
	$(1T_1)^3, (4T_2)$	$8T_{18}^+$
$1, 2^3$	$1T_1, (2T_1)^3$	$8T_6, 8T_8, 8T_{16}, 8T_{20}^+, 8T_{21}, 8T_{22}^+, 8T_{27}, 8T_{31}$
$1, 2, 4$	$1T_1, (2T_1), (4T_1)$	$8T_{19}^+$
	$1T_1, 2T_1, 4T_2$	$8T_{15}$
	$1T_1, 2T_1, 4T_3$	$8T_{26}, 8T_{28}, 8T_{29}^+, 8T_{30}, 8T_{35}$
$1, 3^2$	$1T_1, (3T_1)^2$	$8T_{12}^+, 8T_{13}^+, 8T_{14}^+$
	$1T_1, (3T_2)^2$	$8T_{24}^+$
$1, 6$	$1T_1, (6T_2)$	$8T_{23}$
	$1T_1, (6T_4)$	$8T_{32}^+$
	$1T_1, 6T_6$	$8T_{38}$
	$1T_1, 6T_7$	$8T_{39}^+$
	$1T_1, 6T_8$	$8T_{40}$
	$1T_1, 6T_{11}$	$8T_{44}$
$3, 4$	$3T_1, 4T_4$	$8T_{33}^+, 8T_{34}^+, 8T_{42}^+$
	$3T_2, 4T_5$	$8T_{41}^+, 8T_{45}^+, 8T_{46}, 8T_{47}$
7	$7T_1$	$8T_{25}^+$
	$7T_3$	$8T_{36}^+, 8T_{37}^+$
	$7T_4$	$8T_{43}$
	$7T_5$	$8T_{48}^+$
	$7T_6$	$8T_{49}^+$
	$7T_7$	$8T_{50}$

TAB. 1 – Table de première rupture en degré 8.

Exemple 4.10. Soit le polynôme irréductible $f := x^8 - 4x^7 + 14x^5 - 8x^4 -$

$12x^3 + 7x^2 + 2x - 1$ ref??????????????????. En factorisant f dans sa première extension, nous obtenons quatre facteurs linéaires et un facteur irréductible de degré 4, donc $\Delta_8(f) = 1^3, 4$. Ainsi, d'après la table 1, les groupes candidats à être le groupe de Galois de f sur $\mathbb{Q}$ sont $8T_{17}$ et $8T_{18}^+$. Le discriminant de f étant égal à $300416 = 2^{12}41^3$, qui n'est pas un carré dans $\mathbb{Q}$, le groupe de Galois de f est donc le groupe impair $8T_{17}$.

Cette table ne donne apparemment que des informations sur le groupe de Galois des polynômes. De plus, même en l'étendant aux extensions algébriques supérieures (la théorie étant la même), elle n'est pas toujours suffisante pour déterminer le groupe de Galois d'un polynôme irréductible à partir de ses facteurs de rupture ; la première ligne de la table permet de s'en convaincre. Pourtant, elle fait faire un grand pas vers le calcul simultané du groupe de Galois et d'un idéal des relations (i.e. du corps de décomposition). C'est ce que nous allons développer dans la suite de cet article.

5 Théorèmes fondamentaux

Soit f un polynôme irréductible sur k et $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n)$ un n-uplet de ses racines. Étant donné un $\underline{\alpha}$-idéal de Galois sur $k(\alpha_1)$, nous allons donner dans cette partie les moyens théoriques pour que s'en déduise un $\underline{\alpha}$-idéal de Galois sur k.

??????????????? AILLEURS????Si le groupe de Galois n'est pas 2-transitif, l'idéal initial obtenu contient strictement I^{S_n}. C'est donc à partir de cet idéal que commencera la recherche de l'idéal des relations et de son groupe de décomposition, le groupe de Galois.

Soit I_0 un $\underline{\alpha}$-idéal de Galois sur $k(\alpha_1)$, où $\underline{\alpha}$ est un élément de $\bar{k}^n$ fixé, engendré par l'ensemble triangulaire suivant :

$$\{x_1 - \alpha_1, f_2(x_1, x_2), \cdots, f_n(x_1, \cdots, x_n)\}$$

avec $f_i \in k[x_1, \cdots, x_n]$.

Posons $f_1 = f$ et notons I l'idéal triangulaire de $k[x_1, \cdots, x_n]$ engendré par l'ensemble triangulaire suivant :

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

Lemme 5.1. *Avec les notations précédentes, nous avons :*

$$k[x_1, \cdots, x_n] \cap I_0 = I$$

Démonstration. Soit $g \in k[x_1, \cdots, x_n] \cap I_0$. Montrons que $g \in I$. Posons $u = x_1 - \alpha_1$. Il existe n polynômes $g_1(\alpha_1), g_2(\alpha_1), \cdots, g_n(\alpha_1)$ à coefficients dans $k[x_1, \cdots, x_n]$ tels que :

$$g = g_1(\alpha_1)u + \sum_{i=2}^{n} g_i(\alpha_1) f_i \ .$$

Cette égalité nous donne $g = \sum_{i=2}^{n} g_i(x_1) f_i$ modulo u, où les polynômes $g_2' = g_2(x_1), g_3' = g_3(x_2), \ldots, g_n' = g_n(x_n)$ sont à coefficients dans $k[x_1, \cdots, x_n]$. Ainsi, il existe un polynôme $g_1' \in k(\alpha_1)[x_1, \cdots, x_n]$ tel que

$$g - \sum_{i=2}^{n} g_i' f_i = (x_1 - \alpha_1) g_1' \ .$$

Le membre de gauche de cette dernière égalité appartient à $k[x_1, \cdots, x_n]$. Comme $f(\alpha_1) = 0$ et f irréductible, le polynôme $g_1'(x_1 - \alpha_1)$ qui appartient à $k[x_1, \ldots, x_n]$ est nécessairement un multiple de $f(x_1)$ dans $k[x_1, \ldots, x_n]$. Ce qui permet d'affirmer que $g \in I$.

Nous avons montré l'inclusion $k[x_1, \cdots, x_n] \cap I_0 \subset I$ et l'inclusion inverse est immédiate. □

Proposition 5.2. *I est un $\underline{\alpha}$-idéal de Galois.*

Démonstration. Par construction, la variété de I est un sous-ensemble de $S_n.\underline{\alpha}$. L'idéal I_0 est radical par hypothése. D'aprés le lemme 5.1, il s'en déduit que l'idéal I est radical. Par conséquent, d'après la Proposition 3.3, l'idéal I est un idéal de Galois. □

Soit L le stabilisateur de I relatif à $\underline{\alpha}$, nous avons $V(I) = L.\underline{\alpha}$. Pour tout $i \in \{1, \cdots, n\}$, notons $V(I)_{\{i\}}$ le sous-ensemble de $V(I)$ défini par :

$$V(I)_{\{i\}} := \{\tau.\underline{\alpha} \in \bar{k}^n | \tau \in S_n \text{ et } \tau(1) = i\} \cap V(I).$$

Ces nouveaux ensembles permettent de décomposer la variété $V(I)$ en l'union disjointe :

$$V(I) = \bigcup_{i=1}^{n} V(I)_{\{i\}}. \tag{5.1}$$

Lemme 5.3. *Soit $i \in \{1, \cdots, n\}$. Pour toute permutation $\sigma_i \in G_{\underline{\alpha}}$ telle que $\sigma_i(1) = i$, nous avons,*

$$V(I)_{\{i\}} := \sigma_i.V(I)_{\{1\}} = \sigma_i.V(I_0).$$

Démonstration. Soit $\sigma_i \in G_{\underline{\alpha}}$ telle que $\sigma_i(1) = i$, nous avons,

$$\sigma_i.V(I)_{\{1\}} = \sigma_i.\{\tau.\underline{\alpha} \in \bar{k}^n | \tau \in S_n \text{ et } \tau(1) = 1\} \cap \sigma_i.V(I).$$

Puisque $V(I) = L_{\underline{\alpha}}.\underline{\alpha}$ et que $L = G_{\underline{\alpha}}L$ (voir [Val99]), nous avons $G_{\underline{\alpha}}.V(I) = V(I)$. Il s'en suit les égalités :

$$\begin{array}{rcl} \sigma_i.V(I)_{\{1\}} & = & \sigma_i.\{\tau.\underline{\alpha} \in \bar{k}^n | \tau \in S_n \text{ et } \tau(1) = 1\} \bigcap V(I) \\ & = & \{\tau.\underline{\alpha} \in \bar{k}^n | \tau \in S_n \text{ et } \tau(1) = i\} \bigcap V(I) \\ & = & V(I)_{\{i\}}. \end{array}$$

L'égalité $V(I)_{\{1\}} = V(I_0)$ permet de conclure. □

Théorème 5.4. *Soit L le stabilisateur relatif à $\underline{\alpha}$ de l'idéal de Galois I. Nous avons :*

$$L = \sigma_1 L_0 + \cdots + \sigma_n L_0,$$

pour toute permutation σ_i de $G_{\underline{\alpha}}$ telle que $\sigma_i(1) = i$.

En particulier, $L_{\{1\}} = L_0$ et $Card(L) = n.Card(L_0) = n.m_2 \cdots m_n$, où $m_i = deg_{x_i}(f_i)$.

Démonstration. Le lemme 5.3 et l'égalité 5.1 permettent de décomposer la variété $V(I)$ sous la forme :

$$V(I) = \bigcup_{i=1}^{n} \sigma_i.V(I_0),$$

où $\sigma_i \in G_{\underline{\alpha}}$ est une permutation telle que $\sigma_i(1) = i$. En terme de stabilisateur, nous obtenons :

$$L = \sigma_1 L_0 + \cdots + \sigma_n L_0.$$

□

Définition 5.5. L'idéal I et le stabilisateur L du Théorème 5.4 sont appelés respectivement *l'idéal de départ* et le *stabilisateur de départ* relatif à $\underline{\alpha}$.

Remarque 5.6. D'après la Proposition 3.5, pour un idéal de départ donné, il peut exister plusieurs stabilisateurs de départ différents selon le choix du n-uplet $\underline{\alpha}$ (sauf si les stabilisateurs L sont des groupes ; auquel cas, ils s'identifient tous au groupe de décomposition de l'idéal) . Ainsi, lorsque nous parlerons de stabilisateur de départ, il sera sous entendu qu'il est relatif à un élément de la variété $V(I)$.

Dans le Théorème 5.4, les permutations utilisées pour construire le stabilisateur L appartiennent à $G_{\underline{\alpha}}$. L'utilisation de ce résultat nécessite donc de connaître un sous-groupe transitif de $G_{\underline{\alpha}}$. Dans la pratique, nous utiliserons donc le corollaire direct suivant.

Corollaire 5.7. *Si H est un sous-groupe transitif de $G_{\underline{\alpha}}$, alors le stabilisateur de départ L vérifie :*

$$L = \sigma_1 L_0 + \cdots + \sigma_n L_0$$

pour tout $\sigma_1, \cdots, \sigma_n \in H$ vérifiant $\sigma_i(1) = i$.

Nous montrons à présent comment construire le stabilisateur initial en considérant, non plus des classes à gauches, mais des classes à droite. Pour ce faire, nous devons, à partir de maintenant, supposer que L_0 **est un groupe** (ce qui sera le cas dans la pratique).

Lemme 5.8. *Soit H un sous-groupe transitif de S_n et $\sigma_1, \cdots, \sigma_n$ des permutations de H telles que $\sigma_i(1) = i$. Alors, nous avons,*

$$H = \sigma_1 H_{\{1\}} + \cdots + \sigma_n H_{\{1\}}.$$

Démonstration. Soit $h \in H$ et notons i l'entier de $\{1, \cdots, n\}$ tel que $h(1) = i$. Par définition de σ_i, nous avons $\sigma_i^{-1}(h(1)) = 1$. Ainsi, il vient $h \in \sigma_i H_{\{1\}}$ et $h \in \sigma_1 H_{\{1\}} + \cdots + \sigma_n H_{\{1\}}$. D'où, l'inclusion :

$$H \supset \sigma_1 H_{\{1\}} + \cdots + \sigma_n H_{\{1\}}.$$

L'inclusion inverse est immédiate. □

Proposition 5.9. *Soit H un groupe tel que $H \cap G_{\underline{\alpha}}$ soit un sous-groupe transitif de S_n et tel que $H_{\{1\}} \subset L_0$. Soit la décomposition à droite de $H_{\{1\}}$ dans L_0 (qui est un groupe) :*

$$L_0 = H_{\{1\}}\tau_1 + \cdots + H_{\{1\}}\tau_s$$

alors le stabilisateur initial L vérifie :

$$L = H\tau_1 + \cdots + H\tau_s.$$

En particulier, nous avons,

$$Card(L) = [L_0 : H_{\{1\}}].Card(H).$$

Démonstration. D'après le Corollaire 5.7, nous pouvons supposer que les permutations $\sigma_1, \cdots, \sigma_n$ du Théorème 5.4 appartiennent au groupe $H \cap G_{\underline{\alpha}}$. Nous avons ainsi :

$$\begin{aligned} L &= \sigma_1 L_0 + \cdots + \sigma_n L_0 \\ &= \sigma_1(H_{\{1\}}\tau_1 + \cdots + H_{\{1\}}\tau_s) + \cdots + \sigma_n(H_{\{1\}}\tau_1 + \cdots + H_{\{1\}}\tau_s) \end{aligned}$$

Le résultat s'obtient par associativité et grâce au Lemme 5.8. □

Remarque 5.10. Sous les hypothèses du corollaire précédent, il vient :

$$I = I_{\underline{\alpha}}^L = \bigcap_{i=1}^{s} I_{\underline{\alpha}}^{H\tau_i} = \bigcap_{i=1}^{s} I_{\tau_i.\underline{\alpha}}^{\tau_i^{-1}H\tau_i}.$$

Dans la cas où $H = Gal_k(\underline{\alpha})$, cette égalité redonne la décomposition habituelle des idéaux de relations :

$$I = \bigcap_{i=1}^{n} I_{\tau_i.\underline{\alpha}}$$

car $\tau_i^{-1}H\tau_i = Gal_k(\tau_i.\underline{\alpha})$. Ainsi, si au lieu de choisir $\underline{\alpha}$ pour définir notre idéal initial I était choisi $\tau_i.\underline{\alpha}$, le stabilisateur initial $L_{\tau_i.\underline{\alpha}}$ serait alors $\tau_i^{-1}L$ en vertu de la Proposition 3.5.

Nous terminons cette section en donnant des résultats permettant de construire un idéal de Galois pouvant contenir strictement I, ainsi que son stabilisateur, à l'aide d'informations obtenues sur le groupe de Galois $G_{\underline{\alpha}}$.

Proposition 5.11. *Si H est un sous-groupe de S_n tel que $G_{\underline{\alpha}} \subset H \subset L$, alors,*

$$\forall(\sigma, R) \in H \times I_{\underline{\alpha}}^L, \quad I_{\underline{\alpha}}^L + < \sigma.R > \subset I_{\underline{\alpha}}^H.$$

Démonstration. Puisque $H \subset L$, nous avons $I_{\underline{\alpha}}^L \subset I_{\underline{\alpha}}^H$.

De plus, H contient le groupe de Galois $G_{\underline{\alpha}}$, ainsi, d'après la Proposition 3.30 de [Val99], H est le groupe de décomposition de l'idéal $I_{\underline{\alpha}}^H$. La proposition se déduit alors de la définition du groupe décomposition. □

À des fins algorithmiques, nous devons connaître le stabilisateur du nouvel idéal $I_{\underline{\alpha}}^{L} + < \sigma.R >$:

??
Il FAUT ICI prouver Que J est un idéal se Galois

Proposition 5.12. *Avec les notations de la proposition 5.11, notons* F *le polynôme* $< \sigma.R >$ *et* $J = I_{\underline{\alpha}}^{L} + < F >$.

Soit $L = H\tau_1 + \cdots + H\tau_s$ *une décomposition à droite de* L *donnée par la Proposition 5.9 et soit* $\mathcal{I}$ *l'ensemble d'entiers défini par :*

$$\mathcal{I} := \{i \in \{1, \cdots, s\} | \exists (\sigma, R) \in \tau_i^{-1} H \tau_i \times I_{\underline{\alpha}}^{L},\ \sigma.R = F\}.$$

Si le cardinal de la variété $V(J)$ *est égal à* $Card((I).Card(H)$ *alors le stabilisateur de* J *est* $\sum_{i \in \mathcal{I}} H\tau_i$.

Démonstration. D'après les hypothèses faites sur le cardinal de la variété, il suffit de montrer que $I_{\underline{\alpha}}^{\sum_{i\in\mathcal{I}} H\tau_i} \supset I_{\underline{\alpha}}^{L} + < F >$. Nous avons clairement $I_{\underline{\alpha}}^{\sum_{i\in\mathcal{I}} H\tau_i} \supset I_{\underline{\alpha}}^{L}$, il reste donc à montrer que F est un élément de $I_{\underline{\alpha}}^{\sum_{i\in\mathcal{I}} H\tau_i}$. Soit $\sigma \in \sum_{i\in\mathcal{I}} H\tau_i$, montrons que $\sigma.F(\underline{\alpha}) = 0$. Nous savons qu'il existe $\omega \in H$ et $j \in \mathcal{I}$ tels que $\sigma = \omega\tau_j$. Donc, par définition de $\mathcal{I}$, il existe $v \in H$ et $R \in I_{\underline{\alpha}}^{L}$ tels que :

$$\sigma.F(\underline{\alpha}) = \omega\tau_j\tau_j^{-1} v \tau_j.R(\underline{\alpha}) = \omega v \tau_j.R(\underline{\alpha}),$$

et comme $\omega v \tau_j \in L$ et $R \in I_{\underline{\alpha}}^{L}$ nous avons $\omega v \tau_j.R(\underline{\alpha}) = 0$, ce qui termine la démonstration. □

Remarque 5.13. L'hypothèse faite sur le cardinalité de $V(I)$ dans la proposition précédente s'est toujours réalisée lors de l'étude du degré 8 (Cf Partie 7) l'idéal J que nous calculons a le plus souvent le groupe H comme stabilisateur.

6 Construction d'un idéal de départ

Dans cette partie nous donnons une méthode générale pour la construction d'un idéal courant à partir de la factorisation du polynôme sur son corps de rupture.

6.1 Idéal de première rupture.

Soit $f(x) = (x - \alpha_1).g_2(x, \alpha_1) \cdots g_r(x, \alpha_1)$ une factorisation de f sur $k(\alpha_1)$, un corps de première rupture de f. Nous voulons connaître l'ensemble triangulaire T définissant l'idéal symétrique de f sur $k(\alpha_1)$.
Nous pouvons supposer sans perte de généralité que :

$$f(x) = (x - \alpha_1).g(x, \alpha_1).h(x, \alpha_1).$$

Soit m le degré de g et p celui de h. Soit $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \bar{k}^n$ un n-uplet de racines de f ordonné de tel sorte que $\alpha_2, \cdots, \alpha_{m+1}$ soient les racines de g et que $\alpha_{m+2}, \cdots, \alpha_n$ soient celles de h. D'après [???????????????????SubmitPAA], l'idéal des relations symétriques $I_{\underline{\alpha}}^{S_1 \times S_m \times S_p}$ de $k(\alpha_1)[x_1, x_2, \cdots, x_n]$ est engendré par les générateurs des trois idéaux de Galois suivant :

$$\begin{aligned} I_{(\alpha_1)}^{S_1} &\subset k(\alpha_1)[x_1], \\ I_{(\alpha_2, \cdots, \alpha_{m+1})}^{S_m} &\subset k(\alpha_1)[x_2, \cdots, x_{m+1}], \\ I_{(\alpha_{m+2}, \cdots, \alpha_n)}^{S_p} &\subset k(\alpha_1)[x_{m+2}, \cdots, x_n]. \end{aligned}$$

Soient $g_1, \cdots, g_m$ (resp. $h_1, \cdots, h_p$) les modules de Cauchy de g (resp. h) avec $g_i \in k(\alpha_1)[x_2, \cdots, x_{m+1}]$ (resp. $h_i \in k(\alpha_1)[x_{m+2}, \cdots, x_n]$) pour $i = 2, \cdots, m+1$ (resp. $i = m+2, \cdots, n$). D'après [Val99], les modules de Cauchy de g engendrent l'idéal $I_{(\alpha_2, \cdots, \alpha_{m+1})}^{S_m}$ dans $k(\alpha_1)[x_2, \cdots, x_{m+1}]$, et de même pour le polynôme h. Alors, puisque $I_{(\alpha_1)}^{S_1} =< x_1 - \alpha_1 >$, en prenant $L_0 = S_1 \times S_m \times S_p$ l'idéal de Galois $I_{\underline{\alpha}}^{L_0}$ de $k(\alpha_1)[x_1, \cdots, x_n]$ est engendré par le système triangulaire suivant :

$$\{x_1 - \alpha_1, g_1(x_1, x_2), \cdots, g_m(x_1, \cdots, x_{m+1}), h_1(x_1, x_{m+2}), \cdots, h_p(x_1, x_{m+2}, \cdots, x_n)\}.$$

Par induction, cette construction se généralise à une factorisation quelconque de f dans $k(\alpha_1)[x]$ et permet de construire un idéal de Galois sur $k(\alpha_1)$. Par convention, les facteurs de ruptures seront rangés dans un ordre tel que la suite finie de leur degré soit égale à $\Delta_n(f)$. Ainsi, en notant $S_{m,p} = S_m \times S_p$, nous aurons $L_0 := S_{1, \Delta_n(f)}$.

Définition 6.1. Un tel idéal de Galois sera dit de *première rupture pour f*.

Remarque 6.2. Comme L_0 est un groupe, quelque soit le choix de $\underline{\alpha}$ dans $V(I_0)$, L_0 sera le stabilisateur relatif à $\underline{\alpha}$ de I_0 (voir Proposition 3.5).

Exemple 6.3. Soit le polynôme $f_{29} = x^8 - x^6 - x^4 + x^2 + 1$ irréductible sur $\mathbb{Q}$ de groupe de Galois $8T_{29}^+$. Il se factorise sur un corps de première rupture en :

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

Les modules de Cauchy du facteur de degré 2 et du degré 4 sont respectivement les deux ensembles de polynômes :

$$\begin{aligned} T_1 := & \{x_3^2 - x_1^6 + x_1^4 + x_1^2 - 1, \\ & x_3 + x_4\} \\ T_2 := & \{x_5^4 + (x_1^6 - x_1^4)x_5^2 - 1, \\ & x_5^3 + x_5^2x_6 + x_5x_6^2 + (x_1^6 - x_1^4)x_5 + x_6^3 + (x_1^6 - x_1^4)x_6, \\ & x_5^2 + x_5x_6 + x_5x_7 + x_6^2 + x_6x_7 + x_7^2 + x_1^6 - x_1^4, \\ & x_5 + x_6 + x_7 + x_8\}. \end{aligned}$$

L'idéal de première rupture de f est donc engendré par l'ensemble triangulaire T suivant :

$$T := \{x_1 - \alpha_1\} \cup \{x_2 + x_1\} \cup T_1 \cup T_2,$$

son stabilisateur L_0 est le groupe produit $S_{1^2,3,4}$.

6.2 Idéal de départ.

Nous décrivons à présent les méthodes générales permettant de construire un idéal de départ issu d'un idéal de première rupture et de calculer son stabilisateur. Un idéal de départ est construit à partir d'un idéal de première rupture comme expliqué dans le Théorème ? ? ?refPropCAG. Pour calculer son stabilisateur nous avons besoin de connaître les sous-groupes de S_n susceptibles d'être le groupe de Galois, mais ceci impose de définir une relation d'équivalence sur les groupes transitifs.

6.2.1 Classes de L_0 équivalence.

Fixons n un entier représentant le degré étudié (? ? ? ? ? ? ? ? ? ? ? en pratique $n \leq 15$), les stabilisateurs possibles pour l'idéal de première rupture

sont alors les $L_0 = S_{1,e}$ où $e \in \mathcal{E}(n)$. Pour notre étude, fixons un tel $L_0 = S_{1,e}$.

Un groupe H est susceptible d'être le groupe de Galois que si $\Delta_n(H) = e$, mais comme nous cherchons à calculer un idéal des relations J inclus dans un idéal de départ, tous les conjugués de H ne peuvent être susceptibles d'être le groupe de décomposition de J. Seuls ceux dont le stabilisateur de 1 est inclus dans L_0 pourront l'être (voir Théorème **??**). D'où la définition suivante :

Définition 6.4. L'ensemble $C(L_0)$ des groupes compatibles avec $L_0 = S_{1,e}$ est définie par

$$C(L_0) = \{H \text{ sous-groupe transitif de } S_n \mid \Delta_n(H) = e \text{ et } H_{\{1\}} \subset L_0\}$$

Etant donné un groupe transitif H tel que $\Delta_n(H) = e$, la liste des groupes compatibles avec L_0 conjugués avec H se calcule aisément en cherchant parmi les conjugués de H ceux dont le stabilisateur de 1 est inclus dans L_0. Les groupes H sont eux fournis par la table des groupes de première rupture de degrés n. Par exemple, nous pourrons utiliser la fonction suivante en MAGMA :

C'est ici qu'il faudra mettre les fonction Magma d'Annick

Exemple 6.5. Pour $n = 8$ et $L_0 = S_1^4 \times S_4$. L'ensemble des groupes compatibles avec L_0 est constitué de 18 conjugués de $8T_{17}$ et 6 conjugués de $8T_{18}^+$.

Exemple 6.6. Pour $n = 8$ et $L_0 = S_1^2 \times S_2 \times S_4$. L'ensemble des groupes compatibles avec L_0 sont des conjugués des groupes $8T_{15}$, $8T_{19}^+$, $8T_{26}$, $8T_{28}$, $8T_{29}^+$, $8T_{30}$ et $8T_{35}$.

Exemple 6.7. Prenons $n = 8$ et $L_0 = S_1^4 \times S_2^2$. L'ensemble des groupes compatibles avec L_0 est constituée de 6 conjugués de $8T_7$, et de même pour $8T_9^+$, $8T_{10}^+$ et $8T_{11}^+$. Les 6 conjugués de $8T_7$ sont les groupes suivants :

$$\begin{aligned}
G_1 &= <(1,5,3,7,2,6,4,8),(1,2)(3,4)>,\\
G_2 &= <(1,6,3,7,2,5,4,8),(1,2)(3,4)>,\\
G_3 &= <(1,5,2,7,3,6,4,8),(1,3)(2,4)>,\\
G_4 &= <(1,5,2,8,3,6,4,7),(1,3)(2,4)>,\\
G_5 &= <(1,5,2,7,4,6,3,8),(1,4)(2,3)>,\\
G_6 &= <(1,5,2,8,4,6,3,7),(1,4)(2,3)> .
\end{aligned}$$

Le groupe $8T_7$ possède 6 conjugués compatibles avec L_0. Or le cardinal de L n'est que le double de celui de $8T_7$. En effet, nous avons, en notant H_i le

stabilisateur de 1 de G_i et τ la permutation $(5,6)$: $L_0 = H_1 + H_1\tau = H_3 + H_3.\tau = H_5 + H_5\tau$ avec $G_2 = \tau^{-1}G_1\tau$, $G_4 = \tau^{-1}G_3\tau$ et $G_6 = \tau^{-1}G_5\tau$. Cela provient du fait que les degrés de ruptures ne sont pas distincts et qu'il reste un choix sur l'ordre pour les facteurs de ruptures dans la construction d'un idéal de rupture. Pour $8T_7$, il y a 3 !.2=12 possibilités d'idéaux de rupture. Parmi elles, nous venons de constater qu'il n'y a en fait que 3 idéaux de rupture distincts associés respectivement aux trois couples (G_1, G_2), (G_3, G_4) et (G_5, G_6)

C'est pour répondre au problème posé par l'exemple précédent que nous introduisons ci-dessous les classes de L_0-équivalence :

Proposition 6.8. *Soit G et H deux groupes compatibles avec L_0. La relation $\mathfrak{R}$ donnée par :*

$G\mathfrak{R}H \Leftrightarrow \exists T$ *une transversale à droite de* L_0 *modulo* $G_{\{1\}}$ *telle que* $H = \tau^{-1}G\tau$ *pour* $\tau \in T$.

est une relation d'équivalence. De plus, la longueur de la classe d'équivalence de G est majorée par le cardinal de la transversale T (i.e. $[L_0 : G_{\{1\}}]$).

? ? ? ? ? ? ? ? ? ? ? ? ? ? Question : Cela n'équivaut-il pas au fait que G et H soit conjugués l'un de l'autre par une permutation de L_0 ?

Pour montrer cette proposition nous avons besoin du lemme suivant :

Lemme 6.9. *Soit G et H deux groupes compatibles avec L_0. S'il existe une transversale T à droite de L_0 par $G_{\{1\}}$ telle que $H = \tau^{-1}G\tau$ pour $\tau \in T$, alors, pour toute autre transversale T' à droite de L_0 par $G_{\{1\}}$, il existe $\tau' \in T'$ tel que $H = \tau'^{-1}G\tau'$.*

Démonstration. La permutation $\tau \in T$ est un élément de L_0 et peut donc se décomposer en : $\tau = g\tau'$ avec $g \in G_{\{1\}}$ et $\tau' \in T'$. Ainsi nous obtenons :

$$H = \tau^{-1}G\tau = \tau'^{-1}g^{-1}Gg\tau' = \tau'^{-1}G\tau'.$$

□

Nous pouvons maintenant démontrer la proposition précédente.

Démonstration. **(de la proposition 6.8)** La réflexivité de la relation $\mathfrak{R}$ est immédiate en choisissant pour transversale T celle dont un élément est l'identité.
La relation $\mathfrak{R}$ est symétrique : Soient G et H deux groupes L_0-compatibles tels que $G\mathfrak{R}H$, alors par définition :

$$L_0 = G_{\{1\}}\tau_1 + G_{\{1\}}\tau_2 + \cdots + G_{\{1\}}\tau_e \quad (*)$$

avec, après renumérotations des τ_i :

$$H = \tau_1^{-1} G \tau_1. \quad (**)$$

D'après $(*)$ et $(**)$ nous avons :

$$\begin{aligned} L_0 &= (\tau_1 H_{\{1\}} \tau_1^{-1})\tau_1 + ((\tau_1 H_{\{1\}} \tau_1^{-1})\tau_2 + \cdots + (\tau_1 H_{\{1\}} \tau_1^{-1})\tau_e \\ &= \tau_1^{-1} L_0 \tau_1 \\ &= H_{\{1\}}\sigma_1 + H_{\{1\}}\sigma_2 + \cdots + H_{\{1\}}\sigma_e \text{ avec } \sigma_i = \tau_1^{-1}\tau_i\tau_1 \quad (***). \end{aligned}$$

Comme $G = \sigma_1^{-1} H \sigma_1$, nous avons alors $H\mathfrak{R}G$.
La relation $\mathfrak{R}$ est transitive : Soient G, H, K des groupes L_0-compatibles tels que $G\mathfrak{R}H$ et $H\mathfrak{R}K$. Par symétrie nous avons $H\mathfrak{R}G$ et une décomposition de la forme $(***)$. avec $\sigma_1^{-1} H \sigma_1 = G$. De plus, le lemme 6.9 nous donne l'existence d'un σ_i pour $i \in \{1, \cdots, e\}$ vérifiant $\sigma_i^{-1} H \sigma_i = K$. En utilisant le même procédé que pour la symétrie, nous obtenons :

$$\sigma_1^{-1} L_0 = L_0 = G_{\{1\}}\sigma_1^{-1}\sigma_1 + \cdots + G_{\{1\}}\sigma_1^{-1}\sigma_i + \cdots + G_{\{1\}}\sigma_1^{-1}\sigma_e,$$

avec $(\sigma_1^{-1}\sigma_i)^{-1} G (\sigma_1^{-1}\sigma_i) = K$. Ainsi, nous avons bien $G\mathfrak{R}K$.
L'assertion sur la longueur d'une classe d'équivalence est une conséquence directe du lemme 6.9. □

Remarque 6.10. Il se peut que la longueur de la classe d'équivalence de G soit strictement inférieur à $[L_0 : G_{\{1\}}]$. En effet l'étude de la ligne 4 pour le degré 8, nous donne l'exemple d'un groupe $G \simeq 8T_{29}$ vérifiant $L_0 = G_{\{1\}} + G_{\{1\}}\tau$ avec $G = \tau^{-1} G \tau$, ainsi la classe de L_0-équivalence de G est réduite à un unique élément alors que $[L_0 : G_{\{1\}}] = 2$.

Définition 6.11. La relation d'équivalence $\mathfrak{R}$ définie sur l'ensemble $C(L_0)$ est appelée relation de *L_0-équivalence*.

Proposition 6.12. *La L_0-équivalence est compatible avec le passage aux sous-groupes L_0-compatibles (i.e. si G et H sont L_0-équivalents alors tout sous-groupe de G compatible avec L_0 est L_0-équivalent à un sous-groupe de H).*

Démonstration. ? A recopier □

Exemple 6.13. Reprenons l'exemple précédent, nous avons montré qu'il existe trois classes de L_0-équivalence dont un représentant est un conjugué de $8T_7$, se sont les suivantes : $C_1 = \{G_1, G_2\}$, $C_2 = \{G_3, G_4\}$ et $C_3 = \{G_5, G_6\}$.

Pour les deux autres exemples, lorsque G est un conjugué de $8T_{18}$ ou lorsque G est un groupe de $C(S_1^2 \times S_2 \times S_4)$ nous avons $\text{card}(L) = c.\text{card}(G)$ où c est le nombre de conjugués de G dans $C(L_0)$. Donc pour chacun de ces groupes, il n'y a qu'une classe de L_0-équivalence.

Supposons que $m_2, \cdots, m_s$ soient les degrés des facteurs de rupture du polynôme f et qu'il existe $\underline{\alpha}$ tel que $G \subset G_{\underline{\alpha}}$ ou bien $G_{\underline{\alpha}} \subset G$. Etant donné $\{G_1, G_2, \cdots, G_m\}$, la classe de L_0-équivalence de $G = G_1$, avec $G_i = \tau_i^{-1} G_1 \tau_i$ et $\tau_1 = \text{id}$, alors il existe un idéal de départ I vérifiant :

$$I = I_{\underline{\alpha}}^L \text{ avec } L = G_1 + G_1.\tau_2 + \cdots + G_1.\tau_m.$$

Comme nous avons pu le voir dans la remarque 5.10, ceci nous donne :

$$I = \bigcap_{i=1}^{m} I_{\tau_i.\underline{\alpha}}^{\tau_i^{-1} G_1 \tau_i} = \bigcap_{i=1}^{m} I_{\tau_i.\underline{\alpha}}^{G_i}$$

et nous pouvons choisir indifféremment $\underline{\alpha}, \tau_2.\underline{\alpha}, \cdots, \tau_m.\underline{\alpha}$ comme numérotation possibles des racines de f. En effet, le choix de G_1 pour calculer un stabilisateur initial ne fixe que théoriquement l'ordre $\underline{\alpha}$. Si G_2 était choisit à la place de G_1, nous aurions les mêmes d'idéaux dans la décomposition de l'idéal initial I ; ils seraient indicés avec des permutations de $\tau_2.\underline{\alpha}$ à la place de $\underline{\alpha}$. Nous pouvons ainsi dire que l'idéal I est *associée* à la classe de L_0-équivalence de G.

S'il existe plusieurs classes de L_0-équivalence pour un même groupe, il existe plusieurs idéaux de départ distincts. Nous établissons une proposition qui peut permettre de trouver un critère, dit *critère d'association*, associant un idéal de départ à sa classe de L_0-équivalence.

Proposition 6.14. *Soit A une classe de L_0-équivalence et $E(A) = \bigcap_{G \in A} E(G)$ avec*

$$E(G) = \{\sigma.R(x_1, \cdots, x_n) \mid R \in I \ \ \sigma \in G\} \quad .$$

S'il existe $P \in E(A)$ tel que $P \notin I$ alors A n'est pas une classe de L_0-équivalence associée à I.

Démonstration. Supposons que A soit associé à un idéal de Galois I. Pour tout G dans A, il existe $\underline{\alpha}_G \in V(I)$ tel que $G \subset G_{\underline{\alpha}_G}$ ou bien $G_{\underline{\alpha}_G} \subset G$ et

$$I = \bigcap_{G \in A} I^G_{\underline{\alpha}_G} \quad .$$

Soit $P \in E(A)$ et $R \in I$ tel que $P = \sigma.R$ avec $\sigma \in G$ et $G \in A$. Nous avons $R \in I^G_{\underline{\alpha}_G}$ et donc $P = \sigma.R \in I^G_{\underline{\alpha}_G}$ puisque G est ou bien le groupe de décomposition de $I^G_{\underline{\alpha}_G}$ (si $G_{\underline{\alpha}_G} \subset G$) ou bien un sous-groupe (si $G \subset G_{\underline{\alpha}_G}$ et alors il vient $I^G_{\underline{\alpha}_G} = I_{\underline{\alpha}_G}$). Comme ceci est vrai pour tout $G \in A$, nous avons bien $P \in I$. □

Exemple 6.15. Reprenons l'exemple où $n = 8$ et $L_0 = S_{1^4,2^2}$ et supposons que le groupe de Galois est un conjugué de $8T_7$ (ceci peut être déterminé par un simple calcul de discriminant). Dans ce cas l'idéal initial est engendré par l'ensemble triangulaire T suivant :

$$\begin{aligned} T = \quad & \{f_1(x_1), \\ & x_2 - g_2(x_1), \\ & x_3 - g_3(x_1), \\ & x_4 - g_4(x_1), \\ & x_5^2 - g_5(x_5, x_1), \\ & x_6 - g_6(x_5, x_1), \\ & x_7^2 - g_7(x_7, x_1), \\ & x_8 - g_8(x_6, x_1)\}. \end{aligned}$$

D'après ce que nous venons de voir il y a trois classes de L_0-équivalence de groupes conjugués à $8T_7$ donc trois idéaux initiaux possibles. Soit I l'un d'entre eux, le critère que nous donnons ici permet de dire si I est associé à la classe C_1. Il repose sur le fait que si f est un générateur de l'idéal initial et que ce dernier est inclus dans un idéal des relations I^G alors toute permutation de G envoie f dans I^G. Nous avons par exemple :

$$\text{Si } G \in C_2 \text{ alors } x_6 + g_3(x_5) \in I^G$$

et de même,

$$\text{si } G \in C_3 \text{ alors } x_6 + g_4(x_5) \in I^G.$$

Or les degrés respectifs en $x_1, x_2, \cdots, x_8$ des générateurs des idéaux des relations I^G pour $G \in C_1 \cup C_2 \cup C_3$ sont $8, 1, 1, 1, 2, 1, 1, 1$ (voir **Section sur les**

degrés initiaux) et ceux de I sont $8, 1, 1, 1, 2, 1, 2, 1$. Donc, comme I et I^G sont triangulaires, tester l'appartenance à I^G d'un polynôme qui ne dépend ni x_7 ni de x_8 revient à tester son appartenance à I. Ceci nous donne alors :

Si $x_6 + g_4(x_5) \not\in I$ et $x_6 + g_3(x_5) \not\in I$ alors I est associé àC_1.

Nous allons maintenant donner un méthode générale pour construire un idéal de départ.

6.3 Méthodes générales de construction d'un idéal de départ

6.3.1 Degrés initiaux d'un idéal de Galois

La liste des *degrés initiaux* d'un ensemble triangulaire $T = \{f_1(x_1), \cdots, f_n(x_1, \cdots, x_n)\}$ ou de l'idéal I qu'il engendre est le n-uplet d'entiers $(deg_{x_1}(f_1), deg_{x_2}(f_2), \cdots, deg_{x_n}(f_n))$.
Si l'idéal I est radical, son cardinal est identique au produit c des degrés initiaux. Si I est un idéal de Galois de groupe de décomposition G de cardinal c (i.e. G est aussi le stabilisateur de I), les degrés initiaux sont calculables avec `InitDeg(L,n)` où `InitDeg` est la fonction Magma suivante qui transcrit un résultat de l'article ? ? ?AubryVal :

```
InitDeg:= function(groupe,n);
        ListeStabs:=[];  L:=[]; L[1]:=groupe; Degs:=[];
        for i := 1 to n do     ListeStabs[i]:=Stabilizer(groupe,i);   end for;
        for i:=2 to (n+1) do   L[i]:=ListeStabs[i-1] meet L[i-1];     end for;
        for i:=1 to n do       Degs[i]:=Order(L[i])/Order(L[i+1]);    end for;
        return Degs;
end function;
```

Exemple 6.16. Supposons que $\Delta_8(f) =$????. alors d'après la table ? ? ? ?, nous calculons l'ensemble $C(L_0)$ des groupes L_0-compatibles avec $L_0 =$ ..... Pour chaque groupe G de $C(L_0)$, avec InitDeg nous calculons les degrés initiaux des idéaux de Galois dont il est le stabilisateur. Nous trouvons systématiquement la liste ? ? ? ? . Comme celle d'un idéal de départ est ? ? ? ?. Nous savons que nous n'avons à chercher que ....

6.3.2 L'algorithme `GaloisIdéal`

L'algorithme :

Dans BULL ? ? ?, l'algorithme `GaloisIdéal(G,T,Liste)` a pour paramètres :

- `T` un ensemble triangulaire engendrant un idéal de Galois I,
- le stabilisateur `G` de I qui est supposé être un groupe (i.e. `G` est aussi le groupe de décomposition de I),
- Une liste `Liste` de groupes candidats à être le groupe de Galois,

et il calcule un idéal des $I_{\underline{\alpha}}$ contenant I (avec $\underline{\alpha} \in V(I)$) et le groupe de Galois qui est le groupe de décomposition $G_{\underline{\alpha}}$ de $I_{\underline{\alpha}}$.

Pour ce faire, l'algorithme prend un groupe H dans `Liste` et calcule une H-résolvante G-relative (voir AUbryVal ? ? ? pour le calcul) de degré e l'indice de H dans G. Si de cette résolvante il résulte que G est le groupe de Galois alors l'algorithme retourne I et G. Dans le cas contraire, si H contient le groupe de Galois $G_{\underline{\alpha}}$ avec $\underline{\alpha} \in V(I)$, alors avec un facteur simple sur k de la résolvante, il est déduit un polynôme R de $k[x_1, x_2, \cdots, x_n]$ tel que $I^H_{\underline{\alpha}} = I + < R >$ (où $\underline{\alpha} \in V(I)$) et calcule un ensemble triangulaire T_H engendrant l'idéal de Galois $I^H_{\underline{\alpha}}$. La liste `Liste` des groupes candidats est réduite pour former une nouvelle liste `NListe`. L'algorithme s'appelle alors récursivement avec `GaloisIdéal(H,`T_H`,NListe)`.

Remarque 6.17. Le cas où le groupe H ne contient pas le groupe de Galois (qui est considéré dans l'algorithme `GaloisIdéal`) ne sera pas utilisé dans le cadre de cet article.

Sa Généralisation :

L'algorithme `GaloisIdéal(G,T,Liste)` et le calcul des résolvantes G-relatives sont généralisables lorsque le stabilisateur G de I n'est pas un groupe (voir BullBelge2 ? ? ?). Or, la seul connaissance de T ne permet pas de calculer un stabilisateur si ce n'est pas le groupe de décomposition de I. En effet, dans ce cas son calcul dépend par définition de la connaissance d'un idéal des relations $I_{\underline{\alpha}}$ contenant I. C'est pour cela que les différents résultats de cet article qui permettent de le calculer sont précieux (voir ? ? ?). Cette généralisation sera utilisée au paragraphe 7.7 lorsque le groupe de Galois est $8T_{12}$ (voir Cas 2.).

Exemples :

Exemple 6.18. Au Paragraphe 7.5 Cas 1., nous avons l'appel à `GaloisIdéal(`G_{27}`,` T`,[`G_{16}`])` avec $I = I_{\underline{\alpha}}^{G_{27}}$. Sont calculés un G_{16}-invariant G_{27}-primitif séparable Θ, puis à l'aide de l'ensemble triangulaire T, une résolvante G_{27}-relative de $\underline{\alpha}$ par Θ dont le degré est 2 (l'indice de G_{16} dans G_{27}). Si cette résolvante est irréductible, alors $G_{\underline{\alpha}} = G_{27}$ et $I_{\underline{\alpha}} = I$. Sinon, $G_{\underline{\alpha}} = G_{16}$ et $I_{\underline{\alpha}} = I + < \Theta + \lambda >$ où $x + \lambda$ est un facteur linéaire (simple) de la résolvante. L'ensemble triangulaire engendrant $I_{\underline{\alpha}}$ se calcule rapidement car la liste de ses degrés initiaux est $(8, 1, 2, 1, 2, 1^3)$ et celle de T est $(8, 1, 2, 1, 2, 1, 2, 1)$.

Exemple 6.19. Au paragraphe 7.6, nous avons l'appel à `GaloisIdéal(`G_{35}`,`T`,` $[G_{29}, G_{19}, H_{19}]$`)` et le groupe de Galois est G_{19} ou H_{19}. Nous montrons ici que l'idéal de Galois $I_{\underline{\alpha}}^{G_{29}}$, contient deux idéaux premiers de même groupe de décomposition (G_{19} ou H_{19}) car G_{29} est autoadjoint dans G_{35}. Nous avons $G_{35} = G_{29} + G_{29}(3, 4)$ et avec $u = (1, 2)(5, 6)$, $G_{29} = G_{19} + G_{19}u = H_{19} + H_{19}u$, $G_{19} = u^{-1}G_{19}u$ et $H_{19} = u^{-1}H_{19}u$. Les sous-groupes G_{19} et H_{19} de G_{29} sont conjugués dans S_8 mais pas dans G_{29}. C'est ainsi que si I est l'idéal de Galois engendré par T, alors pour tout $\underline{\alpha} \in V(I)$:

$$I = I_{\underline{\alpha}}^{G_{35}} = I_{\underline{\alpha}}^{G_{29}} \cap I_{(3,4)\underline{\alpha}}^{G_{29}} \qquad .$$

Lorsqu'une G_{29}-résolvante G_{35}-relative (séparable) est calculée à partir d'un invariant Θ, elle se factorise sur k en deux facteurs linéaires $(x+a)$ et $(x+b)$. Il existe alors $\underline{\alpha} \in V(J)$ tel que :

$$\begin{array}{rcl} I_{\alpha}^{G_{29}} & = & I + < \Theta + a >= I_{\alpha}^{G} = I_{\alpha}^{H} \cap I_{u\alpha}^{H} = I_{\alpha} \cap I_{u\alpha} \qquad \text{et} \\ I_{(3,4)\alpha}^{G_{29}} & = & I + < \Theta + b >= I_{(3,4)\alpha}^{H} = I_{(3,4)\alpha}^{G} \cap I_{u(3,4)\alpha}^{G} = I_{(3,4)\alpha} \cap I_{u(3,4)\alpha} \end{array}$$

avec $(G, H) = (G_{19}, H_{19})$ ou $(G, H) = (H_{19}, G_{19})$. Donc il faut chercher un G_{19}-invariant ou un H_{19}-invariant G_{29}-primitif qui ne se réduise pas modulo $I_{\alpha}^{G_{29}}$ à un élément de k. Ce ne sera possible que pour H l'un des deux groupes G_{19} ou H_{19}. A partir de cet invariant, il est possible de calculer un polynôme R tel que $I_{\alpha} = I_{\alpha}^{G_{29}} + < R >$ avec $G_{\alpha} = H$.

Comparaison avec `PrimaryDecomposition`

Dans l'exemple 6.19, la décomposition en deux idéaux premiers de l'idéal $I_{\alpha}^{G_{29}}$ est calculable avec la fonction `PrimaryDecomposition` de Magma. Pour le polynôme $f_{19} = x^8 + x^6 + 2x^2 + 4$, elle se réalise en 0.4 secondes. De manière générale, il est intéressant de savoir si cette fonction est plus efficace que `GaloisIdéal`. Pour I un idéal de Galois, posons $e = \text{card}(V(I))/\text{card}(V(I_{\alpha}))$.

Si $e = 2$, comme pour $I = I_\alpha^{G_{29}}$, le calcul est rapide mais généralement moins que par `GaloisIdéal`. Pour $e > 2$, sur les tests que nous avons effectués en degré 8, le calcul est parfois impossible avec `PrimaryDecomposition` et de plus `GaloisIdéal` est plus efficace dans les autres cas. Le cas où l'utilisation de `PrimaryDecomposition` est intéressante est celui où le stabilisateur de de l'idéal I est inconnu puisqu'alors `GaloisIdéal` n'est pas utilisable (voir, par exemple, Paragraphe 7.5 Cas 3. avec G_6 et G_8).

6.3.3 Résumé de la construction

6.4 Méthodologie générale

Soit $L_0 = S_{1,e}$ avec $e \in \mathcal{E}(8)$. Nous notons I un idéal de départ quelconque d'un polynôme f tel que $\Delta_8(f) = e$. Nous calculons l'ensemble $C(L_0)$.

Soit $8T_i$, tel que $\Delta_8(8T_i) = e$. Supposons que dans $C(L_0)$ il existe plusieurs classes de L_0-équivalence de groupes conjugués à $8T_i$. Nous cherchons alors ou bien un critère d'association pour pouvoir calculer le stabilisateur de I avec ? ? ? ou ? ? ? ou à défaut un nouvel idéal $J = I + < r_1, r_2, \cdots, r_k >$ avec la proposition ? ? ? appliquée à des groupes pris dans chacune des classes de L_0-équivalence. Avec la proposition ? ? ?, nous pouvons savoir à priori si le stabilisateur de J est ou non un groupe. Si c'est un groupe, c'est le groupe de décomposition qu'il il suffira de calculer pour savoir à quelle classe de L_0-équivalence l'idéal I (et donc J) est associé.

Si l'idéal de départ I (ou bien son idéal déduit J) est associable à une classe de L_0-équivalence, nous cherchons à lui appliquer la Proposition ? ? ? pour obtenir un idéal qui le contient (son stabilisateur est calculable). Pour savoir quelles nouvelles relations chercher avec un groupe G, nous comparons la liste des degrés initiaux de l'idéal de Galois donné (I ou J) à celle de l'idéal de Galois dont le stabilisateur serait G (calculable avec la fonction `InitDeg(G,n)` du paragraphe 6.3.1).

Dès qu'un idéal de Galois J engendré par un ensemble triangulaire T_J a un stabilisateur L calculable, il est alors possible de terminer avec l'algorithme `GaloisIdéal(`L`,`T_J`,Liste)`, où `Liste` est une liste de groupes G de $C(L_0)$ vérifiant qu'il existe $\alpha \in V(J)$ tel que $J \subset I_\alpha^G$.

Le groupe de décomposition d'un idéal de Galois est facilement calculable. Donc si un idéal des relation I_α est calculé le groupe de Galois G_α est également connu car c'est son groupe de décomposition.

Si nous aboutissons à un idéal de Galois dont nous ne pouvont calculer le stabilisateur (ce n'est donc pas un groupe), nous terminons avec une décomposition en idéaux premiers et nous en choisissons un pour être l'idéal des relations.

Les groupes de Galois des facteurs de f dans $k(\alpha)$ peuvent être utilisés pour départager des groupes de $C(L_0)$.

7 Étude du degré 8.

7.1 Critère de Dedekind

Nous pouvons exclure de $C(L_0)$ les groupes qui ne répondent pas aux critères de parité et de Dedekind. Par exemple, si $\Delta_8(f) = (1, 2^3)$, que le discriminant de f n'est pas un carré dans k et qu'en factorisant sur k le polynôme f modulo un entier p non ramifié, nous trouvons un des cycles suivants : $(2, 1^6)$ (i.e. un facteur de degré 2 et six linéaires), $(2^3, 1^2)$ ou $(4, 2^2)$, alors le groupe de Galois n'est pas T_{16}.

Nous avons extrait le tableau suivant des tables de ButlerMcKay ? ? ?. Les informations sont regroupées en fonction des $P(T)$. Sur une même ligne, les cycles de la deuxième colonne sont des cycles types des groupes T_i de la troisième colonne (colonne Oui) et pas de la quatrième (colonne Non).

$P(T)$	cycles	Oui	Non
(1^7)	(4^2)	T_1, T_2^+, T_4^+, T_5^+	T_3^+
$(1, 2^3)$	$(4, 2^2)$	T_{21}, T_{27}, T_{31}	T_{16}
	$(2, 1^6)$, $(2^3, 1^2)$	T_{27}, T_{31}	T_{16}, T_{21}
(1,2,4)	$(1^6, 2)$	T_{35}	$T_{15}, T_{26}, T_{28}, T_{30}$
	$(1^2, 2^3)$	$T_{15}, T_{26}, T_{30}, T_{35}$	T_{28}
	$(1^4, 4)$	T_{26}, T_{30}, T_{35}	T_{15}, T_{28}
	$(2^2, 4)$	$T_{26}, T_{28}, T_{30}, T_{35}$	T_{15}
	$(1^2, 2, 4)$	T_{28}, T_{35}	T_{15}, T_{26}, T_{30}
	(8)	$T_{15}, T_{26}, T_{28}, T_{35}$	T_{30}
$(1, 3^2)$	$(2^2, 1^4)$	T_{24}	T_{12}, T_{13}, T_{14}
	(4^2)	T_{12}, T_{14}, T_{24}	T_{13}
	$(6, 2)$	T_{12}, T_{13}, T_{24}	T_{14}
(1,6)	$(2, 1^6)$, $(3^2, 2)$, $(6, 1^2)$	T_{38}, T_{44}	T_{23}, T_{32}^+, T_{39}^+, T_{40}
	$(2^2, 1^4)$	T_{32}^+ T_{38} T_{39}^+ T_{40} T_{44}	T_{23}
	$(4, 1^4)$	T_{40}, T_{44}	T_{23}, T_{32}^+, T_{38}, T_{39}^+
	$(4, 2, 1^2)$	T_{39}^+, T_{44}	T_{23}, T_{32}^+, T_{38}, T_{40}
	$(4, 2^2)$	T_{38}, T_{40},T_{44}	T_{23}, T_{32}^+, T_{39}^+
	(8)	T_{23}, T_{40}, T_{44}	T_{32}^+, T_{38}, T_{39}^+
(3,4)	$(2, 1^6)$, $(2^3, 1^2)$, $(3, 2, 1^3)$, $(4, 1^4)$, $(4, 3, 1)$	T_{47}	T_{33}^+, T_{34}^+, T_{41}^+, T_{42}^+, T_{45}^+, T_{46}
	$(3, 1^5)$, $(3, 2^2, 1)$	T_{42}^+, T_{45}^+, T_{46}, T_{47}	T_{33}^+, T_{34}^+, T_{41}^+
	$(4, 2, 1^2)$	T_{41}^+, T_{45}^+, T_{46}, T_{47}	T_{33}^+, T_{34}^+, T_{42}^+
	$(4, 2^2)$ (8)	T_{46}, T_{47}	T_{33}^+, T_{34}^+, T_{41}^+, T_{42}^+, T_{45}^+
	$(6, 2)$	T_{33}^+, T_{41}^+, T_{42}^+, T_{45}^+, T_{47}	T_{34}^+, T_{46}

7.2 $\Delta_8(f) = (1^7)$ et $L_0 = S_1^8$.

Les groupes de $C(L_0)$, conjugués de T_1, T_2^+, T_3^+, T_4^+ et T_5^+, sont tous de cardinal 8. Tout idéal de départ I a pour liste de degré initiaux $(8, 1^7)$. Donc c'est un idéal des relations. Il suffit d'en calculer un, I_α, puis de chercher son groupe de décomposition G_α parmis les groupes de $C(L_0)$. Nous constatons ici que le problème des classes de L_0-équivalence du à 7 facteurs de rupture de même degré se résout sans recherche de critère d'association.

Exemple 7.1. Soit $f := x^8 + 8x^6 + 20x^4 + 16x^2 + 2$. Ce polynôme se factorise en $(x - x_1)(x + x_1)(x - x_1^3 - 3x_1)(x + x_1^3 + 3x_1)(x - x_1^5 - 5x_1^3 - 5x_1)(x + x_1^5 + 5x_1^3 + 5x_1)(x - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1)(x + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1)$ dans $k[x_1]/f(x_1)$. Nous en déduisons l'idéal de départ

$$\begin{aligned} I = I_\alpha \;\; = \;\; & < f(x_1), x_2 + x_1, x_3 - x_1^3 - 3x_1, x_4 + x_1^3 + 3x_1, x_5 - x_1^5 - 5x_1^3 - 5x_1, \\ & x_6 + x_1^5 + 5x_1^3 + 5x_1, x_7 - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1, x_8 + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1 > \end{aligned}$$

dont le groupe de décomposition est le groupe tT_1t^{-1} avec $t = (2, 3, 7, 8, 5)(4, 6)$.

7.3 $\Delta_8(f) = (1^3, 2^2)$ et $L_0 = S_1^4 \times S_2^2$

Les groupes de $C(L_0)$, conjugués des groupes T_7, T_9^+, T_{10}^+ et T_{11}^+, sont de cardinal 16. Chaque idéal de départ I est de la forme :

$$\begin{aligned} I = < & f(x_1), x_2 + g_2(x_1), x_3 + g_3(x_1), x_4 + g_4(x_1), x_5^2 + g_5(x_1, x_5), \\ & x_6 + g_6(x_1, x_5), x_7^2 + g_7(x_1, x_7), x_8 + g_8(x_1, x_7) > \qquad . \end{aligned}$$

La liste des degrés initiaux de tout idéal des relations I_α est $(8, 1^3, 2, 1^3)$. Si avec la proposition ? ? ? ? nous trouvons une relation de la forme $r_7 = x_7 + h_7(x_1, \cdots, x_6)$ alors il existe $\alpha \in V(I)$ tel que l'idéal des relations I_α soit l'idéal $I + < r_7 >$.

Cas 1 Le groupe de Galois de f est le groupe impair T_7.

Ce cas a été traité comme exemple (voir ? ? ? ? ?). Nous avons montré qu'il y a 3 classes de L_0-équivalence et qu'il suffit d'ordonner les deux facteurs de rupture de degre 1 de telle sorte que $x_6+g_4(x_5)$ et $x_6+g_3(x_5)$ n'appartiennent pas à l'idéal de départ I choisit. Nous trouvons $r_7 =< x_7 + g_3(x_5) >$ et $G_\alpha = G_7$.

Cas 2 Le groupe de Galois de f est pair.

Il y a 3 classes de L_0-équivalence pour chaque groupe : pour $i = 1, 2, 3$, notons A_i celles pour T_9, B_i celles pour pour T_{10} et C_i celles pour T_{11}. Chacune des classes comporte 2 groupes. Le critère d'association est :

1) si $x_6 + g_2(x_5) \notin I$ alors I n'est associé ni à A_2, ni à B_2 et ni à C_2.
2) si $x_6 + g_3(x_5) \notin I$ alors I n'est associé ni à A_3, ni à B_3 et ni à C_3
3) si $x_4 + g_2(x_2) \notin I$ alors I n'est associé à la classe C_1
4) si $x_6 + g_4(x_5) \notin I$ alors I n'est associé ni à A_1 et ni à B_1.

Avec 1) et 2), optons pour l'idéal de départ I associé à A_1, B_1 ou C_1.

Cas 2.1. **I est associé à A_1 ou B_1 (voir 3) et 4)).** Avec les groupes G_9 et G_{10} dans A_1 et B_1 respectivement, nous trouvons $r_7 = x_7 + g_2(x_5)$ avec G_α=G_9 ou G_{10}.

Cas 2.2. I est associé à C_1 (voir 3) et 4)). Avec le groupe $G_\alpha = G_{11}$ de C_1, nous trouvons $r_7 = x_7 + g_2(x_6)$.

Compléments d'Annick permettant de certifier les critère :
Problème A_1 vs C_1 : Montrons que A_1 n'est pas compatible avec C_1.
Soit I un idéal associé à A_1 supposons que $x_4 + g_2(x_2) \in I$ alors

$$R := g_2(x_2) - g_4(x_1) \in I$$

(car $x_4 + g_4(x_1) \in I$). Dans tout les groupes associés à A_1 il existe une permutation de la forme $\sigma = (14)(23)(**)\cdots$ et $\tau = (13)(24)(**)\cdots$. Soit

$$U := \sigma.R = g_2(x_3) - g_4(x_4)$$

et

$$V := \tau.(x_2 + g_2(x_1)) = x_4 + g_2(x_3).$$

Alors $V - U$ est un élément de I i.e. $x_4 + g_4(x_4) \in I$ ce qui impossible puisque ce polynôme est de degré strictement supérieur à 8.
Conclusion : Si I est compatible avec A_1 alors $x_4 + g_2(x_2) \notin I$, et donc I n'est pas compatible avec C_1.

7.4 $\Delta_8(f) = (1^3, 4)$ et $L_0 = S_1^4 \times S_4$

L'ensemble triangulaire engendrant chaque idéal de départ I est de la forme :

$$f(x_1), x_2 + g_2(x_1), x_3 + g_3(x_1), x_4 + g_4(x_1), x_5^4 + g_5(x_1, x_5),$$
$$x_6^3 + g_6(x_1, x_5, x_6), x_7^2 + g_7(x_1, x_5, x_6, x_7), x_8 + g_8(x_1, x_5, x_6, x_7) \quad .$$

Comme la liste des degrés initiaux de tout idéal des relations I_α est $(8, 1^3, 4, 1^3)$, nous recherchons deux relations linéaires $r_6 = x_6 + h_6(x_1, \cdots, x_5)$ et $r_7 = x_7 + h_7(x_1, \cdots, x_6)$ de telle sorte que $I_\alpha = I + < r_6, r_7 >$.

Cas 1. Le groupe de Galois est le groupe impair T_{17}.

L'ensemble $C(L_0)$ comporte 18 groupes conjugués à T_{17} qui se répartissent en 3 classes A_1, A_2 et A_3 de L_0-équivalence comportant chacune 6 groupes et vérifiant le critère d'association suivant :

1) si $x_4 + g_3(x_2) \notin I$ alors I n'est pas associé à A_1,
2) si $x_3 + g_4(x_2) \notin I$ alors I n'est pas associé à A_2 et
3) si $x_4 + g_2(x_3) \notin I$ alors I n'est pas associé à A_3.

Optons pour l'idéal de départ I associé à la classe A_2. Avec $G_\alpha = G_{17}$ dans A_2, nous trouvons $r_6 = x_6 + g_3(x_5)$ et $r_7 = x_7 + g_2(x_5)$.

Cas 2. Le groupe de Galois est le groupe pair T_{18}.

Il n'y a qu'une seule classe de L_0-équivalence. L'ordre des facteurs de rupture est donc indifférent et il n'existe qu'un seul idéal de départ I. Avec $G_\alpha = G_{18}$, nous trouvons $r_6 = x_6 + g_4(x_5)$ et $r_7 = x_7 + g_2(x_5)$.

7.5 $\Delta_8(f) = (1, 2^3)$ et $L_0 = S_1^2 \times S_2^3$

Tout idéal de départ I a $(8, 1, 2, 1, 2, 1, 2, 1)$ comme liste de degré initiaux et nous avons card$(V(I))$ = 64=card(T_{31})=card(T_{27}). Hormis les groupes conjugués à T_6 et T_8 tous les groupes de $C(L_0)$ sont conjugués à des sous-groupes de T_{31} et de T_{27}.

Cas 1. Le groupe de Galois est un sous-groupe de T_{27}

C'est le cas lorsqu'un groupe G_{27} de $C(L_0)$ conjugué de T_{27} est le groupe de décomposition d'un idéal de départ I. Donc I est associé à la classe de L_0-équivalence de G_{27} qui ne contient que ce groupe. Dans $C(L_0)$, il y a 3 classes de L_0-équivalence pour les groupes conjugués à T_{27}. Soient G_{16} et G_{20}^+ deux sous-groupes d'indice 2 dans G_{27} conjugués de T_{16} et de T_{20}^+ respectivement. Si le groupe de Galois est pair, l'algorithme se termine avec `GaloisIdéal(`G_{27}`, `T_I`,[`G_{20}`])` et s'il est impair il se termine avec `GaloisIdéal(`G_{27}`, `T_I`,[`G_{16}`])`. Il n'y a qu'une résolvante de degré 2 à calculer.

Cas 2. Le groupe de Galois est un sous-groupe de T_{31}.

Il n'y a qu'un seule classe de L_0-équivalence pour T_{31}. Donc $G_{31} \in C(L_0)$ est le groupe de décomposition de l' idéal de départ I. Nous nous retrouvons alors dans la même configuration que pour T_{27} avec comme groupe de Galois T_{31} ou l'un de ses deux sous-groupes T_{21} ou T_{22}^+ d'indices respectifs 2. Nous terminons comme pour T_{27}.

Cas 3. Le groupe de Galois est T_6 ou T_8.

C'est le cas lorsque le groupe de décomposition de l'idéal de départ I n'est ni un conjugué de T_{27} ni G_{31}. La liste des degrés initiaux de tout idéal des relations est $(8, 1, 2, 1^5)$. Nous cherchons donc deux relations linéaires $r_5 = x_5 + h_5(x_1, x_3)$ et $r_7 = x_7 + h_7(x_1, x_3)$.

Il y a 3 classes A_1, A_2 et A_3 (resp. B_1, B_2 et B_3) de L_0-équivalence pour les groupes conjugués à T_6 (resp. T_8). Nous avons le critère d'association suivant :

- si $x_4 + g_2(x_3) \notin I$ alors I n'est associé ni à A_1 ni à B_1,
- si $x_6 + g_2(x_5) \notin I$ alors I n'est associé ni à A_2 ni à B_2,
- si $x_8 + g_2(x_7) \notin I$ alors I n'est pas associé à ni A_3 ni à B_3.

Choisissons l'idéal de départ I associé à A_2 ou B_2. Avec le groupe G_6 dans A_2 et le groupe G_8 dans B_2, nous obtenons la relation linéaire $r_7 = x_7 + g_2(x_3)$ et l'idéal $J = I+ < r_7 >$ est l'intersection de deux idéaux de relations. Les autres groupes des classes A_2 et B_2 permettant de rajouter cette relation sont respectivement $H_i = tG_it^{-1}$ avec $t = (5,6)$ pour $i = 6, 8$. Le stabilisateur de J est l'un des $L_i = G_i + G_i(5,6)$, $i = 6, 8$ selon que le groupe de Galois soit G_6 ou G_8 (voir Proposition ? ? ?). Ces deux ensembles sont distincts et ils engendrent le même groupe $tT_{35}t^{-1}$ avec $t = (2,3,5)(6,7)$.

Avec le polynôme $f_6 = x^8 - 3x^5 - x^4 + 3x^3 + 1$, la décomposition de J en deux idéaux premiers I_α et $I_{(5,6)\alpha}$ ($\alpha \in V(J)$) se réalise en 0.3 secondes et avec le polynôme $f_8 = x^8 + 24x^6 + 126x^4 + 216x^2 + 117$, elle se réalise en 0.1 secondes. Il reste à tester lequel des 4 groupes G_i, H_i avec $i = 6, 8$ est le groupe de décomposition de I_α. Ce sera le groupe de Galois G_α.

Remarque 7.2. Avec la méthode de Yokoyama, si le groupe de Galois est connu, il reste un facteur linéaire en x_5 à calculer, soit les 16 coefficients de $x_1^i x_3^j$ avec $i \in [0,7]$ et $j \in \{0,1\}$.

7.6 $\Delta_8(f) = (1,2,4)$ et $L_0 = S_1 \times S_2 \times S_4$.

le polynôme f se factorise en $(x-\alpha)(x+g_2(\alpha))(x^2+g_4(\alpha))(x^4+g_5(\alpha))$ sur $k(\alpha)$. Les groupes de $C(L_0)$ sont des conjugués des groupes $T_{15}, T_{19}^+, T_{26}, T_{28}, T_{29}^+, T_{30}$ et T_{35}. Les groupes G_i, $i = 26, 28, 29, 30, 35$ sont des sous-groupes d'indice 2 dans G_{35} et les groupes G_{19}^+ et G_{15} sont des sous-groupes d'indice 2 dans G_{26} et G_{29}^+ respectivement. Il existe $\alpha \in V(I)$ tel que $I_\alpha^{G_{35}} = J = I+ < x_6 + g_2(x_5) >$ (voir Propo ? ? ?). Les calculs démarrent donc avec l'idéal J.

Si le groupe de Galois est pair et que le groupe de Galois sur $k(\alpha)$ du facteur de rupture $x^4 + g_5(\alpha)$ est $4T_1$ (i.e. C_4) alors le groupe de Galois de f est T_{19} sinon c'est T_{29}. Si le groupe de Galois est T_{29}, l'algorithme se termine avec `GaloisIdéal(`G_{35}`,` T_J`,` $[G_{29}]$`)` et si c'est T_{19}, il se termine `GaloisIdéal(`G_{35}`,`T_J`,` $[G_{29}, G_{19}, H_{19}]$`)` avec $H_{19} = sT_{19}s^{-1}$ avec $s = (2,3)(4,8)(6,7)$. Il y aura au plus deux résolvantes de degré 2 à calculer (voir Exemple 6.19). A noter que `GaloisIdéal` peut aussi servir à tester si T_{29} est ou non le groupe de Galois.

Si le groupe de Galois est impair et celui de $x^4 + g_5(\alpha)$ est pair (i.e. $4T_2^+$) alors le groupe de Galois de f est T_{15} et l'algorithme se termine avec `GaloisIdéal(`G_{35}`,` T_J`,`$[G_{26}, G_{15}, H_{15}]$`)` où $H_{15} = sT_{15}s^{-1}$ avec $s = (2,8,6,7,4,5)$. Les calcul est similaire à l'exemple 6.19 car G_{26} est

autoadjoint dans G_{35}. Dans le cas contraire l'algorithme se termine avec `GaloisIdéal(`G_{35}`,` T_J`,`$[G_{26}, G_{28}, G_{30}]$`)`. Il n'y aura à calculer que des résolvantes de degré 2.

7.7 $\Delta_8(f) = (1, 3^3)$ et $L_0 = S_1 \times S_1 \times S_3 \times S_3$.

Le groupe de Galois est l'un des groupes pairs suivants : T_{12}, T_{13}, T_{14} d'ordres 24 et T_{24} d'ordre 48. La liste des degrés initiaux de tout idéal de départ I est $(8, 1, 3, 2, 1, 3, 2, 1)$. Soit la relation $x_2 + g_2(x_1)$ de I.

Cas 1. Le groupe de Galois est T_{24}, T_{13} ou T_{14}.

Il y a 2 classes de L_0-équivalence C_1 et C_2 pour T_{24} et donc deux idéaux initiaux distincts si le groupe de Galois est T_{24} ou bien l'un de ses deux sous-groupes T_{13} et T_{14}. Les groupes G_{24} dans C_1 et $H_{24} = sT_{24}s^{-1}$ avec $s = (2, 8, 6)(3, 7)$ dans C_2 permettent de rajouter les relations $r_6 = x_6 + g_2(x_3)$ et $r_7 = x_7 + g_2(x_4)$ à l'idéal de départ associé. Soit I un idéal de départ quelconque. L'idéal $J = I + < r_6, r_7 >$ a pour groupe de décomposition G_{24} (resp. H_{24}) ssi I est associé à la classe de L_0-équivalence de G_{24} (resp. H_{24}). Dans la pratique, il faut sélectionner l'idéal de départ de telle sorte que J ait G_{24} comme groupe de décomposition et terminer avec `GaloisIdéal(`G_{24}`,` T_J`,`$[G_{13}, G_{14}]$`)`. Il n'y aura que des résolvantes de degré 2 à calculer.

Cas 2 Le groupe de Galois est T_{12}

Il n'y a qu'une seule classe de L_0-équivalence pour les groupes conjugués à T_{12}. L'idéal $J = I + < r_6, r_7 >$ a pour stabilisateur $L = G_{12} + G_{12}(3, 4)(6, 7)$ (voir Proposition ? ? ?). Le groupe engendrant L est le groupe $sT_{39}s^{-1}$ avec $s = (2, 3, 4, 7, 5, 6)$ d'ordre 192. Ce stabilisateur étant connu, nous pouvons terminer avec `GaloisIdéal(`L`,` T_J`,` $[G_{12}]$`)`. Les G_{12}-résolvantes L-relatives sont de degré 5.

Conclusion. Lorsque $\Delta_8(f) = (1, 3^2)$, il faut calculer un idéal de départ I et en déduire l'idéal de Galois $J = I + < r_6, r_7 >$. Le groupe de Galois est T_{12} si et seulement si le groupe de décomposition de J n'est ni G_{24} ni H_{24}.

Remarque 7.3. La table de première décomposition peut être aussi utilisée pour cela : si le groupe de Galois d'un quelconque des facteurs de rupture de degré 3 est $3T_2$ (i.e. S_3) alors le groupe de Galois de f est T_{24}.

7.8 $\Delta_8(f) = (1,6)$ et $L_0 = S_1 \times S_1 \times S_6$

Le groupe de Galois est un sous-groupe de T_{44} dont l'ordre est 384=8.6.4.2. Soit $x + g_2(x_1)$ le facteur de rupture de degré 1. Les degrés initiaux de l'idéal de départ I sont $8, 1, 6, 4, 3, 2, 1$. Le groupe G_{44} est un des 15 conjugués de T_{44} dans $C(L_0)$. Avec la proposition ? ? ?, nous savons qu'il existe $\alpha \in V(I)$ tel que $J = I_\alpha^{G_{44}} = I + < x_4 + g_2(x_3), x_6 + g_2(x_5) >$. Les groupes de $C(L_0)$ vérifient : G_{38},G_{39}^+ et G_{40} d'indice 2 dans G_{44}, G_{23} d'indice 4 dans G_{40} et G_{32}^+ d'indice 2 dans G_{39}^+. Selon la parité du groupe de Galois les calculs se terminent avec `GaloisIdéal(`G_{44}`,`T_J`,[`G_{39}^+`, `G_{19}^+`])` ou bien avec `GaloisIdéal(`G_{44}`,`T_J`, [`G_{40}, G_{38}, G_{23}`])`.

7.9 $\Delta_8(f) = (3,4)$ et $L_0 = S_1 \times S_3 \times S_4$

Tous les groupes candidats sont des sous-groupes de T_{47} d'ordre 1152=8.144 =8.card(L_0). Les groupes T_{46}, T_{45}^+ sont d'indice 2 dans T_{47}, les groupes T_{41}^+ et T_{42}^+ sont respectivement d'indices 3 et 2 dans T_{45}^+ et les groupes T_{33}^+ et T_{34}^+ sont d'indice 2 dans T_{42}^+. L'idéal de départ I a pour stabilisateur le groupe G_{47}. Selon la parité du groupe de Galois les calculs se terminent avec `GaloisIdéal(`G_{47}`,`T_I`,[`G_{46}`])` ou bien avec `GaloisIdéal(`G_{47}`,`T_I`, [`$G_{45}^+, G_{42}^+, G_{41}^+, G_{34}^+, G_{33}^+$`])`.

Références

[Esc97] J.P. Escofier. *Théorie de Galois*. Masson, 1997.

[Tch50] N. Tchebotarev. *Gründzüge des Galois'shen Theorie*. P. Noordhoff, 1950.

[Val99] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4) :507–535, 1999. (Version longue du rapport LIP6 1997/014).

[Yok97] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118 :617–636, 1997. Algorithms for algebra (Eindhoven, 1996).

[Yok99] K. Yokoyama. A modular method to compute the splitting field of a polynomial. *Communication privée*, 1999.