UNIVERSITE PIERRE & MARIE CURIE
Paris 6

THÈSE DE DOCTORAT DE L'UNIVERSITÉ PARIS 6

Spécialité

Informatique

présentée par

M. Guénaël Renault

Pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ PARIS 6

Calcul efficace de corps de décomposition

Soutenue le 16 juin 2005

Devant le jury composé de :

Rapporteurs :		
M. Antonio Machì	Professeur	Università di Roma (Italia)
M. François Morain	Professeur	École Polytechnique (LIX)
Examinateurs :		
Mme Pascale Charpin	Directeur de recherche	INRIA-Rocquencourt (Projet CODES)
M. Daniel Lazard	Professeur émérite	Université de Paris 6 (LIP6)
M. Felix Ulmer	Professeur	Université de Rennes 1 (IRMAR)
Directrice :		
Mme Annick Valibouze	Professeur	Université de Paris 6 (LIP6)

Remerciements

En premier lieu, je tiens à exprimer tous mes sincères remerciements à ma directrice de thèse, Annick Valibouze. Je lui suis très reconnaissant de m'avoir ouvert les portes de la recherche en calcul formel et indiqué les chemins à suivre. Je garderai longtemps en mémoire ces jeudis de réflexions où Annick nous a fait partager sa vision originale de la théorie de Galois effective.

Je remercie sincèrement Daniel Lazard pour m'avoir accueilli dans son équipe de recherche et qui m'a fait l'honneur de faire partie de mon jury. Les discussions que j'ai eu avec Daniel ont toujours été enrichissantes et ses conseils m'ont été d'une très grande aide.

Je remercie Antonio Machì et François Morain pour avoir accepté d'être les rapporteurs de ma thèse. Je tiens à exprimer toute ma reconnaissance à François Morain pour sa lecture minutieuse et ses remarques qui ont fait progresser la qualité scientifique de ce mémoire. Je remercie chaleureusement Antonio Machì pour les échanges amicaux que nous avons eu tous les deux et pour les encouragements qu'il m'a témoignés.

Je remercie Pascale Charpin et Felix Ulmer pour avoir accepté de faire partie de mon jury et ainsi, de s'être intéressés à mes travaux de recherche.

Je tiens à exprimer tous mes remerciements aux membres de l'équipe CalFor du LIP6. Le cadre agréable de cette équipe m'a permis de préparer au mieux cette thèse. Plus particulièrement, je tiens à remercier Jean-Charles Faugère et Fabrice Rouiller pour leur dynamisme et le soutien qu'ils m'ont apporté ; Sébastien Orange, avec qui j'ai eu la joie de collaborer ; David et Thierry pour leur efficacité en matière de tâches administratives ; Jean-Michel et Cyriaque pour faire en sorte que nos outils de travail soient toujours disponibles ; les personnes avec qui j'ai eu le plaisir de partager un bureau : Magali, Philippe (dit « *la Trébuche* »), Gwénolé et Louis.

Je remercie sincèrement Kazuhiro Yokoyama pour m'avoir invité au sein de son équipe de recherche à l'Université du Kyushu (Fukuoka/Japon). Il a tout fait pour me faciliter la vie au Japon et m'a accueilli dans un cadre de travail très efficace. La collaboration qui en résulte est une chance pour moi.

Je remercie Marc Giusti, ainsi que toute l'équipe de Médicis, pour continuer à mettre à la disposition de toute la communauté du Calcul Formel des moyens matériels nécessaires aux calculs extrêmes.

Je tiens à remercier les collègues de l'UFR d'informatique de Paris 6 qui m'ont transmis le plaisir de l'enseignement. Plus particulièrement, je tiens à remercier Alain Mailles qui m'a supervisé avec beaucoup de sympathie dans son équipe pédagogique lorsque j'ai débuté mes vacations en tant que chargé de TD ; Emmanuel Chailloux qui m'a transmis une partie de son savoir sur le langage OCaml. Travailler à ses côtés fût un plaisir pour moi, il m'a beaucoup appris sur l'organisation des enseignements et l'en-

cadrement des projets ; Christophe Gonzales qui m'a révélé quelques uns de ses secrets de hacker ; Valérie Ménissier-Morain avec qui j'ai appris à monter (avec C. Queinnec et Ph. Trébuchet) un enseignement. Elle a passé plusieurs heures à relire et améliorer les sujets de TD/TME que je préparais. Grâce à elle j'ai beaucoup progressé dans ma façon de rédiger, je lui en suis sincèrement reconnaissant.

Je remercie aussi Messieurs Fombaron et Monvoisin pour m'avoir fait confiance et laissé, un an durant, la responsabilité d'un nouveau cours d'informatique au sein de l'ESITC.

Merci à mes parents pour m'avoir fait confiance. Ils ont été un soutien moral et financier (le seul parfois) très important. Ils ont fait en sorte de me faciliter la vie pendant toutes ces années. Merci aussi à ma sœur Véronique qui m'a remis les pieds sur terre à de nombreuses reprises. Ils ont toujours cru en moi, même lorsque je n'y croyais plus moi-même.

Merci à tous mes amis qui sont encore là malgré toutes mes indisponibilités : Philippe, Servane, Florent, Chloé, Jérome, Audrey, Laurent, Agnès, Arnaud(s), Sophie, Jaff, Myriame, Mimi(s) ...

Comment pourrais-je remercier Muriel ? Pendant ces années de thèse, elle a toujours été à mes côtés et a supporté ces derniers mois où je n'ai rien fait pour me faire aimer. Elle m'a apporté l'amour dont j'avais besoin pour me sortir de mes désespoirs de fin de thèse.

Version du 10/09/2005.

Introduction

L'axe de cette thèse est la théorie de Galois effective. Nous allons nous intéresser à la résolution d'équations polynômiales $f = 0$ de degré n et à l'action du groupe de Galois de f sur ces solutions. Avant de commencer, il nous faut répondre à la question centrale (chère à Daniel Lazard) : *« Que signifie résoudre ? »*.

Dans le cadre du calcul formel, résoudre l'équation $f = 0$, c'est se donner les moyens informatiques permettant de manipuler symboliquement les racines du polynôme f. En plus de pouvoir manipuler ces racines de manière symbolique, nous voulons aussi connaître l'action du groupe de Galois sur celles-ci.

D'un point de vue mathématique, ceci revient à pouvoir calculer dans l'extension du corps des coefficients de f engendrée par les racines de ce polynôme. Cette extension est appelée *corps de décomposition de* f. Il s'agit alors de se donner une représentation effective de ce corps afin de l'implanter en machine. Pour simplifier l'exposé, supposons dans cette introduction que le corps des coefficients de f est le corps $\mathbb{Q}$ des rationnels.

Représentation des données

Représentation sous forme de radicaux

En rajoutant la possibilité de représenter les racines n^e d'entiers, les solutions de certaines équations peuvent être représentées. En effet, il est bien connu que les solutions d'une équation du second degré peuvent être données sous forme de radicaux (c'est-à-dire sous la forme d'expressions algébriques et d'extractions de racines). D'après les travaux de l'école italienne du XVI^e siècle (Cardan, Tartaglia, Ferrari), il en est de même pour les équations du troisième et quatrième degré. Pour les degrés suivants, depuis les travaux de Lagrange, Abel et Galois (voir [4, 63, 62, 44]), nous savons que nous ne pouvons plus en faire de même. Plus précisément, cette représentation est possible uniquement si le groupe de Galois de f est résoluble. Pour de tels polynômes de degré cinq, Dummit donne dans [36] des formules pour exprimer les racines sous forme de radicaux et Lazard, dans [72], expose des formules optimales en terme de nombre de racines à extraire. Plus généralement, des algorithmes pour le calcul des racines (sous forme de radicaux) d'un polynôme de groupe de Galois résoluble sont donnés par Miller et Landau, Anai et Yokoyama, Hanrot et Morain dans [67, 65, 66, 8, 52] (voir aussi [39, 51] pour des résolutions partielles). Toutefois, lorsque l'on peut exprimer les racines sous forme de radicaux, ces formules sont souvent trop compliquées pour pouvoir être manipulées aisément (voir Paragraphe 9 dans [72]). Comme nous voulons travailler avec des polynômes de groupe de Galois quelconque, nous ne choisissons pas cette représentation.

Représentation à la Kronecker

C'est à la fin du XIX^e siècle que Kronecker donne la notion de corps abstrait, construit comme quotient d'algèbre (voir [60, 61]). Cette construction est complètement effective et permet de représenter le corps de décomposition de f de deux manières différentes (au moins).

Une première représentation possible du corps de décomposition K de f, est donnée sous la forme d'une *extension simple* de $\mathbb{Q}$. Ainsi K sera représenté par l'algèbre $\mathbb{Q}[x]$ quotientée par un certain polynôme P de $\mathbb{Q}[x]$. Dans ce cas, les racines de f pourront être représentées symboliquement à partir de l'image de l'indéterminée x modulo P. L'action de son groupe de Galois sur ses racines symboliques pourra être calculé à l'aide de l'un des algorithmes de Klüners (voir [57]), Acciaro et Klüners (voir [5]) ou Allombert (voir [6]).

La seconde représentation possible du corps de décomposition K du polynôme f est donnée sous la forme de l'algèbre $\mathbb{Q}[x_1, \ldots, x_n]$ quotientée par l'idéal $\mathcal{M}$ de toutes les *relations algébriques entre les racines de* f, plus communément appelé *idéal des relations de* f. Dans ce cas, les racines de f sont représentées par les images des indéterminées $x_1, \ldots, x_n$ modulo l'idéal $\mathcal{M}$. Pour pouvoir calculer dans une telle structure, il faut connaître une base de Gröbner de $\mathcal{M}$ qui sera triangulaire (puisque $\mathcal{M}$ est maximal). L'action du groupe de Galois de f sur ces racines est alors calculable à l'aide de l'algorithme de Anai, Noro et Yokoyama (voir [7]) ou celui de meilleur complexité que nous présenterons au chapitre 3 (voir aussi les travaux de Mertens [76] et ceux de Tchebotarev [100]).

La représentation du corps K sous la forme d'une extension simple de $\mathbb{Q}$ est apparemment la mieux adaptée. Toutefois, lorsque l'ordre du groupe de Galois grandit, le calcul du polynôme P devient de plus en plus inefficace. De plus, les algorithmes actuels permettant un tel calcul, à partir du polynôme f, ont pour résultat intermédiaire une base triangulaire de l'idéal des relations de f.

C'est donc la deuxième représentation que nous choisissons pour manipuler les racines de f. Cette représentation de K sera dite en *tour totale d'extensions*.

Problématique

Étant donné le polynôme f, il s'agit de calculer une base triangulaire de l'idéal des relations et l'action du groupe de Galois de f sur les racines symboliques.

L'algorithme classique, noté FE, pour le calcul d'une telle base triangulaire, repose sur la construction de l'algèbre quotient représentant K donnée par Kronecker. Il consiste en la factorisation du polynôme f sur les extensions intermédiaires entre $\mathbb{Q}$ et K (voir par exemple l'article de Anai, Noro et Yokoyama [7] et celui de Roblot [92]).

Une autre méthode pour le calcul d'une base de Göbner de l'idéal des relations est donnée par Annick Valibouze dans [106] (voir aussi l'article [35] de Ducos qui donne le même résultat vu sous un angle différent). L'avantage de cette méthode est de fournir en plus l'action du groupe de Galois sur les racines symboliques du polynôme. Pour cette méthode, de nouveaux objets ont été introduits : *les idéaux de Galois*. Cet algorithme repose sur le calcul symbolique de résolvantes relatives et le calcul de base de Gröbner ou d'ensembles triangulaires (voir les travaux de Arnaudiès, Valibouze, Aubry, Lehobey, Colin, Rennert et Abdeljaoued [9, 14, 28, 90, 73, 2]).

Dans les systèmes de calcul formel, c'est le premier algorithme qui est le plus souvent implanté. Cette implantation est inefficace en pratique dès que l'ordre du groupe devient élevé. Ceci vient du fait que cet algorithme est généraliste. Pour le second algorithme, dans certains cas, des étapes de calculs de résolvantes séparables à l'aide d'outils symboliques sont impraticables. En effet, ces cas se rencontrent lorsque les invariants utilisés pour les cacluls de résolvantes sont de grande taille (nombre de termes et arité).

Dans cette thèse, nous avons pour objectif de fournir des algorithmes et des implantations efficaces permettant un tel calcul (à la fois celui d'une base triangulaire engendrant $\mathcal{M}$ et celui de l'action du groupe de Galois sur les racines symboliques). Nous nous intéresserons à des polynômes séparables dont les coefficients sont dans un corps k supposé infini. Lorsque le corps k est fini et de petit ordre, les algorithmes de factorisation de polynômes sont très efficaces (voir [56, 41, 83, 81]) et ainsi il en va de même pour le calcul d'une représentation du corps de décomposition. Lorsque l'ordre du corps fini k est grand on pourra toujours utiliser l'algorithme de factorisation de Berlekamp (voir [18]) mais le calcul est plus difficil. Cependant, dans certains cas particuliers, l'obtention des racines d'un polynôme modulo un grand premier peut être faite assez efficacement (par exemple, on pourra consulter les sections 3.1 et 3.2 de la thèse de F. Morain [78]).

Contributions et descriptions des chapitres

Nos contributions sur le sujet peuvent être divisées en trois parties. Ce sont aussi ces trois parties qui nous ont servi de cadre pour organiser ce mémoire. Dans la suite de cette introduction, nous ne faisons qu'une brève présentation des chapitres, pour plus de détails le lecteur pourra se reporter à leur introduction.

Dans la première partie, nous nous intéressons aux idéaux de Galois de f et à leur variété. Le chapitre 1 contient des résultats de base sur la représentation des groupes et sur l'algèbre commutative qui seront utilisés dans les chapitres suivants. Le chapitre 2 contient les définitions et résultats de base sur les idéaux de Galois. Nous en présentons aussi de nouveaux portant sur la structure de ces idéaux et sur le cas particulier d'un polynôme réductible f. Ces nouveaux résultats permettent, pour certains, d'améliorer l'algorithme `GaloisIdéal` et pour d'autres, de mieux envisager l'utilisation de ces idéaux dans une nouvelle méthode de calcul de l'idéal des relations (voir Chapitre 5). Ces nouveaux résultats ont été obtenus en collaboration avec S. Orange et A. Valibouze et sont exposés dans les articles [84, 87]. Dans le chapitre 3, nous nous intéresserons aux groupes de permutations laissant globalement invariant des idéaux triangulaires. Plus précisément, si l'on considère l'action naturelle du groupe symétrique S_n sur l'anneau de polynômes $k[x_1, \ldots, x_n]$ définie par

$$\begin{array}{rcl} S_n \times k[x_1, \ldots, x_n] & \longrightarrow & k[x_1, \ldots, x_n] \\ (\sigma, P(x_1, \ldots, x_n)) & \longmapsto & \sigma.P = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \,, \end{array}$$

le sous-groupe de S_n laissant globalement invariant un idéal triangulaire I est noté $\mathrm{Dec}(I)$ et défini par

$$\mathrm{Dec}(I) = \{\sigma \in S_n \,:\, \sigma.I = I\} \,.$$

Dans le cas particulier où I est l'idéal des relations de f, Anai, Noro et Yokoyama donnent, dans [7], un algorithme permettant le calcul du groupe $\mathrm{Dec}(I)$ qui est l'image

de la représentation symétrique de l'action du groupe de Galois de f sur ses racines symboliques. Ils montrent que la complexité de leur algorithme est de l'ordre de $O(n^4)$ en terme de nombre de formes normales modulo I calculées. Dans ce chapitre, nous donnons un algorithme plus général, puisque permettant le calcul de $\mathrm{Dec}(I)$ pour I triangulaire quelconque, et montrons que pour une certaine classe d'idéaux de Galois, dont les idéaux de relations font partie, sa complexité est en $O(n^3)$ formes normales modulo I calculées. De plus, nous verrons que l'implantation de notre algorithme est plus efficace de manière générale. Les résultats de ce chapitre sont issus du travail en collaboration avec I. Abdeljaoued-Tej, S. Orange et A. Valibouze (voir [3]).

Dans la deuxième partie nous nous intéressons au calcul d'une base de Gröbner de l'idéal des relations de f. Comme nous l'avons dit plus haut, l'algorithme FE est trop général pour résoudre efficacement notre problème et l'algorithme `GaloisIdéal` souffre d'inefficacité à cause d'étapes coûteuses. Nous avons donc étudié les possibilités de faire cohabiter ces deux algorithmes au sein d'une seule méthode plus efficace. Plus précisément, nous verrons au chapitre 5, comment, après avoir factorisé f sur son corps de rupture, on peut terminer le calcul de l'idéal des relations de f à l'aide de l'algorithme `GaloisIdéal` tout en évitant des calculs. Nous avons réalisé une implantation de cette méthode dans le cas de polynômes de degré 8 et obtenu des résultats intéressants et encourageants. Pour pouvoir passer de l'algorithme FE à `GaloisIdéal` il nous faut des informations sur le groupe de Galois de f. Pour ce faire, nous avons étudié (voir Chapitre 4) le lien entre la factorisation de f sur son corps de rupture L et ce groupe. Ces informations sont rassemblées dans des tables que nous appelons *tables de rupture*. Ces tables généralisent celles de McKay et Soicher (voir [97]) car elles fournissent le groupe de Galois de chacun des facteurs de f dans $L[x]$ en fonction du groupe de Galois de f. Nous montrons aussi comment utiliser ces tables afin de valider en pratique certains calculs de groupe de Galois en fournissant des polynômes de groupe de Galois donné et à coefficient dans une extension simple de $\mathbb{Q}$. Tous ces résultats ont été obtenus en collaboration avec S. Orange et A. Valibouze (voir [85, 86]). Dans le chapitre 6 nous présentons une application particulière des résultats du chapitre 5. Ici, nous supposons que le groupe de Galois G de f est de type dihédral. Nous montrons comment obtenir l'idéal des relations de f et l'action de G sur ses racines symboliques à partir de la factorisation de f sur son corps de rupture en ne faisant que des calculs de formes normales. Plus précisément nous montrons qu'il faut au plus $O(n^2)$ calculs de formes normales pour terminer le calcul. Ce résultat peut être vu comme une généralisation symbolique de celui de B. K. Spearman et K. S. William (voir [98]). Dans cet article, il est montré comment obtenir les racines d'un polynôme de groupe de Galois D_5 à partir de deux d'entre elles et de la factorisation de f sur son corps de rupture.

Dans la troisième partie, réduite au chapitre 7 rédigé en anglais, nous nous intéressons à un algorithme proposé par Yokoyama (voir la Section 5.3 de [113]) permettant le calcul d'un idéal des relations de f. Dans ce chapitre, le polynôme sera supposé à coefficients dans $\mathbb{Q}$. Cet algorithme a besoin, en entrée, de beaucoup plus de données que les algorithmes étudiés dans la partie précédente. En effet, en plus du polynôme f, il suppose connue l'action du groupe de Galois de f sur des approximations p-adiques de ses racines. Dans ce chapitre, nous donnons une étude approfondie et aussi une amélioration de cet algorithme. Nous montrons comment la connaissance de cette action permet d'éviter et de réduire les calculs nécessaires à cet algorithme. Nous montrons aussi que le choix de la représentation symétrique du groupe de Galois de f ne doit pas

être faite au hasard pour pouvoir optimiser les calculs. L'implantation que nous avons faite de cet algorithme se révèle être très efficace. Ce chapitre est issu d'un travail en cours et en collaboration avec K. Yokoyama.

Table des matières

Liste des Algorithmes

Chapitre 1

Généralités

Dans ce chapitre, nous rappelons les définitions et résultats mathématiques généraux dont nous aurons besoin dans tout le restant de cette thèse. Dans toute la suite, les corps seront supposés commutatifs et la loi des groupes sera toujours notée multiplicativement (l'élément unité d'un groupe G sera alors noté 1_G). Les ensembles que nous considérerons ici ne seront jamais vides.

1.1 Représentation symétrique d'un groupe de Galois

Le but de cette section est de retracer la construction de la représentation symétrique d'un groupe et plus particulièrement celle du groupe de Galois d'une extension galoisienne. Ces résultats peuvent être retrouvés dans le cours de J.-M. Arnaudiès et A. Valibouze (voir [10]) ou dans tout autre ouvrage plus général (voir [68] par exemple).

Représentation par permutations

Soit G un groupe et E un ensemble. On appelle *action* (à gauche) du groupe G sur l'ensemble E, notée ., une application

$$\begin{array}{rcl} G \times E & \longrightarrow & E \\ (g, e) & \longmapsto & g.e \end{array}$$

vérifiant les deux assertions suivantes

i $\forall (g_1, g_2) \in G^2,\ \forall e \in E,\ g_1.(g_2.e) = (g_1 g_2).e$;

ii $\forall e \in E,\ 1_G.e = e$.

À une telle action on peut associer un homomorphisme ρ du groupe G dans le groupe $\mathrm{Perm}(E)$ des permutations de l'ensemble E, où l'image par ρ d'un élément g de G est définie par

$$\begin{array}{rcccl} \rho(g) & : & E & \longrightarrow & E \\ & & e & \longmapsto & g.e \end{array}$$

Inversement, si on se donne un homomorphisme ρ du groupe G dans le groupe $\mathrm{Perm}(E)$, alors on peut en déduire une action de G sur E (notée .). En effet, si on

considère l'application définie par

$$\begin{array}{rcl} G \times E & \longrightarrow & E \\ (g, e) & \longmapsto & g.e := \rho(g)(e) \end{array}$$

on vérifie aisément qu'elle satisfait les assertions i) et ii).

Un homomorphisme du groupe G dans le groupe des permutations $\mathrm{Perm}(E)$ est appelé *représentation par permutations* du groupe G. D'après ce que nous venons de voir, il est donc équivalent de se donner une action d'un groupe G sur un ensemble E ou une représentation par permutations du groupe G. Ainsi nous ne distinguerons plus une action de sa représentation par permutations qui lui est associée. Nous allons maintenant étudier le cas où l'ensemble E est fini.

Représentation symétrique

Soit G un groupe agissant sur un ensemble **fini** E de cardinal l'entier n. Notons ρ la représentation par permutations qui est associée à cette action.

Nous appellerons *numérotation de E* toute application bijective de l'ensemble $\{1, \ldots, n\}$ dans E. Fixons $\mathcal{N}$ une telle numérotation de E. Nous avons alors l'isomorphisme de groupe :

$$\begin{array}{rcl} \mathrm{Perm}(E) & \longrightarrow & S_n \\ s & \longmapsto & \mathcal{N}^{-1} \circ s \circ \mathcal{N} \end{array}$$

et nous en déduisons l'homomorphisme de groupe suivant :

$$\begin{array}{rcl} \phi_{\mathcal{N}} : G & \longrightarrow & S_n \\ g & \longmapsto & \mathcal{N}^{-1} \circ \rho(g) \circ \mathcal{N} \end{array}$$

Un tel homomorphisme sera appelé *représentation symétrique par rapport à la numérotation $\mathcal{N}$* et lorsque la situation est sans ambiguïté sur $\mathcal{N}$, c'est-à-dire lorsque la numérotation est fixée, nous parlerons de *représentation symétrique*.

Soit $\mathcal{N}_1$ et $\mathcal{N}_2$ deux numérotations de E. Alors, il existe une permutation σ dans S_n telle que :

$$\mathcal{N}_2 = \sigma \circ \mathcal{N}_1 \,,$$

et donc :

$$\phi_{\mathcal{N}_2} = \sigma^{-1} \circ \phi_{\mathcal{N}_1} \circ \sigma \,.$$

Soit H le sous-groupe de S_n image d'une représentation symétrique de G. D'après ce qui précède, G peut être représenté par un groupe quelconque de la classe de conjugaison de H dans S_n et uniquement ces groupes.

Soit G un groupe agissant sur un ensemble E. Le *stabilisateur* d'un élément e de E sous l'action de G est le sous-groupe de G noté $\mathrm{Stab}_G(e)$ et défini par

$$\mathrm{Stab}_G(e) := \{g \ : \ g \in G \text{ et } g.e = e\} \,.$$

L'action du groupe G sur l'ensemble E est dite *fidèle* si la représentation symétrique correspondante est injective, ou si, de manière équivalente, le sous-groupe $\cap_{e \in E} \mathrm{Stab}_G(e)$ de G est réduit à l'élément unité.

L'*orbite* d'un élément e de E sous l'action de G est le sous-ensemble noté $G.e$ et défini par

$$G.e := \{g.e \ : \ g \in G\}\,.$$

Plus généralement, un tel ensemble est appelé *G-orbite*. L'action du groupe G sur l'ensemble E est dite *transitive* si l'orbite d'un élément quelconque e de E est l'ensemble E tout entier.

Un sous-groupe G de S_n est dit transitif si l'action canonique de G sur $\{1, \ldots, n\}$ est transitive.

1.2 Groupes de Galois

Soit k un corps commutatif, $\overline{k}$ une clôture algébrique de k et f un polynôme non constant en une variable x et à coefficients dans k. Le polynôme f est dit *séparable* s'il n'a aucune racine multiple dans $\overline{k}$, ou, de manière équivalente, si le pgcd de f et de son polynôme dérivé est constant. Nous avons le résultat bien connu suivant (voir par exemple [21, Chapitre 5]) :

Théorème 1.2.1. *Si le polynôme f est séparable alors son corps de décomposition k_f dans $\overline{k}$ est une extension galoisienne sur toute extension intermédiaire L entre k et k_f.*

Supposons à présent le polynôme f séparable. Soit E l'ensemble fini des racines (distinctes) de f dans $\overline{k}$ et L un corps intermédiaire entre k_f et k. Le corps k_f est alors engendré sur L par E. Comme la restriction à L d'un élément ϕ du groupe des L-automorphismes de k_f se réduit à l'identité, la définition de ϕ ne dépend que des images qu'il prend sur les éléments de E. Ainsi nous pouvons construire un homomorphisme injectif ρ de la forme

$$\mathrm{Aut}_L(k_f) \quad \longrightarrow \quad \mathrm{Perm}(\underline{\alpha})$$

et défini par

$$\begin{array}{rccc} \rho(\phi) \ : & E & \longrightarrow & E \\ & e & \longmapsto & \phi(e) \end{array}$$

De cette manière, nous obtenons une action fidèle du groupe des L-automorphismes sur l'ensemble E. Soit $\mathcal{N}$ une numérotation des racines de f, c'est-à-dire des éléments de E, alors nous avons une représentation symétrique injective du groupe G dans S_n. Soit H l'image dans S_n de cette représentation, alors G est isomorphe à H et, d'après ce que nous avons vu plus haut, nous pouvons construire un isomorphisme entre G et chacun des conjugués de H dans S_n. Ainsi le groupe de Galois d'un corps de décomposition d'un polynôme de degré n pourra toujours être associé à une classe $\mathcal{C}$ de conjugaison d'un groupe H dans S_n.

Définition 1.2.2. Soit f un polynôme séparable de $k[x]$ de degré n un entier strictement positif et L un corps intermédiaire entre k_f et k. Nous appellerons groupe de Galois de f sur L, un représentant quelconque de la classe de conjugaison dans S_n de l'image d'une représentation symétrique du corps de décomposition de f sur L. Ce groupe sera noté $\mathrm{Gal}_L(f)$.

Exemple :

Soit $k = \mathbb{Q}$ et $f = x^6 - 10x^4 + 31x^2 - 30$. Comme f se factorise sur k en $f = (x^2-2)(x^2-3)(x^2-5)$ les racines de f sont toutes réelles et sont données par $E = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5}\}$.

Exhibons le groupe des k-automorphismes du corps $k_f = k[E]$. Le groupe $Aut_k(k_f)$ contient $[k_f : k]$ éléments et ici nous avons clairement $[k_f : k] = 8$. Soit $\phi \in Aut_k(K_f)$ et $\alpha \in E$. Comme l'image de α par ϕ ne peut être qu'un conjugué de α dans E nous avons :

$$\phi(\alpha) = -\alpha\,.$$

Nous obtenons ainsi la définition de chacun des éléments du groupe des k-automorphismes de $k_f = k[E]$ à partir de leur action sur l'ensemble E. Si l'on choisit de numéroter E à l'aide de la fonction $\mathcal{N}$ définie par :

$$\begin{array}{rcl} \mathcal{N} : E & \longrightarrow & \{1, \ldots, 6\} \\ \sqrt{i} & \longmapsto & i + (i \bmod 2) \\ -\sqrt{i} & \longmapsto & \mathcal{N}(\sqrt{i}) - 1 \end{array}$$

alors le groupe $Aut_k(k_f)$ est représenté symétriquement par le sous-groupe H de S_6 engendré par l'ensemble de permutations $\{(12), (34), (56)\}$ noté $C(2)\times C(2)\times C(2)$. Si nous avions choisi une autre numérotation $\mathcal{N}_2$ pour l'ensemble E alors, en notant σ l'unique élément de $\mathrm{Perm}(\{1, \ldots, 6\})$ tel que $\mathcal{N}_2 = \sigma \circ \mathcal{N}$, le groupe des k-automorphismes de k_f serait représenté par le sous-groupe de S_6 engendré par l'ensemble de permutations

$$\{(\sigma(1), \sigma(2)), (\sigma(3), \sigma(4)), (\sigma(5), \sigma(6))\}$$

qui n'est autre que le conjugué de H par σ^{-1}. Quel que soit la numérotation choisie, nous dirons que le polynôme f a pour groupe de Galois $C(2) \times C(2) \times C(2)$.

Soit L le corps $k[\sqrt{2}]$ intermédiaire entre k et k_f. Le groupe des L-automorphismes de k_f est isomorphe à $C(2)\times C(2)$. Si nous choisissons de numéroter l'ensemble E à l'aide de $\mathcal{N}$ alors une représentation symétrique de $Aut_L(k_f)$ sera donnée par le sous-groupe de S_6 engendré par l'ensemble des permutations $\{(3, 4), (5, 6)\}$.

1.3 Algèbre commutative

Dans cette partie, nous donnons les définitions et résultats de base sur le lien entre la géométrie et l'algèbre commutative ainsi que ceux sur les idéaux triangulaires. Le corps k est supposé infini et nous notons $\overline{k}$ une clôture algébrique de k.

1.3.1 Variétés et idéaux radicaux

Soit $S = \{f_1, \ldots, f_s\}$ un ensemble fini de polynômes de l'anneau $k[x_1, \ldots, x_n]$. Le but de la géométrie algébrique est de pouvoir décrire certaines propriétés géométriques à partir de propriétés algébriques. Plus exactement, les propriétés de l'ensemble des solutions du système :

$$f_1 = f_2 = \ldots = f_s = 0\,,$$

c'est-à-dire, l'ensemble des éléments de $\overline{k}^n$ qui annulent simultanément les polynômes $f_1, \ldots, f_s$, sont données à l'aide de propriétés algébriques de l'ensemble S.

Définition 1.3.1. Soit $S = \{f_1, \ldots, f_s\}$ un ensemble fini de polynômes de $k[x_1, \ldots, x_n]$. L'ensemble V des solutions (ou zéros) de S dans $\overline{k}^n$ est appelé *variété* (algébrique affine) de S et est noté $V(f_1, \ldots, f_s)$. Par abus de langage, nous dirons de V que c'est une variété.

Soit I un idéal de $k[x_1, \ldots, x_n]$. D'après le théorème de Hilbert (voir [15]), il existe un ensemble fini S de polynômes de $K[x_1, \ldots, x_n]$ engendrant l'idéal I. Ainsi, la variété $V(I)$ de I sera définie comme celle de S.

Inversement, étant donné un ensemble L d'éléments de $\overline{k}^n$, on peut définir l'idéal $Id_k(L)$ des polynômes de $k[x_1, \ldots, x_n]$ s'annulant sur L. Il est bien connu que cet idéal est radical et le dictionnaire de géométrie algébrique permet de faire le lien entre les idéaux radicaux de $k[x_1, \ldots, x_n]$ et les variétés de $\overline{k}^n$.

Dans cette thèse, nous nous intéressons aux idéaux dont la variété est non vide et de cardinal fini ou autrement dit de *dimension zéro*. Ainsi, nous nous restreignons ici à l'étude de telle variété. Un idéal s'annulant sur une telle variété est lui aussi dit de *dimension zéro*.

Comme le montre l'exemple suivant, un ensemble fini d'éléments de $\overline{k}^n$ ne correspond pas forcément à la variété d'un idéal de $k[x_1, \ldots, x_n]$.

Exemple 1.3.2. Supposons $k = \mathbb{Q}$. Soit $\underline{\alpha} = (\sqrt{2}, -\sqrt{2})$ un élément de $\overline{k}^2$. L'idéal $Id_k(\{\underline{\alpha}\})$ de $k[x_1, x_2]$ est engendré par l'ensemble des polynômes $\{x_1^2 - 2, x_2 - x_1\}$ et sa variété $V(I)$ est donnée par $\{\underline{\alpha}, -\underline{\alpha}\}$.

En fait, un ensemble fini (non vide) L quelconque de $\overline{k}^n$ est toujours la variété d'un idéal de $\overline{k}[x_1, \ldots, x_n]$. En effet, il suffit de prendre l'idéal engendré par l'ensemble de polynômes

$$\bigcup_{e \in L} \{x_1 - e_1, \ldots, x_n - e_n\}\,.$$

Ainsi, nous appelons *variété* un ensemble fini quelconque de $\overline{k}^n$ et nous donnons la définition suivante.

Définition 1.3.3. Une variété V est dite *définie sur* k (ou k-variété) s'il existe un ensemble fini S de polynômes de $k[x_1, \ldots, x_n]$ tel que

$$V(S) = V\,.$$

Pour pouvoir décomposer une variété V comme une réunion de points de l'espace affine, il est inutile de considérer le corps $\overline{k}$. En effet, l'extension $k(V)$ de k obtenue en adjoignant à k toutes les coordonnées de V suffit. En fait, $k(V)$ est la plus petite extension de k ayant cette propriété. Ainsi, une variété V est toujours une $k(V)$-variété.

Exemple 1.3.4. En reprenant les mêmes notations que dans l'exemple 1.3.2, l'ensemble $\{\underline{\alpha}\}$ est une $k(\sqrt{2})$-variété mais n'est pas une k-variété.

Nous supposons, pour toute la suite de ce chapitre, que les variétés considérées sont toutes *séparables*, c'est-à-dire, telles que les coordonnées de leurs éléments soient séparables. Ainsi, les variétés considérées ici sont des sous-ensembles finis de $(\overline{k}^s)^n$ où $\overline{k}^s$ est la clôture séparable de k contenue dans $\overline{k}$. Cette hypothèse permet l'énoncé suivant.

Lemme 1.3.5. *Soit V une variété définie sur k et S un ensemble de polynômes de $k[x_1, \ldots, x_n]$ s'annulant sur V. Alors l'ensemble S est générateur de l'idéal $Id_{\overline{k}}(V)$.*

Démonstration. Comme V est séparable, l'idéal de $\overline{k}[x_1, \ldots, x_n]$ engendré par S est radical et donc s'identifie à $Id_{\overline{k}}(V)$ (voir [15] pour plus de détails). □

L'exemple classique suivant montre que ce dernier lemme n'est plus vrai en toute généralité.

Exemple 1.3.6. Supposons $k = \mathbb{F}_5(T)$. Soit $P = x^5 - T$ et α une racine de P dans $\overline{k}$. Alors P est irréductible sur k et se décompose en $P = (x - \alpha)^5$ sur $\overline{k}$. Ainsi l'ensemble $\{\alpha\}$ est une variété non séparable définie sur k. L'idéal $Id_{\overline{k}}(V)$ est engendré par $x - \alpha$ et non pas par P.

La proposition qui suit généralise le procédé vu dans les exemples 1.3.2 et 1.3.4. Elle permet de construire effectivement la plus petite k-variété contenant une variété V de $\overline{k}^n$.

Proposition 1.3.7. *Soit V une variété de $\overline{k}^n$. La plus petite k-variété contenant V s'identifie à l'ensemble*

$$\bigcup_{\rho \in \mathrm{Gal}_k(L)} \{\rho(\underline{\alpha}) = (\rho(\alpha_1), \ldots, \rho(\alpha_n)) \, : \, \underline{\alpha} \in V\}\,,$$

où L est la clôture galoisienne de $k(V)$.

Démonstration. Par définition de $k(V)$, la variété V est définie sur ce corps et donc sur L. Si k contient L alors le résultat est clair, supposons donc que L est une extension non triviale de k.
Soit S un ensemble fini de polynômes de $k(V)[x_1, \ldots, x_n]$ tel que $V = V(S)$. Comme il y a équivalence entre le fait que S est à coefficients dans k et le fait que $\forall \rho \in \mathrm{Gal}_k(L)$, $\rho(S) = S$, d'après [111, Theorem 3 Chapter IV] ceci équivaut au fait que V vérifie

$$V = \bigcup_{\rho \in \mathrm{Gal}_k(L)} \{\rho(\underline{\alpha}) = (\rho(\alpha_1), \ldots, \rho(\alpha_n)) \, : \, \underline{\alpha} \in V\}\,,$$

et le résultat suit. □

1.3.2 Bases de Gröbner

Parmi tous les ensembles engendrant un idéal I de $k[x_1, \ldots, x_n]$ il y en a des plus intéressants que d'autres. En effet, certains permettent le test d'appartenance à cet idéal.

Parmi ces ensembles intéressants il y a les *bases de Gröbner*. La théorie autour de ces bases a été développée principalement depuis les travaux de Buchberger (voir [22, 23]). En effet, c'est lui qui donna le premier algorithme permettant le calcul d'une telle base à partir d'un ensemble de générateurs de I.

Pour pouvoir généraliser l'algorithme d'Euclide pour le test d'appartenance à l'idéal I, nous avons besoin d'une notion d'ordre sur $k[x_1, \ldots, x_n]$. Dans cette thèse, nous ordonnons les indéterminées de la manière suivante

$$x_1 < x_2 < \ldots < x_n\,,$$

et on s'en sert pour ordonner les monômes.

Définition 1.3.8. Un ordre monomial admissible sur $k[x_1, \ldots, x_n]$ est une relation d'ordre total sur l'ensemble des monômes de cet anneau noté $<$ et vérifiant :
- pour tout monôme m de $k[x_1, \ldots, x_n]$ on a $1 < m$;
- si m_1, m_2, m_3 sont trois monômes de $k[x_1, \ldots, x_n]$ tels que $m_1 < m_2$ alors $m_1 m_3 < m_2 m_3$.

Il existe plusieurs ordres admissibles pour $k[x_1, \ldots, x_n]$. Celui que nous utiliserons dans cette thèse est défini comme suit.

Définition 1.3.9. L'ordre *lexicographique* sur $k[x_1, \ldots, x_n]$ noté $<$ est défini par : $x_1^{\alpha_1} \ldots x_n^{\alpha_n} < x_1^{\beta_1} \ldots x_n^{\beta_n}$ si le premier terme (le plus à gauche) non nul dans $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ est négatif.

Dans cette thèse, l'anneau $k[x_1, \ldots, x_n]$ sera muni par défaut de cet ordre. Maintenant que l'ordre est fixé sur $k[x_1, \ldots, x_n]$ nous pouvons définir le plus grand terme d'un polynôme f, noté $HT(f)$, ainsi que la généralisation de la division euclidienne sur $k[x_1, \ldots, x_n]$.

Définition 1.3.10. Soit f et $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$. Une *forme normale* de f modulo l'ensemble $B = \{f_1, \ldots, f_s\}$ est un polynôme g de $k[x_1, \ldots, x_n]$ tel qu'il existe un s-uplet $(a_1, \ldots, a_s)$ d'éléments de $k[x_1, \ldots, x_n]$ tel que

$$f = a_1 f_1 + \ldots + a_s f_s + g$$

où aucun des termes de tête des f_i ne divise un terme de g. Cette forme normale est notée $\mathrm{NF}(f, B)$.

Nous pouvons à présent donner la définition d'une base de Gröbner.

Définition 1.3.11. Un ensemble fini S d'éléments d'un idéal I de $k[x_1, \ldots, x_n]$ est une *base de Gröbner* (pour un ordre donné) si S vérifie

$$\langle HT(g) \,:\, g \in S \rangle = \langle HT(g) \,:\, g \in I \rangle \,.$$

Nous dirons de S que c'est une *base de Gröbner réduite* s'il vérifie également :
- Pour tout $g \in S$, le terme de tête $HT(g)$ est un monôme ;
- pour tout $g \in S$, $g = \mathrm{NF}(g, S \setminus \{g\})$.

Le théorème suivant récapitule les deux résultats centraux sur les bases de Gröbner, dont une preuve est donnée dans [15] par exemple.

Théorème 1.3.12. *Supposons qu'un ordre admissible pour $k[x_1, \ldots, x_n]$ soit fixé. Soit I un idéal de $k[x_1, \ldots, x_n]$. Nous avons*
- *L'idéal I possède au moins une base de Gröbner et une* unique *qui soit réduite.*
- *Un ensemble fini S de I est une base de Gröbner si et seulement si l'assertion suivante est vérifiée*

$$\forall f \in k[x_1, \ldots, x_n],\ f \in I \Leftrightarrow \mathrm{NF}(f, S) = 0 \,.$$

D'après ce théorème, il devient naturel de parler de *la* base de Gröbner de I pour distinguer la base de Gröbner réduite de cet idéal (une fois qu'un ordre est fixé).

Il existe plusieurs algorithmes permettant le calcul d'une base de Gröbner d'un idéal à partir d'un de ses ensembles de générateurs. Dans notre cadre spécifique d'idéaux de dimension zéro de $k[x_1, \ldots, x_n]$, Faugère, Gianni, Lazard et Mora montrent dans [38] que le calcul d'une base de Gröbner est polynomial en d^n, où d est le degré maximal des polynômes engendrant I. L'algorithme F5 de Jean-Charles Faugère (voir [37]) est celui dont l'implantation est la plus efficace à ce jour. Pourtant, il n'est pas démontré que F5 est de complexité polynomiale en d^n (voir [104] au sujet des dernières avancées concernant la complexité de F5). Dans le paragraphe suivant, nous allons étudier un type particulier de base de Gröbner.

1.3.3 Variétés équiprojectables et ensembles triangulaires

Comme nous l'avons dit plus haut, nous allons nous intéresser à des idéaux de dimension zéro. Lorsque $k[x_1, \ldots, x_n]$ est muni de l'ordre lexicographique, la base de Gröbner d'un tel idéal est toujours de la forme triangulaire générale suivante

$$\begin{aligned}
f_n(x_1, \ldots, x_n) \\
f_{n-1}(x_1, \ldots, x_n) \\
\vdots \\
f_m(x_1, \ldots, x_n) \\
f_{m-1}(x_1, \ldots, x_{n-1}) \\
\vdots \\
f_q(x_1, \ldots, x_{n-1}) \\
f_{q-1}(x_1, \ldots, x_{n-2}) \\
\vdots \\
f_1(x_1)
\end{aligned}$$

Ici, nous allons nous intéresser à des ensembles de forme plus spécifique, c'est-à-dire aux ensembles triangulaires au sens de D. Lazard (voir [71]). Pour les ensembles triangulaires plus généraux on pourra consulter les travaux de Aubry, Kalkbrener, Lazard, Moreno Maza (voir [11, 54, 55, 12, 13].)

Définition 1.3.13. Soit $T = \{f_1, \ldots, f_n\}$ un ensemble de n polynômes de $k[x_1, \ldots, x_n]$. L'ensemble T sera dit *triangulaire* s'il vérifie :

$$f_i \quad = \quad x_i^{d_i} + g_i(x_1, \ldots, x_i)$$

où $d_i > 0$ et $\deg_{x_i}(g_i) < d_i$ pour tout $i \in [\![1, n]\!]$. De plus il sera dit *séparable* si l'idéal $\langle T \rangle$ est radical.

Remarque 1.3.14. Comme les termes de tête des éléments d'un ensemble triangulaire sont des monômes deux à deux premiers entre eux, cet ensemble est une base de Gröbner (voir [30, Chap. 2 §9 Proposition 4]).

Définition 1.3.15. Un idéal I de $k[x_1, \ldots, x_n]$ est dit triangulaire s'il est engendré par un ensemble triangulaire.

Nous allons mettre en relation un certain type de variétés avec les idéaux triangulaires.

Définition 1.3.16. Soit L un sous ensemble fini de $\overline{k}^n$. Pour $i \in [\![1, n]\!]$, notons L_i le sous-ensemble de $\overline{k}^i$ égal à la projection de L sur les i premières coordonnées et π_i la projection de L sur L_i. Pour $i \in [\![1, n]\!]$, l'ensemble L est dit *équiprojectable sur* L_i s'il existe un entier c tel que pour tout point M dans L_i nous avons $\mathrm{Card}(\pi_i^{-1}(M)) = c$. Plus généralement L sera dit *équiprojectable* si L est équiprojectable sur L_i pour $i \in [\![1, n]\!]$.

Un exemple très important d'ensemble équiprojectable est donné par le lemme suivant.

Lemme 1.3.17. *([11, Proposition 6.5.3]) Soit G un sous-groupe de S_n et $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ un n-uplet de valeurs différentes de $\overline{k}$. L'ensemble*

$$\{\sigma.\underline{\alpha} = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \,:\, \sigma \in G\}$$

est équiprojectable.

Le théorème suivant met en relation les ensembles équiprojectables et les ensembles triangulaires.

Théorème 1.3.18. *Soit V une k-variété séparable de dimension zéro. Les deux conditions suivantes sont équivalentes :*
- *V est équiprojectable ;*
- *il existe un ensemble $T = \{f_1, \ldots, f_n\}$ de $k[x_1, \ldots, x_n]$ triangulaire et séparable tel que $Id_k(V) = \langle T \rangle$.*

De plus, nous avons $c_i(V_{i+1}) = \deg_{x_{i+1}}(f_{i+1})$ et $c_i(V) = \prod_{j=i+1}^{n} \deg_{x_j}(f_j)$.

Démonstration. Une démonstration est donnée dans [14] dans le cas où k est supposé parfait, mais comme ici tous les éléments de V sont supposés séparables, cette preuve peut être reprise *mutatis mutandis.* □

Calcul modulo un ensemble triangulaire

Soit $T = \{f_1, \ldots, f_n\}$ un ensemble triangulaire séparable de $k[x_1, \ldots, x_n]$ tel que le polynôme f_i est de degré d_i. Le calcul dans l'algèbre $k[x_1, \ldots, x_n]/\langle T \rangle$ peut être vu comme le calcul dans une tour d'extensions simples.

Notations 1.3.19. Soit D un anneau (commutatif). Notons $\mathsf{M}(d)$ le nombre d'opérations dans D nécessaires pour multiplier deux polynômes à coefficients dans D et de degré d.

Proposition 1.3.20. *([110, Corollary 9.7]) Soit D un anneau (commutatif) et f un polynôme unitaire de degré d à coefficients dans D. Alors une multiplication dans $D[x]/\langle f \rangle$ peut être réalisée en utilisant au plus $6\mathsf{M}(d) + O(d)$ opérations dans D.*

À partir de la proposition 1.3.20 on peut évaluer la complexité du calcul dans le quotient $k[x_1, \ldots, x_n]/\langle T \rangle$.

Notations 1.3.21. La complexité, en terme d'opérations arithmétiques dans k, d'une multiplication dans $k[x_1, \ldots, x_n]/\langle T \rangle$ est notée $\mathcal{M}(d_1, d_2, \ldots, d_n)$.

Proposition 1.3.22. *La complexité $\mathcal{M}(d_1, d_2, \ldots, d_n)$ est majorée par*

$$O(6^n \prod_{i=1}^{n} M(d_i)) .$$

Démonstration. Découle de la proposition 1.3.20, voir aussi [94, 69, 70]. □

Remarque 1.3.23. Lorsque les opérations sont répétés dans $k[x_1, \ldots, x_n]/\langle T \rangle$, on peut stocker une fois pour toutes les premières étapes de calcul. Dans ce cas, la constantes 6 intervenant dans la complexité de la proposition 1.3.22 passe à 3 (voir [110, Page 258]).

Ainsi, la complexité du calcul d'une forme normale d'un polynôme modulo un ensemble triangulaire dépend de la complexité donnée dans la proposition 1.3.22, mais aussi de la taille du polynôme lui même (nombre de termes et de facteurs).

Chapitre 2

Idéaux de Galois

2.1 Introduction

Dans ce chapitre, nous présentons les définitions et résultats sur les *idéaux de Galois*.

Étant donné un polynôme séparable f de degré n et à coefficients dans un corps k, les idéaux de Galois de f sont les idéaux de $k[x_1, \ldots, x_n]$ qui s'annulent sur un ensemble de permutations des racines (distinctes) de f. À un idéal de Galois de f sont associés des ensembles de permutations de S_n appelés *injecteurs*. Les idéaux de Galois ont été introduits par A. Valibouze dans [106] en généralisant les notions classiques d'idéal des relations et d'idéal des relations symétriques. Dans cet article, A. Valibouze utilise ces objets dans le but de fournir des moyens mathématiques à l'établissement de l'algorithme `GaloisIdéal`. Cet algorithme prend en entrée un idéal de Galois de f et un de ses injecteurs et renvoie un idéal des relations $\mathcal{M}$ de f ainsi que la représentation symétrique du groupe de Galois de f correspondant à $\mathcal{M}$.

Dans la première section de ce chapitre, nous donnons les définitions et résultats généraux sur les idéaux de Galois associés à un polynôme séparable et sur les injecteurs de tels idéaux. Ces résultats sont à la fois des rappels des articles [106, 14] mais aussi de nouveaux résultats qui étendent les propriétés de ces objets. Ces nouveaux résultats sont issus d'un travail réalisé en collaboration avec S. Orange et A. Valibouze exposés dans [87, 84] et que nous avons choisi d'étendre ici au cas où le corps de base k n'est pas supposé parfait.

Dans la deuxième section de ce chapitre, nous présentons le lien entre les ensembles triangulaires et les idéaux de Galois. Cette partie est une généralisation au cas d'un corps non parfait des résultats de [14].

Dans la troisième section de ce chapitre, nous présentons l'algorithme `GaloisIdéal` de A. Valibouze (voir [106]). Nous rappellerons les résultats mathématiques nécessaires à l'établissement de cet algorithme.

Dans la quatrième section, nous nous intéressons plus particulièrement au cas où le polynôme f est séparable et réductible. Ce travail est issu d'une collaboration avec S. Orange et A. Valibouze et est exposé dans [87]. Nous montrons comment, à partir de la donnée de facteurs $f_1, \ldots, f_k$ de f et d'un idéal de Galois pour chacun de ces polynômes f_i, on peut construire un idéal de Galois I de f. De plus, nous montrons comment obtenir un injecteur de I à partir d'un injecteur de chacun des idéaux de Galois des f_i. L'utilisation de l'idéal I et d'un de ses injecteurs comme entrée de l'algorithme `GaloisIdéal` permet alors d'améliorer l'efficacité de ce dernier dans le cas où le

polynôme f est réductible.

Dans tout ce chapitre, on suppose le corps k infini, on note $\overline{k}$ une clôture algébrique de k et on fixe K une extension algébrique finie de k contenue dans $\overline{k}$.

2.2 Définitions et résultats généraux

Dans cette section, nous donnons la définition des idéaux de Galois et des injecteurs de ces idéaux. Ces notions furent introduites par A. Valibouze dans [106] en généralisant la définition d'idéal des relations et des relations symétriques (voir [100] par exemple). Nous donnons aussi des résultats généraux sur ces objets. Ces résultats sont à la fois des rappels des articles [106] et [14], et des nouveaux repris des articles [84] et [87].

Dans toute la suite, nous considérons un polynôme f séparable de degré n et à coefficients dans le corps k. Nous notons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ un n-uplet des racines de f dans $\overline{k}^n$ numérotées à l'aide d'une application $\mathcal{N}$, c'est-à-dire $\mathcal{N}(\alpha_i) = i$.

2.2.1 Idéaux de Galois

Définition 2.2.1. Soit L un sous-ensemble de S_n contenant l'identité et $\underline{\alpha}$ un n-uplet de racines (distinctes) d'un polynôme séparable de degré n. L'idéal $Id_K(L.\underline{\alpha})$ de l'anneau $K[x_1, ..., x_n]$ formé des polynômes s'annulant sur l'ensemble de $\overline{k}^n$ donné par

$$L.\underline{\alpha} = \{(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}) \mid \sigma \in L\}$$

est appelé un *idéal de Galois*. Si l'on veut préciser que cet idéal s'annule sur les racines de f, il sera appelé *idéal de Galois de* f et si l'on veut préciser le n-uplet exact des racines de f (c'est-à-dire la numérotation choisie) sur lequel il s'annule, il sera appelé $\underline{\alpha}$-*idéal de Galois* (sur K).

Pour commencer, nous étudions les deux types d'idéaux de Galois qui ont servi de base à l'élaboration de cette théorie.

Idéaux des relations et des relations symétriques

L'idéal $Id_K(\underline{\alpha})$ est un $\underline{\alpha}$-idéal de Galois appelé *idéal des* $\underline{\alpha}$*-relations*. Cet idéal est maximal et permet de représenter le corps de décomposition (sur K) de f. En effet, nous avons le morphisme surjectif suivant

$$\begin{aligned} K[x_1, \ldots, x_n] &\longrightarrow K(\underline{\alpha}) && (2.1)\\ x_i &\longmapsto \mathcal{N}^{-1}(i) = \alpha_i && (2.2) \end{aligned}$$

qui a pour noyau l'idéal des polynômes de $K[x_1, \ldots, x_n]$ s'annulant en $\underline{\alpha}$, c'est-à-dire l'idéal $Id_K(\underline{\alpha})$. Clairement, cet idéal maximal contient tous les $\underline{\alpha}$-idéaux de Galois et en particulier celui que nous allons étudier maintenant.

L'idéal $Id_K(S_n.\underline{\alpha})$ est un $\underline{\alpha}$-idéal de Galois appelé *idéal des relations symétriques* de f. Remarquons que l'idéal ne dépend plus du choix de la numérotation $\mathcal{N}$ mais uniquement de f. En effet, quelque soit la numérotation choisie, la variété associée à cet idéal contiendra, par définition, le n-uplet des racines ainsi numérotées. Cet idéal est engendré par un système triangulaire dont les éléments sont appelés les *modules de Cauchy* de f. Plus précisément nous avons la proposition suivante qui est la traduction moderne d'un résultat dû à Cauchy (voir [26]).

Définition-Proposition 2.2.2. *([90]) Soit les n polynômes $f_1, \ldots, f_n$ de $k[x_1, \ldots, x_n]$ définis par la récurrence :*

$$f_1(x_1) = f(x_1)\,,$$

et $\forall i \in [\![2, n]\!]$

$$f_i(x_i, x_{i-1}, \ldots, x_1) = \frac{f_{i-1}(x_i, x_{i-2}, \ldots, x_1) - f_{i-1}(x_{i-1}, x_{i-2}, \ldots, x_1)}{x_i - x_{i-1}}\,.$$

Alors ces polynômes sont appelés les modules de Cauchy de f et forment un système triangulaire (voir Définition 1.3.15) et donc une base de Gröbner (voir Remarque 1.3.14) de l'idéal des relations symétriques de f.

Exemple 2.2.3. Ici nous avons $k = K = \mathbb{F}_2(t)$. Le polynôme $f = x^4 + tx^3 + x + t + 1$ de $\mathbb{F}_2(t)[x]$ est irréductible et séparable, on peut aisément le vérifier en Magma :

```
> K<t>:=FunctionField(GaloisField(2));
> PR1<x>:=PolynomialRing(K);
> f:=x^4 + t*x^3 + x + t + 1;
>
> // On vérifie que f est séparable
> // Pour ce faire on calcule le PGCD de f et de sa dérivée formelle
> Gcd(f,Derivative(f));
> 1
> // Comme il est différent de 0, f est séparable
> // Reste à tester son irréductibilité.
> // Pour ce faire, on utilise la fonction interne de Magma:
> IsIrreducible(f);
true
```

Les modules de Cauchy de f sont aussi très facilement calculés :

```
> PR4<x4,x3,x2,x1>:=PolynomialRing(K,4);
>
> f1:=Evaluate(f,x1);
> f2:=(f1 - Evaluate(f,x2)) div (x1 - x2);
> f3:=(f2 - Evaluate(f2,x2,x3)) div (x2 - x3);
> f4:=(f3 - Evaluate(f3,x3,x4)) div (x4 - x3);
>
> f1;
x1^4 + t*x1^3 + x1 + t + 1
> f2;
x2^3 + x2^2*x1 + t*x2^2 + x2*x1^2 + t*x2*x1 +
   x1^3 + t*x1^2 + 1
> f3;
x3^2 + x3*x2 + x3*x1 + t*x3 + x2^2 + x2*x1 +
   t*x2 + x1^2 + t*x1
> f4;
x4 + x3 + x2 + x1 + t
```

Ainsi l'idéal

$$\begin{aligned}\langle\, & x_4 + x_3 + x_2 + x_1 + t,\\ & x_3^2 + x_3x_2 + x_3x_1 + tx_3 + x_2^2 + x_2x_1 + tx_2 + x_1^2 + tx_1,\\ & x_2^3 + x_2^2x_1 + tx_2^2 + x_2x_1^2 + tx_2x_1 + x_1^3 + tx_1^2 + 1,\\ & x_1^4 + tx_1^3 + x_1 + t + 1\,\rangle\end{aligned}$$

est l'idéal des relations symétriques de f et on vérifie immédiatement que c'est aussi son idéal des relations puisqu'il est maximal.

```
> I:=ideal<PR4 | f1,f2,f3,f4>;
> IsMaximal(I);
true
```

Étudions maintenant les propriétés des idéaux de Galois généraux.

Propriétés des idéaux de Galois

Les idéaux de Galois sont radicaux par définition et, plus précisément, ils vérifient le critère de radicalité suivant :

Proposition 2.2.4. *Si I est un idéal de Galois de f (donc de dimension 0) de $K[x_1, \ldots, x_n]$, alors il vérifie le critère de radicalité de Seidenberg :*

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

Démonstration. Clairement, si un idéal I de $K[x_1, \ldots, x_n]$ contient un idéal J de dimension zéro vérifiant le critère de Seidenberg, il en va de même pour I. Un idéal de Galois I de f contient l'idéal des relations symétriques S de f qui vérifie le critère de Seidenberg. En effet, l'idéal S est de dimension zéro et il contient, pour tout entier i dans $[\![1, n]\!]$, le polynôme $f(x_i)$ qui est séparable par hypothèse. Ainsi, l'idéal de Galois I vérifie le critère de Seidenberg et nous avons le résultat. □

La proposition suivante donne une caractérisation des idéaux de Galois.

Proposition 2.2.5. *Un idéal propre de $K[x_1, \ldots, x_n]$ est un idéal de Galois de f si et seulement si il contient les modules de Cauchy de f.*

Démonstration. Si un idéal propre I de $K[x_1, \ldots, x_n]$ contient les modules de Cauchy de f alors il vérifie le critère de Seidenberg et est radical (voir Proposition 2.2.4) et il contient $Id_K(S_n.\underline{\alpha})$. Sa variété est alors incluse dans la variété $S_n.\underline{\alpha}$. Il existe donc un sous-ensemble L du groupe symétrique S_n tel que $V(I) = L.\underline{\alpha}$, et nous avons $I = Id_K(V(I)) = Id_K(L.\underline{\alpha})$. La réciproque découle de la définition des idéaux de Galois. □

Il s'ensuit naturellement le corollaire suivant :

Corollaire 2.2.6. *Soient K_1, K_2 deux extensions algébriques de k telles que $K_1 \subset K_2$. Si I (respectivement J) est un idéal de Galois de f dans $K_1[x_1, \ldots, x_n]$ (respectivement $K_2[x_1, \ldots, x_n]$) alors*

1. *l'idéal $K_2 \otimes_{K_1} I$ obtenu par extension des scalaires ;*
2. *et l'idéal trace de J dans $K_1[x_1, \ldots, x_n]$ donné par $K_1[x_1, \ldots, x_n] \cap J$*

sont des idéaux de Galois de f.

Nous allons maintenant étudier les ensembles de permutations qui définissent les idéaux de Galois.

2.2.2 Injecteurs et groupe de décomposition

Définition 2.2.7. Soient I et J deux idéaux de $K[x_1, x_2, \ldots, x_n]$, l'*injecteur* de I dans J, noté $\mathrm{Inj}(I, J)$, est le sous-ensemble des permutations σ de S_n vérifiant $\sigma.I \subset J$.
L'*injecteur de I relatif à $\underline{\alpha}$* est l'injecteur $\mathrm{Inj}(I, Id_K(\underline{\alpha}))$, noté $\mathrm{Inj}(I, \underline{\alpha})$.

Jusqu'à la fin de ce chapitre nous fixons I un $\underline{\alpha}$-idéal de Galois de f sur K. Sa variété $V(I)$ est donnée par (voir [106]) :

$$V(I) = \{\sigma.\underline{\alpha} \mid \sigma \in \mathrm{Inj}(I, \underline{\alpha})\} = \mathrm{Inj}(I, \underline{\alpha}).\underline{\alpha} \tag{2.3}$$

et, comme le polynôme f est séparable, nous avons

$$\mathrm{Card}(\mathrm{Inj}(I, \underline{\alpha})) = \mathrm{Card}(V(I)). \tag{2.4}$$

Remarque 2.2.8. L'identité (2.3) fait apparaître que l'idéal I est entièrement déterminé par un n-uplet de $\overline{k}^n$ sur lequel il s'annule et par l'injecteur de I relatif à ce n-uplet. Ainsi, l'injecteur $\mathrm{Inj}(I, \underline{\alpha})$ est de nature géométrique. En effet, pour toute extension algébrique K' de K, nous avons :

$$\mathrm{Inj}(I, Id_K(\underline{\alpha})) = \mathrm{Inj}(K' \otimes_K I, Id_{K'}(\underline{\alpha}))$$

qui s'écrit plus simplement

$$\mathrm{Inj}(I, Id_K(\underline{\alpha})) = \mathrm{Inj}(K' \otimes_K I, \underline{\alpha})\,. \tag{2.5}$$

Un injecteur peut être un groupe, c'est en particulier le cas de l'injecteur d'un idéal dans lui même.

Définition 2.2.9. Soit I un idéal de Galois de f. Le groupe de permutations laissant stable I, c'est-à-dire

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

est appelé *groupe de décomposition* de I et est noté $\mathrm{Dec}(I)$.

Nous avons le résultat bien connu suivant.

Proposition 2.2.10. *Soit I l'idéal des $\underline{\alpha}$-relations sur K. Alors, le groupe de décomposition* $\mathrm{Dec}(I)$ *est égal à la représentation symétrique G du groupe de Galois du corps de décomposition de f sur K selon la numérotation $\mathcal{N}$.*

Démonstration. Notons ρ l'application qui représente le groupe de Galois de K_f en le sous-groupe G de S_n (voir Chapitre 1) et Ψ l'isomorphisme entre $K[x_1, \ldots, x_n]/I$ et $K(\underline{\alpha})$ (voir 2.1).
Montrons que $G \subset \mathrm{Dec}(I)$. Soit $\sigma \in G$; nous avons pour tout polynôme P de I :

$$\begin{aligned}(\sigma.P)(\underline{\alpha}) &= P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})(\underline{\alpha}) \\ &= P(\sigma.\underline{\alpha}) \\ &= P(\rho^{-1}(\sigma)(\alpha_1), \ldots, \rho^{-1}(\sigma)(\alpha_n))\,.\end{aligned}$$

Comme $\rho^{-1}(\sigma)$ est un K-automorphisme et que P est à coefficients dans K nous obtenons finalement

$$\begin{aligned}(\sigma.P)(\underline{\alpha}) &= \rho^{-1}(\sigma)(P(\underline{\alpha})) \\ &= \rho^{-1}(\sigma)(0) \\ &= 0\end{aligned}$$

et donc $\sigma.P$ est dans I.
Inversement, montrons que $\mathrm{Dec}(I) \subset G$. Soit $\sigma \in \mathrm{Dec}(I)$ et ϕ_σ l'automorphisme de la K-algèbre $K[x_1, \ldots, x_n]$ défini par $\phi_\sigma(x_i) = x_{\sigma(i)}$. Comme $\sigma.I = I$, l'automorphisme passe au quotient et on obtient un K-automorphisme $\overline{\phi}_\sigma$ du corps $K[x_1, \ldots, x_n]/I$ défini par $\overline{\phi}_\sigma(x_i + I) = \phi_\sigma(x_i) + I$. Par transport par Ψ, on obtient un K-automorphisme du corps $K(\underline{\alpha})$ donné par $\omega = \Psi\overline{\phi}_\sigma\Psi^{-1}$ et vérifiant $\omega(\alpha_i) = \alpha_{\sigma(i)}$. Ainsi, σ est un élément de G. □

Définition 2.2.11. Soit I l'idéal des $\underline{\alpha}$-relations sur K. Le groupe $\mathrm{Dec}(I)$ est appelé groupe de Galois de $\underline{\alpha}$ et est noté $\mathrm{Gal}_K(\underline{\alpha})$.

Notations 2.2.12. L'image inverse d'une permutation τ de $\mathrm{Gal}_K(\underline{\alpha})$ par la représentation symétrique ρ du groupe des K-automorphismes de $K(\underline{\alpha})$ selon la numérotation $\mathcal{N}$ sera notée $\overline{\tau} = \rho^{-1}(\tau)$. L'action de $Aut_K(K(\underline{\alpha}))$ sur $K(\underline{\alpha})$ est étendue naturellement à $K(\underline{\alpha})[x_1, \ldots, x_n]$ par action sur les coefficients des polynômes.

Remarque 2.2.13. Pour tout $\tau \in \mathrm{Gal}_K(\underline{\alpha})$ et tout $g \in K(\underline{\alpha})[x_1, \ldots, x_n]$, nous avons donc deux notations distinctes :

- $\overline{\tau}(g)$ désignant le polynôme obtenu par l'action de τ sur les coefficients de g et
- $\tau.g$ désignant le polynôme $g(x_{\tau(1)}, \ldots, x_{\tau(n)})$.

Le lemme suivant nous donne une propriété de translation, selon un K-automorphisme, pour les injecteurs.

Lemme 2.2.14. *Pour tout idéal J de $K(\underline{\alpha})[x_1, \ldots, x_n]$ et tout $\tau \in Gal_K(\underline{\alpha})$, nous avons l'identité suivante :*

$$\mathrm{Inj}(\overline{\tau}(J), \underline{\alpha}) = \tau\,\mathrm{Inj}(J, \underline{\alpha})\ . \tag{2.6}$$

Démonstration. Pour V un sous-ensemble de $S_n.\underline{\alpha}$, montrons que :

$$\overline{\tau}(Id_{K(\underline{\alpha})}(V)) = Id_{K(\underline{\alpha})}(\tau.V)\ . \tag{2.7}$$

Avec les notations de l'énoncé, nous avons les égalités successives :

$$\begin{aligned}Id_{K(\underline{\alpha})}(\tau.V) &= \bigcap_{\underline{\beta}\in V} \langle x_1 - \beta_{\tau(1)}, \ldots, x_n - \beta_{\tau(n)}\rangle_{K(\underline{\alpha})[x_1,\ldots,x_n]} \\ &= \bigcap_{\underline{\beta}\in V} \langle \overline{\tau}(x_1 - \beta_1), \ldots, \overline{\tau}(x_n - \beta_n)\rangle_{K(\underline{\alpha})[x_1,\ldots,x_n]} \\ &= \bigcap_{\underline{\beta}\in V} \overline{\tau}(\langle x_1 - \beta_1, \ldots, x_n - \beta_n\rangle_{\overline{\tau}^{-1}(K(\underline{\alpha})[x_1,\ldots,x_n])}) \\ &= \overline{\tau}(\bigcap_{\underline{\beta}\in V} \langle x_1 - \beta_1, \ldots, x_n - \beta_n\rangle_{K(\underline{\alpha})[x_1,\ldots,x_n]}) \\ &= \overline{\tau}(Id_{K(\underline{\alpha})}(V))\end{aligned}$$

où l'avant dernière égalité est obtenue car $\overline{\tau}$ est K-automorphisme de l'algèbre

$$K(\underline{\alpha})[x_1, \ldots, x_n]\,.$$

Montrons maintenant que :

$$\mathrm{Inj}(\overline{\tau}(J), Id_{K(\underline{\alpha})}(\underline{\alpha})) \;=\; \mathrm{Inj}(J, \overline{\tau}^{-1}(\mathcal{I}_{K(\underline{\alpha})}(\underline{\alpha}))\,. \tag{2.8}$$

Nous avons les égalités suivantes :

$$\begin{aligned}
\mathrm{Inj}(\overline{\tau}(J), Id_{K(\underline{\alpha})}(\underline{\alpha})) &= \{\sigma \in S_n \mid \forall P \in \overline{\tau}(J),\ \sigma.P \in Id_{K(\underline{\alpha})}(\underline{\alpha})\} \\
&= \{\sigma \in S_n \mid \forall P \in J,\ \sigma.\overline{\tau}(P) \in Id_{K(\underline{\alpha})}(\underline{\alpha})\} \\
&= \{\sigma \in S_n \mid \forall P \in J,\ \overline{\tau}(\sigma.P) \in Id_{K(\underline{\alpha})}(\underline{\alpha})\} \\
&= \{\sigma \in S_n \mid \forall P \in J,\ \sigma.J \in \overline{\tau}^{-1}(Id_{K(\underline{\alpha})}(\underline{\alpha}))\},
\end{aligned}$$

d'où l'égalité 2.7. Pour terminer, les égalités successives suivantes prouvent l'identité (2.6) :

$$\begin{aligned}
\mathrm{Inj}(\overline{\tau}(J), Id_{K(\underline{\alpha})}(\underline{\alpha})) &= \mathrm{Inj}(J, \overline{\tau}^{-1}(Id_{K(\underline{\alpha})}(\underline{\alpha}))), \text{ d'après l'identité (2.8) ,} \\
&= \mathrm{Inj}(J, Id_{K(\underline{\alpha})}(\tau^{-1}.\underline{\alpha})), \text{ d'après l'identité (2.7),} \\
&= \tau\,\mathrm{Inj}(J, Id_{K(\underline{\alpha})}(\underline{\alpha})), \text{ d'après la proposition 2.2.18.}
\end{aligned}$$

□

La proposition suivante permet, sous certaines conditions, de déterminer un injecteur de l'idéal I.

Proposition 2.2.15. *(voir [106]) Nous avons* $\mathrm{Gal}_K(\underline{\alpha}) \subset \mathrm{Inj}(I, \underline{\alpha})$. *Si L est une partie de S_n tel que $I = Id_K(L.\underline{\alpha})$ alors*

$$\mathrm{Inj}(I, \underline{\alpha}) = \mathrm{Gal}_K(\underline{\alpha})L\,.$$

De cette proposition découle le résultat immédiat suivant.

Corollaire 2.2.16. *Soit I l'idéal des $\underline{\alpha}$-relations. Alors $V(I) = \mathrm{Gal}_K(\underline{\alpha}).\underline{\alpha}$, en d'autres termes, les injecteurs de I se réduisent tous à* $\mathrm{Dec}(I)$.

Soit I un idéal de Galois de f. Pour tout $\underline{\beta}$ dans $V(I)$, l'idéal I est un $\underline{\beta}$-idéal de Galois. Ainsi, I est contenu dans les idéaux maximaux $Id_K(\underline{\beta})$ où $\underline{\beta}$ parcourt $V(I)$. Il existe alors un entier e et des permutations $\tau_1, \ldots, \tau_e$ tel que I se décompose en intersection d'idéaux comaximaux :

$$I = \bigcap_{i=1}^{e} Id_K(\tau_i.\underline{\alpha}) \tag{2.9}$$

(rappelons que $\underline{\alpha}$ est un n-uplet des racines de f).

Nous en déduisons une décomposition, sous la forme de réunions deux à deux disjointes, de l'injecteur de I relatif à $\underline{\alpha}$ sous la forme d'une réunion disjointe : :

$$\mathrm{Inj}(I, \underline{\alpha}) \;=\; \sum_{i=1}^{e} \mathrm{Gal}_K(\underline{\alpha})\tau_i\,. \tag{2.10}$$

Ainsi les τ_i peuvent être vus comme une *transversale généralisée* à droite de l'ensemble $\mathrm{Inj}(I, \underline{\alpha})$ modulo le groupe $\mathrm{Gal}_K(\underline{\alpha})$.

La proposition qui suit permet de caractériser les parties de S_n pouvant être des injecteurs de I.

Proposition 2.2.17. *Soit E une partie de S_n. Les deux assertions suivantes sont équivalentes :*

1. *Il existe $\underline{\beta} \in V(I)$ tel que $E \subset \mathrm{Inj}(I, \underline{\beta})$.*
2. *L'idéal $\langle I \cup E.I \rangle_{K[x_1,\ldots,x_n]}$ est un idéal de Galois de f.*

Démonstration. D'après la proposition 2.2.5, l'idéal J de $K[x_1, \ldots, x_n]$ engendré par $I \cup E.I$ est un idéal de Galois si et seulement si il est un idéal propre de $K[x_1, \ldots, x_n]$. Soit $\underline{\alpha} \in V(I)$. De l'égalité 2.9 : $I = \cap_{\underline{\beta} \in V(I)} Id_k(\underline{\beta})$, nous déduisons que

$$\begin{array}{rll} J \neq K[x_1, \ldots, x_n] & \text{ssi} & \displaystyle\bigcap_{\underline{\beta} \in V(I)} \langle Id_K(\underline{\beta}) \cup E.I \rangle_{K[x_1,\ldots,x_n]} \neq K[x_1, \ldots, x_n] \\ & \text{ssi} & \exists \underline{\beta} \in V(I),\ \langle Id_K(\underline{\beta}) \cup E.I \rangle_{K[x_1,\ldots,x_n]} \neq K[x_1, \ldots, x_n] \\ & \text{ssi} & \exists \underline{\beta} \in V(I),\ E.I \subset Id_K(\underline{\beta}) \end{array}$$

car $Id_K(\underline{\beta})$ est maximal. Par définition de l'injecteur, cette dernière assertion est équivalente à l'assertion 1 de la proposition, ce qui termine la démonstration. □

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

Proposition 2.2.18. *Si $\sigma \in \mathrm{Inj}(I, \underline{\alpha})$ alors*

$$\mathrm{Inj}(I, \sigma.\underline{\alpha}) = \sigma^{-1} \mathrm{Inj}(I, \underline{\alpha}) \ .$$

Démonstration. Puisque $\sigma \in \mathrm{Inj}(I, \underline{\alpha})$, nous avons bien $\sigma.\underline{\alpha} \in V(I)$ et, par définition de l'injecteur, il vient :

$$\begin{array}{rcl} \mathrm{Inj}(I, \sigma.\underline{\alpha}) & = & \{\tau \in S_n \,|\, \forall R \in I, (\tau.R)(\sigma.\underline{\alpha}) = 0\} \\ & = & \{\tau \in S_n \,|\, \forall R \in I, (\sigma\tau.R)(\underline{\alpha}) = 0\} \ . \end{array}$$

En posant $\rho = \sigma\tau$, nous obtenons le résultat :

$$\mathrm{Inj}(I, \sigma.\underline{\alpha}) = \sigma^{-1}\{\rho \in S_n \,|\, \rho.I \subset Id_K(\underline{\alpha})\} = \sigma^{-1} \mathrm{Inj}(I, \underline{\alpha}) \ . \qquad \square$$

La proposition 2.2.18 généralise le corollaire 2.2.16 en montrant que si un injecteur de I est un groupe alors tous les injecteurs de I coïncident avec son groupe de décomposition. En fait, nous avons la proposition suivante :

Proposition 2.2.19. *Le groupe de décomposition est l'intersection de tous les injecteurs de l'idéal de Galois I :*

$$\mathrm{Dec}(I) = \bigcap_{i=1}^{e} \mathrm{Inj}(I, Id_K(\tau_i.\underline{\alpha})) \ .$$

Démonstration. L'égalité 2.9 nous donne :

$$\begin{aligned}\mathrm{Dec}(I) &= \{\sigma \in S_n | \sigma.I \subset \cap_{i=1}^{e} Id_K(\tau_i.\underline{\alpha})\} \\ &= \cap_{i=1}^{e} \{\sigma \in S_n | \sigma.I \subset Id_K(\tau_i.\underline{\alpha})\} \\ &= \cap_{i=1}^{e} \mathrm{Inj}(I, Id_K(\tau_i.\underline{\alpha}))\end{aligned}$$

□

Proposition 2.2.20. *([106, Proposition 3.6]) Soit H un sous-groupe de S_n. Le groupe de décomposition de l'idéal $Id_K(H.\underline{\alpha})$ contient H.*

Nous allons voir maintenant que certaines propriétés des injecteurs permettent d'avoir des informations sur la structure des idéaux de Galois correspondants.

2.2.3 Idéaux de Galois et triangularité

Définition 2.2.21. Un idéal de Galois I est dit *pur* si tous ses injecteurs sont égaux à son groupe de décomposition.

Proposition 2.2.22. *([14] dans le cas où K est parfait) Si I est un idéal de Galois pur alors I est un idéal triangulaire.*

Démonstration. Découle du théorème 1.3.18. □

Définition 2.2.23. Soit I un idéal engendré par un ensemble triangulaire séparable $\{f_1, \ldots, f_n\}$. Le n-uplet $\mathcal{L}(I)$ défini par

$$\mathcal{L}(I) = (\deg_{x_1}(f_1), \ldots, \deg_{x_n}(f_n))$$

est appelé *liste des degrés initiaux* de I. Nous noterons $\deg_{x_i}(I)$ le $i^{\text{ème}}$ élément de la liste $\mathcal{L}(I)$.

Lorsque I est un idéal de Galois pur, la liste $\mathcal{L}(I)$ ne dépend que de $\mathrm{Dec}(I)$ et se calcule facilement. Nous nous interessons à ce point maintenant.

Notations 2.2.24. Soit G un sous-groupe de S_n. Pour $i \in [\![0, n]\!]$, nous noterons :

$$\begin{aligned}G_0 &= G \\ G_i &= \mathrm{Stab}_G([1, \ldots, i]), \text{ pour } i \in [\![1, n]\!]\end{aligned}$$

Définition 2.2.25. Soit G un sous-groupe de S_n. Le n-uplet $\mathcal{L}(G)$ est défini par :

$$\mathcal{L}(G) = (|G_0|/|G_1|, \ldots, |G_{n-1}|/|G_n|)$$

Le résultat qui suit permet de lier $\mathcal{L}(G)$ à tout idéal de Galois pur de groupe de décomposition G.

Proposition 2.2.26. *([14]) Soit I un idéal de Galois pur de groupe de décomposition G. Alors, nous avons l'égalité*

$$\mathcal{L}(I) = \mathcal{L}(G)\,.$$

Dès que l'idéal I est triangulaire, nous pouvons calculer le cardinal des injecteurs de I par la formule suivante :

$$\mathrm{Card}(V(I)) = \prod_{i=1}^{n} deg_{x_i}(I) = \mathrm{Card}(\mathrm{Inj}(I, \underline{\alpha})). \tag{2.11}$$

Nous verrons, au chapitre 5, des exemples d'idéaux de Galois triangulaires ayant un injecteur différent de son groupe de décomposition. Notons néanmoins que tous les idéaux de Galois ne sont pas triangulaires comme le montre l'exemple ci-dessous :

Exemple 2.2.27. Soit le polynôme $x^4 - x^3 - 3x^2 + x + 1 \in \mathbb{Q}[x]$ de groupe de Galois D_4. Les deux idéaux triangulaires qui suivent sont deux de ses trois idéaux des relations :

$$\begin{aligned}
I_1 &= \langle\, x_4 + x_3 + x_1^3 - x_1^2 - 2x_1, \\
&\quad\ x_3^2 + x_3x_1^3 - x_3x_1^2 - 2x_3x_1 - 1, \\
&\quad\ x_2 - x_1^3 + x_1^2 + 3x_1 - 1, \\
&\quad\ x_1^4 - x_1^3 - 3x_1^2 + x_1 + 1 \,\rangle \\
I_2 &= \langle\, x_4 + x_2 + x_1^3 - x_1^2 - 2x_1, \\
&\quad\ x_3 - x_1^3 + x_1^2 + 3x_1 - 1, \\
&\quad\ x_2^2 + x_2x_1^3 - x_2x_1^2 - 2x_2x_1 - 1, \\
&\quad\ x_1^4 - x_1^3 - 3x_1^2 + x_1 + 1 \,\rangle
\end{aligned}$$

En effet, on peut facilement vérifier que ces deux idéaux vérifient la proposition 2.2.5 et qu'ils sont maximaux. En MAGMA nous avons :

```
> K:=Rationals();
> PR1<x>:=PolynomialRing(K);
> f:=x^4 - x^3 - 3*x^2 + x + 1;
>
> PR4<x4,x3,x2,x1>:=PolynomialRing(K,4);
> //Modules de Cauchy
> f1:=Evaluate(f,x1);
> f2:=(f1 - Evaluate(f,x2)) div (x1 - x2);
> f3:=(f2 - Evaluate(f2,x2,x3)) div (x2 - x3);
> f4:=(f3 - Evaluate(f3,x3,x4)) div (x4 - x3);
> //Idéal des relations symétriques
> IdSym:=ideal<PR4 | f1,f2,f3,f4>;
>
> //Ideaux des relations ?
> I1:=ideal< PR4 |
>         x4 + x3 + x1^3 - x1^2 - 2*x1,
>         x3^2 + x3*x1^3 - x3*x1^2 - 2*x3*x1 - 1,
>         x2 - x1^3 + x1^2 + 3*x1 - 1,
>         x1^4 - x1^3 - 3*x1^2 + x1 + 1
> >;
> I2:=ideal<PR4 |
>         x4 + x2 + x1^3 - x1^2 - 2*x1,
>         x3 - x1^3 + x1^2 + 3*x1 - 1,
>         x2^2 + x2*x1^3 - x2*x1^2 - 2*x2*x1 - 1,
>         x1^4 - x1^3 - 3*x1^2 + x1 + 1
> >;
```

```
>
> // On vérifie que ces deux idéaux sont maximaux
> IsMaximal(I1);
true
> IsMaximal(I2);
true
>
> // On vérifie que ces deux idéaux contiennent l'idéal
> // des relations symétriques.
> // L'opérateur booléen subset permet de faire
> // un tel test :
> IdSym subset I1;
true
> IdSym subset I2;
true
```

L'idéal $I = I_1 \cap I_2$ est alors un idéal de Galois de f et un calcul immédiat d'une base de Gröbner réduite pour l'ordre lexicographique $x_1 < x_2 < x_3 < x_4$, à l'aide de `FGb` (voir [40]) ou de MAGMA,

```
> I:=I1 meet I2;
> GroebnerBasis(I);
[
   x4 + x3 + x2 + x1 - 1,
   x3^2 + x3*x1^3 - x3*x1^2 - 2*x3*x1 + x2^2 + x2*x1^3 -
     x2*x1^2 - 2*x2*x1 - x1^3 + 3*x1^2 + x1 - 7,
   x3*x2 - x3*x1^3 + x3*x1^2 + 3*x3*x1 - x3 - x2*x1^3 +
     x2*x1^2 + 3*x2*x1 - x2 + x1^3 - 2*x1^2 - 2*x1 + 4,
   x2^3 + x2^2*x1 - x2^2 + x2*x1^2 - x2*x1 - 3*x2 + x1^3 -
     x1^2 - 3*x1 + 1,
   x1^4 - x1^3 - 3*x1^2 + x1 + 1
]
```

montre que I est engendré par l'ensemble non triangulaire suivant :

$$\begin{aligned}\{\quad & x_4 + x_3 + x_2 + x_1 - 1,\\ & x_3^2 + x_3x_1^3 - x_3x_1^2 - 2x_3x_1 + x_2^2 + x_2x_1^3 -\\ & \quad x_2x_1^2 - 2x_2x_1 - x_1^3 + 3x_1^2 + x_1 - 7,\\ & x_3x_2 - x_3x_1^3 + x_3x_1^2 + 3x_3x_1 - x_3 - x_2x_1^3 +\\ & \quad x_2x_1^2 + 3x_2x_1 - x_2 + x_1^3 - 2x_1^2 - 2x_1 + 4,\\ & x_2^3 + x_2^2x_1 - x_2^2 + x_2x_1^2 - x_2x_1 - 3x_2 + x_1^3 -\\ & \quad x_1^2 - 3x_1 + 1,\\ & x_1^4 - x_1^3 - 3x_1^2 + x_1 + 1\}\end{aligned}$$

La proposition suivante donne des conditions équivalentes pour qu'un injecteur $\mathrm{Inj}(I, \underline{\alpha})$ soit un groupe ainsi qu'un test effectif.

Proposition 2.2.28. *([106]) Les assertions suivantes sont équivalentes :*

1. $\mathrm{Dec}(I) = \mathrm{Inj}(I, \underline{\alpha})$,
2. $\mathrm{Gal}_K(\underline{\alpha}) \subset \mathrm{Dec}(I)$,

3. $\mathrm{Card}(\mathrm{Dec}(I)) = \prod_{i=1}^{n} deg_{x_i}(I)$,
4. *les injecteurs de I relatifs aux éléments de $V(I)$ sont égaux.*

Il est important de pouvoir tester si $\mathrm{Dec}(I)$ est l'injecteur de I (c'est-à-dire que I est de Galois pur) car le groupe de décomposition est rapidement calculable à partir de I (voir Chapitre 3) alors que le calcul de $\mathrm{Inj}(I, \underline{\alpha})$ nécessite, a priori, la connaissance de $Id_K(\underline{\alpha})$.

2.2.4 Utilisation pratique du n-uplet $\mathcal{L}(G)$

Soit I un $\underline{\alpha}$-idéal de Galois supposé engendré par l'ensemble triangulaire $\mathcal{T}_I = \{f_1(x_1) = f(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ formé de n polynômes de $K[x_1, \ldots, x_n]$. Supposons connu le groupe de décomposition G d'un $\underline{\alpha}$-idéal de Galois pur J contenant I. Dans ce qui suit, nous allons voir comment déduire de $\mathcal{T}_I$ certains générateurs d'un ensemble triangulaire $\mathcal{T}_J$ engendrant J.

Le n-uplet $\mathcal{L}(J) = (d_1, d_2, \ldots, d_n)$ s'identifie à la liste $\mathcal{L}(G)$ (voir Proposition 2.2.26) et nous avons :

$$d_i \leq \mathcal{L}(I)_i \quad \text{pour } i \in [\![1, n]\!].$$

Où $\mathcal{L}(I)_i$ est le i-ème élément de $\mathcal{L}(I)$. La comparaison des listes $\mathcal{L}(I)$ et $\mathcal{L}(G)$ donne alors le résultat suivant :

1. $d_i = \mathcal{L}(I)_i$ si et seulement si on peut choisir le i-ème polynôme de l'ensemble $\mathcal{T}_I$ pour être le i-ème polynôme de l'ensemble $\mathcal{T}_J$;
2. si $d_i < \mathcal{L}(I)_i$ alors on peut prendre pour i-ème polynôme de l'ensemble $\mathcal{T}_J$ un facteur de degré d_i dans $K(\underline{\alpha})$ du i-ème polynôme de l'ensemble $\mathcal{T}_I$ (après avoir remplacés les α_j par x_j pour $j < i$). Ce facteur n'est pas irréductible sur $k(\underline{\alpha})$ si $d_i > 1$.

Pour calculer les polynômes manquants de l'ensemble $\mathcal{T}_J$, il est possible d'employer les factorisations dans les extensions algébriques ou l'algorithme `GaloisIdéal` (que nous allons étudier dans le paragraphe suivant). Quel que soit l'algorithme choisi pour le calcul de $\mathcal{T}_J$ à partir de $\mathcal{T}_I$, les informations ci-dessus pourront être utilisées pour accélérer le calcul.

2.3 L'algorithme `GaloisIdéal`

Dans cette section, nous présentons l'algorithme `GaloisIdéal` de A. Valibouze (voir [106]). Cet algorithme permet le calcul d'une base triangulaire d'un idéal des relations de f à partir d'un idéal de Galois I de f, ou plus exactement à partir d'une base de Gröbner de I et d'un de ses injecteurs.

Dans un premier temps, nous allons considérer le cas où l'idéal de Galois I est pur. Ainsi tous ses injecteurs sont identiques à son groupe de décomposition que nous noterons L. De plus, nous supposons que L contient le groupe $\mathrm{Gal}_K(\underline{\alpha})$ et donc I est un $\underline{\alpha}$-idéal de Galois.

Définition 2.3.1. Soit Θ un polynôme de $K[x_1, \ldots, x_n]$. La *résolvante L-relative de $\underline{\alpha}$ selon Θ* (voir [9, 99]) est le polynôme, en T défini par :

$$\mathcal{L}_{\Theta}^{L.\underline{\alpha}} = \prod_{o \in L.\Theta} (T - o(\underline{\alpha}))\,. \tag{2.1}$$

Si le groupe L est le groupe symétrique S_n, le polynôme $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ est appelé la *résolvante absolue de f selon Θ*. Dans ce cas, ce polynôme ne dépend pas du choix de la numérotation des racines de f.

Définition 2.3.2. Soient H et L deux sous-groupes de S_n tels que $H \subset L$. Un polynôme Θ de $K[x_1, \ldots, x_n]$ est un *H-invariant L-primitif* si

$$H = \mathrm{Stab}_L(\Theta)\,.$$

De plus, il sera dit *$\underline{\alpha}$-séparable* si $\Theta(\underline{\alpha})$ est une racine simple de la résolvante L-relative de $\underline{\alpha}$ selon Θ.

Remarque 2.3.3. Le terme *primitif* vient du fait qu'un polynôme Θ qui est H-invariant L-primitif est un élément primitif de l'extension $K(x_1, \ldots, x_n)^H$ de $K(x_1, \ldots, x_n)^L$.

Le calcul d'un invariant primitif est toujours possible (voir [49] et [2]). Par contre, un tel invariant primitif ne sera pas forcément $\underline{\alpha}$-séparable. Lorsque le corps de base K est infini (ce qui est le cas ici), on peut toujours en calculer un qui le soit. Pour ce faire, il suffit d'appliquer une transformation de Tschirnhaus convenable (voir [103]). Plus précisément, si l'on note $\Theta \in k[x_1, \ldots, x_n]$ un invariant primitif et t un polynôme en une variable la transformation de Tschirnhaus selon t est donnée par

$$\Theta(t(x_1), \ldots, t(x_n))\,. \tag{2.2}$$

Une telle transformation fournit un nouvel invariant primitif. A. Colin donne dans [28, Proposition 8.5] une borne sur le nombre de transformations à réaliser avant d'en trouver une qui fournisse un invariant primitif $\underline{\alpha}$-séparable (voir aussi [48]).

Le théorème qui suit permet de construire un idéal de Galois J de f à partir de l'idéal I. Cet idéal J contient alors l'idéal I et est contenu dans un idéal des relations de f. Ainsi, en itérant le procédé, on obtiendra un idéal des relations.

Théorème 2.3.4. *([106]) Soit H un sous-groupe de L et Θ un H-invariant L-primitif $\underline{\alpha}$-séparable. Alors, le polynôme minimal de $\Theta(\underline{\alpha})$ sur K noté F est un facteur irréductible de la résolvante $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ et vérifie*

$$Id_K(H.\underline{\alpha}) = Id_K(L.\underline{\alpha}) + \langle F(\Theta) \rangle\,.$$

La proposition suivante permet de faire le même genre de construction mais sous des hypothèses moins contraignantes.

Proposition 2.3.5. *([106]) Soit L et H deux sous-groupes de S_n tels que $\mathrm{Gal}_K(\underline{\alpha}) \subset L$ et $\mathrm{Gal}_K(\underline{\alpha})H$ est un groupe. Soit Θ un H-invariant L-primitif et $\theta = \Theta(\underline{\alpha})$. Soit F le polynôme minimal de θ sur K. Si θ est une racine simple de $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ alors*

$$Id_K(H.\underline{\alpha}) = Id_K(L.\underline{\alpha}) + \langle F(\Theta) \rangle\,.$$

Dans le théorème 2.3.4, si l'on désire construire un idéal J qui contient strictement I, le choix du sous-groupe H ne doit pas se faire au hasard. Par exemple, nous avons le résultat suivant déjà utilisé par Stauduhar (voir [99]) pour calculer le groupe de Galois d'un polynôme.

Proposition 2.3.6. *(voir [9]) Soit H un sous-groupe de L et Θ un H-invariant L-primitif. Si l'on note $\theta = \Theta(\underline{\alpha})$ alors on a les deux assertions :*

1. *Si $\mathrm{Gal}_K(\underline{\alpha}) \in H$ alors θ est un élément de K.*
2. *Si θ est un élément de K et est une racine simple de la résolvante $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ alors $\mathrm{Gal}_K(\underline{\alpha})$ est contenu dans un conjugué dans L de H.*

De ces résultats nous déduisons le corollaire suivant.

Corollaire 2.3.7. *Soit H un sous-groupe de L et Θ un H-invariant L-primitif. Supposons $\mathrm{Gal}_K(\underline{\alpha}) \subset L$. Nous avons les deux assertions suivantes :*

- *Si la résolvante $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ n'a pas de racine dans K alors $\mathrm{Gal}_K(\underline{\alpha})$ n'est pas un sous-groupe de H.*
- *Si la résolvante $\mathcal{L}_\Theta^{L.\underline{\alpha}}$ a un facteur simple linéaire $x - a$ alors $\mathrm{Gal}_K(\underline{\alpha})$ est contenu dans un conjugué de H dans L. De plus, l'idéal*

$$Id_K(L.\underline{\alpha}) + \langle \Theta - a \rangle$$

est un idéal de Galois pur d'injecteur H.

Plus généralement, c'est l'étude des résolvantes en utilisant les *tables de partitions* ou *tables de groupes* (voir [105] et [9]) qui fournit la première méthode déterministe pour le calcul du groupe de Galois d'un polynôme.

La dernière chose qu'il nous reste à voir est le calcul d'une résolvante relative. Si l'on connaît un système triangulaire engendrant l'idéal I, il sera toujours possible de calculer une $\underline{\alpha}$-résolvante L-relative pour tout élément $\underline{\alpha}$ de $V(I)$. Ce calcul se fera à l'aide de calculs de résultants (voir [14], [73] par exemple).

En appliquant tous ces résultats, on en déduit l'algorithme 1 qui représente une étape d'une version allégée (ici nous n'utilisons pas toute la puissance des *tables de groupes*) de l'algorithme `GaloisIdéal` (voir [106] pour la version étendue).

Ainsi, en utilisant de manière itérative l'algorithme 1 on construit, à partir d'un idéal de Galois de f et d'une liste de groupes contenant $\mathrm{Gal}_K(f)$, une chaîne croissante d'idéaux de Galois allant jusqu'à un idéal des relations $\mathcal{M}$ de f :

$$I \subset \ldots I_k \subset I_{k+1} \subset \ldots \subset \mathcal{M}\,.$$

Plus généralement, on peut aussi commencer cette chaîne avec un idéal de Galois qui n'est pas pur. Dans ce cas on peut appliquer les résultats introduits dans [107].

2.4 Idéaux de Galois de polynômes réductibles

Dans ce paragraphe, f sera supposé séparable et **réductible**. À partir d'idéaux de Galois de chacun des facteurs de f, nous pouvons déduire un idéal de Galois I de f contenant l'idéal des relations symétriques entre les racines de f. Un injecteur et une base de Gröbner de l'idéal I étant connu, l'algorithme `GaloisIdéal` pourra être utilisé pour calculer l'idéal des $\underline{\alpha}$-relations.

Supposons, pour simplifier l'exposé, que le polynôme f se factorise sur K en deux polynômes g et h de degrés respectifs m et $p = n - m$. Supposons le n-uplet $\underline{\alpha}$ des racines de f ordonné de telle sorte que $\underline{\beta} = (\alpha_1, \ldots, \alpha_m)$ soit un m-uplet des racines de

Algorithme 1 GaloisIdéalUneÉtape($\mathcal{T}$,L,$GrpTest$)

Hypothèse : $\mathcal{T}$ est un ensemble triangulaire engendrant un idéal de Galois I de f d'injecteur le groupe L. L'ensemble $GrpTest$ contient des classes de L-conjugaison de sous-groupes de L. Le groupe de Galois de f est soit L soit l'un des groupes (à conjugaison près) de $GrpTest$

Sortie : $\mathcal{S}$ est un ensemble triangulaire engendrant un idéal de Galois J de f contenant I. Le groupe H est l'injecteur de l'idéal J. L'ensemble $GrpTest$ contient des sous-groupes de H qui sont susceptibles d'être le groupe de Galois de f (à H-conjugaison près). L'idéal J est un idéal des relations de f ssi $GrpTest$ est vide.

$Boucle := True$
while $Boucle$ **do**
  Soit H un représentant d'un élément $\mathcal{C}$ de $GrpTest$.
  $GrpTest := GrpTest \setminus \mathcal{C}$.
  Soit Θ un H-invariant L-primitif.
  Soit R la résolvante $\mathcal{L}_{\Theta}^{L,\underline{\alpha}}$
  if Le polynôme R possède une racine dans K **then**
    On applique des transformations de Tchirnhaus à Θ jusqu'à trouver une résolvante qui est séparable ou au moins possède un facteur linéaire simple.
    if R possède un facteur linéaire simple $x - a$ **then**
      Soit $\mathcal{S}$ la base triangulaire de $\langle \mathcal{T} \cup \{\Theta - a\} \rangle$ obtenue après un calcul de base de Gröbner.
      $Boucle := False$
    end if
  end if
  if L'ensemble $GrpTest$ est vide **then**
    $\mathcal{S} := \mathcal{T}$.
    $H := L$.
    $Boucle = False$
  end if
end while
$GrpTest :=$ l'ensemble des sous-groupes de H contenus dans $GrpTest$.
Return $\mathcal{S}$, H, $GrpTest$

g et que $\underline{\gamma} = (\alpha_{m+1}, \ldots, \alpha_n)$ soit un p-uplet des racines de h. Posons $\mathcal{B} = K[x_1, \ldots, x_m]$ et $\mathcal{C} = K[x_{m+1}, \ldots, x_n]$ et munissons les anneaux $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ de l'ordre lexicographique induit par $x_1 < x_2 < \ldots < x_m < x_{m+1} < \ldots < x_n$. Dans cette partie, les bases de Gröbner considérées le seront toujours relativement à cet ordre et pour tout idéal construit à partir d'une variété, nous spécifierons l'anneau dans lequel il sera considéré. Par exemple, pour une variété V de $\overline{K}^m$ l'idéal de $\mathcal{B}$ des polynômes s'annulant sur V sera noté $Id_{\mathcal{B}}(V)$. Nous avons le résultat bien connu suivant :

Lemme 2.4.1. $\mathrm{Gal}_K(\underline{\alpha}) \subset \mathrm{Gal}_K(\underline{\beta}) \times \mathrm{Gal}_K(\underline{\gamma})$.

Nous démontrons le résultat plus général suivant :

Théorème 2.4.2. *Soient G une partie de S_m et H une partie de S_p. Si G (resp. H) est l'injecteur de l'idéal $Id_{\mathcal{B}}(G.\underline{\beta})$ (resp. $Id_{\mathcal{C}}(H.\underline{\gamma})$) relativement à $\underline{\beta}$ (resp. $\underline{\gamma}$) alors l'$\underline{\alpha}$-idéal de Galois $Id_{\mathcal{A}}((G \times H).\underline{\alpha})$ possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$ et il vérifie :*

$$Id_{\mathcal{A}}((G \times H).\underline{\alpha}) \;=\; Id_{\mathcal{B}}(G.\underline{\beta})\,\mathcal{A} + Id_{\mathcal{C}}(H.\underline{\gamma})\,\mathcal{A}\,. \tag{2.1}$$

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

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

Puisque G (resp. H) est l'injecteur de I_1 (resp. I_2) relatif à $\underline{\beta}$ (resp. $\underline{\gamma}$), nous avons, d'après (2.3),

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

Nous avons donc les deux variétés

$$\begin{aligned} V(I_1\mathcal{A}) &= \{(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}, u_1, \ldots, u_p) \;\mid\; \sigma \in G,\ u_i \in \overline{k}\} \\ V(I_2\mathcal{A}) &= \{(v_1, \ldots, v_m, \alpha_{\tau(m+1)}, \ldots, \alpha_{\tau(n)}) \;\mid\; \tau \in H,\ v_i \in \overline{k}\}\,. \end{aligned}$$

Ainsi,

$$V(J) = V(I_1\mathcal{A} + I_2\mathcal{A}) = V(I_1\mathcal{A}) \cap V(I_2\mathcal{A}) = (G \times H).\underline{\alpha}\,. \tag{2.2}$$

Le radical de l'idéal J est donc l'idéal de Galois $Id_{\mathcal{A}}((G \times H).\underline{\alpha})$ qui, d'après les identités (2.3) et (2.2), possède $G \times H$ comme injecteur relatif à $\underline{\alpha}$. Il reste donc à démontrer que l'idéal J, de dimension 0, est radical. Pour ce faire, nous allons montrer qu'il vérifie le critère de radicalité de Seidenberg (voir, par exemple, Lemma 8.13 dans [15]).
D'après la proposition 2.2.4, les idéaux de Galois I_1 et I_2 vérifient le critère de Seidenberg dans, respectivement, $\mathcal{B}$ et $\mathcal{C}$. Ainsi, pour tout entier i dans $[\![1, m]\!]$ (resp. $[\![m+1, n]\!]$), il existe un polynôme séparable $g_i(x_i)$ dans I_1 (resp. I_2) et donc dans J. Ainsi, l'idéal J vérifie le critère de Seidenberg.

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

$$\mathrm{Dim}(\mathcal{B}/I_1) = \mathrm{Card}(V(I_1)) = \mathrm{Card}(\{\underline{x}^{\underline{a}} \in \mathcal{B} \,|\, \underline{a} \notin \mathrm{In}(\mathcal{G}_1) + \mathbb{N}^m\})\,, \tag{2.3}$$

où $\underline{x}^{\underline{a}} = x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}$ et $\mathrm{In}(\mathcal{G}_1)$ est l'ensemble des exposants des monômes initiaux (pour l'ordre lexicographique) de $\mathcal{G}_1$. Il en va de même pour I_2 et de toute base de Gröbner de J.
De plus, d'après l'égalité (2.4), nous avons $\mathrm{Card}(G) = \mathrm{Card}(V(I_1))$, de même pour I_2 et H, ainsi que pour J et $G \times H$. D'après l'égalité (2.3), il vient alors :

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

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

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

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

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

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

À partir de cet idéal I, pourra être construit un idéal des relations $\mathcal{M}$ de f contenant I.

Remarque 2.4.3. Nous avons les remarques suivantes à faire sur le théorème 2.4.2.

- Par induction, le théorème 2.4.2 se généralise au cas où f se factorise en plus de deux facteurs.
- Lorsque $\mathcal{G}_1$ et $\mathcal{G}_2$ sont des ensembles triangulaires, l'union $\mathcal{G}_1 \cup \mathcal{G}_2$ l'est également car les monômes initiaux sont premiers deux à deux ; elle constitue donc une base de Gröbner de l'idéal J.
- Le théorème 2.4.2 généralise le résultat de Colin qui établit l'identité (2.1) lorsque $G = \mathrm{Gal}_K(\underline{\beta})$, $H = \mathrm{Gal}_K(\underline{\gamma})$ et $G \times H = \mathrm{Gal}_K(\underline{\alpha})$ (voir [28]). De même il généralise le théorème 5.2 de [90] qui donne une base triangulaire pour l'idéal des relations symétriques d'un polynôme réductible séparable.

Nous présentons maintenant quelques exemples.

2.4.1 Exemples

Les polynômes des exemples ci-après ont été pris dans la base de données de J. Klüners et G. Malle disponible sur internet (voir [59]).

Le lemme suivant est utilisé dans les exemples de ce paragraphe. Rappelons que les hypothèses faites sur le n-uplet $\underline{\alpha}$ nous donnent :

Lemme 2.4.4. *Si g et h sont irréductibles sur K alors les $\mathrm{Gal}_K(\underline{\alpha})$-orbites de $\{1, \dots, n\}$ sont $\{1, 2, \dots, m\}$ et $\{m+1, m+2, \dots, n\}$.*

Pour la suite, posons $k = K = \mathbb{Q}$, $m = 5$ et $p = 2$.

Exemple 2.4.5. Soient les polynômes $g = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$, $h = x^2 + 1$ irréductibles (sur $\mathbb{Q}$) et $f = g.h$. Calculons un ensemble triangulaire engendrant un idéal des relations de g.
Le logiciel MAGMAnous donne facilement la factorisation du discriminant de g

```
> Factorization(Integers()!Discriminant(g));
[ <11, 4> ]
```

qui est donc le carré 121^2. Ainsi, le groupe de Galois de g est pair. À une conjugaison près, le groupe de Galois de g est soit le groupe alterné A_5, soit le groupe dihédral D_5, soit le groupe cyclique C_5. Nous avons les inclusions

$$A_5 \supset D_5 \supset C_5 \,.$$

Nous utilisons l'algorithme `GaloisIdéal` pour discriminer ces groupes et calculer un idéal des relations de g. Les représentants que nous choisissons pour les groupes D_5 et C_5 sont tels que $D_5 \supset C_5$:

$$D_5 = \langle (1,3,2,4,5), (4,2)(3,5) \rangle$$

$$C_5 = \langle (1,3,2,4,5) \rangle \,.$$

Le calcul d'une base triangulaire de l'idéal des relations symétriques de g est immédiat

```
> PR1<x>:=PolynomialRing(Rationals());
> PR5<x5,x4,x3,x2,x1>:=PolynomialRing(Rationals(),5);
> g:=x^5 - x^4 - 4*x^3 + 3*x^2 + 3*x - 1;
> f1:=Evaluate(g,x1);
> f2:=(f1 - Evaluate(g,x2)) div (x1 - x2);
> f3:=(f2 - Evaluate(f2,x2,x3)) div (x2 - x3);
> f4:=(f3 - Evaluate(f3,x3,x4)) div (x4 - x3);
> f5:=(f4 - Evaluate(f4,x4,x5)) div (x5 - x4);
> //Ideal des relations symetriques
> IdSym:=ideal<PR5 | f1,f2,f3,f4,f5>;
```

Commençons par tester si le groupe de Galois est contenu dans D_5. Le polynôme suivant est un D_5-invariant S_5-primitif

$$\Theta = x_5x_4 + x_5x_1 + x_4x_2 + x_3x_2 + x_3x_1 \,.$$

À partir de cet invariant et des modules de Cauchy de g nous calculons (voir [73, 14]) la résolvante absolue selon Θ.

$$(x+2)^2(x^5 + 10x^4 + 7x^3 - 118x^2 - 74x + 131)(x^5 + 10x^4 + 7x^3 - 118x^2 - 74x + 373)^2$$

qui ne possède aucune racine simple dans k. Nous ne pouvons pas appliquer la proposition 2.3.6 et devons changer d'invariant. Appliquons alors la transformation de Tchirnhaus

$$\Theta = \Theta(x_1^3 - 2, \ldots, x_5^3 - 2) \,.$$

Cette fois, la résolvante calculée à l'aide de cet invariant est séparable :

$$(x-5)(x+28)(x^5+41x^4-575x^3-18377x^2+62668x+1802503)(x^5+74x^4+943x^3-29762x^2-600698x-2672869).$$

Nous savons alors que le groupe de Galois de g est contenu dans D_5, il reste donc à discriminer D_5 de C_5. En appliquant le théorème 2.3.4, nous calculons une base triangulaire d'un idéal de Galois de g d'injecteur le groupe D_5.

```
> IdD5:=ideal<PR5 | Basis(IdSym),Theta - 5>;
> GroebnerBasis(IdD5);
[
   x5 + x2*x1^4 - 4*x2*x1^2 - x2*x1 + 2*x2 - 1,
   x4 + x2 - x1^4 + x1^3 + 4*x1^2 - 2*x1 - 3,
   x3 - x2*x1^4 + 4*x2*x1^2 + x2*x1 - 2*x2 + x1^4 -
      x1^3 - 4*x1^2 + 3*x1 + 3,
   x2^2 - x2*x1^4 + x2*x1^3 + 4*x2*x1^2 - 2*x2*x1 -
      3*x2 + x1^4 - x1^3 - 4*x1^2 + 3*x1 + 2,
   x1^5 - x1^4 - 4*x1^3 + 3*x1^2 + 3*x1 - 1
]
```

Le polynôme suivant

$$\Theta = x_5^2x_4 + x_5x_1^2 + x_4^2x_2 + x_3^2x_1 + x_3x_2^2$$

est un C_5-invariant D_5-primitif. Grâce à Θ et à la base triangulaire de `IdD5`, nous pouvons calculer la C_5-résolvante D_5-relative selon Θ

$$(x-4)^2$$

qui n'est pas séparable. Si l'on applique la transformation

$$\Theta = \Theta(x_1^3-3,\ldots,x_5^3-3)\,.$$

la résolvante est cette fois séparable

$$(x+176)(x+209)\,.$$

Ainsi, le groupe de Galois de g est C_5 et nous pouvons calculer une base triangulaire d'un de ses idéaux des relations.

```
> IdC5:=ideal<PR5 | Basis(IdD5),Theta + 209>;
> GroebnerBasis(IdC5);
[
    x5 + x1^4 - 4*x1^2 + 2,
    x4 - x1^4 + x1^3 + 3*x1^2 - 2*x1 - 1,
    x3 - x1^3 + 3*x1,
    x2 + x1^2 - 2,
    x1^5 - x1^4 - 4*x1^3 + 3*x1^2 + 3*x1 - 1
]
```

Ainsi, l'ensemble

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

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

Comme le groupe $C_5 \times S_2$ n'a pas de sous-groupe propre dont l'action sur $\{1, 2, \ldots, 7\}$ ait une orbite de longueur 5(=Deg(g)) et une de longueur 2(=Deg(h)), nous avons nécessairement $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) = C_5 \times S_2$ (voir Lemmes 2.4.1 et 2.4.4). D'après le théorème 2.4.2, appliqué à $G = C_5$ et $H = S_2$, l'idéal I de $\mathcal{A}$ engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois d'injecteur $C_5 \times S_2$. Comme $C_5 \times S_2$ est le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$, l'idéal I est celui des $\underline{\alpha}$-relations $\mathcal{M}$.

Exemple 2.4.6. Soient les polynômes irréductibles (sur $\mathbb{Q}$) $g = x^5 - 2x^4 + 2x^3 - x^2 + 1$, $h = x^2 + 1$ et $f = g.h$. De même manière que dans l'exemple précédent, nous calculons l'ensemble triangulaire

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

qui engendre l'idéal I_1 des $\underline{\beta}$-relations d'injecteur le groupe dihédral

$$D_5 = \langle \sigma = (1,5,2,3,4), \tau = (1,3)(2,5) \rangle$$

et $T_2 = \{x_6^2 + 1, x_7 + x_6\}$ engendre l'idéal I_2 des $\underline{\gamma}$-relations d'injecteur le groupe S_2.

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

L'idéal I engendré par $T_1 \cup T_2$ est l'$\underline{\alpha}$-idéal de Galois d'injecteur $D_5 \times S_2$ (voir Théorème 2.4.2). Montrons comment, à partir de I, l'algorithme `GaloisIdéal` calcule l'idéal des $\underline{\alpha}$-relations. Le polynôme Θ donné ci-dessous vérifie $G_2 = \{\sigma \in G_1 \mid \sigma.\Theta = \Theta\}$:

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

Nous avons $G_1 = G_2 + \tau G_2$; le polynôme $R = (x - \Theta(\underline{\alpha}))(x - \tau.\Theta(\underline{\alpha}))$ est une *résolvante G_1-relative de $\underline{\alpha}$ selon* Θ. Si cette résolvante possède un facteur linéaire simple sur $\mathbb{Q}$

alors le groupe de Galois de $\underline{\alpha}$ sur k est contenu dans G_2 (voir Proposition 2.3.6) ; il s'agit donc de G_2. L'ensemble triangulaire $T_1 \cup T_2$ qui engendre l'idéal I est utilisé pour calculer cette résolvante (voir [73, 14]) :

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

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

Chapitre 3

Calcul du groupe de décomposition d'un idéal triangulaire

3.1 Introduction

Ce chapitre est une nouvelle rédaction des résultats publiés dans [3], article réalisé en collaboration avec I. Abdeljaoued-Tej, S. Orange et A. Valibouze. Ici, nous avons choisi d'exposer les résultats sur les algorithmes de *branch-and-cut* d'un point de vue plus général et nous ne supposons plus le corps k parfait.

Dans le chapitre 2, nous avons vu qu'à un idéal de Galois I peut être associé un unique groupe appelé groupe de décomposition de I et noté $\mathrm{Dec}(I)$.

Dans ce chapitre, nous généralisons la définition du groupe de décomposition à un idéal I de $k[x_1, \ldots, x_n]$. En effet, l'action naturelle du groupe S_n sur l'anneau $k[x_1, \ldots, x_n]$ permet de définir le groupe $\mathrm{Dec}(I)$ des permutations de S_n qui laissent globalement invariant l'idéal I. Nous donnons un algorithme Al pour le calcul de $\mathrm{Dec}(I)$ dans le cas où l'idéal I est triangulaire. Cet algorithme est basé sur la méthode classique de *branch-and-cut* (voir [24]) qui renvoie un *ensemble fort de générateurs* (voir [96]). Sa complexité, en toute généralité, est exponentielle en le nombre n de variables.

Dans le cas particulier d'un idéal des relations d'un polynôme séparable f de degré n, Anai, Noro et Yokoyama donnent dans [7] un algorithme calculant son groupe de décomposition. Dans ce cas, ce groupe est une représentation symétrique du groupe de Galois de f et ils montrent que la complexité de leur algorithme est de l'ordre de $O(n^4)$ formes normales modulo I calculées. Ce résultat de complexité était le dernier connu.

Dans ce même cas particulier, nous montrons que notre algorithme a pour complexité $O(n^3)$, en terme de nombre de formes normales modulo l'idéal I calculées. Plus précisément, nous montrons que l'algorithme Al permet, après modification de sa condition d'arrêt, le calcul du prédicat *« l'idéal triangulaire I est-il un idéal de Galois pur ? »*. Un des sous-produits de ce calcul de prédicat, lorsque la réponse est positive, est le groupe de décomposition de l'idéal I et nous montrons que l'obtention de cette réponse nécessite au plus $O(n^3)$ formes normales modulo I calculées. Pour ce faire, nous avons montré une généralisation de [7, Theorem 5] au cas des idéaux de Galois.

Ainsi, notre algorithme est plus général et de meilleur complexité que celui présenté dans [7]. Enfin, nous établirons une liste de tests permettant de comparer l'efficacité de ces deux algorithmes sur des exemples concrets d'idéaux des relations.

3.2 Algorithmes de *branch-and-cut*

Dans cette section, nous retraçons les différentes stratégies pour l'utilisation d'algorithmes de *branch-and-cut* sur les arbres et nous nous intéressons à leur complexité. Pour évaluer la complexité, nous allons compter deux types d'opérations :

Définition 3.2.1. Nous appelons *calcul de prédicat* un calcul permettant de déterminer si une étiquette d'un arbre vérifie une certaine propriété. Les *opérations de base* sont les autres calculs apparaissant dans les algorithmes (calcul de l'image d'un entier par une permutation et l'accès aux cases d'un tableau (ce qui est équivalent ici), les opérations arithmétiques sur les entiers, etc).

Ces algorithmes sont dits de *branch-and-cut* ou *backtrack* (voir [24] et [95] par exemple) et leurs applications dans le cadre de la théorie algorithmique des groupes permettent de résoudre des problèmes du type : *Étant donnée une propriété $\mathcal{P}$ sur S_n, trouver l'ensemble G des éléments de S_n qui vérifient $\mathcal{P}$.*

Pour tout ce chapitre, on se fixe une telle propriété $\mathcal{P}$ dont nous préciserons la nature au fur et à mesure de la lecture.

Les arbres $\mathcal{A}$ et $\mathcal{A}'$

Comme nous l'avons dit plus haut, les algorithmes de *branch-and-cut* sont définis sur des arbres. C'est pourquoi l'ensemble des permutations de S_n sera représenté sous cette forme. Soit $\mathcal{A}$ l'arbre de profondeur $n+1$ défini de la manière suivante : la racine est de niveau 0 et les feuilles de niveau n. Seuls les nœuds de niveau $i \geqslant 1$ ont une étiquette contenant un entier de $[\![1, n]\!]$, la racine a une étiquette égale à 0. Une branche correspond à une permutation de S_n, plus précisément nous avons :
Une permutation σ de S_n est représentée par la branche dont la valeur de l'étiquette de niveau i, pour $i \in [\![1, n]\!]$, est égale à $\sigma(i)$. Toutes ces branches sont alors reliées au niveau de la racine (niveau 0). Ainsi, les nœuds de niveau $i \in [\![1, n]\!]$ sont au nombre de $n!/(n-i)!$. Pour faciliter la représentation de cet arbre nous ordonnons les branches à l'aide de l'ordre lexicographique.

Définition 3.2.2. À un nœud N de niveau i nous associons l'unique i-uplet

$$\phi_i(N) = (a_1, \ldots, a_i)$$

correspondant aux valeurs successives des étiquettes de ses ancêtres (racine exclue) et à la valeur de sa propre étiquette. Ce i-uplet est appelé *racine* de N. De plus, pour toute permutation σ de S_n, nous notons $\phi_i(\sigma)$ la valeur $\phi_i(N)$ où N est le nœud de rang i de la branche représentant σ dans $\mathcal{A}$. Le i-uplet $\phi_i(\sigma)$ est appelé la i-racine de σ.

Remarque 3.2.3. De manière équivalente, étant donné un nœud N de $\mathcal{A}$ de niveau i, $\phi_i(N) = (a_1, \ldots, a_i)$ où $a_j = \sigma(j)$ avec σ une permutation quelconque représentée par une branche de $\mathcal{A}$ passant par N.

Cette représentation de S_n peut aussi être vue comme suit. L'ensemble des branches de l'arbre $\mathcal{A}$ qui passe par un même nœud N de niveau i, correspond à l'ensemble des permutations de la classe C de $S_n/\mathrm{Stab}_{S_n}([1, \ldots, i])$ définie par $C = \{g \in S_n \,|\, \phi_i(g) = \phi_i(N)\}$. Ainsi, nous pouvons associer à $\mathcal{A}$ l'arbre $\mathcal{A}'$ de profondeur $n+1$ défini comme

suit. La racine de $\mathcal{A}'$ (niveau 0) est le groupe S_n et, un nœud de niveau $i \in [\![1, n]\!]$ est la classe de $S_n/\mathrm{Stab}_{S_n}([1, \ldots, i])$ des permutations passant par ce même nœud vu dans $\mathcal{A}$.

Les algorithmes de *branch-and-cut* que nous considérons ici traverseront indifféremment les arbres $\mathcal{A}$ et $\mathcal{A}'$ afin de trouver les permutations vérifiant la propriété $\mathcal{P}$. Ces algorithmes parcourent les arbres en commençant par la plus petite branche (pour l'ordre lexicographique) et en progressant en profondeur (le *branch* du *branch-and-cut*) dans les branches afin de toutes les inspecter de manière croissante. Le but du jeu étant de pouvoir arrêter la recherche dans une branche (le *cut* du *branch-and-cut*) le plus rapidement possible.

Le passage d'un nœud N de niveau i vers ses fils (progression en profondeur), se fait si les informations données par N ne suffisent pas pour contredire la propriété $\mathcal{P}$. Si au contraire les informations données par N suffisent pour contredire $\mathcal{P}$ alors la branche commençant à ce nœd peut être coupée ; dans ce cas l'algorithme retourne sur le nœud père afin de considérer une nouvelle branche. La notion de « *retour en arrière* »et de « *coupage de branche* »est équivalente mais dans ce qui suit, nous utiliserons la première. Donnons une définition plus précise de cette notion :

Définition 3.2.4. Soit N un nœud de $\mathcal{A}$ de niveau $i \in [\![1, n-1]\!]$. Dans un algorithme de *branch-and-cut* sur l'arbre $\mathcal{A}$, nous dirons qu'un *backtrack* est effectué en N, si la progression est possible vers ses fils, mais que la progression plus en profondeur est impossible à partir de tous ces descendants. De manière générale, nous dirons qu'un tel *backtrack* est de niveau i.

Clairement, plus un algorithme de *branch-and-cut* effectue des backtracks de petit niveau et meilleure sera son efficacité. En effet, si l'on reprend la notion de « *coupage de branche* », ceci revient à couper des branches le plus proche possible de la racine de $\mathcal{A}$. Cependant, il faut parfois se contenter de backtrack de niveau $n-1$, c'est le sujet du prochain paragraphe.

Branch-and-cut de base

Pour identifier les éléments de S_n qui vérifient la propriété $\mathcal{P}$, on peut traverser l'arbre $\mathcal{A}$ tout entier et trouver quelles sont les branches qui correspondent à des permutations qui vérifient $\mathcal{P}$. Pour ce faire, l'algorithme 3 de *branch-and-cut* trivial est utilisé.

Le problème de l'algorithme 3 est qu'il parcourt l'ensemble des branches de $\mathcal{A}$ et donc l'ensemble des éléments de S_n en discriminant les permutations les unes après les autres. En fait, dans ce cas, les *backtracks* ne sont effectués qu'en bout de branche (il sont de niveau $n-1$). Ainsi, sa complexité (en terme de nombre de prédicats calculés) est en $n!$.

Ici, les hypothèses faites sur $\mathcal{P}$ ne sont pas assez fortes pour pouvoir utiliser toute la force du *branch-and-cut*.

Une propriété pouvant se décomposer

Nous supposons à présent que la propriété $\mathcal{P}$ peut se décomposer en n sous-propriétés $\mathcal{P}_1, \ldots, \mathcal{P}_n$. Chaque propriété $\mathcal{P}_i$ est définie sur les classes de $S_n/\mathrm{Stab}_{S_n}([1, \ldots, i])$ de la

Algorithme 2 FONCTIONDEBASE(A)

Hypothèse : A est sous-arbre de $\mathcal{A}$ et G est une variable globale initialisée à l'ensemble vide.

Sortie : G est l'ensemble des éléments de S_n qui vérifient la propriété $\mathcal{P}$.

```
if A est une feuille then
  if la branche qui va de la racine jusqu'à A correspond à une permutation σ qui
  vérifie P then
    G = G ∪ {σ}
  end if
else
  for all sous-arbre B de A do
    FONCTIONDEBASE(B)
  end for
end if
```

Algorithme 3 BACKTRACK

Sortie : G est l'ensemble des éléments de S_n qui vérifient la propriété $\mathcal{P}$.

```
G := {}
FONCTIONDEBASE(A)
Return G
```

manière suivante : une classe de $S_n/\mathrm{Stab}_{S_n}([1,\dots,i])$ vérifie $\mathcal{P}_i$ si un de ses représentants vérifie la propriété $\mathcal{P}$. De cette manière, la propriété $\mathcal{P}_n$ est équivalente à $\mathcal{P}$.

À la propriété $\mathcal{P}_i$, est associé le prédicat P_i défini sur l'ensemble des i-arrangements de $\{1,\dots,n\}$ par :

> $P_i(a_1,\dots,a_i)$ est vrai si la classe (dans $\mathcal{A}'$) correspondant au nœud N de niveau i (dans $\mathcal{A}$) tel que $\phi_i(N) = (a_1,\dots,a_i)$ vérifie la propriété $\mathcal{P}_i$.

L'algorithme 3 peut alors être amélioré en utilisant l'algorithme 4 qui prend en entrée un i-arrangement a de $\{1,\dots,n\}$ et permet de déterminer l'ensemble $\{g \in G \,|\, \forall j \in [\![1,i]\!],\ g(j) = a_j\}$ (rappelons que l'ensemble G est la partie de S_n vérifiant la propriété $\mathcal{P}$). En effet, puisque la propriété est décomposée, des backtracks de niveau plus petit que $n-1$ peuvent être effectués.

Remarque 3.2.5. Dans l'algorithme 4, un backtrack de niveau i est effectué lorsque dans la boucle **for** aucun des prédicats n'est vérifié.

De l'algorithme 4 découle le suivant qui, au lieu de renvoyer un ensemble de permutations G, renvoie une unique permutation de cet ensemble.

Ces deux algorithmes sont toujours de complexité factorielle en l'entier n (il suffit de voir ce qui se passe lorsque l'ensemble G des éléments qui vérifient $\mathcal{P}$ est le groupe S_n tout entier). Mais, ils améliorent les calculs en pratique car ils permettent d'éviter beaucoup de tests dès qu'un *backtrack* est détecté à un niveau $i < n$.

Proposition 3.2.6. *Les algorithmes 4 et 5 terminent et renvoient le résultat escompté. De plus, si l'on suppose que l'algorithme 5 ne produit aucun* backtrack *lors de sa progression alors il calcule au plus $O(n^2)$ prédicats.*

Algorithme 4 TOUTESLESPERMUTATIONS(a)

Hypothèse : a est un arrangement de $\{1, \ldots, n\}$ de longueur i vérifiant le prédicat P_i.
Sortie : Renvoie l'ensemble $\{g \in G \,|\, \phi_i(g) = a\}$.

```
i := la longueur de a
N := φ_i^{-1}(a)
E := {}
if N est une feuille (i.e. i = n) then
  σ := la permutation correspondant à la branche passant par N
  Return {σ}
else
  for all nœud N' successeur de N do
    if P_{i+1}(φ_{i+1}(N')) then
      E := E ∪ ToutesLesPermutations(φ_{i+1}(N'))
    end if
  end for
  Return E
end if
```

Algorithme 5 UNEPERMUTATION(a)

Hypothèse : a est un arrangement de $\{1, \ldots, n\}$ de longueur i vérifiant le prédicat P_i.
Sortie : Un ensemble vide ou bien l'ensemble réduit à un élément $g \in G$ tel que $\phi_i(g) = a$ et g est minimal.

On lance TOUTESLESPERMUTATIONS(a) mais dès qu'une permutation σ est trouvée on renvoie $\{\sigma\}$ et si aucune permutation n'est trouvée on renvoie l'ensemble $\{\}$.

Démonstration. L'algorithme 4 fait au plus $n - i$ appels récursifs, où i est le niveau du nœud en entrée, et pour chacun des appels récursifs le nœud donné en entrée est de niveau $i + 1$, ainsi il termine. Il en est donc de même pour l'algorithme 5. Ces deux algorithmes renvoient donc le bon résultat. Pour l'algorithme 5, le nombre de calculs de prédicats pour une entrée de longueur i est majoré par :

$$\sum_{k=n-i}^{n} k$$

qui est de l'ordre de $O((n-i)^2)$. □

Remarque 3.2.7. Le fait de supposer qu'aucun backtrack n'est effectué lors de la progression de l'algorithme 5 semble peu réaliste. Pourtant, ceci nous servira dans le paragraphe 3.3.2 pour montrer un autre résultat de complexité.

L'algorithme 6 est donc une amélioration de l'algorithme 3 dans le cas où la propriété est décomposable.

Algorithme 6 BackTrack2

Hypothèse : La propriété $\mathcal{P}$ est décomposable
Sortie : G est l'ensemble des éléments de S_n qui vérifient la propriété $\mathcal{P}$

$G := \{\}$
for all nœud N de niveau 1 dans $\mathcal{A}$ **do**
  $G := G \cup$ ToutesLesPermutations$(\phi_1(N))$
end for
Return G

Ici, l'algorithme 6 ne fait plus, dans tous les cas, un parcours exhaustif de la totalité des feuilles de l'arbre $\mathcal{A}$ pour calculer l'ensemble G. Nous allons voir maintenant comment améliorer ce dernier lorsque la propriété $\mathcal{P}$ impose à G d'être un groupe.

L'ensemble G est un groupe

Lorsque l'on sait, à l'avance, que l'ensemble G est un groupe, il est possible d'améliorer l'algorithme 6. En effet, on peut alors donner en sortie un ensemble de générateurs de G au lieu de l'ensemble de tous ses éléments.

Nous supposons donc, à partir de maintenant, que la propriété $\mathcal{P}$ impose à G d'être un groupe. Nous noterons G_k ($k \in [\![1, n]\!]$) le sous-groupe $\mathrm{Stab}_G([1, \ldots, k])$ de G, et $G_0 = G$. L'algorithme que nous allons étudier détermine les éléments de la suite croissante :

$$\{Id\} = G_n < G_{n-1} < \ldots < G_1 < G_0 = G$$

Pour ce faire, nous allons montrer comment, à partir d'un ensemble de générateurs de G_k, on peut obtenir un système de générateurs de G_{k-1}.

De G_k vers G_{k-1}

Étant donné un ensemble de générateurs d'un groupe L tel que $G_k \subset L \subset G_{k-1}$, nous allons voir comment construire un ensemble de générateurs d'un groupe L' contenant

strictement L et contenu dans G_{k-1}. En itérant le principe, nous aurons alors une méthode pour construire G_{k-1} à partir de G_k.

Proposition 3.2.8. *Soit $\mathcal{G}$ un ensemble de générateurs d'un groupe L tel que $G_k \subset L \subset G_{k-1}$ et $\mathcal{O}$ une L-orbite de $\{1,\dots,n\}$ incluse dans $\{k+1,\dots,n\}$. Notons $\mathcal{E}$ l'ensemble $\{\sigma \in G_{k-1} \,|\, \sigma(k) \in \mathcal{O}\}$ et $L' = \langle L \cup \mathcal{E}\rangle$. Si $\mathcal{E}$ n'est pas vide alors le groupe L' contient strictement L et est engendré par l'ensemble $\mathcal{G} \cup \{\sigma\} \subset G_{k-1}$ avec σ un élément quelconque de $\mathcal{E}$.*

Démonstration. Supposons que $\mathcal{E}$ n'est pas vide. Comme l'intersection de $\mathcal{E}$ et L est vide, le groupe L' contient strictement L. Soit $\sigma \in \mathcal{E}$. Pour montrer que $\mathcal{G} \cup \{\sigma\}$ engendre L', il suffit de montrer qu'une permutation ω de $L \cup \mathcal{E}$ est un élément de $\langle \mathcal{G} \cup \{\sigma\}\rangle$.
Si ω est dans L, le résultat est immédiat. Supposons donc $\omega \in \mathcal{E}$. Comme $\omega(k)$ et $\sigma(k)$ sont dans la L-orbite $\mathcal{O}$, il existe un élément τ de L tel que $\tau(\sigma(k)) = \omega(k)$ et donc $\sigma^{-1}(\tau^{-1}(\omega(k))) = k$. Ainsi, la permutation $\rho = \sigma^{-1}\tau^{-1}\omega$ est un élément de G_{k-1} qui fixe k et donc appartient à $G_k \subset L$. Finalement, la permutation ω peut s'écrire comme le produit $\tau\sigma\rho$ de trois éléments de $L \cup \{\sigma\}$. □

Remarque 3.2.9. Dans la proposition 3.2.8, lorsque l'ensemble $\mathcal{E}$ n'est pas vide, nous pouvons choisir σ minimal (pour l'ordre lexicographique imposé à l'arbre $\mathcal{A}$) dans $\mathcal{E}$ et donc se restreindre aux permutations de G_{k-1} qui envoient k sur $\min(\mathcal{O})$.

Nous allons voir maintenant comment tester si le groupe L est maximal, c'est-à-dire $L = G_{k-1}$.

Lemme 3.2.10. *Soit L un sous-groupe de S_n tel que $G_k \subset L \subset G_{k-1}$. Alors*

$$\mathrm{Card}(L) = \mathrm{Card}(G_k)\,\mathrm{Card}(\mathrm{Orb}_L(k))\,.$$

Démonstration. Ce résultat est une conséquence immédiate du théorème de Lagrange. □

Proposition 3.2.11. *Soit L un sous-groupe de S_n tel que $G_k \subset L \subset G_{k-1}$. Deux cas sont alors possibles :*

1. *Aucune des L-orbites n'est un sous-ensemble de $\{k+1,\dots,n\}$ et alors $L = G_{k-1}$.*
2. *Il existe au moins une L-orbite sous-ensemble de $\{k+1,\dots,n\}$. Dans ce cas, notons $\mathcal{O} = \{O_1,\dots,O_r\}$ l'ensemble de ces L-orbites. S'il existe i dans $[\![1,r]\!]$ et σ dans G_{k-1} tels que $\sigma(k) \in O_i$ alors $L \neq G_{k-1}$, sinon $L = G_{k-1}$.*

Démonstration. Ce résultat est une conséquence immédiate du lemme 3.2.10. □

Il s'agit à présent, d'utiliser la proposition 3.2.8 afin de construire un algorithme de calcul d'un ensemble de générateurs de G_{k-1} à partir d'un ensemble de générateurs de G_k. Comme nous le montre la proposition 3.2.11, cette mise en œuvre nécessite le calcul d'orbites. Ainsi, nous allons maintenant présenter un algorithme permettant un tel calcul. Plus exactement, étant donné un sous-groupe L de S_n et une permutation σ comme dans la proposition 3.2.8, il s'agit de calculer les orbites de $\{1,\dots,n\}$ sous l'action du groupe $\langle L \cup \{\sigma\}\rangle$.

Proposition 3.2.12. *L'algorithme 7 termine et renvoie le résultat voulu. De plus, il effectue au plus $O(n^3)$ opérations élémentaires pour fournir le résultat.*

Algorithme 7 ORBITES($\mathcal{O}$, σ)

Hypothèse : $\mathcal{O}$ est l'ensemble des L-orbites de $\{1, \ldots, n\}$ où L est un sous-groupe de S_n et σ est une permutation de S_n.

Sortie : $\mathcal{O}'$ est l'ensemble des orbites de $\{1, \ldots, n\}$ sous l'action du groupe $L' = \langle L \cup \{\sigma\}\rangle$.

$\mathcal{O}' := \{\}$
$\Omega := \{\}$
for all $O \in \mathcal{O}$ tel que $O \not\subset \Omega$ **do**
  $E_1 := O$
  $P := \sigma.E_1 \cup E_1$
  $E_2 := \cup_{\{O' \in \mathcal{O} \mid O' \cap P \neq \emptyset\}} O'$
  while $E_1 \neq E_2$ **do**
    $E_1 := E_2$
    $P := \sigma.E_1 \cup E_1$
    $E_2 := \cup_{\{O' \in \mathcal{O} \mid O' \cap P \neq \emptyset\}} O'$
  end while
  $\mathcal{O}' := \mathcal{O}' \cup \{E_1\}$
  $\Omega := \Omega \cup \{E_1\}$
end for
Return $\mathcal{O}'$

Démonstration. Considérons une itération de la boucle **for**, ou de manière équivalente une L-orbite $\mathcal{O}$, et étudions tous les appels effectués lors de cette itération.
Clairement, $E_1 \subset E_2 \subset \{1, \ldots, n\}$ et donc la boucle **while** finit avec au plus n itérations. Ceci nous donne la terminaison de l'algorithme.
Par construction, l'ensemble E_1, une fois sortie de la boucle **while**, est stable par L et σ, ainsi E_1 peut s'écrire comme union disjointe de L'-orbites de $\{1, \ldots, n\}$. Comme E_1 est, à chaque itération de la boucle **while**, contenu dans la L'-orbite de $\{1, \ldots, n\}$ contenant O. Après cette boucle, E_1 est égal à cette L'-orbite.
Le calcul de E_1 et P nécessite au plus n opérations élémentaires et celui de E_2 au plus n^2.
Finalement, comme $\Omega \subset \{1, \ldots, n\}$, il faudra au plus $O(n^3)$ opérations élémentaires pour retourner le résultat. □

Nous pouvons maintenant donner un algorithme pour le calcul d'un ensemble de générateurs de G_{k-1} à partir d'un ensemble de générateurs de G_k.

Proposition 3.2.13. *L'algorithme 8 termine et renvoie le bon résultat. De plus, si l'on suppose qu'aucun backtrack n'est effectué durant la progression, le nombre de prédicats calculés est borné par $O(n^3)$ et le nombre d'opérations élémentaires par $O(n^4)$.*

Démonstration. Pour la terminaison, il suffit de voir qu'à chaque itération de la boucle **while** l'ensemble *elts* perd au moins un de ses éléments.
D'après la proposition 3.2.8, les groupes $\langle \mathcal{G} \rangle$ obtenus au cours du calcul forment une suite croissante vérifiant tous $G_k \subset \langle \mathcal{G} \rangle \subset G_{k-1}$. Notons L un de ces sous-groupe de S_n et $\mathcal{O} = \{O_1, \ldots, O_r\}$ les L-orbites de $\{1, \ldots, n\}$. D'après la proposition 3.2.11, si aucune des orbites O_i n'est incluse dans $\{k+1, \ldots, n\}$ alors $L = G_{k-1}$. De même, si

Algorithme 8 De_Gk_Vers_G(k-1)($\mathcal{G}$,k,$\mathcal{O}$)

Hypothèse : $\mathcal{G}$ un ensemble de générateurs de G_k, k est l'indice du groupe $\langle\mathcal{G}\rangle$, $\mathcal{O}$ est l'ensemble des G_k-orbites de $\{1,\dots,n\}$.

Sortie : $\mathcal{G}$ est un ensemble de générateurs de G_{k-1} et $\mathcal{O}$ est l'ensemble des G_{k-1}-orbites de $\{1,\dots,n\}$.

```
elts := {min(O) | O ∈ 𝒪 et O ⊂ {k+1,...,n}}
while elts ≠ ∅ do
  a := min(elts)
  elts := elts \ {a}
  if P_k(1,2,...,k-1,a) then
    E := UnePermutation([1,2,...,k-1,a])
    if E ≠ ∅ then
      σ := l'unique élément de E
      𝒢 := 𝒢 ∪ {σ}
      𝒪 := Orbites(𝒪, σ)
      elts := {min(O) | O ∈ 𝒪 et O ⊂ {k+1,...,n}}
    end if
  end if
end while
Return 𝒢, 𝒪
```

pour toute orbite O_i incluse dans $\{k+1,\dots,n\}$ on ne peut trouver une permutation $\sigma \in G_{k-1}$ envoyant k dans O_i alors $L = G_{k-1}$. De plus, d'après la remarque 3.2.9, dans le second cas on peut se restreindre à la recherche de permutations de G_k envoyant k sur $\min O_i$. En conclusion, dès que l'on sort de la boucle **while** le groupe L s'identifie à G_{k-1}.
Il est clair que l'étape qui nécessite le plus de calculs de prédicats est l'appel à la fonction `UnePermutation`, et que l'étape qui nécessite le plus d'opérations élémentaires est l'appel à `Orbites`. Ce sont donc ces deux étapes que nous allons dénombrer. À chaque itération de la boucle **while**, il y a au plus un appel à `UnePermutation` et à `Orbites`. Comme il y a au plus n itérations de cette boucle, nous obtenons le résultat car l'hypothèse permet d'appliquer les propositions 3.2.6 et 3.2.12. □

Nous en déduisons l'algorithme 9 qui permet le calcul du groupe G et de son cardinal.

Proposition 3.2.14. *L'algorithme 9 termine et renvoie le bon résultat. De plus, si aucun backtrack n'est effectué durant les appels à* `UnePermutation`*, le nombre de prédicats calculés est de l'ordre de $O(n^3)$ et le nombre d'opérations élémentaires nécessaires est de l'ordre de $O(n^4)$.*

Démonstration. La terminaison est claire. D'après la proposition 3.2.13, en fin de calcul, la variable $\mathcal{G}$ contient un ensemble de générateurs de G. D'après le lemme 3.2.10 nous avons

$$\mathrm{Card}(G) = \prod_{i=0}^{n-1} \mathrm{Card}(\mathrm{Orb}_{G_i}(i+1))$$

Algorithme 9 BACKTRACK3($P_1, \ldots, P_n$)

Hypothèse : la propriété $\mathcal{P}$ est décomposable et nous avons en entrée l'ensemble des prédicats $P_1, \ldots, P_n$.

Sortie : $\mathcal{G}$ est un ensemble de générateurs de G et $Card$ son cardinal.

$\mathcal{G} := \{Id_{S_n}\}$
$orbits := \{\{1\}, \ldots, \{n\}\}$
$k := n - 1$
$Card := 1$
while $k \neq 0$ **do**
  $\mathcal{G}$, $orbits :=$ `De_Gk_vers_G(k-1)`$(k, \mathcal{G}, orbits)$
  $Card := \mathrm{Card}(Orb_{G_k}(k+1)) * Card$
  $k := k - 1$
end while
Return $\mathcal{G}$, $Card$

et ainsi nous obtenons le fait que la variable $Card$ est égale au cardinal de G en fin de calcul.
Pour évaluer le nombre d'opérations élémentaires et le nombre de calculs de prédicats effectués, nous allons, comme pour l'algorithme 8, compter le nombre d'appels à `Orbites` et `UnePermutation`. Une analyse immédiate de l'algorithme 9 nous montre qu'à tout moment du calcul nous avons :

$$\mathrm{Card}(\mathcal{G}) + \mathrm{Card}(orbits) = n + 1\,.$$

Ainsi, il y a en tout, au plus n permutations calculées et donc (voir algorithme 8) au plus n appels à `Orbites` et `UnePermutation`. Nous avons donc le résultat d'après les propositions 3.2.12 et 3.2.6. □

Remarque 3.2.15. Notons respectivement C_1, C_2 les complexités de calcul sur des mots machines d'une opération élémentaire et du calcul de prédicat. Lorsque $C_2 \geqslant nC_1$, la complexité de calcul sur des mots machines de l'algorithme 9 sera donc de l'ordre de $O(n^3 C_2)$ (voir Proposition 3.2.14) et donc il devient naturel de ne plus s'intéresser aux opérations élémentaires.

Nous avons donc maintenant un algorithme permettant le calcul d'un sous-groupe défini à partir d'une propriété décomposable, ainsi que son analyse de complexité lorsqu'aucun backtrack n'est rencontré. Comme nous l'avons dit plus haut, tous ces algorithmes sont, de manière générale, de complexité factorielle en n. C'est la nature même de la propriété $\mathcal{P}$ qui permet de montrer que dans certains cas ces algorithmes sont polynomiaux. Par exemple, le calcul du centralisateur d'un groupe de permutations H utilise la méthode du *branch-and-cut* et est de complexité polynomiale en la taille de la base de H (voir [42]). Nous allons maintenant appliquer ces résultats au calcul du groupe de décomposition d'un idéal.

3.3 Application pour le calcul du groupe de décomposition.

À l'instar des idéaux premiers (voir [21, Définition 2 page 36]) nous définissons la notion de groupe de décomposition d'un idéal I de $k[x_1, \ldots, x_n]$:

Définition-Proposition 3.3.1. *Soit I un idéal de $k[x_1, \ldots, x_n]$. La partie G des permutations σ de S_n vérifiant la propriété*

$$\mathcal{P} \ : \ \sigma.I = I \, ,$$

est un groupe appelé groupe de décomposition de I. *Nous noterons $\mathcal{P}(I)$ cette propriété.*

La propriété $\mathcal{P}(I)$ qui permet de définir le groupe de décomposition d'un idéal peut être défini à l'aide du prédicat P qui suit :
Étant donné $\mathcal{S} = \{f_1, \ldots, f_r\}$ un ensemble de générateurs de I alors

$$P \ : \ \forall i \in [\![1, n]\!], \, \sigma.f_i \in I \, .$$

Pour calculer un tel prédicat, on pourra calculer une base de Gröbner de I ou utiliser les *formes normales généralisées* (voir [79, 80, 102]). Ici, nous supposons que $\mathcal{S}$ est une base de Gröbner de I. Ainsi, le prédicat P peut se récrire sous la forme (voir Théorème 1.3.12) :

$$P \ : \ \forall i \in [\![1, n]\!], \, \mathrm{NF}(\sigma.f_i, \mathcal{S}) = 0 \, .$$

A priori, la propriété $\mathcal{P}(I)$ n'est pas décomposable. Ainsi, le seul moyen de calculer le groupe de décomposition d'un idéal I de $k[x_1, \ldots, x_n]$ est d'utiliser l'algorithme 3 qui est inefficace. Mais, dans certains cas, nous allons pouvoir appliquer les résultats du paragraphe 3.2.

Dans tout le restant de ce chapitre, le calcul d'un prédicat reviendra au calcul d'une forme normale d'un polynôme. La complexité de calcul, sur des mots machines, d'une forme normale modulo une base de Gröbner est clairement n fois plus grande que celle d'une opération élémentaire (voir Proposition 1.3.22). Ainsi (voir Remarque 3.2.15), dans toute la suite de ce chapitre, on ne s'intéressera plus aux calculs d'opérations élémentaires.

3.3.1 Application aux idéaux triangulaires

Fixons un système

$$\mathcal{S} = \{f_1, \ldots, f_n\}$$

triangulaire (voir Définition 1.3.15) de polynômes de $k[x_1, \ldots, x_n]$, et supposons l'idéal I engendré par $\mathcal{S}$. Nous dirons de l'idéal I qu'il est triangulaire.

Nous allons voir que dans ce cas la propriété $\mathcal{P}(I)$ est décomposable. En effet, l'ensemble $\mathcal{S}$ est une base de Gröbner de I et donc, une permutation σ de S_n vérifiera la propriété $\mathcal{P}(I)$ si et seulement si pour tout entier $j \in [\![1, n]\!]$ elle vérifie la propriété $\mathcal{P}(I)_j$ définie à l'aide du prédicat P_j :

$$P_j \ : \ \forall i \in [\![1, j]\!], \, \mathrm{NF}(\sigma.f_i, \{f_1, \ldots, f_j\}) = 0 \, .$$

Soit j un entier de $[\![1, n]\!]$. Reste à montrer que la propriété $\mathcal{P}(I)_j$ passe au quotient, c'est-à-dire qu'elle peut être définie sur les classes de $S_n/\mathrm{Stab}_{S_n}([1, \ldots, j])$. Comme f_i

est un élément de $k[x_1, \ldots, x_j]$ pour tout entier $i \in [\![1, j]\!]$ et pour toute permutation ω de $\mathrm{Stab}_{S_n}([1, \ldots, j])$ nous avons :

$$\omega.f_i = f_i\,.$$

Ainsi, pour toute permutation σ de S_n on obtient

$$\sigma(\omega.f_i) = \sigma.f_i\,,$$

et la propriété passe au quotient. En résumé, nous pouvons énoncer la proposition suivante :

Proposition 3.3.2. *Dans le cas où l'idéal I est triangulaire, la propriété $\mathcal{P}(I)$ est décomposable.*

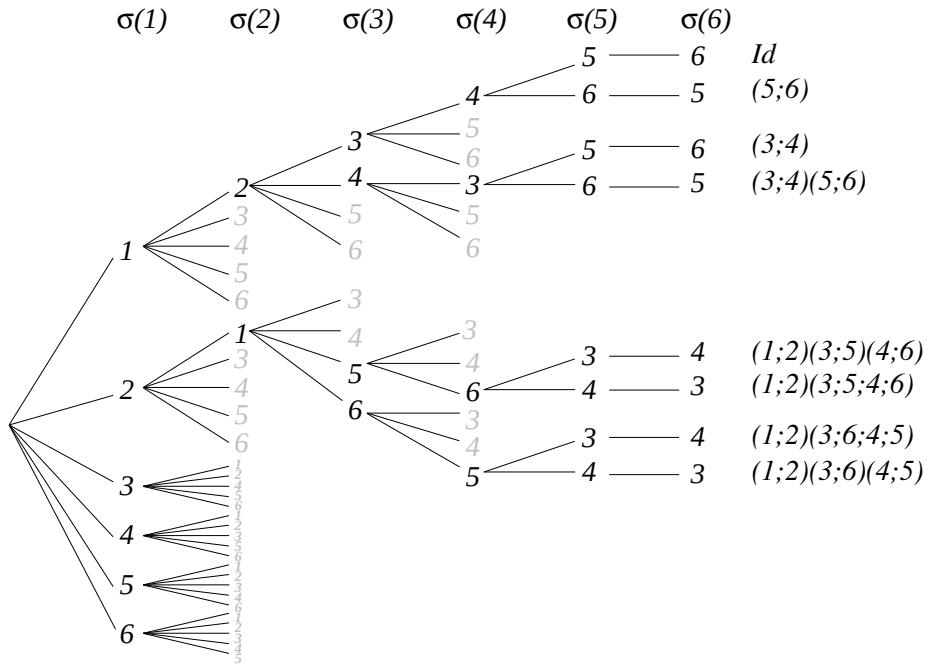
Nous pouvons dès lors donner un exemple de calcul du groupe de décomposition à l'aide de l'algorithme 6.

Exemple 3.3.3. Considérons l'idéal triangulaire J de Galois (voir Définition 2.2.1) de $\mathbb{Q}[x_1, \ldots, x_6]$ engendré par les polynômes :

$$\begin{array}{lcl}
f_1(x_1) & = & x_1^6 - x_1^5 - 10x_1^4 + x_1^3 + 12x_1^2 - 3x_1 - 1, \\
f_2(x_1, x_2) & = & 17x_2 - 5x_1^5 + 4x_1^4 + 44x_1^3 + 14x_1^2 + 4x_1 - 8, \\
f_3(x_1, x_2, x_3) & = & 17x_3^2 - 8x_3x_1^5 + 3x_3x_1^4 + 84x_3x_1^3 + 36x_3x_1^2 - 65x_3x_1 - 6x_3 \\
 & & -29x_1^5 + 13x_1^4 + 296x_1^3 + 139x_1^2 - 276x_1 - 77, \\
f_4(x_1, \ldots, x_4) & = & 17x_4 + 17x_3 - 8x_1^5 + 3x_1^4 + 84x_1^3 + 36x_1^2 - 65x_1 - 6, \\
f_5(x_1, \ldots, x_5) & = & 17x_5^2 + 13x_5x_1^5 - 7x_5x_1^4 - 128x_5x_1^3 - 50x_5x_1^2 + 78x_5x_1 - 3x_5 \\
 & & +11x_1^5 - 19x_1^4 - 107x_1^3 + 95x_1^2 + 168x_1 - 115, \\
f_6(x_1, \ldots, x_6) & = & 17x_6 + 17x_5 + 13x_1^5 - 7x_1^4 - 128x_1^3 - 50x_1^2 + 78x_1 - 3\,.
\end{array}$$

L'algorithme 6 parcourt les branches suivantes de l'arbre $\mathcal{A}$. Dans cette illustration,

chaque étiquette foncée correspond à un calcul de prédicat qui a renvoyé vrai et inversement.



Remarquons que 64 prédicats ont été calculés.

Voyons ce qu'il en est lorsque l'on applique l'algorithme 9.

Exemple 3.3.4. Considérons l'idéal J de l'exemple 3.3.3. Ici, nous allons détailler la marche suivie par l'algorithme 9 pour calculer une base de générateurs du groupe de décomposition G de l'idéal J. Cet algorithme construit successivement les stabilisateurs G_k pour k allant de 5 à 0. Comme $G_5 = \langle Id \rangle$, nous commençons donc par calculer G_4 et G prend pour valeur initiale le groupe identité. Dans le reste de cet exemple, nous noterons les entêtes de permutations sous forme de tableaux. Par exemple, le tableau $[2, 1, 6]$ représentera toutes les permutations de S_6 telles que $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 6$.

Calcul de G_4 : Les G-orbites sont $\{1\}, \ldots, \{6\}$, et une seule est contenue dans $\{6\}$. L'entête $t = [1, 2, 3, 4, 6]$ vérifie le prédicat P_5, ainsi, il faut chercher une permutation d'entête t qui stabilise l'ensemble triangulaire engendrant l'idéal J. La fonction `UnePermutation` se charge de ce travail et nous renvoie la permutation (5, 6). Ainsi, G prend la valeur $\rangle G, (5,\ 6)\langle$ et il n'existe plus de G-orbite contenues dans $\{6\}$. Nous passons donc au calcul de G_3.

Calcul de G_3 : L'ensemble *elts* des G-orbites contenues dans $\{5, 6\}$ est réduit au seul élément $\{5, 6\}$. Le prédicat P_5 est faux lorsqu'on le teste avec l'entête $[1, 2, 3, 5]$. Comme l'ensemble *elts* est réduit à un élément, nous en déduisons alors que $G_3 = G_4$ et nous passons au prochain stabilisateur.

Calcul de G_2 : Dans ce cas, l'ensemble *elts* est

$$\{\{4\},\ \{5, 6\}\}.$$

L'entête $[1, 2, 4]$ vérifie le prédicat P_3 et la fonction `UnePermutation` nous renvoie la permutation (3, 4) que l'on rajoute à G. Il reste la G-orbite $\{5, 6\}$ dans

$\{4, \ldots, 6\}$. L'entête $[1, 2, 5]$ ne vérifie pas le prédicat P_3, ainsi $G = G_2$.

Calcul de G_1 : L'ensemble *elts* des G-orbites contenues dans $\{3, \ldots, 6\}$ est donné par

$$elts = \{\{3, 4\}, \{5, 6\}\}.$$

Les entêtes $[1, 3]$ et $[1, 5]$ ne vérifient pas le prédicat P_2. Le groupe G s'identifie donc à G_1.

Calcul de G_0 : Ici l'ensemble *elts* est

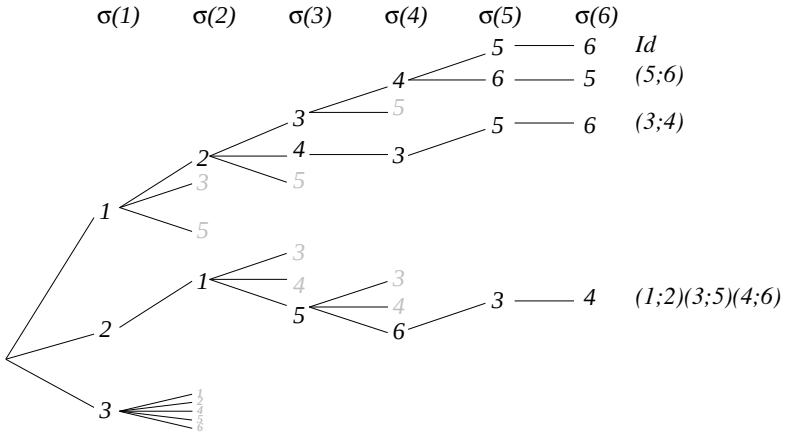
$$\{\{2\}, \{3, 4\}, \{5, 6\}\}.$$

L'entête $[2]$ vérifie le prédicat P_1 et la fonction `UnePermutation` renvoie la permutation (1, 2)(3, 5)(4, 6) que nous rajoutons à G. L'ensemble $\{3, \ldots, 6\}$ est la seule G-orbite de minimum un nombre plus grand que 4. L'entête $[3]$ vérifie le prédicat P_1 mais, la fonction `UnePermutation` renvoie l'identité (c'est un backtrack). Nous avons fini le calcul.

En conclusion, l'algorithme 9 renvoie l'ensemble de générateurs

$$[Id, (5, 6), (3, 4), (1, 2)(3, 5)(4, 6)].$$

Le parcourt effectué sur $\mathcal{A}$ se résume par la figure suivante.



Il effectue 32 calculs de prédicats au lieu de 64 pour l'algorithme 6 ce qui améliore nettement le temps de calcul.

Plus généralement, nous avons effectué plusieurs tests pour le calcul du groupe de décomposition d'un idéal de Galois. Dans le tableau 3.1 qui suit, nous avons recensé le nombre de calculs de prédicats nécessaires à ces deux algorithmes. Dans la première colonne, sont cités les noms des idéaux utilisés. Dans la deuxième, figure le cardinal du groupe de décomposition correspondant. Les deux dernières sont réservées aux nombres de calculs de prédicats effectués.

Idéal	Card(Dec(I))	Algorithme 6	Algorithme 9
$I_{7,1}*$	7	154	31
$I_{7,2}$	8	115	49
$I_{6,4}*$	24	144	28
$I_{9,4}$	24	258	52
$I_{7,3}$	36	193	38
$I_{6,10}*$	72	264	30
$I_{6,13}*$	72	264	30
$I_{9,28}*$	648	2637	64
$I_{6,12}*$	720	1956	20
$I_{9,20}$	2160	5970	42
$I_{7,4}*$	5040	13699	27
$I_{7,5}*$	5040	13699	27
$I_{7,6}*$	5040	13699	27

TAB. 3.1 – Comparaisons des algorithmes 6 et 9.

Les résultats du tableau 3.1 approuvent le fait que l'algorithme 6 est de complexité factorielle. Par contre, ces premières expérimentations sembleraient montrer que l'algorithme 9 est polynomial lorsqu'on l'utilise pour calculer le groupe de décomposition d'un idéal de Galois. En fait, nous allons montrer qu'il existe des exemples où le comportement de cet algorithme est factoriel.

Complexité dans le cas général

Notons $f_1, \ldots, f_6$ les générateurs de l'ensemble triangulaire engendrant l'idéal J de l'exemple 3.3.3. Dans cet exemple, un backtrack apparaît lorsque l'algorithme recherche une permutation σ dans G telle que $\sigma(1) = 3$. En effet, le prédicat P_1 est vérifié pour le nœud de niveau 1 et d'étiquette 3 mais aucun de ses fils ne vérifie le prédicat P_2.

C'est à partir de cette constatation que nous allons construire un exemple d'ensemble triangulaire $\mathcal{T}$ de $n > 6$ éléments tel que l'algorithme 9, appliqué à $\mathcal{P}(\langle\mathcal{T}\rangle)$, calcule un nombre factoriel de prédicats.

Soit n un entier strictement positif et g le polynôme à coefficient rationnels ayant pour racines les entiers $1, \ldots, n$. Notons $g_1, \ldots, g_n$ les modules de Cauchy de g (voir Proposition 2.2.2). L'idéal $I_n \in k[x_1, \ldots, x_{n+6}]$ que nous allons considérer maintenant

est celui engendré par le système triangulaire $\mathcal{T}$ suivant :

$$\begin{aligned} h_1 &= f_1(x_1) \\ h_2 &= g_1(x_2) \\ h_3 &= g_2(x_3, x_2) \\ &\vdots \\ h_{n+1} &= g_n(x_{n+1}, \ldots, x_2) \\ h_{n+2} &= f_2(x_{n+2}, x_1) \\ h_{n+3} &= f_3(x_{n+3}, x_{n+2}, x_1) \\ &\vdots \\ h_{n+6} &= f_6(x_{n+6}, \ldots, x_{n+2}, x_1) \end{aligned}$$

Soit Ψ le morphisme injectif de groupes défini par

$$\begin{aligned} \Psi : S_6 &\longrightarrow S_{n+6} \\ \sigma &\longmapsto \Psi(\sigma) \end{aligned}$$

où $\Psi(\sigma)$ envoie tous les éléments de $\{2, \ldots, n+1\}$ sur eux mêmes et

$$\Psi(\sigma)(i) = \begin{cases} 1 & \text{si } \sigma(i) = 1 \\ \sigma(i) + n + 1 & \text{sinon.} \end{cases}$$

Soit Φ le morphisme injectif de groupes défini par

$$\begin{aligned} \Phi : S_n &\longrightarrow S_{n+6} \\ \sigma &\longmapsto \Phi(\sigma) \end{aligned}$$

où $\Phi(\sigma)$ envoie tous les éléments de $\{1, n+2, \ldots, n+6\}$ sur eux mêmes et

$$\Phi(\sigma)(i) = \sigma(i-1) + 1 \text{ pour } i \in [\![2, n+1]\!] .$$

Puisqu'aucun polynôme engendrant I_n n'a à la fois des indéterminées dans $\{x_1, x_{n+2}, \ldots, x_{n+6}\}$ et dans $\{x_2, \ldots, x_{n+1}\}$, si l'on note G le groupe de décomposition de J et H celui des modules de Cauchy de g alors les groupes $\Psi(G)$ et $\Phi(H)$ sont inclus dans le groupe de décomposition de I_n. De plus, comme g et f n'ont aucune racine en commun, le groupe de décomposition de I_n s'identifie à $\Psi(G)\Phi(H)$ qui est isomorphe au produit direct $G \times H$. Nous en déduisons alors le résultat suivant.

Proposition 3.3.5. *L'algorithme 9 appliqué à la propriété $\mathcal{P}(I_n)$ effectue au moins $n!$ calculs de prédicats.*

Démonstration. Reprenons les mêmes notations que dans l'exemple 3.3.4 et notons L le groupe de décomposition de I_n. Nous avons $L_1 = \Psi(G_1)\Phi(H)$ qui est isomorphe à $G_1 \times H$. Ainsi, lorsque l'algorithme 9 cherche à calculer L_0 à partir de L_1 il va, comme pour le calcul de G, chercher une permutation dont l'entête vérifie le prédicat P_1 mais qui ne pourra être continuée. Dans l'exemple J cette entête était [3], par transport par

Ψ, dans le cas de I_n elle correspond à $[n+3]$. Comme $H = S_n$ (voir Proposition 2.2.2), pour tout n-arrangement $[i_1, \ldots, i_n]$ de $\{2, \ldots, n+1\}$ l'entête $t = [n+3, i_1, \ldots, i_n]$ vérifie le prédicat P_{n+1}. Si l'entête t pouvait être prolongée en une permutation σ de L alors $\Psi^{-1}(\sigma)$ serait une permutation de G qui enverrait 1 sur 3, ce qui est impossible.
Avant de pouvoir arrêter le processus de recherche, l'algorithme a parcouru au moins toutes les branches de l'arbre correspondant à H. Ainsi, il a fait au moins $n!$ calculs de prédicats. □

Corollaire 3.3.6. *La complexité asymptotique de l'algorithme 9 appliqué au calcul du groupe de décomposition d'un idéal triangulaire de $k[x_1, \ldots, x_n]$, est factorielle en n.*

D'après ce que nous venons de voir, l'algorithme 9 est de complexité factorielle lorsqu'il est appliqué aux propriétés $\mathcal{P}(I)$ où I est un idéal de Galois triangulaire. L'exemple permettant de montrer ce dernier résultat est très particulier. Il est donc naturel de se demander dans quelle mesure on peut trouver une classe d'idéaux triangulaires où l'algorithme 9, appliqué au calcul du groupe de décomposition, est de complexité polynomiale. Dans le paragraphe suivant, nous allons étudier cet algorithme dans un cadre plus restreint : celui des idéaux de Galois purs.

3.3.2 Application aux idéaux de Galois purs

Dans ce paragraphe, nous allons étudier l'application de tout ce que nous venons de voir au problème suivant qui porte sur les idéaux de Galois purs (voir Définition 2.2.21) :

Étant donné un idéal triangulaire, pouvoir décider s'il est de Galois pur ou non, et si tel est le cas, calculer son groupe de décomposition.

Pouvoir répondre à ce problème a des applications dans plusieurs cadres de la théorie de Galois effective. Il sera utilisé dans le chapitre 5 et peut être utilisé pour calculer la représentation symétrique du groupe de Galois d'un corps de décomposition donné sous la forme d'une tour complète d'extensions.

Rappelons qu'un idéal de Galois pur I est un idéal triangulaire caractérisé par les deux propriétés suivantes (voir Paragraphe 2.2.3) :

1. L'idéal I est de Galois ;
2. pour tout élément $\underline{\alpha}$ de sa variété $V(I)$ on a $\mathrm{Dec}(I).\underline{\alpha} = V(I)$.

Nous allons fournir les moyens théoriques pour tester ces deux conditions.

Théorème 3.3.7. *Soit I un idéal de Galois de $k[x_1, \ldots, x_n]$ engendré par un système triangulaire*

$$\mathcal{T} = \{f_1, \ldots, f_n\}.$$

Soit $\underline{\alpha}$ un zéro de I et L le $\underline{\alpha}$-injecteur de I. Soit t un entier de $[\![1, n-1]\!]$ et $(c_1, \ldots, c_t)$ un t-arrangement de $\{1, \ldots, n\}$. Soit D le produit $\prod_{i=t+1}^{n} \deg_{x_i} f_i$.
Alors, pour tout entier i dans $[\![1, t]\!]$, $f_i(\alpha_{c_1}, \ldots, \alpha_{c_i}) = 0$ ssi il existe une permutation σ dans L telle que $\phi_i(\sigma) = (c_1, \ldots, c_t)$. Plus précisément, il existe D telles permutations dans L.

Démonstration. Soit t un entier dans $[\![1, n]\!]$. Puisque la variété $V(I)$ est équiprojectable (voir [14]), tout élément $\underline{\beta}$ de la variété $\langle f_1, \ldots, f_t \rangle$ est la projection sur les t premières coordonnées de D éléments de $V(I)$. La bijection entre $V(I)$ et L (voir Égalités 2.3 et 2.4) donne alors le résultat. □

Remarque 3.3.8. En appliquant le théorème 3.3.7 au cas particulier des idéaux de Galois maximaux, on obtient le *Theorem 5* de [7].

La proposition qui suit est la clé pour établir un algorithme permettant de répondre au problème précédemment posé.

Proposition 3.3.9. *Soit I un idéal triangulaire de $k[x_1, \ldots, x_n]$. Si lors de l'appel* `Backtrack3`*$(\mathcal{P}(I))$ un* backtrack *apparaît alors I n'est pas de Galois pur.*

Démonstration. Dans l'algorithme 9, un *backtrack* apparaît lorsqu'un t-arrangement $m = (c_1, \ldots, c_t)$ ($t \in [\![1, n-1]\!]$) vérifiant le prédicat P_t ne peut être complété en un $t+1$ arrangement $n = (c_1, \ldots, c_t, c_{t+1})$ vérifiant le prédicat P_{t+1}. En d'autres termes, ceci veut dire que l'algorithme exhibe une permutation σ de $S_n \backslash\backslash \operatorname{Dec}(I)$ vérifiant seulement les t premières propriétés $\mathcal{P}(I)_i$. D'après le théorème 3.3.7, soit l'idéal I n'est pas un idéal de Galois, soit I est un idéal de Galois tel que son groupe de décomposition n'est pas un de ses injecteurs, c'est-à-dire qui n'est pas pur. Le résultat suit. □

Ainsi, nous en déduisons l'algorithme 10.

Algorithme 10 EstGaloisPur ?(I)

Hypothèse : L'idéal est défini à l'aide d'un système triangulaire de générateurs.
Sortie : Renvoie *vrai* et un ensemble de générateurs $\mathcal{G}$ du groupe $Dec(I)$ si I est de Galois pur, *faux* sinon.

On lance $\mathcal{G}, Card$:=`Backtrack3(`$\mathcal{P}(I)$`)` en inspectant si un *backtrack* est effectué.
if un *backtrack* est effectué **then**
  Return *faux*
else
  if $Card = \operatorname{Card}(V(I))$ **then**
    Return *vrai*, $\mathcal{G}$
  else
    Return *faux*
  end if
end if

Proposition 3.3.10. *L'algorithme 10 termine et renvoie le bon résultat. De plus, le nombre de prédicats calculés est de l'ordre de $O(n^3)$.*

Démonstration. Puisque le calcul arrête à l'apparition d'un *backtrack*, le pire des cas est rencontré lorsque aucun *backtrack* n'est effectué, c'est donc ce que nous supposons à présent. La proposition 3.2.14 nous donne alors la terminaison de l'algorithme et la complexité annoncée. La proposition 3.3.9 et la caractérisation des idéaux de Galois purs nous donnent le fait que le résultat renvoyé est le bon. □

Remarque 3.3.11. Dans l'algorithme 10, il est calculé le cardinal de la variété de l'idéal I. Ce calcul peut être très coûteux. Par contre, si nous savons *a priori* que l'idéal I est radical alors ce cardinal se lit sur les degrés d_i des monômes dominants des éléments de l'ensemble triangulaire engendrant I. En effet, nous avons l'égalité $\operatorname{Card}(V(I)) = \prod_i d_i$. En particulier, si l'on applique cet algorithme au cas des idéaux de Galois triangulaires le calcul du cardinal de sa variété est immédiat.

Corollaire 3.3.12. *La complexité, en terme de nombre de formes normales calculées, du calcul du groupe de décomposition d'un idéal de Galois pur est de l'ordre de* $O(n^3)$.

Démonstration. C'est une conséquence directe de la proposition 3.3.10 et de la remarque 3.3.11. □

Remarque 3.3.13. L'algorithme 10, appliqué aux cas particulier des idéaux de Galois maximaux, permet le calcul d'une représentation symétrique du groupe de Galois associé et donc, la complexité annoncée dans le corollaire précédent est meilleure que celle précédemment connue : $O(n^4)$ (voir [7]).

3.3.3 Expérimentations

Dans ce paragraphe, nous comparons des temps de calcul entre une implantation de l'algorithme `StrongGenerators` de Anai, Noro et Yokoyama (voir [7]) et une implantation de l'algorithme 10 appliqués au cas d'un idéal de Galois maximal $\mathcal{M}$ à coefficients rationnels. Soit $\mathcal{T}$ l'ensemble triangulaire réduit engendrant $\mathcal{M}$.

L'algorithme `StrongGenerators` est de complexité $O(n^4)$ en terme de nombre de formes normales calculées. Toutefois, cet algorithme utilise le fait que l'on connaît *a priori* le nombre de polynômes dans $\mathcal{T}$ qui sont linéaires en leur monôme de tête. Ainsi, il est important de tester si une telle connaissance peut apporter plus d'efficacité par rapport à l'algorithme 10. La table 3.2 recense des temps de calculs effectués sur des idéaux de relations $I_{d,t}$ de groupe de décomposition un conjugué de dT_n (numérotation de Butler et McKay). Ces tests ont été réalisés à l'aide d'implantations en Magma (version 2.10) sur une machine équipée d'un processeur Pentium III à 500Mhtz et 128M de mémoire vive. Pour ces deux implantations, nous avons utilisé des pré-tests modulaires pour le calcul des prédicats. En fait, nous choisissons un premier p (le plus petit possible) ne divisant aucun des dénominateurs des coefficients de $\mathcal{T}$ et, avant chaque calcul de forme normale, nous testons si cette dernière est nulle modulo p. Si tel n'est pas le cas alors le calcul de la forme normale est inutile et nous évitons ainsi des réductions inutiles. Cette stratégie est classique lorsque l'on essaie de calculer une base de Gröbner (voir, par exemple, les versions modulaires des programmes `Gb` et `FGb` de J.-C. Faugère [40]).

TAB. 3.2 – Comparaisons en temps

Idéal	Card(Dec(I))	EstGaloisPur ?	`StrongGenerators`
$I_{8,10}$	16	0.01	0.04
$I_{8,17}$	32	0.4	0.15
$I_{8,26}$	64	0.03	0.06
$I_{8,33}$	96	0.97	49.3
$I_{8,35}$	128	0.129	55.6
$I_{8,36}$	168	6.13	> 700
$I_{8,37}$	168	5.8	> 700
$I_{8,38}$	192	0.4	23.9
$I_{8,39}$	192	2.59	105.16
$I_{8,40}$	192	0.68	17.35
$I_{8,41}$	192	1.66	37.26
$I_{8,46}$	576	15.9	> 700
$I_{9,28}$	648	0.169	3.17
$I_{9,29}$	648	27.22	> 700
$I_{8,47}$	1152	0.05	0.8
$I_{9,31}$	1296	0.81	66.17
$I_{10,43}$	28 800	1.211	> 700
$I_{8,50}$	40 320	0.060	1.719
$I_{12,299}$	1 036 800	10.06	> 700

Comme nous pouvons le voir (les temps notés $>$ *700* sont ceux arrêtés après 700 secondes de calcul), notre algorithme est de meilleur efficacité sur tous ces exemples. En fait, l'efficacité de ces deux implantations dépend surtout des caractéristiques des ensembles $\mathcal{T}$ (tailles des coefficients et arité des polynômes par exemples) qui influencent l'efficacité du calcul de forme normale. Ainsi, on peut s'attendre à une meilleur efficacité de notre algorithme en toute généralité.

Chapitre 4

Factorisation et groupe de Galois d'un polynôme

4.1 Introduction

Soit f un polynôme à coefficients dans k supposé irréductible et séparable, G une représentation symétrique de son groupe de Galois sur k pour une numérotation $\mathcal{N}$ des racines de f (voir Chapitre 1) et α une racine de f dans $\overline{k}$. Dans ce chapitre, nous montrons comment la factorisation de f sur son corps de rupture $k(\alpha)$ fournit des informations sur le groupe G et inversement. De plus, nous donnons la relation entre l'ensemble des représentations symétriques, pour la même numérotation $\mathcal{N}$, des groupes de Galois des facteurs de f sur $k(\alpha)$ et le groupe G. Ce travail peut être vu comme un prolongement de celui de McKay et Soicher (voir [97]) puisque ici nous donnons la représentation symétrique des groupes et non pas seulement leur degré.

Ces informations sont regroupées sous la formes de tables que nous appelons *tables de rupture*. Nous donnerons les moyens algorithmiques permettant de les construire.

Ces informations sont appliquées pour le calcul de polynômes de groupe de Galois donné et à coefficients dans une extension algébrique de k (problème *inverse* effectif de la théorie de Galois). Ceci nous a permis, par exemple, de donner des tests de validité pour le calcul du groupe de Galois d'un polynôme à coefficients dans une extension simple de $\mathbb{Q}$.

Ces tables peuvent être aussi utilisées dans le problème du calcul de l'idéal des relations du polynôme f et de son groupe de Galois sur k. Par exemple, ce sera le cas dans le chapitre 5.

Les résultats de ce chapitre sont issus d'un travail en collaboration avec S. Orange et A. Valibouze et sont présentés dans l'article préliminaire [86]. Ici, nous avons choisi de généraliser au cas d'un corps commutatif k infini quelconque et nous présentons la relation entre l'algorithme de Trager (voir [101]) pour la factorisation dans les extensions et le calcul de résolvante.

4.2 Tables de rupture

Dans cette partie, sont rassemblés tous les résultats théoriques permettant de construire l'objet central de ce chapitre : les *tables de rupture*.

4.2.1 Notations

Dans ce chapitre, nous utiliserons les notations suivantes.
- $\mathcal{T}(n)$ désignera une liste de représentants des classes de conjugaison des groupes transitifs de degré n.
- nT_i est le i-ème groupe de $\mathcal{T}(n)$ conformément à la nomenclature de G. Butler et J. McKay (voir [25]).
- $\ll$ désignera la relation d'ordre sur les groupes transitifs définie par :

$$dT_i \ll mT_j \text{ si } \begin{cases} d < m \\ \text{ou} \\ d = m \text{ et } i \leqslant j \end{cases} .$$

- Pour toute partie $\mathcal{O}$ de l'ensemble $\{1, \ldots, n\}$, nous notons $S_{\mathcal{O}}$ le groupe symétrique de degré $\mathrm{Card}(\mathcal{O})$ agissant sur la partie $\mathcal{O}$.
- Pour G un sous-groupe de S_n et $i \in \{1, \ldots, n\}$, nous noterons $\mathrm{Stab}_G(i)$ le sous-groupe formé par les éléments de G stabilisant i.

4.2.2 Définition de la table de rupture

Fixons G un sous-groupe de S_n et considérons $\mathcal{O}(G)$ l'ensemble des orbites de $\{1, \ldots, n\}$ sous l'action naturelle de $\mathrm{Stab}_G(1)$.

Pour chaque orbite $\mathcal{O} \in \mathcal{O}(G)$, l'action transitive de $\mathrm{Stab}_G(1)$ sur $\mathcal{O}$ s'identifie à celle d'un sous-groupe $G_{\mathcal{O}}$ de $S_{\mathcal{O}}$ appartenant à l'ensemble $\mathcal{T}(\mathrm{Card}(\mathcal{O}))$. Nous noterons $S(G)$ la suite finie des groupes $G_{\mathcal{O}}$ où $\mathcal{O}$ parcourt $\mathcal{O}(G)$ et dans laquelle les groupes sont rangés dans l'ordre $\ll$ croissant. De même, nous noterons $\Delta(G)$ la suite des cardinaux des orbites de $\mathcal{O}(G)$ rangés par ordre croissant.

Soit G' un conjugué du groupe G. Nous avons $S(G) = S(G')$ et donc $\Delta(G) = \Delta(G')$. Ainsi les suites finies $S(G)$ et $\Delta(G)$ sont des *invariants* pour la classe de conjugaison de G.

Définition 4.2.1. La table recensant, pour un entier n fixé, les suites $S(G)$ où G parcourt une liste de représentants des classes de conjugaison des sous-groupes transitifs de S_n (la liste $\mathcal{T}(n)$ par exemple) est appelée *la table de première rupture de degré n.*

À la table de première rupture, nous adjoignons la suite d'entiers $\Delta(G)$. Bien que les entiers de la suite $\Delta(G)$ apparaissent indirectement dans la suite $S(G)$, donner explicitement la suite $\Delta(G)$ dans les tables de rupture facilite leur lecture et leur exploitation.

4.2.3 Construction de la table de rupture

Les tables ont été générées à l'aide du logiciel Magma dans lequel ont été implantées les fonctions calculant les suites $S(G)$ et $\Delta(G)$ décrites au paragraphe 4.2.2. Par exemple, l'implantation suivante permet le calcul de $S(G)$. On en déduira aisément la suite $\Delta(G)$.

```
GroupToSeq:=function(G);
//Etant donne un groupe de permutations G, cette fonction renvoie la
//suite S(G)
```

```
Stab:=Stabilizer(G,1);
OrbsStab:=Orbits(Stab);
TypeGroup:=[];
for o in OrbsStab do
    OrbIm:=OrbitImage(Stab,o);
    NumGroup,DegGroup:=
        TransitiveGroupIdentification(OrbIm);
    TypeGroup[#TypeGroup+1]:=
        [DegGroup,NumGroup];
end for;
return Sort(TypeGroup);
end function;
```

Une base de donnée de la forme $\mathcal{T}(m)$ pour $m \leqslant 23$ est accessible sous Magma (c'est la fonction `TransitiveGroup` qui permet de donner un tel représentant).

La notation exponentielle est utilisée pour représenter les listes d'entiers et les suites de groupes. Par exemple :

- la liste $1,1,1,1,2,3,3,3,4,4$ sera notée $1^4,2,3^3,4^2$;
- la suite $1T_1$, $1T_1$, $2T_1$, $2T_1$, $4T_2$, $4T_3$, $4T_3$ sera notée $1T_1^2$, $2T_1^2$, $4T_2$, $4T_3^2$.

Chaque ligne de la table de rupture de degré n est la ligne d'un groupe $G = nT_i$ de $\mathcal{T}(n)$ et rassemble les informations suivantes :

- la troisième colonne indique le groupe transitif G considéré ; les groupes pairs sont marqués par l'exposant + (par exemple, $6T_{15}^+$) et les résolubles par un astérisque en exposant ; dans cette colonne est aussi inscrit le cardinal du groupe G ;
- la première colonne contient la suite $\Delta(G)$;
- la deuxième colonne contient la suite $S(G)$;

Les lignes de la table de rupture de degré n sont ordonnées comme suit :

- les lignes des groupes G, où G parcourt $\mathcal{T}(n)$, sont ordonnées de haut en bas par ordre lexicographique (induit par l'ordre $\ll$) croissant sur les suites $S(G)$;
- lorsqu'à plusieurs groupes correspondent la même suite $S(G)$, les lignes sont ordonnées selon l'ordre $\ll$ croissant sur les groupes G concernés.

Exemple 4.2.2. Montrons dans cet exemple, comment la table de rupture en degré 3 se construit. En degré 3, il y a deux groupes transitifs $3T_1 = A_3$ et $3T_2 = S_3$. Les éléments de $3T_1$ qui stabilisent l'élément 1 forment le groupe $\mathrm{Stab}_{3T_1}(1)$. L'action de $\mathrm{Stab}_{3T_1}(1)$ sur l'ensemble $\{1,2,3\}$ possède trois orbites. Ainsi les actions de ce groupe sur chacune de ces orbites sont triviales. On obtient donc $\Delta(3T_1) = 1^3$ et $S(3T_1) = \{1T_1, 1T_1, 1T_1\}$. Pour $3T_2$, les orbites de l'action de $\mathrm{Stab}_{3T_2}(1)$ sur l'ensemble $\{1,2,3\}$ sont $\{1\}$ et $\{2,3\}$. L'action de ce groupe sur l'orbite réduit à un point est triviale. Par contre, pour la seconde orbite l'action s'identifie à celle de $2T_1$. Ainsi on obtient, $\Delta(3T_2) = 1,2$ et $S(3T_2) = \{1T_1, 2T_2\}$ et finalement on obtient la table 4.1.

Tab. 4.1: Table de rupture en degré 3

Degrés des facteurs	Groupes de Galois des facteurs	Groupes possibles	Ordre
$[1^3]$	$(1T_1)^3$	$3T_1^{+*}$	$3!\,/\,2$
$[2,\ 1]$	$1T_1,\ 2T_1$	$3T_2^*$	$3!$

De même, on peut on peut obtenir la table de rupture de degré 8 (voir 4.2) qui sera utilisée dans le chapitre 5.

TAB. 4.2: Table de rupture en degré 8

Degrés des facteurs	Groupes de Galois des facteurs	Groupes possibles	Ordre
$[1^8]$	$(1T_1)^8$	$8T_1^*$	8
$[1^8]$	$(1T_1)^8$	$8T_2^{+*}$	8
$[1^8]$	$(1T_1)^8$	$8T_3^{+*}$	8
$[1^8]$	$(1T_1)^8$	$8T_4^{+*}$	8
$[1^8]$	$(1T_1)^8$	$8T_5^{+*}$	8
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_7^*$	16
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_9^{+*}$	16
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_{10}^{+*}$	16
$[2^2,\ 1^4]$	$(1T_1)^4,\ (2T_1)^2$	$8T_{11}^{+*}$	16
$[4,\ 1^4]$	$(1T_1)^4,\ 4T_1^*$	$8T_{17}^*$	32
$[4,\ 1^4]$	$(1T_1)^4,\ 4T_2^{+*}$	$8T_{18}^{+*}$	32
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_6^*$	16
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_8^*$	16
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{16}^*$	32
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{20}^{+*}$	32
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{21}^*$	32
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{22}^{+*}$	32
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{27}^*$	64
$[2^3,\ 1^2]$	$(1T_1)^2,\ (2T_1)^3$	$8T_{31}^*$	64
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_1^*$	$8T_{19}^{+*}$	32
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_2^{+*}$	$8T_{15}^*$	32
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{26}^*$	64
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{28}^*$	64
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{29}^{+*}$	64
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{30}^*$	64
$[4,\ 2,\ 1^2]$	$(1T_1)^2,\ 2T_1,\ 4T_3^*$	$8T_{35}^*$	128
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{12}^{+*}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{13}^{+*}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_1^{+*})^2$	$8T_{14}^{+*}$	24
$[3^2,\ 1^2]$	$(1T_1)^2,\ (3T_2^*)^2$	$8T_{24}^{+*}$	48
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_2^*$	$8T_{23}^*$	48
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_4^{+*}$	$8T_{32}^{+*}$	96
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_6^*$	$8T_{38}^*$	192
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_7^{+*}$	$8T_{39}^{+*}$	192
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_8^*$	$8T_{40}^*$	192
$[6,\ 1^2]$	$(1T_1)^2,\ 6T_{11}^*$	$8T_{44}^*$	384
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{33}^{+*}$	96
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{34}^{+*}$	96
$[4,\ 3,\ 1]$	$1T_1,\ 3T_1^{+*},\ 4T_4^{+*}$	$8T_{42}^{+*}$	288
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{41}^{+*}$	192
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{45}^{+*}$	576
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{46}^*$	576
$[4,\ 3,\ 1]$	$1T_1,\ 3T_2^*,\ 4T_5^*$	$8T_{47}^*$	1152
$[7,\ 1]$	$1T_1,\ 7T_1^{+*}$	$8T_{25}^{+*}$	56
$[7,\ 1]$	$1T_1,\ 7T_3^{+*}$	$8T_{36}^{+*}$	168
$[7,\ 1]$	$1T_1,\ 7T_3^{+*}$	$8T_{37}^{+}$	168
$[7,\ 1]$	$1T_1,\ 7T_4^*$	$8T_{43}$	336
$[7,\ 1]$	$1T_1,\ 7T_5^+$	$8T_{48}^+$	1344
$[7,\ 1]$	$1T_1,\ 7T_6^+$	$8T_{49}^+$	$8!\,/\,2$
$[7,\ 1]$	$1T_1,\ 7T_7$	$8T_{50}$	$8!$

Lorsqu'un groupe G de $\mathcal{T}(n)$ est une représentation symétrique du groupe de Galois d'un polynôme irréductible de degré n, il est naturel de s'intéresser à la correspondance des propriétés de G (ou plus exactement de sa classe de conjugaison) avec celles de f. Par exemple, les *matrices de partitions* (ou celles *de groupes*) établissent un lien entre une paire (G, H), où $H \subset S_n$, et la résolvante de Lagrange associée à f et selon un certain invariant (voir Paragraphe 2.3). Plus exactement, ces tables et une telle résolvante R permettent d'obtenir des informations sur le groupe de Galois de f à partir des degrés des facteurs R ou de leur groupe de Galois (voir [9] et [105]).

Dans la partie suivante nous allons étudier l'utilisation des tables de rupture pour obtenir ce type de correspondance.

4.3 Tables de rupture et groupes de Galois

Dans cette partie on considère un polynôme irréductible f à coefficients dans k de degré n et α une racine quelconque de f dans une clôture algébrique de k. Nous allons étudier le lien entre les propriétés des facteurs de f sur $k(\alpha)$ et le groupe de Galois de f.

4.3.1 Degrés et groupes de Galois des facteurs de rupture

Notons $g_1(\alpha, x) = x - \alpha$,$g_2(\alpha, x)$, ..., $g_s(\alpha, x)$ les s facteurs de f (avec $s > 1$) sur son corps de rupture $K = k(\alpha)$.

Définition 4.3.1. Les polynômes $g_2, \ldots, g_s$ de f sont appelés les *facteurs de rupture* du polynôme f. Les facteurs de rupture $g_2, \ldots, g_s$ seront rangés dans l'ordre croissant de leurs degrés en x.

Pour tout $i \in [\![1, s]\!]$, le groupe de Galois de g_i sur K est conjugué à un groupe G_i de $\mathcal{T}(deg_x(g_i))$. Nous complétons l'ordre des polynômes g_i, en décidant que $g_i < g_j$ dès que $G_i \ll G_j$.

La suite $\Delta(f) = deg_x(g_2), \ldots, deg_x(g_s)$ sera appelée *suite des degrés de rupture de* f et la suite $S(f) = G_1, \ldots, G_s$ sera appelée *suite des groupes de rupture de* f (notons que G_1 est toujours le groupe réduit à l'identité).

La théorie de Galois classique établit naturellement la proposition suivante :

Proposition 4.3.2. *Nous avons*

$$S(f) = S(G_f)$$

et par conséquent, $\Delta(G_f) = 1, \Delta(f)$. *En d'autres termes, les groupes de Galois sur* K *des facteurs de rupture du polynôme* f *sont les groupes (à conjugaison près) de la suite* $S(G_f)$ *qui ne dépend que du groupe de Galois du polynôme* f *sur* k.

Démonstration. Soit M une extension algébrique de k et g un facteur irréductible de f sur M. Notons $\mathcal{O}_f$ (resp. $\mathcal{O}_g$) l'ensemble des racines de f (resp. de g) dans une clôture algébrique de k contenant M.

Comme g est irréductible sur M, la théorie classique de Galois (voir [29] par exemple) assure le fait que l'ensemble $\mathcal{O}_g$ est l'orbite d'une racine de g sous l'action

$$Aut_M(M(\mathcal{O}_f)) \times \mathcal{O}_f \longrightarrow \mathcal{O}_f\,.$$

Comme tout automorphisme de $Aut_M(M(\mathcal{O}_g))$ peut être relevé en un automorphisme de $Aut_M(M(\mathcal{O}_f))$ l'homomorphisme de restriction

$$\begin{array}{ccc} Aut_M(M(\mathcal{O}_f)) & \longrightarrow & Aut_M(M(\mathcal{O}_g)) \\ \sigma & \longmapsto & \sigma_{|_{M(\mathcal{O}_g)}} \end{array}$$

est surjectif.

Ainsi, l'action de $Aut_M(M(\mathcal{O}_f))$ sur $\mathcal{O}_g$ est identique à celle de $Aut_M(M(\mathcal{O}_g))$ sur $\mathcal{O}_g$. Cette action peut être représentée de manière fidèle dans le groupe symétrique $S_{|\mathcal{O}_g|}$ (voir le paragraphe 1.1) et est alors le groupe de Galois de g sur M.

Lorsque $M = k(\alpha)$, ce résultat montre que G_g est l'un des groupes de $S(G)$. Réciproquement, un groupe de $S(G)$ correspond à une unique orbite de l'action de $\mathrm{Stab}_G(1)$ sur $\{1, \ldots, n\}$ qui est un sous ensemble $\mathcal{O}$ de $\mathcal{O}_f$. La théorie de Galois classique assure que l'ensemble $\mathcal{O}$ est celui de tous les conjugués (sur K) d'un de ses éléments β. Ainsi, le polynôme minimal de β sur K est un facteur irréductible de f dont le groupe de Galois s'identifiera à la représentation symétrique de l'action de $\mathrm{Stab}_G(1)$ sur $\mathcal{O}$. L'égalité $S(f) = S(G_f)$ suit. □

La fonction qui suit est une implantation en MAGMA qui permet le calcul de $S(f)$.

```
PolToSeq:=function(f);
//Etant donne un polynome f,
//cette fonction renvoie la suite S_1,S(f).
//Elle teste aussi la factorisation de f.

N:=NumberField(f);
PRN:=PolynomialRing(N);
ff:=Factorization(PRN!f);
TypeGroup:=[];
for f in ff do
    NumGroup,DegGroup:=
        TransitiveGroupIdentification(GaloisGroup(f[1]));
    TypeGroup[#TypeGroup+1]:=
        [DegGroup,NumGroup];
end for;
/* Test de factorisation */
g:=&*[f[1] : f in ff];
if g ne f then
    print "*** ERROR FACT ***";
    print f;
    print "******************";
end if;
return Sort(TypeGroup);
end function;
```

La proposition 4.3.2 met donc en lien les informations contenues dans la table de rupture de degré donné n et le degré, ainsi que la représentation symétrique du groupe de Galois, de chacun des facteurs irréductibles de f sur K. Dans la partie qui suit nous allons mettre en rapport ces informations avec des résultats sur les résolvantes.

4.3.2 La factorisation dans le corps de rupture et calcul de résolvante

La factorisation de f sur son corps de rupture $K = k(\alpha)$ peut être donnée en utilisant l'algorithme de Trager (voir [101] et [27, Algorithm 3.6.4]). D'après S. Landau (voir [64]), lorsque $k = \mathbb{Q}$, la complexité de cet algorithme est de l'ordre de

$$O(n^{16+\epsilon} \log^2 |f|_2 \log^{2+\epsilon}(|f|_2^{n+1} n^{3n}))$$

où $|f|_2$ est la norme euclidienne de f vu comme vecteur de ses coefficients (voir [77]). Comme $x - \alpha$ divise f sur K on ne s'intéresse qu'au polynôme $h = f/(x - \alpha)$. Dans cet algorithme on calcule la norme $N_m(h)$ sur K d'une transformation $h(x - m\alpha)$ de Tschirnhaus de h ($m \in k$). Le polynôme N_m est à coefficients dans le corps k et est donné par :

$$N_m(h) = \prod_{i=1}^{n} h(x - m\alpha_i)\,. \tag{4.1}$$

Comme le corps k est infini on peut toujours trouver un élément m de k tel que $N_m(h)$ soit séparable. Supposons qu'il en soit ainsi, $N_m(h)$ est de degré $n(n-1)$ et ses facteurs permettent de trouver les facteurs de f sur K. En effet, d'après l'algorithme de Trager, si l'on note $N_1, \ldots, N_t$ les facteurs de N_m on a :

$$\begin{aligned} t &= s - 1 \\ g_i(x - m\alpha) &= \text{pgcd}(N_{i-1}, f(x + m\alpha)) \text{ sur } K \text{ pour } i \in [\![2, s]\!] \\ n \deg(g_i) &= \deg(N_i) \end{aligned}$$

Ainsi, la connaissance des degrés des facteurs de la norme $N_m(h)$ est identique à la connaissance des degrés des facteurs de f sur K. En fait cette norme est aussi une résolvante.

Proposition 4.3.3. *Soit $\Theta = -x_1 + mx_2$ un $S_1 \times S_1 \times S_{n-2}$ invariant S_n-relatif. La résolvante absolue L de f selon Θ est égale à la norme $N_m(h)$.*

Démonstration. Nous avons la suite d'égalités

$$\begin{aligned} N_m(h) &= \prod_{i=1}^{n} \frac{f(x - m\alpha)}{(x - (m+1)\alpha)} \\ &= \prod_{i=1}^{n} \prod_{j \neq i} ((x - m\alpha_i) - \alpha_j) \\ &= \prod_{o \in S_n.\Theta} (x - o(\underline{\alpha})) \\ &= \mathcal{L}_{\Theta}^{S_n \cdot \underline{\alpha}}(x) \end{aligned}$$

et le résultat suit. □

L'étude des degrés des facteurs irréductibles de cette résolvante, tout comme la factorisation de f sur K, permet de donner une liste de sous-groupes de S_n susceptibles d'être une représentation symétrique du groupe de Galois de f. Ce sont McKay et

Soicher qui proposèrent les premiers l'étude de ces résolvantes linéaires dans [97]. Ici, en plus de l'étude des degrés nous étudions aussi les groupes de Galois des facteurs et nous verrons comment utiliser toutes ces informations dans le cadre plus général du calcul d'un idéal des relations de f.

Ce sont ces applications des tables de ruptures que nous détaillons dans la partie suivante.

4.4 Applications

Dans cette partie, nous donnons des applications exploitant les tables de rupture.

4.4.1 Détermination du groupe de Galois

Nous savons, d'après la proposition 4.3.2, que le groupe de Galois G_f figure parmi les groupes H de l'ensemble $\mathcal{T}(n)$ vérifiant $S(H) = S(f)$. Nous appelons *groupes candidats* ceux vérifiant $\Delta(H) = 1, \Delta(f)$.

Une fois la factorisation de f sur K effectuée, la liste $\Delta(f)$ est connue.

S'il n'existe qu'un seul groupe candidat H ou si un seul des groupes H candidats vérifie $S(f) = S(H)$ alors nous savons que $H = G_f$.

Pour déterminer, parmi les groupes candidats, le ou les groupes H vérifiant $S(f) = S(H)$, il n'est pas toujours nécessaire de calculer toute la suite $S(f)$: le calcul de certains des groupes de Galois des facteurs de rupture de f peuvent suffire. D'autres méthodes efficaces peuvent venir compléter cette recherche. Par exemple, en factorisant f modulo un entier premier ne divisant pas son discriminant (voir [25] et [74]) ou en utilisant la parité du groupe de Galois de f.

Les exemples ci-après font référence aux tables que nous donnons dans les annexes.

Exemple 4.4.1. Lorsque le groupe de Galois G_f est l'un des groupes $6T_5$, $7T_4$, $10T_6$, $13T_5^+$, $14T_8$, $14T_{16}$, $15T_2$, $15T_6^+$, $15T_7$, il suffit de calculer $\Delta(f)$ pour le déterminer.

Exemple 4.4.2. Si un polynôme f de degré 15 vérifie $\Delta(f) = 2, 4, 8$ alors, d'après la table de rupture de degré 15, nous savons que son groupe de Galois est l'un des groupes $15T_{10}^+$, $15T_{11}$, $15T_{22}^+$, $15T_{23}$ ou $15T_{29}$. Le calcul du groupe de Galois sur $k(\alpha)$ du facteur de rupture de degré 4 suffit à la détermination du groupe de Galois de f.

Exemple 4.4.3. Si un polynôme f de degré 15 vérifie $\Delta(f) = 4, 5^2$ et si le discriminant de l'un de ses facteurs de rupture de degré 5 est un carré dans le corps de rupture $k(\alpha)$ alors le groupe de Galois de f est $15T_{92}^+$.

Exemple 4.4.4. Si un polynôme f de degré 9 vérifie $\Delta(f) = 2, 3^2$, la liste des groupes candidats est $9T_{13}$, $9T_{22}$, $9T_{25}^+$, $9T_{28}$.

Exemple 4.4.5. Si le polynôme f est de degré 16 et $\Delta(f) = 1^7, 8$, il y a alors trois groupes candidats à être le groupe de Galois de f. Si, de plus, le calcul de son discriminant montre que le groupe de Galois de ce polynôme est impair alors, d'après la table de rupture en degré 16, $G_f = 16T_{289}$.

Exemple 4.4.6. Si f est de degré 15 et $\Delta(f) = 2, 3^4$ alors f admet pour groupe de Galois G_f l'un des quatre groupes suivants : $15T_{33}$, $15T_{44}$, $15T_{71}^+$ et $15T_{81}$ et $S(f)$ ne peut les distinguer. Si G_f est impair, il reste 3 groupes possibles. Donc les tables de rupture ne sont pas suffisantes à la détermination de tous les groupes de Galois.

4.4.2 Factorisation des polynômes sur leur corps de rupture

La table de rupture pour un degré donné n permet de connaître l'ensemble $\Delta(n)$ des listes de degrés possibles des facteurs de rupture d'un polynôme irréductible f de degré n. Ainsi, lors de la factorisation de f sur son corps de rupture, la recherche des facteurs possibles peut se limiter à ceux dont la liste des degrés est dans $\Delta(n)$. De cette manière, on peut éviter des calculs inutiles dans les algorithmes de factorisation classiques en utilisant un algorithme interactif (voir [73] par exemple).

Exemple 4.4.7. *A priori*, le cardinal de l'ensemble $\Delta(7)$ est majoré par le nombre de partions de l'entier 6, c'est-à-dire 11. La table de première rupture en degré 7 nous renseigne sur le cardinal exact de cet ensemble $\mathrm{Card}(\Delta(7)) = 4$. Ainsi on peut éviter un nombre considérable de recombinaisons de facteurs probables dans un algorithme de factorisation modulaire.

Bien sûr, si l'on connait des informations sur le groupe de Galois de f on peut se limiter à un sous-ensemble de $\Delta(n)$.

4.4.3 Obtention de polynômes de groupe de Galois donné dans une extension algébrique

Soit $r \in \mathbb{N}$ et H un sous-groupe transitif de S_r. Les tables de rupture permettent aussi la recherche de polynômes à coefficients dans une extension algébrique ayant pour groupe de Galois le groupe H donné.

Supposons que, pour un entier n, il existe un sous-groupe G de S_n tel que le groupe H apparaisse dans la suite $S(G)$.

Supposons que l'on dispose d'un polynôme f de $k[x]$ de groupe de Galois sur k isomorphe au groupe G. Actuellement, lorsque $n \leqslant 15$, la base de donnée `galpols` de Magma comporte un tel polynôme pour $k = \mathbb{Q}$.

Soit α une racine f. Nous savons que, parmi les facteurs de rupture du polynôme f, il existe au moins un polynôme h de groupe de Galois H sur $K = k(\alpha)$.

Remarque 4.4.8. Si, dans la suite $S(G)$, il existe au moins un sous-groupe de S_r distinct de H, il s'agit alors de déterminer lequel des facteurs de rupture du polynôme f possède H comme groupe de Galois. La méthode de détermination du groupe de Galois par des calculs algébriques de résolvantes (voir par exemples, [19], [43], [48], [97] ou [9]) est alors la méthode la plus fiable pour cette détermination.

Exemple 4.4.9. Un polynôme de groupe de Galois $10T_{39}$ sur une extension monogène de $\mathbb{Q}$ peut être obtenu à partir d'un polynôme de groupe de Galois $12T_{293}$. En effet, la table de rupture en degré 12 montre que :

1. tout polynôme $f \in k[x]$ de groupe de Galois $12T_{293}$ sur k se factorise dans un de ses corps de rupture K en deux facteurs linéaires et un facteur de degré 10 ;
2. le facteur de degré 10 possède $10T_{39}$ comme groupe de Galois sur K.

Le polynôme suivant est celui de groupe de Galois $12T_{293}$ présent dans la base de donnée `galpols` de Magma.

$$f(x) = x^{12} - 13x^{10} + 65x^8 - 156x^6 + 181x^4 - 86x^2 + 7.$$

Son facteur de rupture de degré 10 :

$$\begin{aligned} h(x) &= x^{10} + x^8\alpha^2 - 13x^8 + \alpha^4x^6 - 13\alpha^2x^6 + 65x^6 + \alpha^6x^4 - 13\alpha^4x^4 \\ &\quad +65\alpha^2x^4 - 156x^4 + \alpha^8x^2 - 13\alpha^6x^2 + 65\alpha^4x^2 - 156\alpha^2x^2 \\ &\quad +181x^2 + \alpha^{10} - 13\alpha^8 + 65\alpha^6 - 156x^4 + 181\alpha^2 - 86 \end{aligned}$$

possède $10T_{39}$ comme groupe de Galois sur $\mathbb{Q}(\alpha)$.

Des polynômes ainsi construits sont utilisables pour la validation de programmes de calculs de groupes de Galois à coefficients dans des extensions algébriques. Le logiciel de calcul formel MAGMA est le seul permettant le calcul du groupe de Galois d'un polynôme à coefficient dans une extension simple de $\mathbb{Q}$ ou $\mathbb{F}_p[x]$. Pour pouvoir valider (en partie) de tels calculs nous avons utilisé ces tables. Pour ce faire on peut utiliser les fonctions présentées plus haut.

Nous avons réalisé des tests à l'aide de la base de données de J. Klüners et G. Malle (voir [58]) et nous avons mis à jour plusieurs bogues dans la version 2.11-10 de MAGMA. Nous avons depuis communiqué ces erreurs à l'équipe responsable du développement de ce logiciel qui reste extraordinaire. Par exemple, nous avons pour un des polynômes de plus petit degré mettant à jour un de ces bogues :

```
> PR<x>:=PolynomialRing(Rationals());
> f:=x^6 + 11*x^4 - 42*x^3 + 85*x^2 - 12*x + 3;
>
> GroupToSeq(GaloisGroup(f));
[
    [ 1, 1 ],
    [ 1, 1 ],
    [ 4, 1 ]
]
> PolToSeq(f);
[
    [ 1, 1 ],
    [ 1, 1 ],
    [ 4, 5 ]
]
```

Ainsi, l'erreur est sur le facteur g de degré 4 de f sur $\mathbb{Q}(\alpha)$ donné par :

$$\begin{aligned} g(x) &= 1/1117(1117x^4 + (125\alpha^5 + 22\alpha^4 + 1361\alpha^3 \\ &\quad -4796\alpha^2 + 10326\alpha + 1068)x^3 + (386\alpha^5 + 59\alpha^4 \\ &\quad +4310\alpha^3 - 15096\alpha^2 + 32262\alpha + 10277)x^2 \\ &\quad +(2007\alpha^5 + 246\alpha^4 + 23139\alpha^3 - 80436\alpha^2 \\ &\quad +170298\alpha - 46548)x + (-522\alpha^5 - 74\alpha^4 \\ &\quad -5898\alpha^3 + 20600\alpha^2 - 43872\alpha + 571) \end{aligned}$$

Le groupe de Galois calculé pour g est $4T_5$, celui attendu était $4T_1$.

4.4.4 Détermination d'un idéal des relations d'un polynôme

Nous verrons au chapitre 5 comment les informations obtenues après la factorisation du polynôme f sur son corps de rupture et à l'aide de la table de rupture de degré n, peuvent aider à la construction de l'idéal des relations de f.

Chapitre 5

Méthode hybride pour le calcul de l'idéal des relations

5.1 Introduction

Ce chapitre est une nouvelle rédaction faite en collaboration avec S. Orange et A. Valibouze des résultats présentés dans [85]. Cette nouvelle rédaction est à la fois une simplification et une algébrisation du rapport de recherche cité ci-avant.

Soit f un polynôme irréductible séparable de degré n à coefficients dans un corps k supposé infini. Dans ce chapitre, nous proposons une nouvelle méthode pour le calcul d'un ensemble triangulaire de générateurs d'un idéal des relations I de f et de son groupe de décomposition $\mathrm{Dec}(I)$ (ce groupe est alors une représentation symétrique du groupe de Galois de f).

De manière générale, cette méthode peut être décrite à l'aide de trois étapes E_1, E_2, E_3 définies comme suit. *Soient A_1 et A_2 deux algorithmes permettant le calcul d'une base triangulaire de I à partir de f. Les s_1 premières étapes de A_1 sont utilisées pour débuter le calcul et les s_2 dernières étapes de A_2 pour le terminer. De plus, les informations galoisiennes (nature du groupe de Galois de f) obtenues après les s_1 premières étapes de A_1 sont utilisées pour éviter des calculs, c'est-à-dire diminuer s_2 au maximum. Ainsi, E_1 est le calcul des s_1 premières étapes de A_1, E_2 est le passage de l'algorithme A_1 à A_2 en essayant de minimiser s_2 et E_3 est la terminaison du calcul à l'aide de A_2.* L'étape E_2 se révèle être le point délicat de cette méthode. En effet, il n'est pas forcément évident de récupérer après E_1, les entrées nécessaires pour débuter l'algorithme A_2.

Dans ce chapitre, nous étudions une spécification particulière de cette méthode générale. Ici, l'algorithme A_1 est l'algorithme de factorisation dans les extensions successives, A_2 est l'algorithme `GaloisIdéal` et nous n'utilisons que la première étape ($s_1 = 1$) de l'algorithme A_1 (c'est-à-dire la factorisation de f sur son corps de rupture). Les informations galoisiennes sont obtenues après E_1 en utilisant les tables de première rupture (voir Chapitre 4) et se résument en un ensemble de groupes de permutations susceptibles d'être le groupe de Galois de f (à conjugaison près).

Quel que soit l'entier s_2, les entrées pour débuter E_3 sont : un idéal de Galois de f ainsi que l'un de ses injecteurs. Nous verrons qu'une fois E_1 passée il est facile de construire un idéal de Galois I_1 de f (voir Paragraphe 5.2). Identifier un injecteur de I_1 est nettement moins facile. Il faut faire une étude préliminaire en fonction du degré

de f. En effet, les informations galoisiennes obtenues après E_1 (un ensemble de groupes de permutations contenant le groupe de Galois de f) ne sont données qu'à un certain nombre de conjugaisons près et pour construire un injecteur de I_1 il faut, le plus souvent, identifier un plus petit nombre de ces conjugués. Nous montrerons donc comment établir des critères qui permettent de reconnaître ces groupes (voir Paragraphe 5.4).

Dans le paragraphe 5.5, nous présentons des techniques qui, à partir d'informations partielles sur le groupe de Galois de f obtenues après E_1, permettent d'éviter un certain nombre d'étapes de l'algorithme A_2.

Nous appliquons cette étude dans le cas d'un polynôme irréductible de degré 8 et de groupe de Galois non 2-transitif (voir Paragraphe 5.7). Nous donnons ensuite des résultats expérimentaux obtenus à l'aide de cette méthode.

Il est à noter que A. Valibouze expose, dans [108], un exemple de deux autres spécifications de cette méthode générale. Si nous voulions généraliser cet exemple en un algorithme, il faudrait, comme ici, faire une étude péalable cas par cas.

5.2 Idéal de rupture et idéal induit

Dans ce paragraphe nous allons construire, à partir de la factorisation de f sur son corps de rupture, un idéal de Galois de f sur k.

Soit $f_2, \ldots, f_r$ les facteurs de rupture de f sur $k(\alpha_1)$ (voir Définition 4.3.1) et $\Delta(f) = d_2, \ldots, d_r$ les degrés respectifs de ces polynômes. Soit $\underline{\alpha}$ un n-uplet de racines de f dans $\overline{k}$ numéroté de telle manière que $\alpha_{d_{i-1}+1}, \ldots, \alpha_{d_i}$ soient les racines de f_i.

Pour tout $i \in [\![1, n]\!]$, l'anneau de polynômes $k(\alpha_1)[x_{d_{i-1}+1}, \ldots, x_{d_{i-1}+1+d_i}]$ est noté $\mathcal{A}_i$ (où $d_0 = 1$ par convention) muni de l'ordre lexicographique induit par $x_1 < x_2 < \ldots < x_n$. Soit $T_i(\alpha_1)$ l'ensemble triangulaire formé par les modules de Cauchy du facteur f_i dans l'anneau de polynômes $\mathcal{A}_i$.

D'après le théorème 2.4.2 l'idéal de $k(\alpha_1)[x_1, \ldots, x_n]$ engendré par l'ensemble triangulaire :

$$\{x_1 - \alpha_1\} \cup T_{f_1}(x_1) \cup \cdots \cup T_{f_r}(x_1)$$

est un $\underline{\alpha}$-idéal de Galois sur $k(\alpha_1)$. De plus, son groupe de décomposition est son injecteur et est le produit direct de groupes symétriques

$$S_{1,\Delta(f)} = S_1 \times S_{d_2} \times \ldots \times S_{d_r}\,.$$

Définition 5.2.1. L'idéal de Galois I_r de $k(\alpha_1)[x_1, \ldots, x_n]$ inclus dans $Id_{k(\alpha_1)}(\underline{\alpha})$ et d'injecteur $S_{1,\Delta(f)}$ est appelé un *idéal de rupture de* f.

Exemple 5.2.2. Dans cet exemple, k désigne le corps des rationnels $\mathbb{Q}$. Soit le polynôme $f = x^8 - x^6 - x^4 + x^2 + 1$, irréductible sur k. Il se factorise sur son corps de rupture $k(\alpha_1)$ en :

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

et $\Delta(f) = 1, 2, 4$. D'après la table de rupture en degré 8, $\mathrm{Gal}_{\mathbb{Q}}(f)$ est un sous-groupe de $8T_{35}$. Les modules de Cauchy des facteurs de rupture de degré 2 et de degré 4 sont

respectivement les deux ensembles de polynômes :

$$\begin{aligned} T_1(\alpha_1) &= \{ \quad x_3^2 - \alpha_1^6 + \alpha_1^4 + \alpha_1^2 - 1, \\ &\qquad x_4 + x_3\} \text{ dans } k(\alpha_1)[x_3, x_4] \text{ et} \\ T_2(\alpha_1) &= \{ \quad x_5^4 + (\alpha_1^6 - \alpha_1^4)x_5^2 - 1, \\ &\qquad x_6^3 + x_5^3 + x_5^2 x_6 + x_5 x_6^2 + (\alpha_1^6 - \alpha_1^4)x_5 + (\alpha_1^6 - \alpha_1^4)x_6, \\ &\qquad x_7^2 + x_5^2 + x_5 x_6 + x_5 x_7 + x_6^2 + x_6 x_7 + \alpha_1^6 - \alpha_1^4, \\ &\qquad x_8 + x_7 + x_6 + x_5\} \text{ dans } k(\alpha_1)[x_5, x_6, x_7, x_8]\,. \end{aligned}$$

Il n'existe qu'un idéal de rupture de f d'injecteur $S_{1^2,2,4}$ (inclus dans l'idéal $Id_{k(\alpha_1)}(\underline{\alpha})$, où $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ est ordonné correctement) ; il est donc engendré par l'ensemble triangulaire T :

$$T = \{x_1 - \alpha_1\} \cup \{x_2 + x_1\} \cup T_1(x_1) \cup T_2(x_1)\,.$$

Remarque 5.2.3. À partir des facteurs de rupture de f, peuvent être construits autant d'idéaux de rupture que de permutations de S_r laissant la suite $\Delta(f)$ invariante (l'ordre des facteurs de rupture n'est pas unique dès que deux d'entre eux ont le même degré). Néanmoins, tous admettent $S_{1,\Delta(f)}$ comme injecteur.

Notations 5.2.4. Dans toute la suite de ce chapitre $\underline{\alpha}$ sera un élément de $V(I_1)$ où I_1 désignera un idéal de $k(\alpha_1)[x_1, \ldots, x_n]$ vérifiant :

$$I_r \subset I_1 \subset Id_{k(\alpha_1)}(\underline{\alpha}) \tag{5.1}$$

L'idéal I_1 est un idéal de Galois de f (voir Proposition 2.2.5). Nous supposons qu'il possède pour injecteur L son groupe de décomposition. D'après la proposition 2.2.22, l'idéal I_1 est engendré par un ensemble triangulaire

$$\{x_1 - \alpha_1, F_2(x_1, x_2), \ldots, F_n(x_1, \ldots, x_n)\}$$

où les polynômes $F_2, \ldots, F_n$ sont à coefficients dans k.

Pour tout $\sigma \in S_n$ et K une extension algébrique de k, nous avons $\sigma.Id_K(\underline{\alpha}) = Id_K(\sigma^{-1}.\underline{\alpha})$. Par définition du groupe de décomposition et puisque $V(I_1) = L.\underline{\alpha}$, pour tout $\underline{\beta} \in V(I_1)$ (nécessairement $\beta_1 = \alpha_1$), les inclusions (5.1) s'étendent à $\underline{\beta}$:

$$I_r \subset I_1 \subset Id_{k(\beta_1)}(\underline{\beta})\,. \tag{5.2}$$

De l'idéal I_1 se déduit naturellement un idéal de Galois de f de l'anneau $k[x_1, \ldots, x_n]$ (voir Corollaire 2.2.6) :

Définition 5.2.5. L'*idéal induit de l'idéal* I_1 est l'idéal I de Galois de f sur k défini par :

$$I = I_1 \cap k[x_1, \ldots, x_n]\,.$$

Par extension, nous dirons qu'un idéal de Galois de f est *induit* s'il satisfait la condition précédente pour un idéal de Galois I_1 contenant un idéal de rupture de f.

Notations 5.2.6. Nous notons $\mathcal{M}(I)$ l'ensemble des idéaux maximaux contenant I.

Proposition 5.2.7. *Pour tout $\mathcal{M} \in \mathcal{M}(I)$,*

$$\mathcal{M}(I) = \{\sigma.\mathcal{M} \mid \sigma \in L\}.$$

Autrement formulé :

$$\mathcal{M}(I) = \{Id_k(\underline{\beta}) \mid \underline{\beta} \in V(I_1)\} .$$

Démonstration. La proposition est démontrée par la suite d'égalités suivantes.

$$\begin{aligned} I &= I_1 \cap k[x_1, \ldots, x_n] = Id_{k(\alpha_1)}(V(I_1)) \cap k[x_1, \ldots, x_n] \\ &= Id_k(V(I_1)) = \bigcap_{\underline{\beta} \in V(I_1)} Id_k(\underline{\beta}) = \bigcap_{\sigma \in L} \sigma.Id_k(\underline{\alpha}) . \end{aligned}$$

□

Proposition 5.2.8. *Tout $\mathcal{M} \in \mathcal{M}(I)$ vérifie :*
(1) $\mathrm{Dec}(\mathcal{M})_{\{1\}} \subset L \subset S_{1,\Delta(f)}$ *;*
(2) $\mathrm{Orb}(\mathrm{Dec}(\mathcal{M})_{\{1\}}) = \mathrm{Orb}(L) = \mathrm{Orb}(S_{1,\Delta(f)})$.

Démonstration. Nous pouvons supposer que $\mathcal{M} = Id_k(\underline{\alpha})$; i.e. $\mathrm{Dec}(\mathcal{M}) = \mathrm{Gal}_k(\underline{\alpha})$. Nous obtenons les inclusions inverses des injecteurs (relatifs à $\underline{\alpha}$) des idéaux de (5.2) :

$$\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha}) \subset L \subset S_{1,\Delta(f)} . \quad (*)$$

Des identités $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha}) = \mathrm{Gal}_k(\underline{\alpha})_{\{1\}}$ et $\mathrm{Orb}(\mathrm{Gal}_k(\underline{\beta})_{\{1\}}) = \mathrm{Orb}(S_{1,\Delta(f)})$ (par définition de $\Delta(f)$), nous en déduisons, avec $(*)$, les assertions (1) et (2) de la proposition.

□

Nous allons maintenant donner une décomposition de l'idéal I sur le corps $k(\underline{\alpha})$:

Proposition 5.2.9. *Soit $\mathcal{M} \in \mathcal{M}(I)$ et soient $\tau_1, \ldots, \tau_n$, des permutations du groupe* $\mathrm{Dec}(\mathcal{M})$ *telles que, pour tout $i \in [\![1, n]\!]$, $\tau_i(1) = i$. Nous avons :*

$$k(\underline{\alpha}) \otimes_k I = \bigcap_{i=1}^{n} \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1) .$$

Démonstration. Nous pouvons supposer que $\mathcal{M} = Id_k(\underline{\alpha})$ car pour tout $\underline{\beta} \in V(I_1)$, $\beta_1 = \alpha_1$. Notons $V = L.\underline{\alpha}$ la variété de I_1 et posons $W = \mathrm{Gal}_k(\underline{\alpha}).V$. Comme V est stable par $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha})$ (voir Proposition 2.2.15) et que $\tau_1, \ldots, \tau_n$ est une transversale à gauche de $\mathrm{Gal}_k(\underline{\alpha})$ modulo $\mathrm{Gal}_{k(\alpha_1)}(\underline{\alpha})$, nous avons

$$W = \bigcup_{i \in [\![1,n]\!]} \tau_i.V .$$

Par définitionle corps $K(V)$ le corps $K(V)$, W est la variété de l'idéal de Galois $Id_k(V)$ (voir Proposition 2.2.15). Ainsi,

$$Id_k(W) = Id_k(V) = I_1 \cap k[x_1, \ldots, x_n]$$

et donc, comme W est une variété définie sur k (i.e. son idéal possède un système de générateurs à coefficients dans k)

$$Id_{k(\underline{\alpha})}(W) = k(\underline{\alpha}) \otimes_k (I_1 \cap k[x_1, \ldots, x_n]) .$$

Par définition de I, il vient

$$k(\underline{\alpha}) \otimes_k I = k(\underline{\alpha}) \otimes_k (I_1 \cap k[x_1, \ldots, x_n]) = Id_{k(\underline{\alpha})}(W) = \bigcap_{i \in [\![1,n]\!]} Id_{k(\underline{\alpha})}(\tau_i.V)$$

Or, d'après le lemme 2.2.14, nous avons les égalités

$$\forall i \in [\![1, n]\!],\ Id_{k(\underline{\alpha})}(\tau_i.V) = \overline{\tau_i}(Id_{k(\underline{\alpha})}(V)) = \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1) ,$$

d'où le résultat. □

De cette proposition, nous déduisons un ensemble de générateurs de l'idéal induit I :

Corollaire 5.2.10. *Posons $F_1 = f$ et $\mathcal{A} = k(\alpha_1)[x_1, \ldots, x_n]$. L'idéal I induit de $I_1 = \langle x_1 - \alpha_1, F_2, F_3, \ldots, F_n \rangle_{\mathcal{A}}$ est engendré par l'ensemble :*

$$\mathcal{S} = \{F_1(x_1), F_2(x_1, x_2), \ldots, F_n(x_1, \ldots, x_n)\}$$

qui est triangulaire.

Démonstration. Comme les polynômes $F_2, \ldots, F_n$ sont à coefficients dans k, d'après la proposition 5.2.9, nous avons :

$$\begin{aligned} k(\underline{\alpha}) \otimes_k I &= \bigcap_{i=1}^{n} \langle x_1 - \overline{\tau_i}(\alpha_1) \rangle_{\mathcal{A}} + \langle F_2, \ldots, F_n \rangle_{\mathcal{A}} \\ &= \prod_{i=1}^{n} \langle x_1 - \alpha_i \rangle_{\mathcal{A}} + \langle F_2, \ldots, F_n \rangle_{\mathcal{A}} \\ &= \langle F_1(x_1), F_2, \ldots, F_n \rangle_{\mathcal{A}} . \end{aligned}$$

Nous avons donc démontré que l'ensemble $\mathcal{S}$ engendre I et comme $\{x_1 - \alpha_1, F_2, F_3, \ldots, F_n\}$ est un ensemble triangulaire il en est de même pour $\mathcal{S}$. □

Étant donné $L = \mathrm{Inj}(I_1, \underline{\alpha})$, l'objectif est maintenant de calculer un injecteur de l'idéal I induit de I_1 (voir Paragraphe 5.4) pour le cas où ce n'est pas le groupe de décomposition de I. Pour cela, nous ferons appel aux résultats techniques du paragraphe suivant.

5.3 Ensemble $\mathcal{A}(L)$, application Ψ et groupes L-conjugués

Dans ce paragraphe, sont présentés les résultats portant uniquement sur les ensembles de permutations. Ils seront utilisés dans les paragraphes suivants.
Considérons un sous-groupe L de $S_{1,n-1}$ (i.e. tel que $\forall \sigma \in L,\ \sigma(1) = 1$).

Définition 5.3.1. Nous appellerons *groupe admissible* tout sous-groupe transitif H de S_n vérifiant $H_{\{1\}} \subset L$ et tel que $\mathrm{Orb}(L) = \mathrm{Orb}(H_{\{1\}})$. L'ensemble des groupes admissibles sera noté $\mathcal{A}(L)$.

Remarque 5.3.2. Notons $1, e$ la suite croissante des cardinaux des éléments de $\mathrm{Orb}(L)$. Pour H un sous-groupe transitif de S_n, il est facile de montrer l'équivalence :

$$H \in \mathcal{A}(L) \text{ ssi } \Delta(H) = 1, e \text{ et } H_{\{1\}} \subset L.$$

Ainsi, pour obtenir $\mathcal{A}(L)$, il suffit de déterminer les groupes H' de $\mathcal{T}(n)$ tel que $\Delta(H') = 1, e$ (à l'aide de la table de rupture en degré n), puis de calculer les groupes H conjugués de H' vérifiant $H_{\{1\}} \subset L$.

Proposition 5.3.3. *Soit $H \in \mathcal{A}(L)$ et soient $\{\sigma_1, \ldots, \sigma_s\}$ et $\{\sigma'_1, \ldots, \sigma'_s\}$ deux transversales à droite de L modulo $H_{\{1\}}$. Alors*

$$H\sigma_1 + \cdots + H\sigma_s = H\sigma'_1 + \cdots + H\sigma'_s \,.$$

Démonstration. Puisque $\forall i \in [\![1, n]\!],\ \sigma_i \in L$, il vient $\sigma_i \in H_{\{1\}}\sigma'_1 + \cdots + H_{\{1\}}\sigma'_s$, puis successivement,

$$\forall i \in [\![1, n]\!],\ H\sigma_i \subset H\sigma'_1 + \cdots + H\sigma'_s,$$
$$H\sigma_1 + \cdots + H\sigma_s \subset H\sigma'_1 + \cdots + H\sigma'_s.$$

L'inclusion réciproque se démontre de la même manière. □

Cette proposition montre que l'application Ψ ci-dessous est bien définie.

Notations 5.3.4. Nous noterons Ψ l'application de $\mathcal{A}(L)$ dans l'ensemble des parties de S_n définie pour tout $H \in \mathcal{A}(L)$ par :

$$\Psi(H) = H\sigma_1 + \cdots + H\sigma_s \,,$$

où $\{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ est une transversale à droite de L modulo $H_{\{1\}}$.

Proposition 5.3.5. *L'application Ψ possède les propriétés suivantes :*

1. *Si $H \in \mathcal{A}(L)$ et si $\tau_1 = id, \ldots, \tau_n$ désignent n permutations de H telles que, pour tout $i \in [\![1, n]\!]$ $\tau_i(1) = i$, alors*

$$\Psi(H) = \tau_1 L + \cdots + \tau_n L \,.$$

2. *Si H et G appartiennent à $\mathcal{A}(L)$ et si $H \cap G$ est un sous-groupe transitif de S_n alors $\Psi(G) = \Psi(H)$.*

Démonstration. Démontrons la première assertion. Puisque le groupe H est transitif, les permutations τ_i existent et $H = \tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}}$. Nous avons alors, pour $\{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ une transversale à droite de L modulo $H_{\{1\}}$:

$$\begin{aligned} \Psi(H) &= (\tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}})\sigma_1 + \cdots + (\tau_1 H_{\{1\}} + \cdots + \tau_n H_{\{1\}})\sigma_s \\ &= \tau_1 L + \cdots + \tau_n L \,. \end{aligned}$$

Pour la seconde assertion, il suffit de prendre $\tau_1, \ldots, \tau_n$ dans l'intersection transitive $H \cap G$ et l'assertion (1) donne $\Psi(H) = \tau_1 L + \cdots + \tau_n L = \Psi(G)$. □

Corollaire 5.3.6. *Soit $H \in \mathcal{A}(L)$. Alors, le cardinal de $\Psi(H)$ ne dépend que de celui de L :*

$$\mathrm{Card}(\Psi(H)) = s\,\mathrm{Card}(H) = n\,\mathrm{Card}(L)\ .$$

Définition 5.3.7. Soient deux sous-groupes G et H de S_n. Le groupe G est dit *L-conjugué à H* s'il existe σ dans L tel que $H = G^\sigma = \sigma G \sigma^{-1}$.

Proposition 5.3.8. *Soient H et G deux groupes L-conjugués appartenant à $\mathcal{A}(L)$. Nous avons les assertions suivantes :*

1. *si σ désigne une permutation de L telle que $H = G^\sigma$, alors*

$$\Psi(H) = \sigma\,\Psi(G)\,;$$

2. *si $\{\sigma_1, \ldots, \sigma_s\}$ désigne une transversale à droite de L modulo $H_{\{1\}}$ alors il existe $i \in [\![1, s]\!]$ tel que $H = G^{\sigma_i}$; en particulier, le nombre de groupes L-conjugués à H est majoré par s.*

Démonstration. Montrons l'assertion (1) et reprenons les notations de la Proposition 5.3.5. Posons, pour tout $i \in [\![1, n]\!]$, $\rho_i = \sigma^{-1}\,\tau_i\,\sigma$. Les permutations $\rho_1, \ldots, \rho_n$ appartiennent à $G = H^{\sigma^{-1}}$ et nous avons successivement,

$$\begin{aligned}
\Psi(H) &= \tau_1 L + \cdots + \tau_n L \\
&= \sigma\,\rho_1\sigma^{-1} L + \cdots + \sigma\,\rho_n\sigma^{-1} L \\
&= \sigma\,\rho_1 L + \cdots + \sigma\,\rho_n L \\
&= \sigma\,\Psi(G),
\end{aligned}$$

d'après l'assertion (1) de la proposition 5.3.5 et le fait que $\{\rho_i(1) \mid i \in [\![1, n]\!]\} = \{1, \ldots, n\}$.

Montrons l'assertion (2). Si G et H sont L-conjugués, il existe $\sigma \in L$ tel que $H = G^\sigma$. L'égalité $L = H_{\{1\}}\sigma_1 + H_{\{1\}}\sigma_2 + \cdots + H_{\{1\}}\sigma_s$ impose à σ d'appartenir à l'un des ensembles $H_{\{1\}}\sigma_i$, pour un entier $i \in [\![1, s]\!]$, et donc de s'écrire $\sigma = h\sigma_i$, où h désigne une permutation de H. Le résultat se déduit alors des égalités successives : $G = \sigma_i^{-1}h^{-1}H\,h\,\sigma_i = \sigma_i^{-1}\,H\,\sigma_i$. □

Les deux propositions suivantes nous seront utiles pour exprimer l'ensemble des injecteurs d'un idéal induit de I_1 et pour déterminer de manière constructive cet ensemble même lorsqu'il existe plusieurs idéaux de rupture (voir Remarque 5.2.3).

Proposition 5.3.9. *Soit H un groupe appartenant à $\mathcal{A}(L)$. Alors, pour tout $\sigma \in L$, le groupe H^σ appartient à $\mathcal{A}(L)$.*

Démonstration. Pour tout sous-groupe G de S_n et toute permutation $\sigma \in S_n$, nous avons :

$$(G^\sigma)_{\{1\}} = (G_{\{\sigma^{-1}(1)\}})^\sigma \text{ et} \tag{5.1}$$

$$\mathrm{Orb}(G^\sigma) = \sigma.\mathrm{Orb}(G)\ . \tag{5.2}$$

Il s'ensuit les égalités successives suivantes :

$$\begin{aligned}\mathrm{Orb}((H^\sigma)_{\{1\}}) &= \mathrm{Orb}((H_{\{1\}})^\sigma), \text{ d'après l'égalité (5.1) et puisque } \sigma(1)=1,\\ &= \sigma.\mathrm{Orb}(H_{\{1\}}), \text{ d'après l'égalité (5.2)},\\ &= \sigma.\mathrm{Orb}(L), \text{ car } H \in \mathcal{A}(L),\\ &= \mathrm{Orb}(L), \text{ car } \sigma \in L\ .\end{aligned}$$

Le groupe H^σ étant transitif, H^σ appartient à $\mathcal{A}(L)$. □

Nous avons maintenant assez de résultats sur les groupes admissibles pour exhiber un des injecteurs d'un idéal induit.

5.4 Calcul des injecteurs d'un idéal induit

L'idéal I_1 de ce paragraphe est celui du paragraphe 5.2 (voir Notation 5.2.4). L'injecteur L de I_1 vérifie $L \subset S_{1,\Delta(f)}$ (voir Proposition 5.2.8). L'idéal I est induit de I_1 (voir Définition 5.2.5) et $\mathcal{M}(I)$ est l'ensemble des idéaux maximaux contenant I. Nous cherchons à déterminer les injecteurs de I dans les idéaux de $\mathcal{M}(I)$.

5.4.1 Formulation des injecteurs de l'idéal induit

Dans ce paragraphe, sont exposés des résultats théoriques pour le calcul d'un injecteur de I.

Proposition 5.4.1. *Pour tout $\mathcal{M} \in \mathcal{M}(I)$, le groupe de Galois* $\mathrm{Dec}(\mathcal{M})$ *appartient à* $\mathcal{A}(L)$ *et*

$$\mathrm{Inj}(I,\mathcal{M}) = \Psi(\mathrm{Dec}(\mathcal{M}))\ ,$$

où Ψ est l'application définie dans la notation 5.3.4.

Démonstration. Le groupe $\mathrm{Dec}(\mathcal{M})$ appartient à $\mathcal{A}(L)$ d'après la proposition 5.2.8. D'après la proposition 5.2.7, nous pouvons supposer que $\mathcal{M} = Id_k(\underline{\alpha})$ avec $\underline{\alpha} \in V(I_1)$; i.e. $\mathrm{Inj}(I,\mathcal{M}) = \mathrm{Inj}(I,\underline{\alpha})$. Soient n permutations $\tau_1,\ldots,\tau_n$ de $\mathrm{Dec}(\mathcal{M})$ telles que, pour tout $i \in [\![1,n]\!]$, $\tau_i(1) = i$. D'après la proposition 5.2.9, nous avons l'égalité :

$$k(\underline{\alpha}) \otimes_k I = \bigcap_{i=1}^{n} \overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)\ .$$

L'idéal $\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)$ contient le polynôme $x_1 - \alpha_i$. Puisque les racines $\alpha_1,\ldots,\alpha_n$ sont distinctes, les idéaux $\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1)$, pour $i \in [\![1,n]\!]$, sont deux à deux comaximaux. Nous avons les égalités suivantes :

$$\begin{aligned}\mathrm{Inj}(I,\underline{\alpha}) &= \mathrm{Inj}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I, \underline{\alpha}), \text{ d'après l'égalité (2.5)},\\ &= \sum_{i=1}^{n} \mathrm{Inj}(\overline{\tau_i}(k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha})\\ &= \sum_{i=1}^{n} \tau_i\ \mathrm{Inj}((k(\underline{\alpha}) \otimes_{k(\alpha_1)} I_1), \underline{\alpha}), \text{ d'après le lemme 2.2.14},\\ &= \sum_{i=1}^{n} \tau_i\, \mathrm{Inj}(I_1, \underline{\alpha}), \text{ d'après la remarque 2.2.8},\\ &= \Psi(\mathrm{Dec}(\mathcal{M})),\end{aligned}$$

où la dernière égalité est obtenue en appliquant l'assertion (1) de la proposition 5.3.5 à $L = \mathrm{Inj}(I_1, \underline{\alpha})$. □

Théorème 5.4.2. *Soit $H \in \mathcal{A}(L)$ et $\mathcal{M} \in \mathcal{M}(I)$ tels que $H \cap \mathrm{Dec}(\mathcal{M})$ soit un sous-groupe transitif de S_n. Alors l'ensemble des injecteurs de l'idéal I induit de I_1 dans les idéaux maximaux qui le contiennent est formé des*

$$\mathrm{Inj}(I, \sigma.\mathcal{M}) = \Psi(H^\sigma)$$

où σ parcourt l'injecteur L de I_1.

Démonstration. D'après les propositions 5.2.7 et 5.4.1, l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent est formé des $\mathrm{Inj}(I, \sigma.\mathcal{M}) = \Psi(\mathrm{Dec}(\sigma.\mathcal{M}))$ où σ parcourt L. Soit $\sigma \in L$. Comme $H \cap \mathrm{Dec}(\mathcal{M})$ est transitif, le groupe $H^\sigma \cap \mathrm{Dec}(\mathcal{M})^\sigma = H^\sigma \cap \mathrm{Dec}(\sigma.\mathcal{M})$ est aussi transitif. Selon l'assertion (2) de la proposition 5.3.5 appliquée à $G = \mathrm{Dec}(\sigma.\mathcal{M})$, nous avons donc $\Psi(H^\sigma) = \Psi(G)$. □

Corollaire 5.4.3. *Reprenons les hypothèses du théorème 5.4.2 et notons s l'indice de $H_{\{1\}}$ dans L. Alors*

$$\mathrm{Card}(\mathrm{Inj}(I, \mathcal{M})) = s.\,\mathrm{Card}(H) = n.\,\mathrm{Card}(L)\ .$$

Démonstration. Ces deux égalités sont des conséquences immédiates du corollaire 5.3.6 et du théorème 5.4.2. □

5.4.2 Classes de L-conjugaison associées aux idéaux induits

Si un groupe H vérifiant les hypothèses du théorème 5.4.2 est connu, il est alors possible de calculer un injecteur de I. Ici, nous voulons construire un des idéaux $\mathcal{M}$ de $\mathcal{M}(I)$ à partir de I, il n'est donc pas immédiat de tester si $H \cap \mathrm{Dec}(\mathcal{M})$ est transitif. Il nous faut donc trouver un moyen effectif pour réaliser ce test. C'est à cette question qu'est consacré ce paragraphe.

Définition 5.4.4. Un groupe $H \in \mathcal{A}(L)$ est dit *associé à l'idéal I* s'il existe $\mathcal{M} \in \mathcal{M}(I)$ tel que $H \cap \mathrm{Dec}(\mathcal{M})$ soit transitif (i.e. si H vérifie les hypothèses du théorème 5.4.2).

Il s'agit d'étudier à quels idéaux sont associés les différents conjugués dans $\mathcal{A}(L)$ d'un groupe H de $\mathcal{A}(L)$. Les groupes L-conjugués à H appartiennent aussi à $\mathcal{A}(L)$ (voir Proposition 5.3.9) et si H est associé à I alors tout groupe de sa classe de L-conjugaison $\mathcal{C}$ l'est aussi (voir Démonstration du théorème 5.4.2). Nous pouvons donc introduire la définition suivante :

Définition 5.4.5. La classe $\mathcal{C}$ de L-conjugaison d'un groupe $H \in \mathcal{A}(L)$ est dite *associée à l'idéal I* si H est associé à I.

Remarque 5.4.6. Si la classe $\mathcal{C}$ est associée à l'idéal I alors, d'après le théorème 5.4.2, $\{\Psi(H') \mid H' \in \mathcal{C}\}$ est l'ensemble des injecteurs de I dans les idéaux maximaux qui le contiennent.

Nous commençons notre étude par celle plus simple de $\mathcal{A}(S_{1,e})$, c'est-à-dire dans le cas où l'idéal I est induit d'un idéal de rupture I_r, avec $e = (e_1, \ldots, e_r) \in \mathbb{N}^r$, un r-uplet d'entiers croissants de somme $n-1$. Les résultats sur $\mathcal{A}(L)$ avec L un sous-groupe de $S_{1,e}$ s'en déduiront aisément.

Soit le sous-groupe de S_n

$$M = \{\sigma \in S_n \,|\, \sigma(1) = 1 \text{ et } \mathrm{Orb}(S_{1,e}) = \sigma.\mathrm{Orb}(S_{1,e})\}$$

D'après l'identité (5.2), le groupe M est le normalisateur de $S_{1,e}$ dans $S_{1,n-1}$; en particulier, le groupe $S_{1,e}$ est distingué dans M.

Le groupe M agit naturellement sur l'ensemble $\mathrm{Orb}(S_{1,e})$ en laissant fixe une orbite ou en l'envoyant sur une autre orbite de même cardinal. Notons $O_0 = \{1\}, O_1, \ldots, O_r$ les orbites de $\{1, \ldots, n\}$ sous l'action $S_{1,e}$ et supposons les indicées par cardinalité croissante (i.e. $\mathrm{Card}(O_i) = e_i$ pour $i = 1, \ldots, r$). Le groupe $S_{1,e}$ (distingué dans M) est le noyau du morphisme surjectif :

$$\begin{array}{rccl} \phi : & M & \longrightarrow & \mathrm{Stab}_{S_r}(e) \\ & \sigma & \longmapsto & \tau : \tau(i) = j \text{ si } \sigma.O_i = O_j (i = 1, \ldots, r)\,. \end{array}$$

Le cardinal N du stabilisateur $\mathrm{Stab}_{S_r}(e)$ de e dans S_r est aussi l'ordre du groupe $M/S_{1,e}$.

Lemme 5.4.7. *Soit $H \in \mathcal{A}(S_{1,e})$. Alors l'ensemble des groupes S_n-conjugués à H appartenant à $\mathcal{A}(S_{1,e})$ est formé des H^σ où σ parcourt M.*

Démonstration. Soit $\sigma \in M$. Nous avons d'une part (voir (5.1)) :

$$(H^\sigma)_{\{1\}} = (H_{\{\sigma^{-1}(1)\}})^\sigma = (H_{\{1\}})^\sigma \subset S_{1,e}^\sigma = S_{1,e}$$

et d'autre part (voir (5.2)) :

$$\mathrm{Orb}(H^\sigma) = \sigma.\mathrm{Orb}(H) = \sigma.\mathrm{Orb}(S_{1,e}) = \mathrm{Orb}(S_{1,e})\,.$$

Donc $H^\sigma \in \mathcal{A}(S_{1,e})$. Pour l'inclusion inverse, prenons $\tau \in S_n$ tel que $H^\tau \in \mathcal{A}(S_{1,e})$. Puisque H est transitif, il existe $h \in H$ tel que $\tau h(1) = 1$. Posons $\sigma = \tau h$. Nous avons $H^\tau = H^\sigma$. Donc, d'une part, $\sigma(1) = 1$ et, d'autre part, $\mathrm{Orb}(S_{1,e}) = \sigma.\mathrm{Orb}(S_{1,e})$ puisque $\mathrm{Orb}(H^\sigma) = \mathrm{Orb}(S_{1,e})$ et que $\mathrm{Orb}(H) = \mathrm{Orb}(S_{1,e})$. D'où $\sigma \in M$. □

Considérons $\{\tau_1 = id, \ldots, \tau_N\}$ une transversale à droite de $M \mod S_{1,e}$ (c'est aussi une transversale à gauche).

Lemme 5.4.8. *Soit $H \in \mathcal{A}(S_{1,e})$ et considérons les m classes de conjugaison par $S_{1,e}$ des S_n-conjugués de H appartenant à $\mathcal{A}(S_{1,e})$ (i.e. les H^σ où σ parcourt M). Alors nous avons les assertions suivantes :*

(1) Soit $\sigma \in S_{1,e}\tau_i$; la conjugaison par σ induit une bijection entre la classe de H et celle de H^{τ_i}.

(2) Chaque classe est celle d'un groupe H^{τ_i}, où $i \in [\![1, N]\!]$ formé des H^σ où $\sigma \in S_{1,e}\tau_i$.

(3) le nombre m de classes est majoré par N.

Démonstration. Pour montrer l'assertion (1), il suffit de constater que si $l \in S_{1,e}$, alors $(H^l)^\sigma = (H^\sigma)^{\sigma l \sigma^{-1}}$ appartient à la même classe que H^σ puisque $S_{1,e}$ est distingué dans M. Cette orbite est celle de H^{τ_i} puisque $\sigma = \tau\tau_i \in M$ avec $\tau \in S_{1,e}$ et donc $H^\sigma = (H^{\tau_i})^\tau$.
Pour montrer l'assertion (2), considérons une classe. Elle est celle d'un groupe H^σ où $\sigma \in M$ (voir Lemme 5.4.7) ; c'est-à-dire qu'il existe $i \in [\![1, N]\!]$ tel que $\sigma \in S_{1,e}\tau_i$. Donc la classe est celle de H^{τ_i}.
Il est évident que le nombre de classes est inférieur à N. □

Ayant étudié les classes de conjugaison par $S_{1,e}$ des conjugués H dans $\mathcal{A}(S_{1,e})$, nous cherchons à savoir les associer aux idéaux induits des idéaux de rupture d'un polynôme f où :

- $e = \Delta(f)$, la suite croissante des degrés des facteurs de rupture $f_2, \ldots, f_r$ (voir Chapitre 4), que
- H est associé à l'idéal de rupture I_r construit à partir de $f_2, \ldots, f_r$ (voir Paragraphe 5.2) et que
- J est l'idéal induit de I_r (i.e. $J = I_r \cap k[x_1, \ldots, x_n]$).

Les facteurs de rupture sont ordonnés en respectant la croissance des degrés. Donc il existe exactement N, le cardinal de $\mathrm{Stab}_{S_r}(e)$, listes de facteurs de ruptures distinctes (car les racines de f le sont) induisant par construction N idéaux de rupture distincts. Plus précisément, comme $S_{1,e}$ est le noyau du morphisme surjectif ϕ, ces N listes sont les

$$(f_{\phi(\tau_i)(2)}, \ldots, f_{\phi(\tau_i)(r)}) \quad i = 1, \ldots, N$$

Chacune de ces N listes permettent de construire respectivement les N idéaux de rupture $\tau_i.I_r$, d'idéaux induits respectifs :

$$\tau_1.J, \tau_2.J, \ldots, \tau_N.J \ .$$

Remarque 5.4.9. Le groupe $S_{1,e}$ étant celui de décomposition de chaque idéal de rupture, par définition de $\tau_1, \ldots, \tau_N$, l'ensemble $\{\sigma.J \mid \sigma \in M\}$ est l'ensemble des idéaux induits des idéaux de rupture. Soit $\mathcal{M} \in \mathcal{M}(J)$. Nous avons $\mathrm{Dec}(\mathcal{M}) \in \mathcal{A}(S_{1,e})$ (voir Proposition 5.2.8). Comme $\mathcal{M}(J) = \{\tau.\mathcal{M} \mid \tau \in S_{1,e}\}$ (voir Proposition 5.2.7) , l'ensemble des idéaux maximaux contenant un idéal induit est

$$\mathcal{F} = \{\sigma.\mathcal{M} \mid \sigma \in M\}.$$

L'ensemble des groupes de décomposition des idéaux de $\mathcal{F}$ est formé des $\mathrm{Dec}(\mathcal{M})^\sigma$ (=$\mathrm{Dec}(\sigma.\mathcal{M})$) où σ parcourt M ; c'est-à-dire l'ensemble des conjugués de $\mathrm{Gal}_k(f)$ (i.e. de $\mathrm{Dec}(\mathcal{M})$) appartenant à $\mathcal{A}(S_{1,e})$ (voir Lemme 5.4.7).

Lemme 5.4.10. *Soit $\sigma \in M$. Si le groupe H est associé à l'idéal J alors le groupe H^σ est associé à l'idéal $\sigma.J$ induit de $\sigma.I_r$.*

Démonstration. Soit $\mathcal{M} \in \mathcal{M}(J)$ tel que $H \cap \mathrm{Dec}(\mathcal{M})$ soit un sous-groupe transitif de S_n. Alors $H^\sigma \cap \mathrm{Dec}(\sigma.\mathcal{M})$ est également transitif avec $\sigma.\mathcal{M} \in \mathcal{M}(\sigma.J)$ (i.e. l'idéal $\sigma.\mathcal{M}$ est un idéal maximal contenant $\sigma.J$). □

Les résultats précédents permettent d'énoncer le théorème suivant :

Théorème 5.4.11. *Soit $H \in \mathcal{A}(S_{1,e})$ supposé être associé à l'idéal J induit de I_r. Alors :*

(1) à chaque idéal $\tau_i.J$ induit de l'idéal de rupture $\tau_i.I_r$, $i = 1, \ldots, N$, est associée la classe de $S_{1,e}$-conjugaison du groupe H^{τ_i} ;

(2) tout groupe $H^\sigma \in \mathcal{A}(S_{1,e})$ (i.e. $\sigma \in M$) est associé à l'idéal $\sigma.J$ induit de l'idéal de rupture $\sigma.I_r$. Donc toute la classe de $S_{1,e}$-conjugaison de H^σ est associée à $\sigma.J$.

Nous en déduisons le corollaire suivant :

Corollaire 5.4.12. *Soient G, un conjugué de $\mathrm{Gal}_k(f)$, et H deux groupes de $\mathcal{A}(S_{1,e})$ tels que $H \cap G$ soit un sous-groupe transitif de S_n. Alors il existe un groupe conjugué de H appartenant à $\mathcal{A}(S_{1,e})$ qui est associé à J (ainsi que sa classe de $S_{1,e}$-conjugaison). En particulier, si les groupes conjugués à H appartenant à $\mathcal{A}(S_{1,e})$ sont tous $S_{1,e}$-conjugués alors H est associé à J.*

Remarque 5.4.13. L'hypothèse du corollaire 5.4.12 est vérifiée lorsque nous savons que le groupe de Galois $\mathrm{Gal}_k(f)$ appartient à un ensemble et que tout groupe de cet ensemble possède un conjugué dans $\mathcal{A}(S_{1,e})$ d'intersection transitive avec le groupe H.

Remarque 5.4.14. Plaçons-nous dans le cas où les parts e_i du n-uplet $e = (e_1, \ldots, e_r)$ sont distinctes deux à deux (i.e. $N = 1$, $M = S_{1,e}$ et $\mathrm{Stab}_{S_r}(e)$ est réduit à l'identité). Il n'existe qu'un seul idéal de rupture de f. Si $H \in \mathcal{A}(S_{1,e})$ alors les conjugués de H dans $\mathcal{A}(S_{1,e})$ sont $S_{1,e}$-conjugués à H (voir Lemme 5.4.7).

Nous pouvons désormais revenir au cas d'un groupe L, injecteur de l'idéal I_1 dont I est l'idéal induit. Soit $H \in \mathcal{A}(L)$. D'après la proposition 5.3.9, les S_n-conjugués de H qui appartiennent à $\mathcal{A}(L)$ se répartissent en classes de L-conjugaison.

Corollaire 5.4.15. *Supposons le groupe H associé à l'idéal I. Alors, pour tout conjugué G de H appartenant à $\mathcal{A}(L)$, il existe $\sigma \in M$ tels que $G = H^\sigma$ et G est associé à l'idéal $\sigma.I$ induit de $\sigma.I_1$.*

Démonstration. Comme $\mathcal{A}(L) \subset \mathcal{A}(S_{1,e})$ (voir Proposition 5.2.8), il existe $\sigma \in M$ tels que $G = H^\sigma$ (voir Lemme 5.4.7). L'idéal $\sigma.I_1$ contient l'idéal $\sigma.I_r$ qui est de rupture puisque $\sigma \in M$ (voir Remarque 5.4.9). En reprenant la démonstration du lemme 5.4.10, le groupe H^σ est bien associé à l'idéal $\sigma.I$ induit de $\sigma.I_1$. □

Remarque 5.4.16. Pour tout $\mathcal{M} \in \mathcal{M}(I)$, $\mathrm{Dec}(\mathcal{M}) \in \mathcal{A}(L)$ (voir Proposition 5.2.8) est associé I. Lorsque $\mathrm{Gal}_k(f)$ est déterminé, nous connaissons ses S_n-conjugués appartenant à $\mathcal{A}(L)$. Il s'agit de pouvoir identifier la lasse de L-conjugaison de $\mathcal{M}$.

5.4.3 Association d'une classe de L-conjugaison à l'idéal induit I

Nous venons d'étudier les liens entre les classes de $S_{1,e}$-conjugaisons et les idéaux induits d'idéaux de rupture. Nous n'avons pas résolu le problème d'identification de la classe associée à I. C'est ce à quoi nous allons nous consacrer maintenant.

Dans ce paragraphe, I désignera un idéal induit d'un idéal I_1 contenant un idéal de rupture I_r et $\mathfrak{C}$ l'ensemble des classes de L-conjugaison de groupes appartenant à $\mathcal{A}(L)$.

Nous savons qu'au moins une de ces classes est associée à I (voir Remarque 5.4.16). Les résultats de ce paragraphe permettent de tester si une classe de L-conjugaison de $\mathfrak{C}$ est associée ou non à l'idéal I.

La proposition suivante permet toujours de déterminer un injecteur de I.

Proposition 5.4.17. *Un groupe H de $\mathcal{A}(L)$ est associé à I si et seulement si il vérifie*

$$I + \Psi(H).I \neq k[x_1, \ldots, x_n] \, .$$

Démonstration. Cette dernière inégalité est vérifiée si et seulement si il existe $\underline{\beta} \in V(I)$ tel que $\Psi(H) \subset \mathrm{Inj}(I, \underline{\beta})$ (voir Proposition 2.2.17). Puisque $\mathrm{Card}(\Psi(H))$ est le cardinal de tout injecteur de I (voir Corollaire 5.3.6 et Corollaire 5.4.3), $\Psi(H)$ est égal à $\mathrm{Inj}(I, \underline{\beta})$. □

Remarque 5.4.18. Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux classes de $\mathfrak{C}$. D'après les propositions 5.3.5 et 5.3.8, s'il existe deux groupes $H_1 \in \mathcal{C}_1$ et $H_2 \in \mathcal{C}_2$ tels que $H_1 \cap H_2$ soit un sous-groupe transitif de S_n alors

$$\{\Psi(H) \mid H \in \mathcal{C}_1\} = \{\Psi(H) \mid H \in \mathcal{C}_2\} \, .$$

Supposons que $I + \Psi(H_1).I = k[x_1, \ldots, x_n]$. Avec cette hypothèse, la proposition 5.4.17 prouve qu'aucun des groupes de $\mathcal{C}_1$ et de $\mathcal{C}_2$ ne permet le calcul d'un injecteur de I.
Supposons que $I + \Psi(H_1).I \neq k[x_1, \ldots, x_n]$. Avec cette hypothèse, la proposition 5.4.17 montre que $\Psi(H_1)$ est un injecteur de I et qu'aucune des classes $\mathcal{C}$ telle que $\Psi(H_1) \notin \{\Psi(H) \mid H \in \mathcal{C}\}$ n'est associée à I.

La proposition 5.4.17 ne permet pas de pré-établir des *critères d'association* entre les classes de $\mathfrak{C}$ et les idéaux induits ce qui sera souvent possible avec la proposition suivante :

Proposition 5.4.19. *Si $\mathcal{C} \in \mathfrak{C}$ est associée à l'idéal induit I, alors*

$$I = \bigcap_{H \in \mathcal{C}} H.I \quad \left(= \bigcap_{H \in \mathcal{C}} \{\sigma.R \;\mid\; \sigma \in H, \;\; R \in I\} \right) \, .$$

Démonstration. Soit $H \in \mathcal{C}$. Par hypothèse, il existe $\underline{\alpha} \in V(I)$ tel que $\mathrm{Inj}(I, \underline{\alpha}) = \Psi(H)$ (voir Théorème 5.4.2). Par définition de Ψ, l'injecteur $\mathrm{Inj}(I, \underline{\alpha})$ s'écrit donc

$$\mathrm{Inj}(I, \underline{\alpha}) = H\sigma_1 + \cdots + H\sigma_s \, ,$$

où $\{\sigma_1, \ldots, \sigma_s\}$ est une transversale à droite de L modulo $H_{\{1\}}$. Par suite, l'idéal I se décompose comme suit :

$$I = Id_k(\mathrm{Inj}(I, \underline{\alpha}).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k((H\sigma_i).\underline{\alpha}) = \bigcap_{i=1}^{s} Id_k(H^{\sigma_i^{-1}}.(\sigma_i.\underline{\alpha})) \, , \tag{5.1}$$

Soient $H^\sigma \in \mathcal{C}$ où $\sigma \in \{\sigma_1^{-1}, \ldots, \sigma_n^{-1}\} \subset L$ et $R \in I$.
D'après l'égalité (5.1), nous avons $R \in Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$ et donc, par la proposition 2.2.20, il vient $H^\sigma.I \subset Id_k(H^\sigma.(\sigma^{-1}.\underline{\alpha}))$. La décomposition (5.1) permet d'en déduire l'inclusion $\bigcap_{H' \in \mathcal{C}} H'.I \subset I$. Or $I \subset \bigcap_{H' \in \mathcal{C}} H'.I$, d'où le résultat. □

L'étude du degré 8 que nous menons au paragraphe 5.7 fait apparaître, qu'en dehors du cas $\mathrm{Gal}_k(f) \in \{8T_6, 8T_8\}$, la proposition 5.4.19 est suffisante pour établir des critères d'association tels que celui présenté dans l'exemple 5.4.20 qui suit.

Exemple 5.4.20. Supposons que f soit un polynôme de degré 8 tel que $\Delta(f) = 1^3, 2^2$. L'injecteur de tout idéal de rupture I_r est $L = S_{1^4,2^2}$. Tout idéal initial I induit par un idéal de rupture est engendré par un ensemble triangulaire T de la forme :

$$\begin{aligned} T \;=\; \{&f(x_1),\ x_2 + g_2(x_1),\ x_3 + g_3(x_1),\ x_4 + g_4(x_1),\\ &f_5(x_5, x_1),\ x_6 + g_6(x_5, x_1),\ f_7(x_7, x_1),\ f_8(x_6, x_1)\}, \end{aligned}$$

où les polynômes g_2, g_3, g_4 sont distincts.

Supposons que $\mathrm{Gal}_k(f)$ soit impair, il s'agit alors d'un conjugué de $8T_7$, c'est à dire l'un de ses 6 conjugués dans $\mathcal{A}(L)$ qui sont :

$$\begin{aligned} &H_1 = \langle (1,5,3,7,2,6,4,8), \sigma_1 = (1,2)(3,4)\rangle, \quad H_2 = \langle (1,6,3,7,2,5,4,8), \sigma_1\rangle,\\ &H_3 = \langle (1,5,2,7,3,6,4,8), \sigma_2 = (1,3)(2,4)\rangle, \quad H_4 = \langle (1,5,2,8,3,6,4,7), \sigma_2\rangle,\\ &H_5 = \langle (1,5,2,7,4,6,3,8), \sigma_3 = (1,4)(2,3)\rangle, \quad H_6 = \langle (1,5,2,8,4,6,3,7), \sigma_3\rangle. \end{aligned}$$

Ces 6 groupes se répartissent en trois classes de L-conjugaison :

$$\mathcal{C}_1 = \{H_1, H_2\},\ \mathcal{C}_2 = \{H_3, H_4\} \text{ et } \mathcal{C}_3 = \{H_5, H_6\},$$

avec $H_2 = \tau^{-1} H_1 \tau$, $H_4 = \tau^{-1} H_3 \tau$ et $H_6 = \tau^{-1} H_5 \tau$ et $\tau = (5,6) \in L$.

D'après le théorème 5.4.11, il existe $i \in \{1,2,3\}$ tel que $I = \bigcap_{H \in \mathcal{C}_i} H.I$. La proposition 5.4.19 permet ensuite de déterminer la classe associée à I sous la forme d'un critère d'association.

À partir du polynôme $R = x_2 + g_2(x_1)$ de T et des permutations $\sigma_1 = (1,5,3,7,2,6,4,8)$ de H_1 et $\sigma_2 = (1,6,2,5,3,7,4,8)(1,2)(3,4)$ de H_2, nous formons le polynôme $P_1 = \sigma_1.R = \sigma_2.R = x_6 + g_2(x_5)$ qui appartient à $\bigcap_{H \in \mathcal{C}_1} H.I$. De même, nous construisons le polynôme $P_2 = x_6 + g_3(x_5)$ de $\bigcap_{H \in \mathcal{C}_2} H.I$ et le polynôme $P_3 = x_6 + g_4(x_5)$ de $\bigcap_{H \in \mathcal{C}_3} H.I$. Les polynômes P_1 et P_2 ne peuvent appartenir simultanément à I car, si tel était le cas, le polynôme $g_2(x_5) - g_3(x_5) = P_1 - P_2$ appartiendrait à I et, étant de degré strictement inférieur à f, il diviserait f sur k. Il en va de même, pour les couples (P_1, P_3) et (P_2, P_3). Nous obtenons ainsi les critères d'association :

1. si $P_1 \in I$ alors la classe $\mathcal{C}_1$ est associée à I ;
2. si $P_2 \in I$ alors la classe $\mathcal{C}_2$ est associée à I ;
3. si $P_3 \in I$ alors la classe $\mathcal{C}_3$ est associée à I.

Supposons que $\mathcal{C}_1$ soit associée à I. Alors I est l'intersection de deux idéaux maximaux (ceux de $\mathcal{M}(I)$) : $I = \mathcal{M}_1 \cap \mathcal{M}_2$ avec $H_i = \mathrm{Dec}(\mathcal{M}_i)$, $i = 1, 2$. Les ensembles $\Psi(H_1) = H_1 + H_1\tau$ et $\Psi(H_2)$ sont les injecteurs de I dans $\mathcal{M}_1$ et $\mathcal{M}_2$, respectivement (voir Théorème 5.4.2).

Remarque 5.4.21. Nous constatons sur l'exemple ci-dessus que la proposition 5.4.19 est utilisable pour pré-établir des critères d'association. Il s'agit d'une conséquence du fait que les variables et les degrés des polynômes intervenant dans l'ensemble triangulaire engendrant l'idéal induit ne dépendent que du groupe de Galois de f.

Le résultat de la proposition suivante est moins fort que celui de la proposition 5.4.19, mais il est parfois suffisant :

Proposition 5.4.22. *S'il existe $\sigma \in \bigcap_{H\in\mathcal{C}} \Psi(H)$ et g dans I tel que $\sigma.g \notin I$ alors $\mathcal{C}$ n'est pas associée à I.*

Démonstration. Montrons la contraposée de la proposition. Supposons donc la classe $\mathcal{C}$ associée à I. D'après le théorème 5.4.2, les injecteurs de I sont les $\Psi(H)$ où H parcourt la classe $\mathcal{C}$. La proposition 2.2.19 montre qu'alors

$$\mathrm{Dec}(I) = \bigcap_{H\in\mathcal{C}} \Psi(H)\,.$$

Le résultat découle alors de la définition du groupe de décomposition d'un idéal. □

Remarque 5.4.23. La recherche d'un polynôme $g \in I$ de la proposition 5.4.22 peut être restreinte à un ensemble de polynômes engendrant I.

5.5 Adjonction de relations à l'idéal induit

Donnons-nous un idéal I induit d'un idéal I_1. Il est parfois possible de construire, sans coût supplémentaire, un idéal de Galois contenant strictement I. Dans ce paragraphe, nous décrivons un tel procédé.

Pour pouvoir appliquer l'algorithme `GaloisIdéal` à ce nouvel idéal, nous devons, comme pour I, connaître un de ses injecteurs.

Proposition 5.5.1. *Soit H un sous-groupe de S_n vérifiant $H \subset \mathrm{Inj}(I, \underline{\alpha})$. Soient $\sigma \in H$ et $R \in I$. L'idéal $J = I + \langle \sigma.R \rangle$ est un idéal de Galois contenu dans $Id_k(H.\underline{\alpha})$.*

Démonstration. Montrons l'inclusion $J \subset Id_k(H.\underline{\alpha})$. Puisque $H \subset \mathrm{Inj}(I, \underline{\alpha})$, nous avons $I \subset Id_k(H.\underline{\alpha})$ et il suffit donc de montrer que $\sigma.R$ appartient à $Id_k(H.\underline{\alpha})$.
D'après la proposition 2.2.20, le groupe H est inclus dans le groupe de décomposition de $Id_k(H.\underline{\alpha})$ et donc $\sigma.R \in Id_k(H.\underline{\alpha})$, d'où l'inclusion.
Ceci implique, en particulier, que J est un idéal propre et, comme il contient les relations symétriques, J est un idéal de Galois (voir Proposition 2.2.5). □

Une conséquence immédiate de cette proposition est le corollaire suivant :

Corollaire 5.5.2. *Reprenons les notations de la proposition 5.5.1. Si $F = \sigma.R$ est de la forme $x_j^d + g(x_1, \ldots, x_j)$ avec $d > 0$ et $\deg_{x_j}(g) < d$ et si l'ensemble $S = \{f_1, \ldots, f_{j-1}, F, f_{j+1}, \ldots, f_n\}$ engendre un idéal I' contenant I, alors S est triangulaire séparable et $I' = J$.*

Dans le corollaire 5.5.2, il suffit que F soit un facteur de f_j dans $k[x_1, \ldots x_j]$ pour que l'hypothèse d'inclusion soit vérifiée.
Le résultat suivant montre que cette même hypothèse d'inclusion est vérifiée sous certaines conditions moins contraignantes.

Corollaire 5.5.3. *Reprenons les notations du corollaire 5.5.2 et supposons que F soit de la forme $x_j^d + g(x_1, \ldots, x_j)$, avec $d = \deg_{x_j}(Id_k(H.\underline{\alpha}))$ et $\deg_{x_j}(g) < d$. Alors, J est un idéal de Galois de f et il est engendré par l'ensemble S.*

Démonstration. D'après le corollaire 5.5.2, il suffit de montrer que $f_j \in \langle S \rangle$. D'après la proposition 5.5.1, nous avons la suite d'inclusions d'idéaux de $k[x_1, \ldots, x_j]$:

$$\langle f_1, \ldots, f_{j-1}, F \rangle \subset \langle f_1, \ldots, f_{j-1}, F, f_j \rangle \subset Id_k(H.\underline{\alpha}) \cap k[x_1, \ldots, x_j].$$

Supposons, sans perte de généralité, l'ensemble $\mathcal{T} = \{f_1, \ldots, f_n\}$ réduit et F égal à sa forme normale modulo $\mathcal{T}$. Nous avons l'isomorphisme suivant :

$$k[x_1, \ldots, x_j]/\langle f_1, \ldots, f_j, F \rangle \simeq \Big(k[x_1, \ldots, x_{j-1}]/\langle f_1, \ldots, f_{j-1} \rangle\Big)[x_j]/\langle f_j, F \rangle.$$

L'anneau $R = k[x_1, \ldots, x_{j-1}]/\langle f_1, \ldots, f_{j-1} \rangle$ est un produit de corps (voir [11, Théorème 4.4.14]), ainsi nous pouvons considérer le pgcd P de F et f_j en tant que polynôme à coefficients dans R (voir [11, Chapitre 3]). L'idéal $\langle f_j, F \rangle$ de R est donc monogène engendré par P et, en tant qu'idéaux de $k[x_1, \ldots, x_n]$, nous avons l'égalité

$$\langle f_1, \ldots, f_n, F \rangle = \langle f_1, \ldots, f_{j-1}, P, f_{j+1}, \ldots, f_n \rangle .$$

Comme P est de la forme $x_j^k + h(x_1, \ldots, x_j)$ avec $\deg_{x_j}(h) < k$ et qu'il est inclus dans $Id_k(H.\underline{\alpha})$ nous avons $k \geqslant d$. Mais comme P est le pgcd de F et f_j nous avons $k \leqslant d$ et donc $k = d$. Ainsi nous avons $P = F$ et le corollaire s'ensuit. □

Soit H un groupe associé à I et contenant $\mathrm{Gal}_k(\underline{\alpha})$, le corollaire 5.5.2 (ou le corollaire 5.5.3) permet d'en déduire un polynôme F et un idéal de Galois $J = I + \langle F \rangle$ de f. Connaissant une ensemble triangulaire de générateurs de J, nous pouvons calculer le cardinal de sa variété (voir Égalité (2.11)). Si $\mathrm{Card}(V(J)) = \mathrm{Card}(H)$ alors, d'après la proposition 2.2.28, $J = Id_k(H.\underline{\alpha})$ et H est l'injecteur de J. Dans le cas où H n'est pas l'injecteur de J, nous pouvons, dans certains cas, calculer un injecteur de J.

Rappelons que L est l'injecteur de l'idéal I_1 dont I est induit. Soit E une transversale à droite de L modulo $H_{\{1\}}$. Nous avons :

$$J = I + \langle F \rangle = \bigcap_{\tau \in E} Id_k(H\tau.\underline{\alpha}) + \langle F \rangle .$$

Soit E_1 l'ensemble des permutations $\tau \in E$ telles que $F \in Id_k(H\tau.\underline{\alpha})$. Comme les idéaux I et $\langle F \rangle$ sont inclus dans $\bigcap_{\tau \in E_1} Id_k(H\tau.\underline{\alpha})$, l'idéal $J = I + \langle F \rangle$ l'est également.

La proposition immédiate suivante permet, dans certains cas, de calculer un injecteur de J :

Proposition 5.5.4. *Supposons que* $\mathrm{Gal}_k(\underline{\alpha}) \subset H$. *Si nous avons l'égalité* $\mathrm{Card}(V(J)) = \mathrm{Card}(E_1)\,.\,\mathrm{Card}(H)$ *alors* $J = \bigcap_{\tau \in E_1} Id_k(H\tau.\underline{\alpha})$ *et l'injecteur de* J *s'écrit :*

$$Inj(J, \underline{\alpha}) = \sum_{\tau \in E_1} H\tau .$$

Ainsi, pour construire un injecteur de l'idéal J à partir de I et de la classe de L-conjugaison de H, il faut pouvoir tester la condition de la proposition 5.5.4 ; autrement dit, nous devons connaître E_1. La proposition suivante permet, dans certains cas, de calculer cet ensemble :

Proposition 5.5.5. *Reprenons les notations précédentes. Une permutation* $\tau \in \{\tau_1, \ldots, \tau_s\}$ *appartient à* E_1 *dès qu'elle vérifie la condition suivante :*

$$\exists (R, \sigma) \in I \times H^{\tau^{-1}},\ F = \sigma.R .$$

Démonstration. Montrons la contraposée de cette condition. Supposons donc que la permutation τ n'appartient pas à E_1, i.e. $F \notin \mathcal{I} = Id_k(H\tau.\underline{\alpha})$. Nous avons donc, par définition du groupe de décomposition :

$$\forall (R, \sigma) \in \mathcal{I} \times \mathrm{Dec}(\mathcal{I}),\ F \neq \sigma.R\ ,$$

puisque $\sigma.R \in \mathcal{I}$.
Comme $I \subset \mathcal{I}$, d'après la proposition 2.2.20 nous avons

$$H^{\tau^{-1}} \subset \mathrm{Dec}(Id_k(H^{\tau^{-1}}.\tau\underline{\alpha}))\,(= \mathrm{Dec}(Id_k(H\tau.\underline{\alpha})))\ .$$

Donc, $\forall (R, \sigma) \in I \times H^{\tau^{-1}},\ F \neq \sigma.R$. □

Application des résultats du paragraphe 5.5

Soit H un sous-groupe de S_n vérifiant $\mathrm{Gal}_k(\underline{\alpha}) \subset H$ (donc H est associé à I). Supposons que nous ayons calculé un polynôme $F = \sigma.R$ comme dans le corollaire 5.5.3. Soit

$$\Psi(H) = H\tau_1 + \ldots + H\tau_s\ ,$$

où $\tau_1, \ldots, \tau_r$ sont les permutations tels que $\tau_i^{-1} H \tau_i$ vérifient les mêmes hypothèses que H pour le même polynôme F (au signe près). D'après la proposition 5.5.5, nous avons $\{\tau_1, \ldots, \tau_r\} \subset E$ et donc :

$$\mathrm{Card}(V(J)) \geqslant \mathrm{Card}(E_1)\,\mathrm{Card}(H) \geqslant r\,\mathrm{Card}(H)\ .$$

Le cardinal de $V(J)$ étant connu, si $r\,\mathrm{Card}(H) = \mathrm{Card}(V(J))$ alors, d'après la proposition 5.5.5, nous avons $E_1 = \{\tau_1, \ldots, \tau_r\}$ et

$$\mathrm{Inj}(J, \underline{\alpha}) = \sum_{i=1}^{r} H\tau_i\ .$$

Exemple 5.5.6. Soit I un idéal induit d'un idéal de rupture d'un polynôme f de degré 8. Supposons que $\Delta(f) = 1^3, 2^2$. Notons $f_7(x_1, x_7)$ le 7-ième polynôme de T_I. À l'aide de la table 4.2, nous calculons l'ensemble des groupes H vérifiant $H_{\{1\}} \subset S_{1^4,2^2}$ et $\Delta(H) = \Delta(f)$. Tous ces groupes vérifient $\mathcal{L}(H) = (8, 1^3, 2, 1^3)$. En comparant avec $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$, nous en déduisons, qu'en remplaçant le polynôme f_7 de T_I par une relation $r_7(x_1, x_5, x_7)$ linéaire en x_7, nous obtiendrons un idéal des relations de f.

5.6 Construction d'un algorithme

Dans ce paragraphe, nous décrivons une méthodologie à suivre pour établir les précalculs d'un algorithme de détermination des injecteurs de tout idéal induit (voir Définition 5.2.5). Cette méthodologie met en œuvre les résultats théoriques des paragraphes précédents.

Ici nous nous restreignons au cas des idéaux induits d'idéaux de rupture. Cette étude pourra être généralisée au cas d'un idéal induit d'un idéal de Galois de $k(\alpha_1)[x_1, \ldots, x_n]$ puisque les résultats généraux des paragraphes précédents ont été écrits dans ce sens.

Soit n un entier positif. Nous allons établir les dífférentes étapes permettant de construire un algorithme de calcul d'un idéal de Galois, ainsi que d'un de ses injecteurs,

d'un polynôme irréductible f de degré n à partir d'un de ses idéaux de rupture. L'idéal de Galois ainsi construit sera le plus proche possible d'un idéal des relations. Pour ce faire nous allons étudier comment distinguer au mieux le groupe de Galois du polynôme f.

Étape 1 : Distinction des degrés de rupture

Avec la table de rupture en degré n, nous déterminons l'ensemble E des entiers e tels que $1, e \in \{\Delta(G) \mid G \in \mathcal{T}(n)\}$ (voir Chapitre 4 pour la notation $\mathcal{T}(n)$). Les groupes susceptibles d'être les injecteurs des idéaux de rupture d'un polynôme de degré n sont les $S_{1,e}$ où e parcourt E.

Pour chaque élément e de E nous suivons alors les étapes qui suivent. Fixons e dans E, $L = S_{1,e}$ l'injecteur d'un idéal de rupture d'un polynôme f tel que $\Delta(f) = e$ et I un idéal induit d'un de ces idéaux de rupture. À l'aide de la table de rupture de degré n nous pouvons déterminer l'ensemble

$$\mathcal{G} = \{G \in \mathcal{T}(n) \mid \Delta(G) = 1, e\}.$$

Un polynôme f tel que $\Delta(f) = e$ aura donc son groupe de Galois dans $\mathcal{G}$.

Pour un groupe G dans $\mathcal{G}$, nous avons vu au paragraphe 5.4, que les S_n-conjugués de G qui sont des groupes de décomposition d'un idéal maximal contenant I sont exactement ceux qui sont dans $\mathcal{A}(L)$. Il devient naturel de définir l'ensemble

$$\mathcal{A}(L, G) = \{G^\sigma \mid \sigma \in S_n\} \cap \mathcal{A}(L).$$

Étape 2 : Calcul de $\mathcal{A}(L)$ et des ensembles $\mathcal{A}(L, G)$

Avec l'un des systèmes `GAP` (voir [45]) ou Magma(voir [20]), sont calculés les ensembles $\mathcal{A}(L, G)$, pour tout groupe $G \in \mathcal{G}$. L'ensemble $\mathcal{A}(L)$ est obtenu avec l'égalité

$$\mathcal{A}(L) = \bigcup_{G \in \mathcal{G}} \mathcal{A}(L, G). \tag{5.1}$$

D'après le théorème 5.4.2, comme nous cherchons à exhiber un injecteur de l'idéal I nous pouvons nous restreindre aux classes de $\mathcal{G}$ selon la relation $\mathcal{R}$ définie par : Soient G_1 et G_2 deux groupes de $\mathcal{G}$. Alors

$$G_1 \mathcal{R} G_2 \text{ si } \exists (H_1, H_2) \in \mathcal{A}(L, G_1) \times \mathcal{A}(L, G_2) \text{ tq } \Psi(H_1) = \Psi(H_2).$$

Nous cherchons maintenant à discriminer certaines de ces classes.

Étape 3 : Discrimination des classes de $\mathcal{G}/\mathcal{R}$

Il s'agit d'utiliser des critères pour distinguer les classes de $\mathcal{R}$-équivalence de $\mathcal{G}$ afin d'être en mesure de déterminer la classe de $\mathcal{R}$-équivalence du groupe $\mathrm{Gal}_k(f)$ (parité du groupe de Galois, critère de Dedekind, etc). En fait, il faut chercher, pour chaque classe, des informations communes aux groupes de cette classe qui la discriminent des autres classes. Dans le cadre de cette étude, en plus des critères classiques (parité du groupe de Galois, critère de Dedekind, etc), nous disposons du critère décrit ci-après.

Test du groupe de décomposition
D'après le corollaire 5.4.3, nous savons que si L est l'injecteur de l'idéal I_1 alors $\mathrm{Card}(V(I)) = n\,\mathrm{Card}(L)$. Supposons que, pour un groupe $G \in \mathcal{G}$, nous ayons $\mathrm{Card}(G) = n.\,\mathrm{Card}(L)$ alors

$$\mathrm{Card}(G) = \mathrm{Card}(V(I)).$$

Par suite, pour tout $H \in \mathcal{A}(L,G)$, $\Psi(H) = H$ et nous sommes en présence de deux cas :

1. Cas où $\mathrm{Dec}(I) \in \mathcal{A}(L,G)$. Comme, dans ce cas particulier, pour tout $\mathcal{M} \in \mathcal{M}(I)$, $\mathrm{Dec}(\mathcal{M}) \subset \mathrm{Dec}(I)$ (voir Proposition 2.2.15) et $\mathrm{Dec}(\mathcal{M}) \in \mathcal{A}(L)$ (voir Remarque 5.4.16), l'algorithme `GaloisIdéal` peut être utilisé avec pour paramètres I, son injecteur $\mathrm{Dec}(I)$ et la liste des sous-groupes de $\mathrm{Dec}(I)$ dans $\mathcal{A}(L)$.
2. Cas où $\mathrm{Dec}(I) \notin \mathcal{A}(L,G)$. Le groupe de Galois $\mathrm{Gal}_k(f)$ n'est pas dans la classe de $\mathcal{R}$-équivalence du groupe G. Pour tout groupe G' de cette classe, aucun groupe de $\mathcal{A}(L,G')$ n'est associé à l'idéal I.

Une fois qu'un maximum de classes de $\mathcal{R}$-équivalence de $\mathcal{G}$ ont été discriminées, nous cherchons à associer une classe de L-conjugaison à l'idéal I pour calculer son injecteur.

Étape 4 : Discrimination des classes de L-conjugaison dans $\mathcal{A}(L,G)$

Dans cette partie, nous considérons C_0 une classe de $\mathcal{R}$-équivalence de $\mathcal{G}$. Nous sommes en présence de deux cas :

4.1 Il existe $G \in C_0$ tel que tous les groupes de $\mathcal{A}(L,G)$ soient L-conjugués entre eux. Si $\mathrm{Gal}_k(f) \in C_0$ (pour ce test, voir Étape 3) alors tous les groupes de $\mathcal{A}(L,G)$ sont associés à I et ses injecteurs sont les $\Psi(H)$ où H parcourt $\mathcal{A}(L,G)$ (voir Théorème 5.4.2).

4.2 l'hypothèse du Cas 4.1 n'est pas vérifiée. Soit $G \in C_0$. Les résultats du paragraphe 5.4.3 sont utilisés pour se ramener au Cas 4.1. Afin de pouvoir faire des pré-calculs, la méthode est de fixer une classe de L-conjugaison dans $\mathcal{A}(L,G)$ et de déterminer quelles permutations il faudra opérer sur tout idéal induit I afin que cette classe lui soit associée (dans le cas où $\mathrm{Gal}_k(f) \in C_0$ sinon ce sera impossible).

Il est aussi possible d'appliquer cette étape avant la troisième afin d'éliminer plus facilement des classes de $\mathcal{R}$-équivalence de $\mathcal{G}$. Ce qui suit n'est pas exactement une étape puisque cette étude peut être faite après ou avant chacune des étapes 2 et 3.

Étape 5 : Adjonction de relations

Nous utilisons les résultats du paragraphe 5.5 (Corollaire 5.5.3 et Proposition 5.5.4) afin de savoir s'il sera possible de calculer un idéal J contenant strictement I. Cette étape 5 peut intervenir à tout niveau de l'étude et permet parfois d'éviter de résoudre les problèmes soulevés dans l'étape 3 et/ou dans le cas 4.2 de l'étape 4. À cet égard, l'étude faite pour le degré 8 illustrera parfaitement toutes les situations possibles.

5.7 Étude en degré 8

Pour illustrer ces résultats, nous avons choisi d'étudier le degré $n = 8$. L'objectif est l'élaboration d'un algorithme de calcul d'un idéal des relations $\mathcal{M} = Id_k(\underline{\alpha})$, où $\underline{\alpha}$ est

un octuplet des racines de f, et du groupe de Galois correspondant $\mathrm{Gal}_k(\underline{\alpha}) = \mathrm{Dec}(\mathcal{M})$ (ce groupe est rapidement calculable avec l'algorithme décrit dans [3]).

Nous excluons le cas où $\Delta(f) = 7$, c'est-à-dire celui où le groupe de Galois de f est 2-transitif. Nous supposons construit un ensemble triangulaire

$$T_I = \{f_1(x_1), \ldots, f_8(x_1, \ldots, x_8)\},$$

de générateurs de l'idéal I induit d'un idéal de rupture de f d'injecteur L. Nous avons $L = S_{1,\Delta(f)}$.

Les groupes $8T_i$ de l'ensemble $\mathcal{T}(8)$ sont notés T_i. Nous utilisons des groupes conjugués $G_i = T_i^{\sigma_i}$ des groupes T_i où les permutations σ_i sont données ci-dessous :

σ_6	=	$(2,7,6,3,5)$	σ_7	=	$(2,7,3,4,5)(6,8)$
σ_8	=	$(4,8)(2,5,3,6,7)$	σ_{12}	=	$(2,7,6,4,5)$
σ_{13}	=	$\sigma_{24} = (2,4,6)(5,7,8)$	σ_{14}	=	$(2,4,6,7,8,3,5)$
σ_{17}	=	$(2,3,4,5,6,8)$	σ_{18}	=	$(1,5)(2,7)(3,8)(4,6)$
σ_{19}	=	$(2,3)(4,7,6,8)$	σ_{31}	=	$(2,7,6,8,3,5)$
σ_{39}	=	$(2,6)(7,8)$	σ_{33}	=	$(4,8)$

– pour $i \in \{23, 38, 40, 44\}$, $\sigma_i = (2,5)(4,7)$ et,
– pour $i \in \{46, 45, 42, 41, 34, 33\}$, $\sigma_i = \sigma_{47}$.

Dans les paragraphes suivants et à l'aide de la table de rupture en degré 8 (voir Tables 4.2), nous appliquons la méthodologie prescrite au paragraphe 5.6 en examinant les différentes situations possibles en fonction de $\Delta(f)$.

5.7.1 $\Delta(f) = 1^7$; i.e. $L = S_{1^8}$ et $\mathcal{L}(I) = (8, 1^7)$

$\mathcal{G}/\mathcal{R} = \{\{T_1\}, \{T_2^+\}, \{T_3^+\}, \{T_4^+\}, \{T_5^+\}\}$. L'idéal induit I est un idéal $\mathcal{M}$ des relations du polynôme f ;

Exemple 5.7.1. Le polynôme irréductible $f = x^8 + 8x^6 + 20x^4 + 16x^2 + 2$ se factorise, dans $k(\alpha_1)$, en le produit de facteurs irréductibles :

$$(x-\alpha_1)(x+\alpha_1)(x-\alpha_1^3-3\alpha_1)(x+\alpha_1^3+3\alpha_1)(x-\alpha_1^5-5\alpha_1^3-5\alpha_1)$$
$$(x+\alpha_1^5+5\alpha_1^3+5\alpha_1)(x-\alpha_1^7-7\alpha_1^5-14\alpha_1^3-7\alpha_1)(x+\alpha_1^7+7\alpha_1^5+14\alpha_1^3+7\alpha_1).$$

Nous avons $\mathrm{Dec}(\mathcal{M}) = T_1^\sigma$ avec $\sigma = (2,3,7,8,5)(4,6)$ et

$$\begin{aligned}\mathcal{M} = \langle & f(x_1),\ x_2 + x_1,\ x_3 - x_1^3 - 3x_1,\\ & x_4 + x_1^3 + 3x_1,\ x_5 - x_1^5 - 5x_1^3 - 5x_1,\ x_6 + x_1^5 + 5x_1^3 + 5x_1,\\ & x_7 - x_1^7 - 7x_1^5 - 14x_1^3 - 7x_1,\ x_8 + x_1^7 + 7x_1^5 + 14x_1^3 + 7x_1\rangle\ .\end{aligned}$$

5.7.2 $\Delta(f) = 1^3, 2^2$; i.e. $L = S_{1^4,2^2}$ et $\mathcal{L}(I) = (8, 1^3, 2, 1, 2, 1)$

$\mathcal{G}/\mathcal{R} = \{\{T_7\}, \{T_9^+\}, \{T_{10}^+\}, \{T_{11}^+\}\}$. Pour tout $H \in \mathcal{A}(L)$, nous avons $\mathcal{L}(H) = (8, 1^3, 2, 1^3)$. En comparant avec $\mathcal{L}(I)$, nous savons que nous cherchons une relation de la forme $r_7 = x_7 + h_7(x_1, \ldots, x_6)$ pour obtenir un ensemble triangulaire $T' = \{f_1, \ldots, f_6, r_7, f_8\}$ engendrant un idéal des relations $\mathcal{M}$. Les polynômes f_2 et f_3 de T_I sont respectivement de la forme $x_2 + g_2(x_1)$ et $x_3 + g_3(x_1)$.

La parité de $\mathrm{Gal}_k(f)$ permet de distinguer deux cas (voir Étape 3).

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

Ce cas a été traité dans l'exemple 5.4.20 où est décrit un critère d'association (Étape 4). En utilisant le théorème 5.4.11, il est possible de réordonner les facteurs de première rupture pour que la classe de L-conjugaison dans $\mathcal{A}(L)$ associée à I soit celle de G_7 (ceci est équivalent à $x_6 + g_2(x_5) \in I$).
En appliquant le corollaires 5.5.3 et la proposition 5.5.4 à $H = G_7$, nous obtenons la relation $r_7 = x_7 + g_3(x_5)$ de T' avec $\mathrm{Dec}(\mathcal{M}) = G_7$ (Étape 5).

Cas B $\mathrm{Gal}_k(f) \in \mathcal{G}^+ = \{T_9^+, T_{10}^+, T_{11}^+\}$.
Pour $G \in \mathcal{G}^+$, notons $\mathcal{C}_i(G)$, $i = 1, 2, 3$, les trois classes de L-conjugaison dans $\mathcal{A}(L, G)$. Chaque classe est constituée de 2 groupes. En raisonnant comme dans l'exemple 5.4.20, pour chaque groupe $G \in \mathcal{G}^+$, nous obtenons le critère d'association suivant (Étape 4) :
1) si $x_6 + g_4(x_5) \in I$ alors I est associé à $\mathcal{C}_1(G)$;
2) si $x_6 + g_2(x_5) \in I$ alors I est associé à $\mathcal{C}_2(G)$;
3) si $x_6 + g_3(x_5) \in I$ alors I est associé à $\mathcal{C}_3(G)$.

Supposons l'idéal I induit de f associé à $\mathcal{C}_1(\mathrm{Gal}_k(f))$. Quelque soit $i \in \{9, 10, 11\}$ il existe $H_i \in \mathcal{C}_1(T_i^+)$ et une permutation $\sigma \in H_i$ telle que $r_7 = \sigma.f_2 = x_7 + g_2(x_5)$ (Étape 5). L'ensemble triangulaire T' étant ainsi obtenu, il reste à déterminer lequel des trois groupes H_i, $i = 9, 10, 11$, est le groupe de décomposition de $\mathcal{M} = \langle T' \rangle$.

5.7.3 $\Delta(f) = 1^3, 4$; i.e. $L = S_{1^4,4}$ et $\mathcal{L}(I) = (8, 1^3, 4, 3, 2, 1)$

$\mathcal{G}/\mathcal{R} = \{\{T_{17}\}, \{T_{18}^+\}\}$. Pour tout $H \in \mathcal{A}(L)$, $\mathcal{L}(H) = (8, 1^3, 4, 1, 1, 1)$. Nous cherchons deux relations de la forme $r_6 = x_6 + h_6(x_1, \ldots, x_5)$ et $r_7 = x_7 + h_7(x_1, \ldots, x_6)$ pour obtenir un ensemble $T' = \{f_1, \ldots f_5, r_6, r_7, f_8\}$ engendrant l'idéal $\mathcal{M}$. Les polynômes f_2 et f_3 de T_I sont respectivement de la forme $x_2 + g_2(x_1)$ et $x_3 + g_3(x_1)$. Le calcul du discriminant de f permet de distinguer deux cas.

Cas A Le groupe de Galois de f est le groupe pair T_{18}^+.
Les groupes de $\mathcal{A}(L, T_{18}^+)$ sont L-conjugués (Étape 4, Cas 4.1). À l'étape 5, nous trouvons les relations $r_6 = x_6 + g_4(x_5)$ et $r_7 = x_7 + g_2(x_5)$ de T' avec $\mathrm{Dec}(\mathcal{M}) = G_{18}$.

Cas B Le groupe de Galois de f est le groupe impair T_{17}.
L'ensemble $\mathcal{A}(L, T_{17})$ est constitué de 3 classes $\mathcal{C}_i$ de L-conjugaison de 6 groupes chacune et satisfaisant le critère d'association suivant :

1) si $x_1 + g_4(x_2) \in I$ alors I est associé à $\mathcal{C}_1$;
2) si $x_1 + g_3(x_2) \in I$ alors I est associé à $\mathcal{C}_2$;
3) si $x_1 + g_2(x_2) \in I$ alors I est associé à $\mathcal{C}_3$.

Supposons la classe $\mathcal{C}_2$ associée à l'idéal induit I. À l'étape 5, nous trouvons les relations $r_6 = x_6 + g_3(x_5)$ et $r_7 = x_7 + g_2(x_5)$ de T' et $\mathrm{Dec}(\mathcal{M}) = G_{17}$.

5.7.4 $\Delta(f) = 1, 2^3$; i.e. $L = S_{1^2,2^3}$ et $\mathcal{L}(I) = (8, 1, 2, 1, 2, 1, 2, 1)$

Il y a 4 classes de $\mathcal{R}$-conjugaison dans $\mathcal{G}$: $\{T_6\}, \{T_8\}$, les sous-groupes de T_{27} et ceux de T_{31} dans $\mathcal{G}$. Comme $\mathrm{Card}(T_{27}) = \mathrm{Card}(T_{31}) = 8.\,\mathrm{Card}(L) = 64$, le calcul du groupe de décomposition $\mathrm{Dec}(I)$ permet de distinguer trois cas (voir Étape 3) :

Cas A. $\mathrm{Dec}(I) \in \mathcal{A}(L, T_{27})$ (i.e. $\mathrm{Dec}(I)$ est conjugué à T_{27}).
Nous avons, pour tout $\underline{\alpha} \in V(I)$, $\mathrm{Gal}_k(\underline{\alpha}) \subset \mathrm{Dec}(I) = \mathrm{Inj}(I)$. Selon la parité du groupe de Galois, le calcul de $\mathcal{M}$ est réalisé avec l'un des appels `GaloisIdéal(`$\mathrm{Dec}(I)$`, `T_I`,`

`[`H_{20}`])` ou `GaloisIdéal(`Dec(I)`, `T_I`, [`H_{16}`])`, où H_{16} et H_{20} sont des sous-groupes de Dec(I) conjugués respectifs de T_{16} et T_{20}^+.

Cas B. Dec(I) $= G_{31}$ (car $\mathcal{A}(L, T_{31}) = \{G_{31}\}$).
Selon la parité du groupe de Galois, le calcul de $\mathcal{M}$ est réalisé avec l'un des appels `GaloisIdéal(`G_{31}`,`T_I`,[`G_{21}`])` ou `GaloisIdéal(`G_{31}`,`T_I`,[`G_{22}`])`, où les groupes G_{21} et G_{22} sont les uniques sous-groupes de G_{31} conjugués respectifs des groupes T_{21} et T_{22}^+.

Cas C. Dec(I) $\notin \mathcal{A}(L, T_{27})$ et Dec(I) $\neq G_{31}$
Lorsque les cas A. et B. ne sont pas vérifiés, $\mathrm{Gal}_k(f) \in \{T_6, T_8\}$. Or, tout groupe G de $\mathcal{A}(L, T_6) \cup \mathcal{A}(L, T_8)$ vérifie $\mathcal{L}(G) = (8, 1, 2, 1^5)$. Nous savons donc que deux relations linéaires $r_5 = x_5 + h_5(x_1, x_3)$ et $r_7 = x_7 + h_7(x_1, x_3)$ sont à déterminer. Le polynôme f_2 de T_I est de la forme $x_2 + g_2(x_1)$.

Pour $G = T_6$ ou $G = T_8$, en notant $C_i(G)$ les 3 classes de L-conjugaison de $\mathcal{A}(L, G)$, nous avons le critère d'association suivant :

1) si $x_4 + g_2(x_3) \in I$ alors I est associé à $\mathcal{C}_1(G)$;
2) si $x_6 + g_2(x_5) \in I$ alors I est associé à $\mathcal{C}_2(G)$;
3) si $x_8 + g_2(x_7) \in I$ alors I est associé à $\mathcal{C}_3(G)$.

Supposons $\mathcal{C}_2(\mathrm{Gal}_k(f))$ associée à l'idéal I. Les groupes G_6 de $\mathcal{C}_2(T_6)$ et G_8 de $\mathcal{C}_2(T_8)$ permettent d'obtenir la relation linéaire $r_7 = x_7 + g_2(x_3)$ et l'idéal $J = I + \langle r_7 \rangle$ est l'intersection de deux idéaux des relations (voir Égalités (2.4) et 2.9). Pour $i = 6, 8$, l'autre groupe de la classe $\mathcal{C}_2(T_i)$ permettant de rajouter cette relation est $H_i = G_i^\sigma$ avec $\sigma = (5, 6)$.
Le calcul d'un idéal des relations peut alors être réalisé par l'appel

`GaloisIdéal(`L_i`,`T_J`,[`G_i`])`

où $L_i = G_i + G_i\sigma$ ($i = 6, 8$) est l'injecteur de J selon que le groupe de Galois est T_6 ou T_8. (Pour le calcul de L_i, voir Théorème 5.4.2 et Proposition 5.5.5). La proposition 5.4.17 permet d'identifier le groupe de Galois en déterminant lequel des ensembles L_6 ou L_8 est un injecteur de J.

5.7.5 $\Delta(f) = 1, 2, 4$; i.e. $L_0 = S_{1^2,2,4}$ et $\mathcal{L}(I) = (8, 1, 2, 1, 4, 3, 2, 1)$

Dans l'ensemble $\mathcal{G}$, tous les groupes sont $\mathcal{R}$-équivalents car ils sont tous des sous-groupes du groupe T_{35} de $\mathcal{G}$. Les degrés des facteurs de ruptures étant distincts deux-à-deux, il n'y a qu'une classe de L-conjugaison dans chaque ensemble $\mathcal{A}(L, G)$, pour tout $G \in \mathcal{G}$. Nous passons donc les étapes 3 et 4 et arrivons à l'étape 5.

En comparant $\mathcal{L}(G_{35}) = (8, 1, 2, 1, 4, 1, 2, 1)$ à $\mathcal{L}(I)$ et en considérant le polynôme f_2 de la forme $x_2 + g_2(x_1)$, nous trouvons l'idéal J d'injecteur G_{35} et engendré par

$$T_J = \{f_1, \ldots, f_5, x_6 + g_2(x_5), f_7, f_8\}.$$

L'ensemble des groupes de Galois des éléments de $V(J)$ est celui des sous-groupes de G_{35} inclus dans $\mathcal{A}(L, \mathrm{Gal}_k(f))$. Selon que le groupe de Galois $\mathrm{Gal}_k(f)$ soit pair ou impair, le calcul se termine par les appels respectifs :

`GaloisIdéal(`G_{35}`,`T_J`, [`G_{29}, G_{19}, H_{19}`])` et
`GaloisIdéal(`G_{35}`, `T_J`,[`$G_{26}, G_{28}, G_{30}, G_{15}, H_{15}$`])`,

où $H_{19} = T_{19}^{(2,3)(4,8)(6,7)}$ et $H_{15} = T_{15}^{(2,8,6,7,4,5)}$.

Le groupe de Galois sur $k(\alpha_1)$ du facteur de rupture $f_5(\alpha_1, x) = x^4 + g(\alpha_1, x)$ de f départage T_{19}^+ et T_{29}^+ ; de plus, la parité de ce groupe de Galois détermine si $\mathrm{Gal}_k(f)$ est ou non T_{15} (voir Table 4.2).

5.7.6 $\Delta(f) = 1, 3^2$; i.e. $L = S_{1^2,3^2}$ et $\mathcal{L}(I) = (8, 1, 3, 2, 1, 3, 2, 1)$

Nous avons $\mathcal{G}/\mathcal{R} = \{\{T_{13}^+, T_{14}^+, T_{24}^+\}, \{T_{12}^+\}\}$. Bien que, pour chaque groupe de $\mathcal{G}$, l'ensemble $\mathcal{A}(L, G)$ possède plusieurs classes de L-conjugaison et que $\mathcal{G}$ possède plusieurs classes de $\mathcal{R}$-équivalence, l'étape 5 va pouvoir s'appliquer dès le départ. La relation f_2 de T_I est de la forme $x_2 + g_2(x_1)$. Pour tout groupe de $\mathcal{A}(L)$, il existe un groupe G dans sa classe de L-conjugaison tel que $r_6 = x_6 + g_2(x_3)$ et $r_7 = x_7 + g_2(x_4)$ appartiennent à $Id_k(G.\underline{\alpha})$ (voir Corollaire 5.5.3). L'ensemble $T_J = \{f_1, \ldots, f_5, r_6, r_7, f_8\}$ engendre un idéal de Galois J tel que $\prod_{i=1}^{8} deg_{x_i}(J) = \mathrm{Card}(T_{24}) = 48$. Nous passons à l'étape 3 avec l'idéal J à la place de I.

Cas A $\mathrm{Dec}(J) \in \mathcal{A}(L, T_{24}) = \{G_{24}, T_{24}^{(2,8,6)(3,7)}\}$.
$\mathrm{Gal}_k(f) \in \{T_{24}, T_{13}, T_{14}\}$. Ordonnons les facteurs de première rupture de f de sorte que $\mathrm{Dec}(J) = G_{24}$. Le calcul de l'idéal $\mathcal{M}$ est réalisé avec l'appel

$$\texttt{GaloisIdéal(}G_{24}\texttt{, }T_J\texttt{,[}G_{13}, G_{14}\texttt{])}.$$

Cas B $\mathrm{Dec}(J)$ n'est pas un conjugué de T_{24}.
Le groupe de Galois est alors T_{12}. Les conjugués de T_{12} appartenant à $\mathcal{A}(L)$ ne forment qu'une seule classe de L-conjugaison. D'après le théorème 5.4.2, nous savons que l'idéal des relations $\mathcal{M}$ peut être choisi de telle sorte que $\mathrm{Inj}(J, \mathcal{M}) = G_{12} + G_{12}(3,4)(6,7)$. Son calcul peut se faire avec l'appel

$$\texttt{GaloisIdéal(}G_{12} + G_{12}(3,4)(6,7)\texttt{, }T_J\texttt{, [}G_{12}\texttt{])}.$$

Remarque 5.7.2. Si le groupe de Galois d'un des facteurs de rupture de degré 3 est $3T_2$ (i.e. S_3) alors $\mathrm{Gal}_k(f) = T_{24}^+$ (voir Table 4.2).

5.7.7 $\Delta(f) = 1, 6$; i.e. $L = S_{1^2,6}$ et $\mathcal{L}(I) = (8, 1, 6, 5, 4, 3, 2, 1)$

Le groupe de Galois est un sous-groupe de T_{44}. Le polynôme f_2 de T_i est de la forme $x_2 + g_2(x_1)$. À l'étape 5, avec $\mathcal{L}(G_{44}) = (8, 1, 6, 1, 4, 1, 2, 1)$, nous trouvons l'ensemble triangulaire $T_J = \{f_1, f_2, f_3, x_4 + g_2(x_3), f_5, x_6 + g_2(x_5), f_7, f_8\}$ engendrant l'idéal J d'injecteur G_{44}. Les calculs se terminent, selon la parité de $\mathrm{Gal}_k(f)$, avec

$$\texttt{GaloisIdéal(}G_{44}\texttt{,}T_J\texttt{,[}G_{39}^+\texttt{, }G_{19}^+\texttt{])} \text{ ou}$$
$$\texttt{GaloisIdéal(}G_{44}\texttt{,}T_J\texttt{,[}G_{40}, G_{38}, G_{23}\texttt{])}$$

5.7.8 $\Delta(f) = 3, 4$, $L = S_{1,3,4}$ et $\mathcal{L}(I) = (8, 3, 2, 1, 4, 3, 2, 1)$

Le groupe de Galois est un sous-groupe de G_{47}. Nous avons $\prod_{i=1}^{n} deg_{x_i}(I) = \mathrm{Card}(G_{47})$. D'après la proposition 2.2.28, le groupe G_{47} est l'unique injecteur de I. Selon la parité du groupe de Galois de f, nous terminons le calcul de $\mathcal{M}$ avec

$$\texttt{GaloisIdéal(}G_{47}\texttt{,}T_I\texttt{,[}G_{45}^+, G_{42}^+, G_{41}^+, G_{34}^+, G_{33}^+\texttt{])}$$
$$\text{ou } \texttt{GaloisIdéal(}G_{47}\texttt{,}T_I\texttt{,[}G_{46}\texttt{])}.$$

5.8 Expérimentations et remarques

Dans cette partie, nous comparons notre algorithme à l'algorithme classique de factorisation dans les extensions successives. Nous avons fait nos comparaisons pour des polynômes irréductibles de degré 8 à coefficients dans $\mathbb{Q}$ en nous basant sur l'étude du paragraphe précédent.

Nous appellerons `FEGI` (algorithme de Factorisation dans les Extensions puis algorithme `GaloisIdéal`) l'algorithme que nous proposons dans ce chapitre. Nous allons le comparer à celui de [7] que nous appellerons `FE`.

Nous avons implanté les deux algorithmes dans le système de calcul formel Magma. Nous avons choisi ce logiciel car il permet de travailler avec toutes les structures mathématiques dont nous avons besoin (groupes symétriques, polynômes univariés et multivariés, algèbres affines ...).

L'utilisation de la factorisation de polynômes à coefficients dans un corps de nombres (non trivial) a mis en évidence un bogue (maintenant connue par l'équipe de développement du logiciel Magma). Nous avons donc implanté l'algorithme de factorisation donné dans [7], version améliorée de celui de Trager (voir [101]) et utilisé cet algorithme dans les cas où des problèmes se sont posés.

Pour nos comparaisons, nous avons utilisé des polynômes de la base de données de J. Klüners et G. Malle (voir [59]). Les temps de calcul, en "cpu-seconde", sont recensés dans le tableau 5.1. Pour chaque ligne, la première colonne contient le polynôme considéré, la seconde son groupe de Galois sur $\mathbb{Q}$, la suivante l'ordre de ce groupe, et les deux dernières donnent respectivement le temps de calcul des algorithmes `FE` et `FEGI`. Tous ces tests ont été effectués sur Giulia4 [50] de la grappe Médicis. Remarquons que l'implantation de l'algorithme `FE` faite dans le logiciel Risa/Asir [91] (interfacé avec PARI [88] version 2.2.5 pour la factorisation des polynômes à coefficients rationnels) nous a donné des temps équivalents à ceux de notre implantation en Magma.

f	$\mathrm{Gal}(f)$	$\lvert\mathrm{Gal}(f)\rvert$	`FE`	`FEGI`
$x^8 - x^7 - 7x^6 + 5x^5 + 15x^4 - 7x^3 - 10x^2 + 2x + 1$	$8T_{47}$	1152	1085.54	0.10
$x^8 + 7x^7 - 10x^6 - 131x^5 - 200x^4 + 131x^3 + 382x^2 - 191$	$8T_{46}$	576	2509.58	16.81
$x^8 - x^5 - x^4 - x^3 + 1$	$8T_{44}$	384	37.8	0.11
$x^8 - x^7 - 4x^5 + 2x^4 + 3x^2 - x - 1$	$8T_{40}$	192	50.7	58.1
$x^8 + x^4 - 4x^2 + 1$	$8T_{39}$	192	10.54	0.17
$x^8 - 3x^7 - 13x^6 + 18x^5 + 42x^4 - 17x^3 - 31x^2 + 2x + 4$	$8T_{38}$	192	59.78	> 200
$x^8 + 2x^6 - 12x^4 - 3x^2 + 11$	$8T_{35}$	128	3.53	0.32
$x^8 + 2x^7 - 27x^6 - 93x^5 - 3x^4 + 272x^3 + 263x^2 + 35x - 2$	$8T_{32}$	96	51.8	> 100
$x^8 + 12x^6 + 48x^4 + 72x^2 + 31$	$8T_{31}$	64	0.66	0.26
$x^8 - x^6 - x^4 + x^2 + 1$	$8T_{29}$	64	2.03	0.65
$x^8 - 5x^5 - 3x^4 - 5x^3 + 1$	$8T_{26}$	64	1.8	1.44
$x^8 - x^7 - x^5 + 25x^4 - 54x^3 + 50x^2 - 8x + 9$	$8T_{23}$	48	2.9	0.87
$x^8 + x^6 + 2x^2 + 4$	$8T_{19}$	32	0.63	0.82

Tab. 5.1 – Temps de calcul.

Même si le logiciel Magma est doté d'une implantation de l'algorithme de factorisation de van Hoeij (voir [109]) pour les polynômes à coefficients rationnels, si un tel algorithme adapté aux polynômes à coefficients dans une tour d'extensions existait nous obtiendrions probablement de meilleurs temps pour l'algorithme `FE`. Dans le cas où les

coefficients appartiennent à une extension simple de $\mathbb{Q}$, une telle factorisation existe dans le système PARI depuis la version 2.2.5 (voir [88]). C'est une implantation d'un algorithme de K. Belabas (voir [16]).

Comme nous pouvons le voir dans le tableau 5.1, notre méthode nous a donné des résultats intéressants. Pourtant, nous ne pouvons garantir de tels temps pour d'autres exemples. En effet, l'algorithme `GaloisIdéal` nécessite des calculs de résolvantes séparables qui peuvent être parfois laborieux à mener à terme. Lors d'un tel calcul il faut pouvoir trouver un *élément séparant* et ceci se fait de manière aléatoire, tout en étant assuré que l'on finira par en trouver un. Dans [28], A. Colin donne un ensemble fini d'invariants dans lequel on est sûr d'en trouver un qui soit séparable. Dans nos tests, c'est par exemple ce qui s'est passé pour les polynômes de groupe de Galois $8T_{38}$ et $8T_{32}$. Dans ces deux cas nous avons arrêté les calculs après plusieurs calculs (une centaine au moins) de résolvantes qui n'étaient pas séparables. Ce même genre de problème est aussi rencontré dans les algorithmes de calcul de *représentation univariée rationelle* (voir [93]), mais dans ce cas, les invariants permettant de trouver un élément séparant sont tous linéaires et ce dernier est beaucoup plus facil à calculer.

Il devient alors naturel de penser à remplacer l'utilisation de l'algorithme `GaloisIdéal` par un autre calculant des corps de décomposition.
Par exemple, A. Valibouze propose de le remplacer (voir [108]) par l'algorithme de Yokoyama (voir [113, Section 5.3] et Chapitre 7) dès que la connaissance du groupe de Galois est acquise (on pourra aussi appliquer la méthode de Mckay et Stauduhar (voir [75])). Pour pouvoir faire un tel remplacement, il faut encore étudier le moyen de passer des informations obtenues après des factorisations dans des extensions aux objets nécessaires à l'entrée de l'algorithme de Yokoyama. En effet, cette méthode nécessite de connaître l'action exacte du groupe de Galois sur des approximations p-adiques des racines du polynômes. Tout de même, cette idée est très prometteuse dans le cadre du calcul simultané du groupe de Galois et de l'idéal des relations. C'est pourquoi, il serait intéressant de poursuivre cette étude dans un travail futur.

Tout au long de ce chapitre nous avons supposé le polynôme f irréductible sur k, mais notre méthode est généralisable aux polynômes réductibles en l'appliquant à chacun de ses facteurs et en utilisant les résultats du paragraphe 2.4. De plus, les résultats de ce chapitre permettent d'utiliser inductivement notre méthode dans les extensions supérieures. Pour pouvoir mettre en pratique cette généralisation, nous nous sommes placés dans le cas d'un idéal I_1 contenant un idéal de rupture de f dès le paragraphe 5.2. Elle pourra donc, en particulier, être appliquée à certains polynômes de groupe de Galois 2-transitif.

Chapitre 6

Idéal des relations d'un polynôme dihédral

6.1 Introduction

Soit f un polynôme à coefficients dans k de degré $n \geqslant 5$. Dans ce chapitre nous appliquons les résultats du chapitre 5 dans le cas particulier où l'on sait que le groupe de Galois de f est de type dihédral. Ainsi, nous voulons calculer une base triangulaire d'un idéal des relations I de f et $\mathrm{Dec}(I)$ à partir de la factorisation de f sur un de ses corps de rupture L.

Dans le cas particulier $n = 5$ et $k = \mathbb{Q}$, Spearman et Williams donnent dans [98], des formules qui, à partir de deux racines de f et de sa factorisation sur son corps de rupture L, permettent de retrouver les trois autres. Dans ce chapitre nous proposons un algorithme qui, à partir de la factorisation de f sur L, permet de calculer un ensemble triangulaire de générateurs d'un idéal des relations de f et ceci en ne faisant que des calculs de formes normales. De plus, nous aurons en sortie le groupe de décomposition de cet idéal.

La méthode que nous proposons ici est symbolique puisque nous fournissons une représentation en tour d'extensions du corps de décomposition de f. Elle peut donc être vue comme une généralisation symbolique du résultat de Spearman et Williams.

De plus, nous donnons le nombre maximal de formes normales nécessaires au calcul de l'idéal des relations. Ce nombre est borné par $O(n^2)$ mais nous obtenons aussi le résultat particulier suivant : dans le cas $n = 5$ aucun calcul n'est nécessaire pour construire un idéal des relations de f à partir des données du problème f.

Notation Dans ce chapitre nous utiliserons la notation suivante :

D_n sera la représentation symétrique du groupe dihédral de degré n, défini comme le sous-groupe de S_n engendré par le produit de transpositions :

$$\tau = \begin{cases} (2,3)\cdots(n-1,n) & n \text{ impair} \\ (2,3)\cdots(n-2,n-1) & n \text{ pair} \end{cases}$$

et le cycle

$$\sigma = \begin{cases} (1,2,4\ldots,2k,\ldots,n-1,n,\ldots,2k-1,\ldots,5,3) & n \text{ impair} \\ (1,2,4\ldots,2k,\ldots,n,n-1,\ldots,2k-1,\ldots,5,3) & n \text{ pair} \end{cases}$$

par exemple, si $n = 5$ (resp. $n = 8$) alors $\tau = (2,3)(4,5)$ (resp. $\tau = (2,3)(4,5)(6,7)$) et $\sigma = (1,2,4,5,3)$ (resp. $\sigma = (1,2,4,6,8,7,5,3)$).

6.2 Résultat principal

Dans ce paragraphe, nous fixons un polynôme $g \in k[x]$ irréductible de degré $n \geqslant 5$. Nous supposons que son groupe de Galois est de type dihédral, c'est-à-dire $\mathrm{Gal}_k(f) = D_n$. Un tel polynôme sera dit *dihédral*.

Le résultat qui suit donne le type de factorisation d'un polynôme dihédral dans son corps de rupture.

Proposition 6.2.1. *Soit α_1 une racine g.*
La factorisation de g sur son corps de rupture $k(\alpha_1)$ est de la forme :

$$\begin{array}{ll} (x-\alpha_1)g_2(\alpha_1,x)\dots g_{\frac{n+1}{2}}(\alpha_1,x) & n \text{ impair} \\ (x-\alpha_1)g_2(\alpha_1,x)\dots g_{\frac{n}{2}}(\alpha_1,x)(x-b_{\frac{n}{2}+1}(\alpha_1)) & n \text{ pair} \end{array}$$

où $g_i(t,x) = x^2 + b_i(t)x + a_i(t)$ et a_i, b_i sont des polynôme en une variable de degré au plus $n-1$.

Démonstration. Le groupe de Galois de g sur le corps $k(\alpha_1)$ est donné par

$$\mathrm{Stab}_{D_n}(1) = \{s \in D_n \mid s(1) = 1\},$$

qui est défini explicitement par :

$$\mathrm{Stab}_{D_n}(1) = \begin{cases} \langle (2,3)\cdots(n-1,n)\rangle & n \text{ impair} \\ \langle (2,3)\cdots(n-2,n-1)\rangle & n \text{ pair} \end{cases}$$

Les orbites de l'action de $\mathrm{Stab}_{D_n}(1)$ sur l'ensemble $\{1,\dots,n\}$ sont :

$$\begin{array}{ll} \{1\},\{2,3\},\dots,\{n-1,n\} & n \text{ impair} \\ \{1\},\{2,3\},\dots,\{n-2,n-1\},\{n\} & n \text{ pair.} \end{array}$$

D'après la proposition 4.3.2 le résultat suit. □

Nous étudions maintenant les idéaux de rupture (voir Définition 5.2.1) de g. En fait, ici les idéaux considérés ne sont pas de rupture au sens strict du terme puisque l'ordre croissant selon les degrés de rupture n'est pas conservé (dans le cas n pair) mais la théorie reste la même.

Proposition 6.2.2. *Reprenons les mêmes notations que dans la Proposition 6.2.1. Nous pouvons renuméroter les facteurs quadratiques de g (sur $k(\alpha_1)$) de telle sorte que l'idéal I_1, engendré par l'ensemble triangulaire $\mathcal{T}_1$, est un $\underline{\alpha}$-idéal de Galois où $\underline{\alpha}$ est un n-uplet de racines de g vérifiant $\mathrm{Gal}_k(\underline{\alpha}) = D_n$.*

n impair :

$$\mathcal{T}_1 = \begin{cases} f_1 = g(x_1) \\ f_2 = g_2(x_1, x_2) \\ f_3 = x_3 + x_2 + b_2(x_1) \\ \quad \vdots \\ f_{2i} = g_{i+1}(x_1, x_{2i}) \\ f_{2i+1} = x_{2i+1} + x_{2i} + b_{2i}(x_1) \\ \quad \vdots \\ f_{n-1} = g_{(n+1)/2}(x_1, x_{n-1}) \\ f_n = x_n + x_{n-1} + b_{(n+1)/2}(x_1) \end{cases}$$

n pair :

$$\mathcal{T}_1 = \begin{cases} f_1 = g(x_1) \\ f_2 = g_2(x_1, x_2) \\ f_3 = x_3 + x_2 + b_2(x_1) \\ \quad \vdots \\ f_{2i} = g_{i+1}(x_1, x_{2i}) \\ f_{2i+1} = x_{2i+1} + x_{2i} + b_{2i}(x_1) \\ \quad \vdots \\ f_{n-2} = g_{n/2}(x_1, x_{n-2}) \\ f_{n-1} = x_{n-1} + x_{n-2} + b_{n/2}(x_1) \\ f_n = x_n + b_{n/2+1}(x_1) \end{cases}$$

Démonstration. Comme $\Delta(D_n) = 1, 2, \ldots, 2$ dans le cas où l'entier n est impair et $\Delta(D_n) = 1, 2, \ldots, 2, 1$ dans le cas où n est pair, en appliquant le théorème 5.4.11 nous avons le résultat. □

Plus particulièrement, nous avons dans le cas $n = 5$:

Corollaire 6.2.3. *En reprenant les même notations que dans la proposition 6.2.2. Si le degré de g est 5 alors aucune renumérotation n'est nécessaire pour obtenir l'idéal I_1.*

Démonstration. Lorsque $n = 5$, d'après la proposition 6.2.1, nous avons deux facteurs quadratiques de g sur $k(\alpha_1)$, ainsi il y a deux numérotations possibles. Soient $\langle \mathcal{T}_1 \rangle$ et $\langle \mathcal{T}_2 \rangle$ les deux idéaux triangulaires correspondants, construits comme dans la proposition 6.2.2. D'après la proposition 6.2.2, au moins un des deux idéaux est un $\underline{\alpha}$-idéal de Galois avec $\mathrm{Gal}_k(\underline{\alpha}) = D_n$, fixons $\langle \mathcal{T}_1 \rangle$ comme étant un tel idéal. Clairement nous avons

$$\mathcal{T}_2 = \{\omega.f\}_{f \in \mathcal{T}_1}$$

où $\omega = (5\,3)(2\,4)$. Ainsi $\langle \mathcal{T}_2 \rangle$ est un $(\omega^{-1}.\underline{\alpha})$-idéal de Galois avec

$$\mathrm{Gal}_k(\omega^{-1}.\underline{\alpha}) = \omega^{-1}.\,\mathrm{Gal}_k(\underline{\alpha}).\omega\,.$$

Le groupe $G = \omega^{-1}\,\mathrm{Gal}_k(\underline{\alpha})\omega = \omega^{-1} D_5 \omega$ est engendré par les permutations

$$(2\,3)(4\,5)(1\,4\,2\,3\,5)$$

Soient $\tau = (2\,3)$ une permutation de $S_{1,2,2}$ qui est une partie de son injecteur de $\langle \mathcal{T}_2 \rangle$ et posons $\underline{\beta} = \underline{\alpha}$. Alors $\langle \mathcal{T}_2 \rangle$ est un $((2\,3).\underline{\beta})$-idéal de Galois avec

$$\mathrm{Gal}_k((2\,3).\underline{\beta}) = G^{(2\,3)} = D_5\,.$$

Le résultat suit. □

Remarque 6.2.4. En terme d'association (voir Paragraphe 5.4.3) le résultat précédent revient à dire que tous les S_n-conjugués de D_5 dans $\mathcal{A}(S_{1,2,2})$ sont $S_{1,2,2}$ conjugués. On pourrait se demander s'il en est de même pour D_6 mais ça n'est pas le cas. En effet, en partant d'un ensemble triangulaire $\mathcal{T}_1$, la seule renumérotation possible se fait à l'aide de la permutation $\tau = (3\,4)(5\,2)$ (par exemple) et nous avons en Magma :

```
> D6:=PermutationGroup<6|S!(2,3)(4,5), S!(1,2,4,6,5,3)>;
> tau:=S!(3,4)(5,2);
> S1e:=PermutationGroup<6|S!(2,3), S!(5,4)>;
> ens:={D6^(s^(-1)) : s in S1e};
> D6^tau in ens;
false
```

Ainsi D_6^τ n'est pas un $S_{1,2,2,1}$-conjugué de D_6.

Le proposition qui suit permet de construire l'idéal des relations $I(\underline{\alpha})$ avec $\mathrm{Gal}_k(\underline{\alpha}) = D_n$ à partir de l'idéal I_1. Ici nous appliquons les résultats du paragraphe 5.5.

Proposition 6.2.5. *En reprenant les mêmes notations que dans la proposition 6.2.2. L'ensemble $\mathcal{T}_1$ qui suit est une base de Gröbner de l'idéal $I(\underline{\alpha})$.*

n impair :

$$\mathcal{T} = \left\{ \begin{array}{l} f_1 \\ f_2 \\ f_3 \\ x_4 + x_1 + b_2(x_2) \\ \quad \vdots \\ x_{2i} + x_{2i-3} + b_i(x_2) \\ f_{2i+1} \\ \quad \vdots \\ x_{n-1} + x_1 + b_{(n-1)/2}(x_2) \\ f_n \end{array} \right.$$

n pair :

$$\mathcal{T} = \left\{ \begin{array}{l} f_1 \\ f_2 \\ f_3 \\ x_4 + x_1 + b_2(x_2) \\ \quad \vdots \\ x_{2i} + x_{2i-3} + b_i(x_2) \\ f_{2i+1} \\ \quad \vdots \\ x_{n-2} + x_1 + b_{(n-2)/2}(x_2) \\ f_{n-1} \\ f_n \end{array} \right.$$

Démonstration. Par construction l'ensemble $\mathcal{T}$ est triangulaire, ainsi c'est une base de Gröbner et il suffit de montrer qu'il engendre l'$\underline{\alpha}$-idéal des relations.

Soit ω la permutation de D_n définie par $\omega = \sigma\tau$. Alors

$$\omega = \left\{ \begin{array}{ll} (1\ 2)(3\ 4)\dots(n-2\ n-1) & n \text{ impair} \\ (1\ 2)(3\ 4)\dots(n-1\ n) & n \text{ pair} \end{array} \right.$$

Pour tout entier impair $k = 2i-1$ où $i \in [\![2, \lfloor \frac{n-1}{2} \rfloor]\!]$, nous avons :

$$\omega.f_k = \omega.(x_k + x_{k-1} + b_{i+1}(x_1)) = x_{k+1} + x_{k-2} + b_{i+1}(x_2).$$

Comme les ensembles

$$\{f_1, f_2, x_3 + h_3(x_1, x_2), \dots, x_i + h_i(x_1, \dots, x_{i-1})\}$$

sont clairement triangulaires, nous pouvons appliquer la proposition 5.5.3 inductivement :

$$I = \langle T_1 \rangle + \langle \omega.f_3 \rangle + \langle \omega.f_5 \rangle + \dots + \langle \omega.f_m \rangle,$$

où m est le plus grand entier impair inférieur à $n-1$. Finalement I est engendré par l'ensemble $\mathcal{T}$ et est clairement maximal. La proposition 5.5.1 assure l'inclusion $I \subset I(\underline{\alpha})$ et donc I est l'$\underline{\alpha}$-idéal des relations. □

Remarque 6.2.6. Bien sûr, la dernière relation de l'ensemble $\mathcal{T}$ peut être remplacé par la dernier module de Cauchy $x_n + x_{n-1} + \ldots + x_1 + c$ où c est le coefficient de x^{n-1} dans g.

Maintenant, si l'on veut pouvoir utiliser la proposition 6.2.5 il faut avoir une méthode effective pour renuméroter les facteurs quadratiques de g sur $k(\alpha_1)$ pour avoir un idéal I_1 associé à D_n. Ainsi nous allons fournir des critères d'association (voir Paragraphe 5.4.3).

Proposition 6.2.7. *Avec les notations de la proposition 6.2.2 et la proposition 6.2.5. Si les facteurs de g sur $k(\alpha_1)$ sont numérotés de telle sorte que*

$$\langle \mathcal{T}_1 \rangle \subset \langle \mathcal{T} \rangle$$

alors $\mathcal{T}_1$ est associé au groupe D_n.

Démonstration. Supposons les facteurs $g_1, \ldots, g_s$ de g numérotés de telle sorte que l'inclusion $\langle \mathcal{T}_1 \rangle \subset \langle \mathcal{T} \rangle$, soit vérifiée. Comme nous l'avons vu dans la preuve de la proposition 6.2.5, l'idéal $\langle \mathcal{T} \rangle$ est maximal. Ainsi, si l'on note $\underline{\beta}$ un élément de $V(\langle \mathcal{T} \rangle)$ alors $\langle \mathcal{T} \rangle$ est un $\underline{\beta}$-idéal de Galois

La forme de l'ensemble $\mathcal{T}$ nous renseigne sur le fait que $\mathrm{Gal}_k(\underline{\beta})$, qui est un conjugué de D_n, contient ces deux permutations :

$$\omega = \begin{cases} (1\ 2)(3\ 4)\ldots(n-2\ n-1) & n \text{ impair} \\ (1\ 2)(3\ 4)\ldots(n-1\ n) & n \text{ pair} \end{cases}$$

$$\mu = \begin{cases} (2\ 3)(4\ 5)\ldots(n-1\ n) & n \text{ impair} \\ (2\ 3)(4\ 5)\ldots(n-2\ n-1) & n \text{ pair} \end{cases}$$

Ainsi $\mathrm{Gal}_k(\underline{\beta})$ contient $\omega\mu = \sigma$, donc $\langle \mathcal{T}_1 \rangle$ contient $\underline{\beta}$ et $\mathrm{Gal}_k(\underline{\beta}) = D_n$. □

Nous pouvons à présent donner un algorithme pour le calcul d'une base triangulaire d'un idéal des relations de g à partir d'une factorisation de g sur $k(\alpha_1)$. Pour ce faire, nous devons trouver une bonne numérotation des facteurs g_i, comme expliqué dans la proposition 6.2.7, et puis nous utilisons la proposition 6.2.5. Nous rappelons qu'un facteur quadratique $g_i(t, x)$ de g est de la forme $g(t, x) = x^2 + b(t).x + a(t)$.

Théorème 6.2.8. *L'algorithme 11 termine et renvoie le bon résultat. De plus, le nombre de formes normales calculées lors de l'appel de cet algorithme est de l'ordre de $O(n^2)$. Plus précisément, ce nombre est majoré par*

$$\Psi(n) = \begin{cases} 0 & n = 5 \\ 1 & n = 6 \\ \frac{1}{2}(3m^2 - 7m + 6) & n \geqslant 7 \end{cases}$$

où n est le degré du polynôme g et $m := \lfloor \frac{n-1}{2} \rfloor$.

Démonstration. Les propositions 6.2.5 et 6.2.7 assurent le fait que l'algorithme 11 termine et renvoie le bon résultat. Toutes les formes normales sont calculées lorsque que l'on cherche la bonne numérotation des g_i, ainsi le cas $n = 5$ n'est pas concerné. Trouver f_2 et f_3 demande au plus $\frac{m!}{(m-2)!} = m^2 - m$ formes normales calculées, ainsi il y en a exactement une de calculée lorsque $n = 6$. Toutes les autres formes normales sont calculées durant la boucle while. Lors de chaque boucle, il y a au plus $|S| - 1$ formes normales

Algorithme 11 DihedralRelationsIdeal(g, S)

Hypothèse : g is a dihedral polynomial of degree $n \geqslant 5$and S is the set of its irreducible quadratic factors over its root field.

Sortie : The set T is a triangular Gröbner basis of a relations ideal $I(\underline{\alpha})$ of g with $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha}) = D_n$.

$n := Degree(g)$;
$f_1(x_1) := g(x_1)$;

if $n = 5$ **then**
  Let $f_2(t,x) = x^2 + b(t).x + a(t)$ and $f_3(t,x) = x^2 + d(t).x + c(t)$ be the two elements of S ;
  $T := [f_1(x_1), f_2(x_1,x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2), x_5 + x_4 + d(x_4)]$;
  Return T ;
end if

Let $f_2(t,x) = x^2 + b(t).x + a(t)$ and $f_3(t,x) = x^2 + d(t).x + c(t)$ be two elements of S such that

$$\mathrm{NF}(f_3(x_1,x_4), [f_1(x_1), f_2(x_1,x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2)]) = 0;$$

$S := S \setminus \{f_2, f_3\}$;
$T := [f_1(x_1), f_2(x_1,x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2), x_5 + x_4 + d(x_1), x_6 + x_3 + d(x_2)]$;
if $n = 6$ **then**
  Return T ;
end if

$i := 3$;
while $|S| > 1$ **do**
  $i := i + 1$;
  Let $f(t,x) := x^2 + b(t).x + a(t)$ an element of S so that $\mathrm{NF}(f(x_1, x_{2i}), T) = 0$;
  $S := S \setminus \{f\}$;
  $T := \mathrm{Concat}(T, [x_{2i-1} + x_{2i-2} + b(x_1), x_{2i} + x_{2i-3} + b(x_2)])$;
end while
$i := i + 1$;
$f(t,x) := x^2 + b(t).x + a(t)$ the last element of S ;
$T := \mathrm{Concat}(T, [x_{2i+1} + x_{2i} + b(x_1)])$;
if n is even **then**
  $c :=$ the coefficient of x^{n-1} in g ;
  $T := \mathrm{Concat}(T, [x_{2i+2} + x_{2i+1} + \ldots + x_1 - c])$;
end if
Return T ;

calculées. Comme $|S| = m - 2$ juste avant le début de la boucle while, le nombre total de formes normales calculées est majoré par :

$$\sum_{k=2}^{m-2} (k-1) = \frac{1}{2}(m-3)(m-2)$$

et le résultat suit. □

Remarque 6.2.9. Comme dans le cas $n = 5$, il est possible de donner une meilleur estimation sur le nombre $\Psi(n)$ pour $n \geqslant 7$ mais ceci ne jouera pas sur la complexité asymptotique.

6.3 Exemples

Dans cette partie nous donnons deux exemples d'application de l'algorithme 11.

6.3.1 Calcul de l'idéal des relations générique de groupe de décomposition D_5

Dans ce premier exemple nous montrons comment les résultats de ce chapitre peuvent s'appliquer pour calculer efficacement l'idéal des relations du polynôme générique f_{D_5}. Le polynôme f_{D_5} a D_5 pour groupe de Galois et a été donné par Brumer (voir [53, Theorem 2.3.5]). Ce polynôme a ses coefficients dans le corps des fonctions rationnelles $\mathbb{Q}(s,t)$ et est défini par :

$$x^5 + (t-3)x^4 + (s-t+3)x^3 + (t^2-t-2s-1)x^2 + sx + t\,.$$

On calcule facilement une factorisation de f_{D_5} sur son corps de rupture à l'aide de Magma :

```
> K<s,t>:=FunctionField(Rationals(),2);
> PRK<x>:=PolynomialRing(K);
> f:=PRK!(x^5+(t-3)*x^4+(s-t+3)*x^3+(t^2-t-2*s-1)*x^2+s*x+t);
> Q:=quo<PRK|f>;
> PRQ<x>:=PolynomialRing(Q);
> Factorization(PRQ!f);
[
  <x - a, 1>,
  <x^2 + (-1/t*a^4 + (-t + 2)/t*a^3 + (-s - 1)/t*a^2 + (s - t^2
      + 2*t)/t*a - 1)*x - a + 1, 1>,
  <x^2 + (1/t*a^4 + (t - 2)/t*a^3 + (s + 1)/t*a^2 + (-s + t^2 -
      t)/t*a + (t - 2))*x + (t - 1)/t*a^4 + (t^2 - 4*t +
      2)/t*a^3 + (s*t - s - t^2 + 3*t - 1)/t*a^2 + (-2*s*t + s
      + t^3 - 2*t^2)/t*a + s - t + 1, 1>
]
```

Nous obtenons donc les facteurs suivants :

$$x^2+\frac{1}{t}(-\alpha_1^4+(-t+2)\alpha_1^3+(-s-1)\alpha_1^2+(s-t^2+2t)\alpha_1-t)x-\alpha_1+1\,,$$
$$x^2+\frac{1}{t}(\alpha_1^4+(t-2)\alpha_1^3+(s+1)\alpha_1^2+(-s+t^2-t)\alpha_1+t(t-2))x$$
$$+\frac{1}{t}((t-1)\alpha_1^4+(t^2-4t+2)\alpha_1^3+(st-s-t^2+3t-1)\alpha_1^2+(-2st+s+t^3-2t^2)\alpha_1)$$
$$+s-t+1$$

Le corollaire 6.2.3 nous donne alors, sans aucun autre calcul, la base triangulaire $\mathcal{T}$ de l'idéal des relations I de f_{D_5} tel que $\mathrm{Dec}(I)=D_5$.

$$x_1^5+(t-3)x_1^4+(s-t+3)x_1^3+(-2s+t^2-t-1)x_1^2+sx_1+t\,,$$
$$x_2^2-\frac{1}{t}x_2x_1^4+\frac{t+2}{t}x_2x_1^3+\frac{-s-1}{t}x_2x_1^2+\frac{s-t^2+2t}{t}x_2x_1-x_2-x_1+1\,,$$
$$x_3+x_2-\frac{1}{t}x_1^4+\frac{-t+2}{t}x_1^3+\frac{-s-1}{t}x_1^2+\frac{s-t^2+2t}{t}x_1-1\,,$$
$$x_4-\frac{1}{t}x_2^4+\frac{-t+2}{t}x_2^3+\frac{-s-1}{t}x_2^2+\frac{s-t^2+2t}{t}x_2+x_1-1\,,$$
$$x_5+x_4+\frac{1}{t}x_1^4+\frac{t-2}{t}x_1^3+\frac{s+1}{t}x_1^2+\frac{-s+t^2-t}{t}x_1+t-2$$

Rappelons que tout polynôme f de groupe de Galois D_5 est Tchirnhaus-équivalent à une spécialisation de f_{D_5}, c'est-à-dire qu'il existe un rationnel r tel que $f(x+r)$ soit une spécialisation de f_{D_5}. Ainsi, cet idéal peut être appelé *générique* puisque l'idéal des relations I de f tel que $\mathrm{Dec}(I)=D_5$ pourra être engendré par l'image de la spécialisation de $\mathcal{T}$ par la transformation $x_i\longmapsto x_i+r$.

6.3.2 Un exemple en degré 8

Soit $g=x^8-3x^5-x^4+3x^3+1$ un polynôme à coefficients rationnels et de groupe de Galois D_8 de la base de donnée *Database for Number Fields* de J. Klüners and G. Malle (voir [59]). À l'aide de Magma nous obtenons sa factorisation sur son corps de rupture. Ses trois facteurs sont :

$$\begin{aligned}
g_2(\alpha_1,x) &= x^2+\frac{1}{3}(5\alpha_1^7-2\alpha_1^6+4\alpha_1^5-15\alpha_1^4+5\alpha_1^3+7\alpha_1^2-5\alpha_1+3)x-1\,,\\
g_3(\alpha_1,x) &= x^2+\frac{1}{3}(-2\alpha_1^7+\alpha_1^6-3\alpha_1^5+7\alpha_1^4-2\alpha_1^3+\alpha_1^2+3\alpha_1-5)x\\
&\quad+\frac{1}{3}(2\alpha_1^7-3\alpha_1^6+2\alpha_1^5-8\alpha_1^4+8\alpha_1^3-4\alpha_1+4)\,,\\
g_4(\alpha_1,x) &= x^2+\frac{1}{3}(\alpha_1^6-\alpha_1^5-\alpha_1^4-6\alpha_1^3+\alpha_1^2+5\alpha_1+2)x\\
&\quad+\frac{1}{3}(\alpha_1^7+3\alpha_1^6+\alpha_1^5-\alpha_1^4-8\alpha_1^3+4\alpha_1-1)
\end{aligned}$$

Suivons l'algorithme 11 afin de construire un idéal des relations de g. Nous obtenons deux numérotations possibles permettant d'obtenir une inclusion comme dans la proposition 6.2.7. En fait, si nous posons $f_1(x_1)=g(x_1)$ et choisissons $f_2(x_1,x_2)=g_4(x_1,x_2$ ou $f_2(x_1,x_2)=g_3(x_1,x_2)$ et $f_3(x_1,x_4)=g_2(x_1,x_4)$ dans tous les cas nous obtenons :

$$\mathrm{NF}(f_3(x_1,x_4),[f_1(x_1),f_2(x_1,x_2),x_3+x_2+b(x_1),x_4+x_1+b(x_2)])=0$$

où b est (comme dans l'algorithme 11) le coefficient en x_1 de $f_2(x_1, x_2)$. Si nous choisissons la première numérotation possible nous obtenons le système triangulaire suivant :

$$
\begin{aligned}
& x_1^8 - 3x_1^5 - x_1^4 + 3x_1^3 + 1\,, \\
& x_2^2 + \frac{1}{3}(x_1^6 - x_1^5 - x_1^4 - 6x_1^3 + x_1^2 + 5x_1 + 2)x_2 \\
& \quad + \frac{1}{3}(x_1^7 + 3x_1^6 + x_1^5 - x_1^4 - 8x_1^3 + 4x_1 - 1)\,, \\
& x_3 + x_2 + \frac{1}{3}(x_1^6 - x_1^5 - x_1^4 - 6x_1^3 + x_1^2 + 5x_1 + 2)\,, \\
& x_4 + x_1 + \frac{1}{3}(x_2^6 - x_2^5 - x_2^4 - 6x_2^3 + x_2^2 + 5x_2 + 2)\,, \\
& x_5 + x_4 + \frac{1}{3}(5x_1^7 - 2x_1^6 + 4x_1^5 - 15x_1^4 + 5x_1^3 + 7x_1^2 - 5x_1 + 1)\,, \\
& x_6 + x_3 + \frac{1}{3}(5x_2^7 - 2x_2^6 + 4x_2^5 - 15x_2^4 + 5x_2^3 + 7x_2^2 - 5x_2 + 1)\,, \\
& x_7 + x_6 - \frac{1}{3}(2x_1^7 + x_1^6 - x_1^5 + 7x_1^4 - 2x_1^3 + x_1^2 + x_1 - 5)\,, \\
& x_8 + x_7 + x_6 + x_5 + x_4 + x_3 + x_2 + x_1 - 3
\end{aligned}
$$

Chapitre 7

L'algorithme de Yokoyama revisité

7.1 Introduction

Ce chapitre correspond à un travail en cours et en collaboration avec Kazuhiro Yokoyama initié par une invitation en septembre 2004 à l'université du Kyushu (Japon).

Cette partie consiste en l'étude approfondie et aussi l'amélioration de l'algorithme proposé par K. Yokoyama dans la Section 5.3 de son article [113]. Celui-ci sera appelé *algorithme de Yokoyama* et peut être résumé de la manière suivante : Étant donné un polynôme f séparable à coefficients rationnels et l'action de son groupe de Galois G sur des approximations p-adiques de ses racine, nous voulons construire une base triangulaire

$$\begin{aligned} &f_n(x_n, \ldots, x_1)\,, \\ &\vdots \\ &f_2(x_2, x_1)\,, \\ &f_1(x_1) \end{aligned}$$

d'un idéal des relations I de f tel que $\mathrm{Dec}(I) = G$. Cet algorithme itératif calcule pour i prenant les valeurs consécutives $1, \ldots, n$, le polynôme f_i en ne faisant que des résolutions de systèmes linéaires (modulo une certaine puissance de p) et des remontées de Hensel.

Cet algorithme est intrinsèquement lié au calcul du groupe de Galois à l'aide des outils p-adiques.

Pour le calcul du groupe de Galois d'un polynôme à coefficients rationnels, l'utilisation des outils p-adiques se révèlent très efficaces. En utilisant des approximations p-adiques des racines d'un tel polynôme, on peut trouver les racines entières de résolvantes relatives utilisées dans la méthode de Stauduhar (voir [99]). Dans [33], Darmond et Ford utilisent un tel principe pour vérifier que des polynômes (donnés par Malle) ont bien pour groupe de Galois M_{11} et M_{12}. Plus tard, K. Yokoyama décrira une méthode générale (voir [113]) pour le calcul du groupe de Galois d'un polynôme à coefficients rationnels en utilisant des approximations de ses racines dans des extensions algébriques de $\mathbb{Q}_p$. Dans [47] Geissler et Klüners utilisent cette approche afin de donner un algorithme de calcul du groupe de Galois pour des polynômes de $\mathbb{Q}[x]$ de degré inférieur ou égal à 15. De plus, ils utilisent le calcul de sous-corps pour encore améliorer l'efficacité.

Dans sa thèse (voir [46]), K. Geissler étend cet algorithme dans le cas de polynômes de degré ≤ 23 et à coefficients dans un corps de nombres ou de fonctions (c'est-à-dire une extension algébrique simple de $\mathbb{Q}$, $\mathbb{Q}(x)$ ou $\mathbb{F}_q(x)$, où $\mathbb{F}_q$ est le corps fini à q éléments). Ces algorithmes sont implantés dans les systèmes de calcul formel MAGMA(voir [20]) et `Kant/Kash` (voir [31]). Dans tout ce chapitre, cette approche sera appelée *p-adic Stauduhar's method*.

Comme ces algorithmes de calcul de groupe de Galois donnent en sortie les objets nécessaires pour débuter l'algorithme de Yokoyama, il est naturel de vouloir l'étudier, l'améliorer et en réaliser une implantation efficace .

Dans la situation présente, les données du problème sont maximales en comparaison avec celles du chapitre 5 et du chapitre 6. En effet, nous avons à notre disposition le polynôme f et l'action de son groupe de Galois G sur des approximations p-adiques de ses racines. Nous montrons comment la connaissance de $G = \mathrm{Dec}(I)$ permet d'améliorer l'algorithme de Yokoyama en utilisant les techniques suivantes :

- *Réduction du nombre de systèmes à calculer.* À l'aide des résultats du paragraphe 5.5 on peut éviter des calculs (en fait seule la définition du groupe de décomposition est utilisée ici). De même, nous montrerons comment appliquer les résultats du paragraphe 2.2.4 de manière récursive à cette même fin.
- *Réduction de la taille des systèmes.* La connaissance de $\mathrm{Dec}(I)$ permet de déterminer les plus petits systèmes possibles pour le calcul des f_i. Ce genre de réduction (dans le cas où $G = PSL(2,7)$) est aussi proposé par A. Valibouze dans [108] en raisonnant sur les factorisations de f sur des extensions intermédiaires entre $\mathbb{Q}$ et le corps de décomposition de f. Ici, l'utilisation de $\mathrm{Dec}(I)$ permet d'optimiser cette réduction ce que nous pourrions pas faire en ne raisonnant que sur les factorisations successives.

Nous montrerons que le choix de la représentation symétrique du groupe de Galois (ou de manière équivalente, la numérotation des racines), doit se faire de manière précise pour que ces techniques de réduction soient optimales. Pour ce faire, nous définissons un invariant sur les groupes de permutations permettant de déterminer les représentants d'une classe de conjugaison pour lesquels le calcul sera facile. Une étude de la complexité de cet algorithme amélioré sera établie en fonction de cet invariant.

Ce chapitre est organisé de la manière suivante. Dans la section 7.2 nous rappelons le lien entre le corps de décomposition d'un polynôme f à coefficients rationnels et le corps de décomposition de ce même polynôme vu avec des coefficients dans $\mathbb{Q}_p$. La section 7.3 décrit les outils utilisés pour résoudre notre problème. Dans la section 7.4 nous décrivons l'algorithme obtenu et nous étudions sa complexité ainsi que l'efficacité de son implantation.

Dans ce chapitre les polynômes considérés sont à coefficients dans $\mathbb{Q}$ mais tout ce qui suit peut être transposé au cas des polynômes à coefficients dans un corps global (comme K. Geissler l'a fait dans le cadre du calcul du groupe de Galois).

7.2 Preliminaries

We provide necessary notions and summarize the paper [113]. So, we expose theorems and lemmas without proof except for the theorem 7.2.3 where a new proof is given with a quadratic Hensel lift.

7.2.1 Splitting field and Galois group over $\mathbb{Q}$

Let $f(x)$ be a monic square-free polynomial of degree n over $\mathbb{Q}$ and Ω_f the set of all roots of f in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. The splitting field K_f of f is the extension field $\mathbb{Q}(\Omega_f)$ obtained by adjoining Ω_f to $\mathbb{Q}$. The group of $\mathbb{Q}$-automorphisms of K_f over $\mathbb{Q}$ acts faithfully on Ω_f, thus one can consider the permutation representation G_f of this group. We fix an indexation of the roots $\Omega_f = \{\alpha_1, \ldots, \alpha_n\}$ of f, so the group G_f is viewed as a subgroup of S_n. The group G_f is called the Galois group of f (for this indexation).

To express K_f symbolically, the following epimorphism ϕ of $\mathbb{Q}$-algebra is considered:

$$\begin{array}{rcl} \mathbb{Q}[x_1, \ldots, x_n] & \longrightarrow & K_f \\ x_i & \longmapsto & \alpha_i \end{array}$$

For simplicity, we write $X = \{x_1, \ldots, x_n\}$ and more generally if E is a part of $\{1, \ldots, n\}$ then we write $X_E = \{x_i : i \in E\}$. Then K_f is represented by the residue class ring $\mathcal{A}$ of the polynomials ring $\mathbb{Q}[X]$ factored by the kernel $\mathcal{M}$ of ϕ. We call $\mathcal{M}$ *the splitting ideal of f associated with the assignment of the roots $\alpha_1, \ldots, \alpha_n$.*

In this setting, computing K_f means to compute a *Gröbner basis* of $\mathcal{M}$ (see [15]). Especially, if we choose the lexicographic order $<$ on terms with $x_1 < \cdots < x_n$, then the reduced Gröbner basis $\mathcal{G}$ of $\mathcal{M}$ coincides with the generating set $\{g_1, g_2, \ldots, g_n\}$ obtained by *successive extensions*, that is, for each i,

1. g_i is a polynomial in $x_1, \ldots, x_i$ and monic with respect to x_i, and
2. $\mathbb{Q}(\alpha_1, \ldots, \alpha_i) \cong \mathbb{Q}[x_1, \ldots, x_i]/\langle g_1, \ldots, g_i \rangle$, where $\langle F \rangle$ denotes the ideal generated by an element or a set F. This implies that g_i is an irreducible factor of $f(x_i)$ over $\mathbb{Q}[X_{\{1,\ldots,i-1\}}]/\langle g_1, \ldots, g_{i-1} \rangle$ such that $g_i(\alpha_1, \ldots, \alpha_i) = 0$.

Thus $\mathcal{G}$ can be obtained by "algebraic factoring methods" (see [7]) and is said to be a *triangular basis* (see 1.3.13).

Remark 7.2.1. Let $\mathcal{G}$ be a Gröbner basis of $\mathcal{M}$ and $\mathrm{NF}(P, \mathcal{G})$ denotes the normal form of a polynomial P in $\mathbb{Q}[X]$ with respect to $\mathcal{G}$ (see [30, page 80]). Since $\phi(\mathcal{M}) = \{0\}$, $\phi(P) = \phi(\mathrm{NF}(P, \mathcal{G}))$ for every P in $\mathbb{Q}[X]$ and especially, $\phi(P) = \mathrm{NF}(P, \mathcal{G})$ if $\phi(P)$ belongs to $\mathbb{Q}$.

The group S_n acts naturally on $\mathbb{Q}[X]$ with $x_i^\sigma = x_{i^\sigma}$ for $1 \leqslant i \leqslant n$ and $\sigma \in S_n$. Thus G_f is the $\mathbb{Q}$-ring automorphism group of $\mathcal{A}$ denoted by $\mathrm{Aut}_{\mathbb{Q}}(\mathcal{A})$ (see [7] and [3]).

We use the following notation for groups: For a group G acting on a set $\mathcal{S}$, the stabilizer in G of an element or a subset A of $\mathcal{S}$ is denoted by $\mathrm{Stab}_G(A)$, i.e. $\mathrm{Stab}_G(A) = \{\sigma \in G \mid A^\sigma = A\}$. If G is the full symmetric group on $\mathcal{S}$, we simply write $\mathrm{Stab}(A)$ for $\mathrm{Stab}_G(A)$. We denote by $\mathrm{Stab}_G([a_1, \ldots, a_k])$ the pointwise stabilizer of a subset $A = \{a_1, \ldots, a_k\}$ of $\mathcal{S}$, i.e. $\mathrm{Stab}_G([a_1, \ldots, a_k]) = \{\sigma \in G \mid a_i^\sigma = a_i,\ \forall i \in [\![1, k]\!]\}$. The set of right cosets of H in G is denoted by $H\backslash G$ and the set of all representatives of $H\backslash G$ by $H\backslash\backslash G$.

Next, we introduce the notion of *splitting rings*.

Definition 7.2.2. We call the ideal generated by $t_1 + a_1, \ldots, t_n + (-1)^{n-1}a_n$, where t_i is the i-th elementary symmetric function on X and $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, the *universal splitting ideal* of f and we denote it by $\mathcal{M}_0$. We call the residue class ring $\mathbb{Q}[X]/\mathcal{M}_0$ *the universal splitting ring of* f *over* $\mathbb{Q}$ and we denote it by $\mathcal{A}_0$. Moreover, we call the following set generated by the *Cauchy's moduls* of f (see Proposition 2.2.2) the *standard generating set* of $\mathcal{M}_0$:

$$\{c_1(x_1), c_2(x_1, x_2), \ldots, c_n(x_1, \ldots, x_n)\},$$

where

$$\begin{aligned} c_1(x_1) &= f(x_1) \\ c_i(x_1, \ldots, x_i) &= \frac{c_{i-1}(x_i, x_{i-2}, \ldots, x_1) - c_{i-1}(x_{i-1}, \ldots, x_1)}{(x_i - x_{i-1})}, i \in [\![2, n]\!]. \end{aligned}$$

The standard generating set is the reduced Gröbner basis of $\mathcal{M}_0$ with respect to the lexicographic order $<$ on terms with $x_1 < \cdots < x_n$. The universal splitting ideals and the universal splitting rings can be defined over rings.

Since S_n stabilizes $\mathcal{M}_0$, S_n also acts faithfully on $\mathcal{A}_0$, i.e. $S_n \subset \mathrm{Aut}_{\mathbb{Q}}(\mathcal{A}_0)$. We have the following theorem (see [89], [9], and [113] for details and other references.)

Theorem 7.2.1. *If the polynomial f is square-free then we have*

1. *The universal splitting ring $\mathcal{A}_0$ has finitely many primitive idempotents $e_1, \ldots, e_\ell$ such that $\{e_1, \ldots, e_\ell\}$ forms an S_n-orbit. Moreover, $Stab(e_1) \cong G_f$ and $\ell = |S_n : G_f|$.*

2. *There is a one-to-one correspondence between the set of all primitive idempotents of $\mathcal{A}_0$ and the set of all prime divisors of $\mathcal{M}_0$. Let e be the primitive element corresponding to the fixed prime divisor $\mathcal{M}$. Then, $G_f = Stab(\mathcal{M}) = Stab(e)$ and*

$$\mathcal{M}^\sigma = \{g \in \mathbb{Q}[X] \mid ge^\sigma = 0 \in \mathcal{A}_0\}.$$

3. *There is a one-to-one correspondence between the set of all idempotents of $\mathcal{A}_0$ and the set of all radical ideals containing $\mathcal{M}_0$. More precisely, for a subset $\mathcal{S}$ of $G_f \backslash\backslash S_n$,*

$$\cap_{\sigma \in \mathcal{S}} \mathcal{M}^\sigma = \{g \in \mathbb{Q}[X] \mid g \sum_{\sigma \in \mathcal{S}} e^\sigma \in \mathcal{M}_0\}.$$

Moreover, we have

$$\mathcal{M}_0 = \cap_{\sigma \in G_f \backslash\backslash S_n} \mathcal{M}^\sigma \text{ and } \mathcal{A}_0 = \oplus_{\sigma \in G_f \backslash\backslash S_n} e^\sigma \mathcal{A}_0 = \oplus_{\sigma \in G_f \backslash\backslash S_n} \mathbb{Q}[X]/\mathcal{M}^\sigma.$$

7.2.2 Splitting field over p-adic number field

Now we consider the relation between the splitting ring over $\mathbb{Q}$ and that over a p-adic field $\mathbb{Q}_p$. From now on, we suppose the polynomial f square-free, monic with coefficients in the ring $\mathbb{Z}$ of integers

Remark 7.2.3. with a Tschirnaus' transformation (see [103]), from a polynomial g with rational coefficients, it is always possible to produce a monic polynomial f with integer coefficients so that the roots of f are linear transformations of the roots of g.

The n-tuple $\Omega_f = \{\alpha_1, \ldots, \alpha_n\}$ and the splitting ideal $\mathcal{M}$ associated with the assignment x_i to α_i are fixed. The primitive idempotent of $\mathcal{A}$ corresponding to $\mathcal{M}$ is denoted by e.

For a prime integer p, we denote by $\mathbb{Z}_p^0$ (resp. $\mathbb{Z}_p$) the localization of $\mathbb{Z}$ at p (resp. the completion of $\mathbb{Z}_p^0$). We denote by π_p the projection from $\mathbb{Z}_p[X]$ to $GF(p)[X]$ which is the natural extension of the projection from $\mathbb{Z}$ to $GF(p)$.

We fix a prime number p such that $\pi_p(f)$ is square-free, i.e. p does not divide the discriminant $\mathrm{disc}(f)$ of f. Let $\bar{\mathcal{M}}_0$ denotes the ideal $\pi_p(\mathcal{M}_0 \cap \mathbb{Z}_p^0[X])$ in $GF(p)[X]$ and $\mathcal{G}_0$ denotes the standard generating set of $\mathcal{M}_0$.

By construction, the Cauchy's moduls of f are polynomials with integral coefficients and monic in their greatest monomial. Thus, the set $\pi_p(\mathcal{G}_0)$ is the standard generating set of $\pi_p(f)$, hence it is a Gröbner basis of $\pi_p(\mathcal{M}_0 \cap \mathbb{Z}_p^0[X])$.

Moreover, $\mathcal{G}_0$ is the standard generating set of the universal splitting ideal $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}_0$ of f as a polynomial with coefficients in $\mathbb{Q}_p$ and that of $\mathbb{Z}_p[X] \otimes_{\mathbb{Z}_p^0} (\mathcal{M}_0 \cap \mathbb{Z}_p^0[X])$ over $\mathbb{Z}_p$. The ideal $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}_0$ is denoted by $\mathcal{M}_0^{(\infty)}$. (this result is in relation with the notion of *compatibility* of primes with Gröbner bases in [82]).

We denote the universal splittings rings $GF(p)[X]/\bar{\mathcal{M}}_0$ by $\bar{\mathcal{A}}_0$ and $\mathbb{Q}_p[X]/\mathcal{M}_0^{(\infty)}$ by $\mathcal{A}_0^{(\infty)}$.

Theorem 7.2.2. *We have the following assertions*

1. *The projection π_p gives a one-to-one correspondence between the set of all idempotents of $\mathcal{A}_0^{(\infty)}$ and that of $\bar{\mathcal{A}}_0$.*

2. *The projection π_p gives a one-to-one correspondence between the set of all primitive idempotents of $\mathcal{A}_0^{(\infty)}$ and that of $\bar{\mathcal{A}}_0$. Moreover, for each pair $(\bar{e}, e^{(\infty)})$ of corresponding primitive idempotents, $Stab(\bar{e}) = Stab(e^{(\infty)})$.*

3. *Let $\bar{e}$ be a component of $\pi_p(e)$ and let $e^{(\infty)}$ be the primitive idempotent of $\mathcal{A}_0^{(\infty)}$ corresponding to $\bar{e}$. Then $Stab(e)$ contains $Stab(\bar{e})(= Stab(e^{(\infty)}))$ and $Stab(\pi_p(e)) = Stab(e)$. Moreover, by letting $\mathcal{S} =$,*

$$\pi_p(e) = \sum_{\sigma \in Stab(\bar{e}) \backslash\backslash Stab(e)} \bar{e}^{\sigma} \text{ and } e = \sum_{\sigma \in Stab(\bar{e}) \backslash\backslash Stab(e)} e^{(\infty)^{\sigma}}.$$

Now we fix a primitive idempotent $\bar{e}$ of $\bar{\mathcal{A}}_0$ and its corresponding idempotent $e^{(\infty)}$ of $\mathcal{A}_0^{(\infty)}$ (see Theorem 7.2.2 (1)). Let $\bar{\mathcal{M}}$ be the maximal ideal of $GF(p)[X]$ corresponding to $\bar{e}$ and $\mathcal{M}^{(\infty)}$ the maximal ideal of $\mathbb{Q}_p[X]$ corresponding to $e^{(\infty)}$. Moreover, let $\bar{\mathcal{G}} = \{\bar{g}_1, \ldots, \bar{g}_n\}$ the reduced Gröbner basis of $\bar{\mathcal{M}}$ with respect to the lexicographic order $<$ such that $x_1 < \cdots < x_n$.

Definition 7.2.4. Let $\mathcal{G}^{(\infty)} = \{g_1^{(\infty)}, \ldots, g_n^{(\infty)}\}$. For a positive integer k, we call the set $\{g_1^{(\infty)} \bmod p^{k+1}, \ldots, g_n^{(\infty)} \bmod p^{k+1}\}$ the *k-th approximation to* $\mathcal{G}^{(\infty)}$ and denote it by $\mathcal{G}^{(k)}$. We note that $\mathcal{G}^{(0)} = \bar{\mathcal{G}}$.

We can lift $\bar{\mathcal{G}}$ to a Gröbner basis $\mathcal{G}^{(\infty)}$ of $\mathcal{M}^{(\infty)}$ by Hensel construction. More precisely we have:

Theorem 7.2.3. *The reduced Gröbner basis $\mathcal{G}^{(\infty)}$ of $\mathcal{M}^{(\infty)}$ with respect to $<$ is contained in $\mathbb{Z}_p[X]$, and the Gröbner basis $\bar{\mathcal{G}}$ is lifted uniquely to $\mathcal{G}^{(\infty)}$ by Hensel construction.*

Proof. In [113] the theorem 21 gives the result and a construction based on a *simple Hensel lifting* which is a generalization of the one given in [112]. Here we give a *quadratic* version of the *Hensel lifting*.
Assume the k-th approximation $\mathcal{G}^{(k)}$ to $\mathcal{G}^{(\infty)}$ computed. We give the construction by induction on i. The case $i = 1$ is trivial so $i \in [\![2, n]\!]$. By induction, we can consider the ideal

$$I_{i-1}^{2k} = \langle g_1 \bmod p^{(2k)}, \ldots, g_{(i-1)} \bmod p^{2k} \rangle$$

of $\mathbb{Z}_p[X_{i-1}]$ and R the factor ring $\mathbb{Z}_p[X_{i-1}]/I_{i-1}^{2k}$. We now view $f(x_i)$ and g_i as polynomials in $R[x_i]$. Let $\mathfrak{P}$ be the image of p^k in R. If h_i, s, t are polynomials of $R[x_i]$ such that

$$\begin{aligned} f(x_i) &= g_i h_i (\mathrm{mod}\mathfrak{P}) \\ 1 &= s g_i + t h_i (\mathrm{mod}\mathfrak{P}) \end{aligned}$$

and

$$\deg_{x_i}(s) < \deg_{x_i}(h_i),\ \deg_{x_i}(t) < \deg_{x_i}(g_i)$$

then the *quadratic Hensel lift* (see [110, Algorithm 15.10]) constructs polynomials g_i^*, h_i^*, s^*, t^* of $R[x_i]$ so that

$$\begin{aligned} f(x_i) &= g_i^* h_i^* (\mathrm{mod}\mathfrak{P}^2) \\ 1 &= s^* g_i^* + t^* h_i^* (\mathrm{mod}\mathfrak{P}^2) \end{aligned}$$

and

$$\deg_{x_i}(s^*) < \deg_{x_i}(h_i^*),\ \deg_{x_i}(t^*) < \deg_{x_i}(g_i^*)\,.$$

The polynomial g_i^* can be viewed as an element of $\mathbb{Z}_p[X_i]$ and we can set $g_i^{(2k)} = g_i^*$. Since $R[x_i]/\langle\mathfrak{P}\rangle$ is isomorphic to $(\mathbb{Z}_p[X_{i-1}]/\langle p^k + I_{i-1}^k\rangle)[x_i]$, this construction could be used inductively on k as soon as the polynomials h_i, s and t are given.
Finally, it remains to prove that polynomials h_i, s and t can be constructed, for each $i \in [\![2, n]\!]$, when $k = 1$. In this case the ring R is a field for all $i \in [\![2, n]\!]$, so these polynomials are constructed by using the *extended Euclid algorithm* (see [110]). □

Remark 7.2.5. As $\mathcal{A}^{(\infty)} = \mathbb{Q}_p[X]/\mathcal{G}^{(\infty)}$ is the splitting field of f over $\mathbb{Q}_p$, we can handle the approximation of each root of f by the approximation $\mathcal{G}^{(k)}$.

For a polynomial P in $\mathbb{Q}[X]$, $\mathrm{NF}(P, \mathcal{G}^{(\infty)})$ is considered as the evaluation of P over $\mathcal{A}^{(\infty)}$ and hence, $\mathrm{NF}(P, \mathcal{G}^{(k)})$ corresponds to the approximation of the evaluation of P.

7.3 Computing Splitting Fields

Here, we give the details of the method to compute the splitting field of a polynomial f over $\mathbb{Q}$ based on "p-adic approach". In the sequel, the polynomial f is supposed to be monic and square-free with integral coefficients (this hypothesis is not restrictive, see Remark 7.2.3).

Now we assume that we have already computed the Galois group G_f of f by the p-adic Stauduhar's method, and we have obtained the approximation of roots of f in $\bar{\mathbb{Q}}_p$ and the explicit action of G_f on them as a sub-group of S_n. The group G_f is now seen as this symmetric representation and the approximation of the p-adics roots are given as the zeros of the ideal $\langle \mathcal{G}^{(k)} \rangle$ for a given integer k. From now on, for a given ideal I of a polynomials ring with coefficients in a field k, we denote by $Z(I)$ the set of zeroes of I in an algebraic closure of k.

The method computes, from $\mathcal{G}^{(k)}$ and G_f, the Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_n\}$ of the prime divisor $\mathcal{M}$ of $\mathcal{M}_0$ which verifies $G_f = Stab(\mathcal{M})$.

7.3.1 Computation by solving systems of linear equations

Here we show that we can compute $g_1, \ldots, g_n$ by a *method of indeterminate coefficients*. Let $\alpha_1, \ldots, \alpha_n$ be all roots of f in $\bar{\mathbb{Q}}$ and suppose $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in Z(\mathcal{M})$.

Recall that G_f is already presented as a sub-group of S_n and

$$Stab(\mathcal{M}^{(\infty)}) = \mathrm{Aut}_{GF(p)}(GF(p)[X]/\bar{\mathcal{M}}) = G_{\pi_p(f)} \subset G_f \,.$$

We denote $|G_f|$ and $|G_{\pi_p(f)}|$ by N and $\bar{N}$, respectively.

The i-relations

The following proposition allows to deduce $\deg_i(g_i)$, the degree in x_i of g_i, from $G_f = Stab(\mathcal{M})$.

Proposition 7.3.1 (Theorem 5.3 [14])**.** *The degree d_i of g_i in x_i is given by*

$$d_i = |Stab_{G_f}([1, \ldots, i-1])|/|Stab_{G_f}([1, \ldots, i])| \,.$$

If we find a triangular set $\mathcal{T} = \{f_1, \ldots, f_n\}$ (see Definition 1.3.13) of polynomials in $\mathcal{M}$ such that $\deg_i(f_i) = n_i$ then it forms a (not necessarily reduced) Gröbner basis of $\mathcal{M}$. So, the computation of the polynomials g_i is deduced from the computation of such a triangular set $\mathcal{T}$ and its reduction.

Definition 7.3.2. Let i be an integer in $[\![1, n]\!]$. A part E of $\{1, \ldots, i\}$ containing i is said to be a *i-relation* if there exists a polynomial r_i in $\mathbb{Q}[X_E]$ such that

$$\alpha_i^{d_i} + r_i(\underline{\alpha}) = 0 \text{ and } \deg_i(r_i) < n_i \,.$$

The following proposition permits us to easily find a i-relation.

Proposition 7.3.3. *Let i be an integer in $[\![1, n]\!]$ and m be the minimal integer in $\{1, \ldots, i-1\}$ such that*

$$|Stab_G([1, \ldots, m])|/|Stab_G([1, \ldots, m, i])| = n_i \,.$$

Then, there exists a i-relation in $\{1, \ldots, m, i\}$.

Proof. Let μ be the minimal polynomial of α_i over the field $k(\alpha_1, \ldots, \alpha_m)$. By hypothesis μ is of degree n_i and we can, whithout lost of generality, assume that the coefficient in degree n_i is 1. Let g denotes the polynomial $\mu - x^{n_j}$, then, if we replace the roots α_j in g by x_j, we have $g \in k[X_E \cup \{x_i\}]$ with $deg_{x_i}(g) < n_i$ and E is the part of $\{1, \ldots, m\}$ consisting in the indices of the indeterminates which appear in g. Moreover

$$\alpha_i^{n_i} + g(\underline{\alpha}) = 0\,.$$

Thus, E is a i-relation. □

If E_i is the i-relation given by $\{1, \ldots, i\}$ then we can find a polynomial r_i, as in Definition 7.3.2, satisfying:

$$\deg_j(r_i) < n_j,\ \forall j \in \{1, \ldots, i\}\,.$$

For example we can take r_i which is given by the equality $g_i = x_i^{n_i} + r_i$. More generally, we have the classical result :

Proposition 7.3.4. *Let $E = \{e_1 < e_2 < \cdots < e_k = i\}$ be a i-relation. Then, there exists a polynomial r_i as in Definition 7.3.2 verifying:*

$$deg_j(r_i) < |Stab_{G_f}([e_1, \ldots, e_{j-1}])|/|Stab_{G_f}([e_1, \ldots, e_j])|,\ \forall j \in [\![1, i]\!]\,.$$

Definition 7.3.5. Let $E_i = \{e_1 < e_2 < \cdots < e_k\}$ be a i-relation. We define the finite sequence $d(E_i)_{j=1,\ldots,k}$ by

$$d(E_i)_j = |\mathrm{Stab}_{G_f}([e_1, \ldots, e_{j-1}])|/|\mathrm{Stab}_{G_f}([e_1, \ldots, e_j])|,\ \forall j \in [\![1, k]\!]\,.$$

The *degree of* E_i is given by $\prod_{j=1}^{k} d(E_i)_j$ and is denoted by $D(E_i)$.

It is possible to find different i-relations for a same integer $i \in [\![1, n]\!]$. We will give a notion of partial order over the i-relations.

Definition 7.3.6. Let i be an integer in $[\![1, n]\!]$ and E a i-relation. The i-relation E is said to be *minimal* if $D(E)$ is minimal (among all the i-relation) and not any proper subset of E is a i-relation.

Computing a minimal i-relation for each i is a combinatorial problem because we have to consider a big part of the subsets of $\{1, \ldots, i-1\}$. But we can reduce the problem by computing a i-relation with minimal degree according to the proposition 7.3.3. Actually, there may not exist such a i-relation which would be minimal, as in the following example.

Example 7.3.7. Let H be the transitive group of degree 9 and generated by the following permutations

$$\begin{aligned}&(2,3,4)(5,7,6),\\ &(1,7,4)(2,8,5)(3,9,6),\\ &(1,9,8)(2,4,3)(5,7,6),\\ &(3,4)(5,7)(8,9)\,.\end{aligned}$$

A minimal 7-relation is given by the set $E_1 = \{5, 6, 7\}$ with $D(E_1) = 18$. The integer m as in proposition 7.3.3 is 3 and the only 7-relation E_2 in $\{1, 2, 3, 7\}$ is this full set. The 7-relation E_2 is not be minimal since $D(E_2) = 54$.

Our strategy is to deduce a Göbner basis $\mathcal{T} = \{f_1 = x_1^{d_1} + r_1, \ldots, f_n = x_n^{d_n} + r_n\}$ of the ideal $\mathcal{M}$ from the computation of the polynomials r_i associated to each E_i. This is what we present now.

Systems over the rationals

We fix an integer $i \in [\![1, n]\!]$. Each coefficient of f_i is replaced with an indeterminate, for simplicity, the terms $\prod_{e \in E_i} x_e^{m_e}$, where $0 \leqslant m_e < d(E_i)_e$, are sorted with respect to the lexicographic order and denoted by $t_1, \ldots, t_{D(E_i)}$. Then, with indeterminates $a_j^{(i)}$, we have

$$f_i = x_i^{d_i} + \sum_{j=1}^{D(E_i)} a_j^{(i)} t_j \,.$$

Since $\mathcal{T}$ is a Gröbner basis of $\mathcal{M}$, the following equation holds for i.

$$f_i(\gamma) = 0 \;\text{ for every } \gamma \in Z(\mathcal{M}). \tag{7.1}$$

Let $E_i = \{e_1 < e_2 < \cdots < e_k\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ an element of $Z(\mathcal{M})$. We denote by $\gamma(E_i)$ the projection on the index in E_i (i.e. $(\gamma_{e_1}, \ldots, \gamma_{e_k})$) of γ and $Z(\mathcal{M})(E_i) = \{\gamma(E_i) \mid \gamma \in Z(\mathcal{M})\}$. Clearly, we have $|Z(\mathcal{M})(E_i)| = D(E_i)$.

Let G_{E_i} be the pointwise stabilizer $\mathrm{Stab}_{G_f}([e_1, \ldots, e_k])$ and

$$G_{E_i} \backslash\backslash G_f = \{\sigma_1, \ldots, \sigma_{D(E_i)}\} \,,$$

we have $Z(\mathcal{M})(E_i) = \{\alpha(E_i)^{\sigma_1}, \ldots, \alpha(E_i)^{\sigma_{D(E_i)}}\}$ and

$$f_i(\gamma) = 0 \;\text{ for every } \gamma \in Z(\mathcal{M})(E_i). \tag{7.2}$$

The system (7.2) of equations becomes a system of linear equations of $D(E_i)$ variables and $D(E_i)$ equations, and its matrix representation is

$$-V_i = M_i A_i, \tag{7.3}$$

where $A_i = (a_j^{(i)})$, $V_i = ((\alpha_i^{n_i})^{\sigma_j})$, and

$$M_i = \begin{pmatrix} t_1(\alpha(i)^{\sigma_1}) & t_2(\alpha(i)^{\sigma_1}) & \cdots & t_{N_i}(\alpha(i)^{\sigma_1}) \\ \vdots & \vdots & & \vdots \\ t_1(\alpha(i)^{\sigma_{D(E_i)}}) & t_2(\alpha(i)^{\sigma_{D(E_i)}}) & \cdots & t_{D(E_i)}(\alpha(i)^{\sigma_{D(E_i)}}) \end{pmatrix}.$$

On the other hand, $\{t_1(\alpha(E_i)), \ldots, t_{D(E_i)}(\alpha(E_i))\}$ is a $\mathbb{Q}$-linear basis of $\mathbb{Q}(\{\alpha_e : e \in E_i\})$ and so $\det(M_i) \neq 0$. Thus we can compute f_i by solving the system of linear equations if we already know the *exact value of each root α_i of f*.

As one can see, the degree $D(E_i)$ can be seen as a complexity measure of the computation of f_i. So, one wants to compute a minimal i-relation. As said above, finding such a minimal i-relation is a combinatorial problem but, it depends only of the symmetric representation of G_f and can be stored once it is computed.

Systems over p-adic numbers

As we do not know the exact value of each α_i, we use the approximate value of roots of f in $\bar{\mathbb{Q}}_p$. The maximal ideal $\mathcal{M}$ may not be maximal if it is considered as an ideal in $\mathbb{Q}_p[X]$, more precisely we have:

Proposition 7.3.8. *We use the same notation as in Theorem 7.2.2. Let $\mathcal{S}$ be the transversal $Stab(\bar{e})\backslash\backslash Stab(e)$, then*

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M} = \cap_{\sigma\in\mathcal{S}}(\mathcal{M}^{(\infty)})^{\sigma}, \text{ and } \pi_p(\mathcal{M}\cap\mathbb{Z}_p^0) = \cap_{\sigma\in\mathcal{S}}(\bar{\mathcal{M}})^{\sigma}.$$

Proof. Let e be the idempotent of $\mathcal{A}_0$ corresponding to $\mathcal{M}$. As $\mathcal{M} = \{h \in \mathbb{Q}[X] \mid eg = 0 \in \mathbb{Q}[X]/\mathcal{M}_0\}$, the first equation can be derived directly from Theorem 7.2.1 (3) and Theorem 7.2.2 (3). The second equation can be also derived by considering the projection π_p. □

By Proposition 7.3.8, we can reduce the system (7.1) to the following. Here we use the same notation as in Theorem 7.2.2.

$$f_i(\gamma) = 0 \text{ for every } \gamma \in \cup_{\sigma} Z((\mathcal{M}^{(\infty)})^{\sigma})(E_i), \tag{7.4}$$

where σ ranges in $\mathcal{S} = G_{\pi_p(f)}\backslash\backslash G_f$.

The system (7.4) consists of $D(E_i)$ variables and $D(E_i)$ linear equations over

$$\mathbb{Q}_p[X_n]/\mathcal{M}^{(\infty)}$$

and it is equivalent to the following

$$\mathrm{NF}(f_i, (\mathcal{G}^{(\infty)})^{\sigma}) = 0 \text{ for every } \sigma \in G_{E_i}\backslash\backslash G_f. \tag{7.5}$$

Moreover, replacing $\mathcal{G}^{(\infty)}$ with $\mathcal{G}^{(k)}$, we have the following system which $f_i \bmod p^{k+1}$ must satisfy.

$$\mathrm{NF}(f_i, (\mathcal{G}^{(k)})^{\sigma}) = 0 \text{ for every } \sigma \in G_{E_i}\backslash\backslash G_f. \tag{7.6}$$

The system (7.6) is considered as a system of $D(E_i)$ variables and $D(E_i)$ linear equations with coefficients in $\mathbb{Z}/p^{k+1}\mathbb{Z}[X_n]/\mathcal{M}^{(k)}$. Especially, for the case $k = 0$, the system (7.6) is translated to the following system which $\pi_p(f_i)$ must satisfy:

Fix a zero $\bar{\alpha} = (\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ in $Z(\bar{\mathcal{M}})$, and set $\pi_p(f_i) = x_i^{n_i} + \sum_{j=1}^{D(E_i)} \bar{a}_j^{(i)} t_j$. If the vector $(\bar{a}_j^{(i)})$ is denoted by A_i, the vector $((\bar{\alpha}_{E_i}^{n_i})^{\sigma_j})$ by V_i and the matrix

$$\begin{pmatrix} t_1(\bar{\alpha}(E_i)^{\sigma_1}) & t_2(\bar{\alpha}(E_i)^{\sigma_1}) & \cdots & t_{D(E_i)}(\bar{\alpha}(E_i)^{\sigma_1}) \\ \vdots & \vdots & & \vdots \\ t_1(\bar{\alpha}(E_i)^{\sigma_{D(E_i)}}) & t_2(\bar{\alpha}(E_i)^{\sigma_{D(E_i)}}) & \cdots & t_{D(E_i)}(\bar{\alpha}(E_i)^{\sigma_{D(E_i)}}) \end{pmatrix}$$

by $\bar{M}_i$, then we have the identity

$$-\bar{V}_i = \bar{M}_i \bar{A}_i, \tag{7.7}$$

Theorem 7.3.1. *For each i, $1 \leqslant i \leqslant n$, the following holds.*

1. *The system (7.7) has a unique solution over $GF(p)$ which gives $\pi_p(f_i)$.*

2. *For a positive integer k, the system (7.6) has a unique solution which gives the approximation $f_i \bmod p^{k+1}$. Moreover, we can construct $f_i \bmod p^{k+1}$ from $\pi_p(f_i)$ by Hensel lifting.*

Proof. Consider the expansion of $\det(M_i)$ and that of $\mathrm{disc}(f)$, where we consider each root α_i as an indeterminate y_i. Then, it can be shown that $\mathrm{disc}(f) = \prod_{j\neq k}(y_j - y_k)$ and by *discriminant composition formula* (see [89]) there exist integers $e_{j,k}$ such that

$$\det(M_i) = \prod_{1\leqslant j<k\leqslant n} (y_j - y_k)^{e_{j,k}}, \tag{7.8}$$

As $\pi_p(f)$ is square-free, we conclude that $\det(\bar{M}_i) \neq 0$ and so the system (7.7) has a unique solution and thus, the unique solution gives $\pi_p(f_i)$. We can show the second statement by the same argument and the fact that $\det(\bar{M}_i) \neq 0$.

For the Hensel lifting we want to use the same algorithm than the one given in the proof of Theorem 7.2.3 but here the ideal $I = \pi_p(\mathcal{M} \cap \mathbb{Z}_p^0)$ is not maximal in $\mathbb{F}_p[X]$. By Proposition 7.3.8 the ideal I is the intersection of comaximal ideals. So, we can use the *chinese remainder strategy* in order to compute the polynomials h_i, s and t, for each $i \in [\![2, n]\!]$, in the case $k = 1$ and then apply the *quadratic Hensel lift* inductively. □

Theorem 7.3.1 gives two possible strategies for the computation of

$$\mathcal{T}_k = \{f_1 \bmod p^{k+1}, \ldots, f_n \bmod p^{k+1}\}$$

a k-approximation of a triangular basis of $\mathcal{M}$:

1. By Hensel lifting, $\mathcal{G}^{(k)}$ is constructed from $\overline{\mathcal{G}}$ (see Theorem 7.2.3). From $\mathcal{G}^{(k)}$ we construct and solve the system 7.6 for each $i \in [\![1, n]\!]$. The solutions are then $\mathcal{T}_k$ (see assertion (2) of Theorem 7.3.1).

2. From $\overline{\mathcal{G}}$ we construct and solve the systems 7.6 for each $i \in [\![1, n]\!]$. The solutions are $\mathcal{T}_0$ and we can construct $\mathcal{T}_k$ by Hensel lifting (see Theorem 7.3.1).

Now, assume $\mathcal{T}_k = \{f_1 \bmod p^{k+1}, \ldots, f_n \bmod p^{k+1}\}$ is computed. Then we convert each $f_i \bmod p^{k+1}$ to a polynomial over $\mathbb{Q}$ by the following well-known technique (see [34] and [110]).

Lemma 7.3.9. *Let c be a positive integer smaller than p^{k+1}. If there are non-zero integers a, b such that $c \equiv \frac{a}{b} \pmod{p^{k+1}}$, $|a|, |b| < \sqrt{p^{k+1}/2}$, $b > 0$, then such a pair (a, b) is unique and it is determined by the extended GCD computation of c and p^{k+1}.*

Corollary 7.3.10. *Let $B_i = \max\{\mathrm{den}(c), \mathrm{num}(c) \mid c \text{ is a coefficient of } f_i\}$, where $\mathrm{den}(c)$ and $\mathrm{num}(c)$ denote the denominator and the numerator of c, respectively. Then, if $2B_i^2 < p^{k+1}$, the polynomial converted from $f_i \bmod p^{k+1}$ coincides with f_i.*

7.3.2 Estimation of the bound B_i

Here we give details on the bound B_i. Since coefficients of f_i correspond to the solution of the system (7.3), by Cramer's rule (see [68, Theorem 4.4]), the denominator of each coefficient of f_i divides $\det(M_i)$ and the numerator of the j-th coefficient of f_i divides $\det(M_i^{(j)})$, where $M_i^{(j)}$ is the matrix obtained by replacing the j-th column with V_i.

Lemma 7.3.11. *Let B_0 be the maximum of the absolute values of roots α_i's of f in $\mathbb{C}$. Then, for each i, the bound B_i can be computed from the set of degrees $\{d(E_i)_e : e \in E_i\}$ and B_0.*

Proof. Without lost of generality, we can assume the bound B_0 greater than 1. For each row of $M_i^{(j)}$ and each row of M_i, we have the following bound $\mathbb{B}_i$ on its square-norm by replacing each α_k with B_0 and by denoting $d(E_i)_e$ by d_e:

$$\mathbb{B}_i^2 = \prod_{e \in E_i} (1 + B_0^2 + \cdots + B_0^{2(d_e-1)}) + B_0^{2d_i} = \prod_{e \in E_i} \frac{B_0^{2d_e} - 1}{B_0^2 - 1} + B_0^{2d_i}.$$

Thus, as the determinant of a matrix is bounded by the product of square-norms of its lows (by the inequality of Hadamard), we have $B_i = \mathbb{B}_i^{D(E_i)}$. □

If $B_0 > 2$, then we can set B_i as $B_0^{D(E_i)(\sum_{e \in E_i} d(E_i)_e)}$ and, since

$$\sum_{e \in E_i} d(E_i)_e \leqslant \sum_{1 \leqslant k \leqslant i} d_k \leqslant \sum_{1 \leqslant k \leqslant i} k\,,$$

the bit size of B_i is bounded by $O(n^2 D(E_i) \log(B_0))$.

For the denominator, we can give a precise bound (see [1], and [70]).

Lemma 7.3.12. *For each i, there is a positive integer C_i computed from the set of degrees $\{d(E_i)_e : e \in E_i\}$ such that each $d(f)^{C_i} f_i$ belongs to $\mathbb{Z}[X]$.*

Proof. By the equation (7.8), $\det(M_i)$ is considered as a polynomial in each α_i. Then estimating the degree of $\det(M_i)$ in each α_j, we can obtain a bound on the denominators of coefficients of f_i. In fact, the degree of $\det(M_i)$ in α_j is bounded by the following D_i:

$$D_i = \frac{D(E_i)(\sum_{e \in E_i} d_e)}{n_0}\,,$$

where $n_0 = n_1 = n$ if f is irreducible over $\mathbb{Q}$, and $n_0 = 1$ otherwise. Then, from the shape of $\mathrm{disc}(f)$, it can be shown easily that $C_i = \frac{D_i}{2}$ satisfies the statement. Moreover, if f is irreducible, we can set $C_i = \frac{D_i}{2(n-1)}$. □

The following example show that the bound B_i, given in Lemma 7.3.11, is very pessimistic.

Example 7.3.13. The polynomial with integral coefficients

$$f = x^9 - 2x^8 - 17x^7 + 33x^6 + 90x^5 - 183x^4 - 161x^3 + 379x^2 + 36x - 193$$

has all its roots in the real field and are bounded by 3.3. If we use our method for the computation of the splitting field of f, the largest theoretical bound encountered is:

$$\simeq 4 * 10^{997}\,.$$

But, after computation we have the following bound on the absolute value of the denominators and numerators of the coefficients:

$$307025101\,.$$

We will see in the section 7.3.4 how the problem of pessimistic theoretical bound can be avoided. Now, we see how the knowledge of the symmetric representation of G_f can be used to minimize the computations.

7.3.3 Reducing the number of systems to compute

In this section we suppose a symmetric representation of G_f and a i-relation E_i for each i in $[\![1, n]\!]$ are known. As stated in the section 7.3.1, we have to solve a system of size $D(E_i)^2$ for each $i \in [\![1, n]\!]$ in order to compute the polynomial f_i corresponding to E_i. Here we give some techniques to avoid some computations. These techniques depend only on the symmetric representation of G_f and can be pre-computed and stored before any splitting field computation.

The two following techniques were already used in section 5.5 with a partial knowledge of G_f. Here, since we know the exact symmetric representation of G_f, we use the whole power of these techniques.

Cauchy moduls technique

Let $\mathcal{T} = \{f_1, \ldots, f_n\}$ be a triangular basis of the ideal $\mathcal{M}$ with $\deg_i(f_i) = d_i$. Let $\mathcal{O} = \{i_1 < i_2 < \cdots < i_k\}$ be the orbit of i under the action of $\mathrm{Stab}_{G_f}([1, \ldots, i-1])$ then $i_1 = i$ and $k = d_i$ the degree of f_i in x_i. If g is multivariate polynomial and u an indeterminate then we denote by $\mathrm{Ev}(g, u)$ the multivariate polynomial obtained by replacing the greatest variable in g by u. The d_i (generalised) *Cauchy moduls* of f_i are defined by:

$$\begin{aligned} c_1(f_i) &= f_i \\ c_2(f_i) &= \frac{\mathrm{Ev}(c_1, x_{i_2}) - \mathrm{Ev}(c_1, x_{i_1})}{(x_{i_2} - x_{i_1})} \\ &\vdots \\ c_{d_i}(f_i) &= \frac{\mathrm{Ev}(c_{d_i-1}, x_{i_{d_i}}) - \mathrm{Ev}(c_{d_i-1}, x_{i_{d_i-1}})}{(x_{i_{d_i}} - x_{i_{d_i-1}})} \end{aligned}$$

By construction, the following holds:

Lemma 7.3.14. *The Cauchy modul $c_j(f_i)$ is a polynomial of $\mathbb{Q}[x_1, \ldots, x_{i_j}]$ which is monic as a polynomial in x_{i_j} with $deg_{i_j}(c_j(f_i)) = d_i - j + 1$. Moreover, the polynomial $c_j(f_i)$ is in $\mathcal{M}$.*

As we know the symmetric representation of G_f we could know by advance if the polynomial $c_j(f_i)$ has the same degree, in x_{i_j}, as the polynomial f_{i_j}. In this case, in the system $\mathcal{T}$, the polynomial f_{i_j} can be replaced by $c_j(f_i)$ and $\mathcal{T}$ is still a Gröbner basis of $\mathcal{M}$. So, in the construction of $\mathcal{T}$ we avoid the computation of the system corresponding to f_{i_j}.

Transporters technique

Here we use the fact that the group G_f is the stabilizer of the ideal $\mathcal{M}$.

Let $E_i = \{e_1 < e_2 < \cdots < e_k\}$ be a i-relation (then $e_k = i$) and $j \in [\![i+1, n]\!]$. A permutation $\sigma \in G_f$ is said to be a (i, j)-*transporter* if it satisfies:

$$\sigma(i) = j \text{ and } j = \max(\{\sigma(e) : e \in E_i\})$$

Proposition 7.3.15. *Let σ be a (i,j)-transporter and f_i the polynomial corresponding to E_i. Then,* $\mathrm{NF}(\sigma.f_i, \{g_1, \ldots, g_{j-1}\})$ *is a multiple of g_j as polynomials in* $\mathcal{A} = (\mathbb{Q}[x_1, \ldots, x_{j-1}]/\langle g_1, \ldots, g_{j-1}\rangle)[x_j]$.

Proof. This result appears in the proof of Corollaire 5.5.2 but we give here a short proof. Since σ is a (i,j)-transporter, the polynomial $\mathrm{NF}(\sigma.f_i, \{g_1, \ldots, g_{j-1}\})$ can be viewed as a univariate polynomial h in the indeterminate x_j with coefficients in $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$. Moreover, since $\sigma.f_i \in \mathcal{M}$, we have $h(\alpha_j) = 0$. Thus h is a multiple of the minimal polynomial of α_j over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$, hence h is a multiple of g_i as a polynomial of $\mathcal{A}$. □

From this proposition we have the two following results.

Corollary 7.3.16. *With the same notations as in Proposition 7.3.15. If we denote by c_j the j-th Cauchy moduls of f and by P the g.c.d. of c_j and* $\mathrm{NF}(\sigma.f_i, \{g_1, \ldots, g_{j-1}\})$ *as polynomials in $\mathcal{A}$. Then P, as a polynomial in $\mathbb{Q}[X_n]$, is in $\mathcal{M}$.*

Corollary 7.3.17. *With the same notations as in Proposition 7.3.15, if the degree d_j is equal to d_i then we can replace the polynomial f_j by $\sigma.f_i$.*

From the knowledge of G_f, a i-relation E_i and the degree d_i for each i in $[\![1, n]\!]$ can be computed. Then, we search for transporters which verify the conditions of Corollary 7.3.17. If a (i,j)-transporter is found then the computation of the polynomial f_j is avoided because this polynomial can be replaced with the image of a polynomial f_i. We can also search for transporters which verify the conditions of Corollary 7.3.16. In this case, we replace the system resolution by a g.c.d. computation in a tower of fields which may be more efficient in practice.

From these two techniques, we can attach to a subgroup G of S_n a scheme for the computation of the splitting field of a polynomial with a Galois group isomorphic to G. This scheme contains all the i-relations and indexes where we can use one of these techniques in order to avoid the resolution of the corresponding systems.

7.3.4 Check of correctness and early detection

To improve the efficiency of the method, we can incorporate "early detection strategy" which is widely used in polynomial factoring algorithms. As shown in Section 7.3.2, the bound computed from the i-relations and B_0 tends to be large compared to the exact value. So, the technique is supposed to work very well in our case.

In this section we suppose, for simplicity, that we use the second strategy of the theorem 7.3.1 in order to compute $\mathcal{G}$. This technique can also be easily applied to the first one.

Conversion at Early Stage

During the Hensel lifting of $\bar{\mathcal{G}}$ we stop the calculation at a certain degree k in the middle, even though p^{k+1} does not exceed the bound. In this case, we may generate the systems of linear equations modulo p^{k+1} corresponding to the i-relations we have to compute. Assume that we have obtained the first $j-1$ polynomials $\{g_1, \ldots, g_{j-1}\}$ of $\mathcal{G}$.

Then, we solve the system (7.6) corresponding to E_j and we obtain g_i modulo p^{k+1}. We try to convert it to a candidate polynomial over $\mathbb{Q}$ by the technique given in Lemma 7.3.9. In this case, we use the following conditions as criteria for correctness.

1. The conversion is done successfully for every coefficient of g_i.
2. The denominator of each coefficient of a candidate polynomial divides a certain power of $\mathrm{disc}(f)$. (See Lemma 7.3.12.)

If the conversion does not satisfy the criteria above then p^{k+1} is not sufficient to afford the correct f_j. Thus, we continue the lifting process and we generate a new system of linear equations again, if necessary. If, in the contrary, the conversion, say h_j, satisfy the criteria we have not proven that $h_j = f_j$ this is what we do now.

7.3.5 Correctness of Solution

Assume we have a candidate polynomial h_j for the polynomial f_j corresponding to the j-relation E_j. We can check if $h_j = f_j$ by the following theorem.

Theorem 7.3.2. *$h_j = f_j$ if and only if* $\mathrm{NF}(c_j(f), \{g_1, \ldots, g_{j-1}, h_j\}) = 0$.

Proof. If $h_j = f_j$ then the normal form is clearly equal to 0. Reciprocally, assume that $\mathrm{NF}(c_j(f), \{g_1, \ldots, g_{j-1}, h_j\}) = 0$. So, if we consider the polynomials h_j and $c_j(f)$ as univariate polynomials with coefficients in $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$ then

$$h_j(x, \alpha_{j-1}, \ldots, \alpha_1) \,|\, c_j(f)(x, \alpha_{j-1}, \ldots, \alpha_1)\,.$$

Since h_j has the same degree than f_j, which is a divisor of $c_j(f)$, we have two possibilities: $h_j = f_j$ or h_j is an other divisor of $c_j(f)$. As $h_j \bmod p = f_j \bmod p$, if $h_j \neq f_j$ then the polynomial $c_j(f) \bmod p$ is not separable which is impossible. Hence, we have $h_j = f_j$. □

7.4 Algorithm

Here we give a brief survey on the practical implementation of this method for the computation of the splitting field of polynomial.

7.4.1 Pre-computations

Given a subgroup G of S_n, as we saw in the section 7.3.3, we can prepare the computation of the Gröbner basis $\mathcal{G}$ of a polynomial f with Galois group isomorphic to G.

Step 1: First, the Cauchy's technique (see Lemma 7.3.14) is applied. After this step we obtain a set $\mathcal{I}$ of integers corresponding to the indexes of the g_i which can not be obtained with the Cauchy's technique.

Step 2: For each integer i in $\mathcal{I}$ a i-relation is computed.

Step 3: The transporter technique is applied on the i-relations computed in step 2. After this step, a set $\mathcal{E}$ is obtained. It consists of i-relations corresponding to the g_i which have to be computed by systems resolution.

These three steps can be done using only the knowledge of G and can be stored. So, we do not consider these pre-computations as a part of the total cost of our method. The set $\mathcal{E}$ depends only on the choice of G and the i-relations chosen in Step 2. This set represents all the linear systems we have to solve in our method. So, a measure of complexity can be given by the following integer

$$|\mathcal{E}| = \sum_{E \in \mathcal{E}} D(E)\,.$$

For a given permutations group G we can suppose that we choose i-relations in step 2 which minimize $|\mathcal{E}|$ (for example, we can choose only minimal i-relations). Moreover, since we can reorder the roots of f, we choose the conjugate of G which minimises $|\mathcal{E}|$ too, such a group is called a *c-minimal* conjugate of G. The invariant of the conjugacy class of G corresponding to the integer $|\mathcal{E}|$ obtained with a c-minimal conjugate of G is denoted $c(G)$ and is called the *c-size* of G.

Example 7.4.1. Assume $G \simeq [2^4]S_4$ as a group of permutations of degree 8. With the nomenclature of Butler and McKay this group corresponds to $8T_{44}$. We can choose one of these two following representatives:

$$\begin{aligned} G_1 &= \langle (8,7,6,1)(5,4,3,2), (8,1)(4,5), (5,1)\rangle \\ G_2 &= \langle (2,1), (8,6,4,1)(7,5,3,2), (8,1)(7,2)\rangle \end{aligned}$$

If we choose G_1 then the degrees d_i are given by $d_1 = 8, d_2 = 6, d_3 = 4, d_4 = 2, d_5 = d_6 = d_7 = d_8 = 1$. The Cauchy technique can be applied to avoid the system corresponding to the polynomial g_8 (it is the linear Cauchy modul of f). We find the following minimal relations

$$\begin{aligned} \mathcal{E} &= \{E_2 = \{2,1\}, E_3 = \{3,2,1\}, E_4 = \{4,3,2,1\}, \\ &\quad E_5 = \{5,1\}, E_6 = \{6,2\}, E_7 = \{7,3\}\} \end{aligned}$$

We find a $(5,6)$-transporter $(8,1,2,3)(7,4,5,6)$ and a $(5,7)$-transporter $(7,1,3,5)$. Thus the remaining systems to compute corresponds to the following i-relations:

$$\mathcal{E} = \{E_2 = \{2,1\}, E_3 = \{3,2,1\}, E_4 = \{4,3,2,1\}, E_5 = \{5,1\}\}$$

In this case we obtain $|\mathcal{E}| = 632$.

If we choose G_2 then the degrees d_i are given by $d_1 = 8, d_2 = 1, d_3 = 6, d_4 = 1, d_5 = 4, d_6 = 1, d_7 = 2, d_8 = 1$. The Cauchy technique can be applied for avoiding the system corresponding to the polynomial g_8, g_7, g_5, g_3 (Cauchy moduls of f). We find the following minimal relations

$$\mathcal{E} = \{E_2 = \{2,1\}, E_4 = \{4,3\}, E_6 = \{6,5\}\}$$

We find a $(2,4)$-transporter and a $(2,6)$-transporter. Thus the remaining system to compute correspond to the following i-relation:

$$\mathcal{E} = \{E_2 = \{2,1\}\}$$

In this case we obtain $|\mathcal{E}| = 8$.

This example shows that the representative of the conjugacy class of G has to be chosen very precisely.

7.4.2 Algorithm

Here we give an analysis of the second strategy of Theorem 7.3.1. We will give, in a future work, the total study of the other strategy. Moreover, for the transporter's technique, we do not use the result of corollary 7.3.16.

Assume we have pre-computed a database of c-minimal representative of each conjugacy class of permutations group of degree n. This database contains also for each representative G:

- The set $\mathcal{E}$ of i-relations corresponding to the polynomials g_i we have to compute;
- the transversal $G\backslash\backslash\mathrm{Stab}_G(E_i)$ for each $E_i \in \mathcal{E}$;
- the techniques (Cauchy or transporters) used to obtain the others polynomials;

Given a polynomial f of degree n, our method for finding the Gröbner basis $\mathcal{G} = \{g_1, g_2, \ldots, g_n\}$ can be implemented following this algorithm. First we give the one using the theoretical bound (see Algorithm 12), then the one using the early detection (see Algorithm 13).

Algorithme 12 RelationIdealTheoriticalBound($\mathcal{G}^{(k_0)}$,G_f,p)

Hypothèse : p is a prime integer, $\mathcal{G}^{(k_0)}$ is a k_0 approximation of $\mathcal{G}^{(\infty)}$ in $\mathbb{Q}_p$. G_f is the symmetric representation of the Galois group of f corresponding to the approximation of the roots of f given by $\mathcal{G}^{(k_0)}$. We suppose that G_f is a symmetric representative stored in our database.

Sortie : $\mathcal{G} = \{g_1, \ldots, g_n\}$ and $\mathcal{T} = \{f_1, \ldots, f_n\}$ are triangular basis of a relation ideal of f with G_f as stabilizer. The basis $\mathcal{G}$ is reduced.

From the database we obtain the set $\mathcal{I}$ corresponding to the indexes of the f_i we have to compute with linear systems.
Compute the maximal bound B over all the B_i (see Section 7.3.2).
Let k be the minimal integer such that $2B^2 < p^{k+1}$. Construct $\mathcal{G}^{(k)}$ from $\mathcal{G}^{(k_0)}$ by Hensel lifting.
for $i = 1$ to n **do**
  if $i \in \mathcal{I}$ **then**
    Solve the linear system corresponding to E_i and convert the solution to the polynomial f_i with rational coefficients.
  else
    Apply the Cauchy's and transporters techniques (Corollary 7.3.17) over one f_j with $j < i$ in order to obtain f_i without any computation.
  end if
  Reduce f_i modulo $\{g_1, \ldots, g_{i-1}\}$ in order to obtain g_i.
end for
Return $\mathcal{T}$, $\mathcal{G}$, G_f.

Clearly these two algorithms give a proven result. Now we give a brief analysis of the complexity of this method.

Algorithme 13 RelationIdealEarlyDetection($\mathcal{G}^{(k_0)}$,G_f,p)

Hypothèse : p is a prime integer, $\mathcal{G}^{(k_0)}$ is a k_0 approximation of $\mathcal{G}^{(\infty)}$ in $\mathbb{Q}_p$. G_f is the symmetric representation of the Galois group of f corresponding to the approximation of the roots of f given by $\mathcal{G}^{(k_0)}$.We suppose that G_f is a symmetric representative stored in our database.

Sortie : $\mathcal{G} = \{g_1, \ldots, g_n\}$ and $\mathcal{T} = \{f_1, \ldots, f_n\}$ are triangular basis of a relation ideal of f with G_f as stabilizer. The basis $\mathcal{G}$ is reduced.

From the database we obtain the set $\mathcal{I}$ corresponding to the indexes of the g_i we have to compute with linear systems.
for $i = 1$ to n **do**
  if $i \in \mathcal{I}$ **then**
    S1: Solve the linear system corresponding to E_i. Let s_i be the solution.
    if s_i can be converted to a rational polynomial h_i **and** h_i satisfies the correctness test **then**
      The polynomial h_i is f_i.
    else
      Construct a better approximation of $\mathcal{G}^{(\infty)}$ by Hensel lifting and goto step **S1**.
    end if
  else
    Apply the Cauchy's and transporters techniques over one f_j with $j < i$ in order to obtain f_i without any computation.
  end if
  Reduce f_i modulo $\{g_1, \ldots, g_{i-1}\}$ in order to obtain g_i.
end for
Return $\mathcal{T}$, $\mathcal{G}$, G_f.

7.4.3 Complexity

In this section we study the complexity of our method when the polynomial is irreducible, monic with integral coefficients and degree n. We first study the case where the theoretical bound B_i (see Section 7.3.2) is used, then we study the case of the early detection strategy (see Section 7.3.4).

In all this part the following hypothesis is supposed:

> *A database of c-minimal symmetric representation of each degree n transitive group is known. For each element G of this database the pre-computation (see Section 7.4.1) is done and all the transversals of G modulo the stabilizers are pre-computed too.*

Moreover, we study the complexity of our algorithm when only the *transporters* and *Cauchy's* techniques are used (we do not consider the calculation of a g.c.d. in replacement of a linear system construction and resolution). The cost of the Cauchy moduls computations is not taken into account because they could be pre-computed generically (see [90]). We only consider the computation of the triangular basis $\mathcal{T}$, so we do not consider the complexity of normal forms computations in order to compute $\mathcal{G}$ from $\mathcal{T}$.

The case where the theoretical bound B_i is used

In this case, the Hensel lift is computed only one time. Let D be the maximal degree $D(E_i)$, where E_i ranges into the i-relations, and let B_0 be a bound over the absolute values of the roots of f. Then we choose k to be an integer so that $k\log(p) > O(n^2 D\log(B_0))$ (see Section 7.3.2). Let $\mathsf{M}_R(n)$ denotes the number of operations needed in $R = (\mathbb{Z}/p^{k+1}\mathbb{Z})[X_n]/\mathcal{G}^{(k+1)}$ for the arithmetic operations of polynomials of degree n with coefficients in R. Let $\mathcal{M}(\overline{N})$ denotes the cost of an arithmetic operation in R as the number of operations in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ (see Proposition 1.3.20). All the arithmetic operations for the Hensel lifts can be done in the ring $(\mathbb{Z}/p^{k+1}\mathbb{Z})[X_n]/\mathcal{G}^{(k+1)}$. Thus, the quadratic Hensel lift of the n polynomials (which are of degree at most n) of $\overline{\mathcal{G}}$ to $\mathcal{G}^{(k+1)}$, takes (see [110])

$$O(n\mathsf{M}_R(n)\mathcal{M}(\overline{N}))$$

operations in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.

Then, we analyse the cost of constructing and solving the linear systems M_i. Let E_i be an i-relation which corresponds to a linear system to be constructed. In the theoretical construction (see system (7.6)) of M_i we construct a matrix M_i with $\overline{N}D(E_i)$ linear equations (with repetitions) and $D(E_i)$ variables. Producing one line of this matrix can be done with $D(E_i)$ multiplications in $(\mathbb{Z}/p^{k+1}\mathbb{Z})[X_n]/\mathcal{G}^{(k+1)}$. Thus, the construction of M_i takes

$$T_1(E_i) = O(\overline{N}D(E_i)^2\mathcal{M}(\overline{N}))$$

operations in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.
During the construction we take off the repetitive lines, then we solve the remaining $D(E_i)\times D(E_i)$ linear system which takes

$$T_2(E_i) = O(D(E_i)^\omega\mathcal{M}(\overline{N}))$$

operations in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ (the power ω represents the cost of the linear algebra). Thus the construction and resolution of all the matrices M_i take

$$\sum_{i\in\mathcal{I}} T_1(E_i) + T_2(E_i) = O((c(G)^\omega + \overline{N}c(G)^2)\mathcal{M}(\overline{N}))$$

operations in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.

Now, we denote by $\mathbb{M}(\overline{N}, n^2 D\log(B_0))$ the cost, in word operations, of an arithmetic operation in R. In total, since $c(G)^\omega > n\mathsf{M}_R(n)$, we obtain the following result:

Theorem 7.4.1. *Algorithm 12 takes*

$$O((c(G)^\omega + \overline{N}c(G)^2)\mathbb{M}(\overline{N}, n^2 D\log(B_0)))$$

word operations.

The case where the early detection is used.

Let B_{true} be the maximum of the absolute values of denominators and numerators of coefficients of g_i's. Then, we can find the true answer at the step p^{k+1} which just exceeds the bound B_{true}. So, we may assume that $p^{k+1} = O(B_{true})$. Then, by applying the results of the paragraph above, we have

Theorem 7.4.2. *The algorithm 13 takes*

$$O((c(G)^\omega + \overline{N}c(G)^2)\mathbb{M}(\overline{N}, \log(B_{true})) + L)$$

word operations, where L is the total cost of computations of normal forms for correctness tests.

Remark 7.4.2. The normal forms are computed over the rationals. Thus, we can not put, in Theorem 7.4.2, all the operations in a same complexity group.

7.5 Experiments and remarks

First we give an example of our algorithm 13 for a polynomial of degree 6. For this experiment we will use the *computer algebra system* Magma. In this software, a multivariate polynomials ring with n variables is given with the lexicographic order $x_1 > x_2 > \ldots > x_6$. So in all this example we adopt this order which is not the same convention as in the rest of this chapter.

Example

We will construct the relations ideal of the polynomial

$$f = x^6 - 2x^5 - 4x^4 + 5x^3 + 4x^2 - 2x - 1\,.$$

Actually, we will construct the reduced triangular basis of this ideal which has the following form

$$
\begin{aligned}
&f_1(x_1, x_2, \ldots, x_6)\\
&f_2(x_2, \ldots, x_6)\\
&f_3(x_3, \ldots, x_6)\\
&f_4(x_4, \ldots, x_6)\\
&f_5(x_5, x_6)\\
&f_6(x_6)
\end{aligned}
$$

Before beginning our algorithm we have to know the action of the Galois group of f over the its p-adic roots. For this, we choose the first prime which split completely in the number field defined by f (in fact, a prime such that f is separable modulo p is enougth).

```
> p:=1;
> test:=true;
> d:=Degree(f);
>
> while test do
while>       p:=NextPrime(p+1);
while>       PR:=PolynomialRing(GaloisField(p));
while>       if IsSquarefree(PR!f) then
while|if>        ff:=Factorization(PR!f);
while|if>        test:=not((#ff eq d));
while|if>       end if;
while>       p_old:=p;
while> end while;
> p;
449
```

Thus 449 is this prime and we can now compute the Galois group of f. In this case, all the roots of f modulo p are in the field $\mathbb{F}_p$. So, we obtain a symmetric representation of the Galois group of f with its action over the roots of f modulo p.

```
> G, rmodp, _ := GaloisGroup(f:Prime:=p);
> G;
Permutation group acting on a set of cardinality 6
Order = 24 = 2^3 * 3
    (2, 5)
    (1, 2, 4)(3, 6, 5)
>rmodp;
[ 320, 28, 275, 80, 16, 181 ]
```

From the knowledge of G we retrieve the corresponding scheme stored in our database. This scheme guide our algorithm and is given by

f_1	Cauchy modul of f_6
f_2	Cauchy modul of f_5
f_3	Cauchy modul of f_4
f_4	Transporter : $f_5^{(1,2,3,6,5,4)}$
f_5	System x_5, x_6, $d_5 = 2, d_6 = 5$
f_6	$f(x_6)$

Since f_6 is already known, we begin by computing the polynomial $f_5(x_5, x_6)$. From the scheme, we know that the polynomial f_5 is of degree 2 in x_5 and of degree at most 5 in x_6. So we construct the corresponding system 7.7. The roots of f modulo p are numbered in the following manner

$$\alpha_1 = 320,\ \alpha_2 = 28,\ \alpha_3 = 275,\ \alpha_4 = 80,\ \alpha_5 = 16,\ \alpha_6 = 181$$

and a transversal of G modulo $\mathrm{Stab}(G, [5, 6])$ is computed by

```
> RightTransversal(G,Stabilizer(G,[5,6]));
{@
    Id(G),
    (2, 5),
    (1, 2, 4)(3, 6, 5),
    (1, 2, 3, 6, 5, 4),
    (1, 5, 3, 6, 2, 4),
    (1, 4, 2)(3, 5, 6),
    (1, 5, 4)(2, 3, 6),
    (1, 4, 2, 6, 3, 5),
    (1, 3, 5, 6, 4, 2),
    (1, 3, 5)(2, 6, 4),
    (1, 6),
    (1, 6)(2, 5)
@}
```

So the first line of the matrix M_5 is

$$\alpha_5\alpha_6^5 \quad \alpha_5\alpha_6^4 \quad \alpha_5\alpha_6^3 \quad \alpha_5\alpha_6^2 \quad \alpha_5\alpha_6 \quad \alpha_5 \quad \alpha_6^5 \quad \alpha_6^4 \quad \alpha_6^3 \quad \alpha_6^2 \quad \alpha_6 \quad 1$$

and the second is the image by $(2,\ 5)$ of the first one:

$$\alpha_2\alpha_6^5 \quad \alpha_2\alpha_6^4 \quad \alpha_2\alpha_6^3 \quad \alpha_2\alpha_6^2 \quad \alpha_2\alpha_6 \quad \alpha_2 \quad \alpha_6^5 \quad \alpha_6^4 \quad \alpha_6^3 \quad \alpha_6^2 \quad \alpha_6 \quad 1$$

Actually, we obtain the following system with coefficients in $\mathbb{F}_{449}$:

```
>M5;
[77   55   360  193  202  16   89   256  247  433  181  1]
[247  433  181  1    129  28   89   256  247  433  181  1]
[273  438  308  356  359  275  161  431  55   256  16   1]
[308  356  359  275  382  80   161  431  55   256  16   1]
[121  309  444  80   67   275  198  424  400  335  28   1]
[254  334  220  360  385  181  438  431  93   193  275  1]
[125  245  121  309  444  80   198  424  400  335  28   1]
[72   77   126  247  445  320  438  431  93   193  275  1]
[343  414  196  429  112  181  245  424  140  114  80   1]
[274  82   349  111  7    320  245  424  140  114  80   1]
[20   421  129  448  181  16   338  335  429  28   320  1]
[35   400  338  335  429  28   338  335  429  28   320  1]
```

The vector V_5 is given by

```
> V5
(335  256  28   433  28   114  433  193  114  193  335  256)
```

and MAGMA computes the following solution in $\mathbb{F}_{449}^{12}$

```
> S:=Solution(Transpose(M5),-V5);
> S;
(448  3    2   441   0    2    0    0    0    0    0    448)
```

Now we have to try to reconstruct the coefficients of f_5 from this modular solution. For example, for the first coefficient we have

```
> test, r := RationalReconstruction(S[1]);
> test;
true
> r;
-1
```

Actually, all the coefficients can be recover and we obtain the following polynomial:

$$h_5 = x_5^2 - x_5x_6^5 + 3x_5x_6^4 + 2x_5x_6^3 - 8x_5x_6^2 + 2x_5 - 1\,.$$

Finally, it remains to prove that h_i is equal to f_i. For this, we use the correctness test using the computation of a normal form. Let c_5 be the Cauchy modul of f with degree 5 in its dominant monomial. The polynomial h_5 is f_i if and only

$$\mathrm{NF}(c_5, [h_5, f_6]) = 0\,.$$

With MAGMA we obtain

```
> h5;
x5^2 - x5*x6^5 + 3*x5*x6^4 + 2*x5*x6^3 - 8*x5*x6^2 + 2*x5 - 1
> f6;
x6^6 - 2*x6^5 - 4*x6^4 + 5*x6^3 + 4*x6^2 - 2*x6 - 1
> c5:=(f6-Evaluate(f6,x6,x5)) div (x6-x5);
> c5;
x5^5 + x5^4*x6 - 2*x5^4 + x5^3*x6^2 - 2*x5^3*x6 - 4*x5^3 +
    x5^2*x6^3 - 2*x5^2*x6^2 - 4*x5^2*x6 + 5*x5^2 + x5*x6^4 -
    2*x5*x6^3 - 4*x5*x6^2 + 5*x5*x6 + 4*x5 + x6^5 - 2*x6^4 - 4*x6^3
    + 5*x6^2 + 4*x6 - 2
> NormalForm(c5,[h5,f6]);
0
> f5:=h5;
```

Thus, it is not necessary to increase the precision and the polynomial f_5 is now constructed. All the remaining polynomials of the triangular systems can be obtain by applications of techniques. For example, the polynomials f_4 and f_3 are respectively computed by transporter and Cauchy techniques.

```
> f4:=f5^Sym(6)!(1, 2, 3, 6, 5, 4);
> f4;
x4^2 - x4*x5^5 + 3*x4*x5^4 + 2*x4*x5^3 - 8*x4*x5^2 + 2*x4 - 1
> f3:=(f4-Evaluate(f4,x4,x3)) div (x4-x3);
> f3;
x3 + x4 - x5^5 + 3*x5^4 + 2*x5^3 - 8*x5^2 + 2-
```

Finally, after reduction, we obtain the triangular basis of the relations ideal of f:

$$\begin{aligned}
f_1 &= x_1 + x_6^5 - 2x_6^4 - 4x_6^3 + 5x_6^2 + 4x_6 - 2,\\
f_2 &= x_2 + x_5 - x_6^5 + 3x_6^4 + 2x_6^3 - 8x_6^2 + 2,\\
f_3 &= x_3 + x_4 - x_6^4 + 2x_6^3 + 3x_6^2 - 3x_6 - 2,\\
f_4 &= x_4^2 - x_4x_6^4 + 2x_4x_6^3 + 3x_4x_6^2 - 3x_4x_6 - 2x_4 - 1,\\
f_5 &= x_5^2 - x_5x_6^5 + 3x_5x_6^4 + 2x_5x_6^3 - 8x_5x_6^2 + 2x_5 - 1,\\
f_6 &= x_6^6 - 2x_6^5 - 4x_6^4 + 5x_6^3 + 4x_6^2 - 2x_6 - 1
\end{aligned}$$

We now give some remarks about the other experiments we made.

Experiments

We have implemented algorithm 13 with the *computer algebra system* MAGMA (version 2.11) in the case of an irreducible monic polynomial with degree up to 9 and coefficients in $\mathbb{Z}$. Since MAGMA has a lot of functionalities our code contends at most five hundred lines (here we do not take into account the functions for the pre-computation). We have computed our database of representatives G of conjugacy classes of transitive groups of degree up to 9, but we did not prove that they are c-minimal (even if it seems to be true).

Choice of the prime p: As one can see in Theorem 7.4.2 the quantity $\overline{N}$ has to be chosen as small as possible. By Tchebotarev's density theorem, it is possible to find a prime p such that $\overline{N} = 1$ but it may be a hard procedure (the complexity of finding such a prime is $O(|G|)$). In our implementation, we choose to use this sort of prime. One can see in Table 7.5.0.0 that the time taken by the procedure which find such a prime is not significant in front of the rest of the computation.

The power k_0: In our implantation we begin by computing $\mathcal{G}^{(k_0)}$, with an Hensel lift, for an integer k_0 sufficiently large. In our experiments we choose $k_0 = 10$. Let p be the smaller prime with $\overline{N} = 1$, it seems that p^{10} is a good heuristic for a larger bound over the size of the coefficients of the wanted triangular basis. Actually, during all the computations we made, few correctness tests fail. The search of a better heuristic for k_0 (which depends of the discriminant of the polynomial) is in progress.

Comments on Table 7.5.0.0: For these experiments we used polynomials of the database `galpols` of MAGMA. We give, for each example, the name of the group G with the Butler and McKay's nomenclature, the order of G and the integer $c(G)$ for the representative of our database. The column `Tcheb.` shows the timings of computing a prime p such that $\overline{N} = 1$, the column p gives this prime. Column `Galois` shows the timings of computing the Galois group, `Matrix/Solve` respectively the time consuming in the construction and solving the matrices, `NF` for the normal forms computations and `Total` the total timing of the procedure. The measurements were made on a personal computer with a 1.5Ghtz Intel Pentium 4 and 512MB of memory.

As one can see, the size of the invariant $c(G)$ and the size of p has an influence over the time for the computation and resolution of the matrices. The size of p^{10} is a bound for the size of the coefficients of the matrices and $c(G)$ is the sum of all the size of the matrices to compute. When $c(G)$ is big, two cases are possible: few big matrices to compute or a lot of little matrices to compute. The first case is more time consuming than the second. This is why there are some difference between examples with same

size of the constants $c(G)$ and p. For example we can not compute the relation ideal when G is the alternating group of degree $n > 6$, the size of the systems to compute and solve are too big (in this case there is only one system to compute but its size is $|G|^2$ and even if we chose $k_0 = 1$ the computation was impossible).

As we said above, in these examples, none of the correctness fails, thus we compute only one normal form for each correctness test. The other normal forms are computed for the reduction of the triangular basis given at the end of the algorithm. The cost of the normal forms computations is not negligible for certain examples (see the lines $9T_{32}$ and $9T_{29}$). If we change the output of our algorithm by a non reduced triangular basis it would be possible to reduce this time consuming. For example, in the case of $9T_{32}$, the reduction of the basis takes 1600 seconds. The same phenomena appear in the example $9T_{29}$. For the correctness test, we could do a modular pre-test (see Section 3.3.3). If this pre-test fails then the test over the rationals will fail too, so we can avoid its computation. Moreover, a tricky implementation of the computation of normal form in a low level language may increase the efficiency of this part of our implementation.

To improve this algorithm we can also, for a given index k, use the intermediate computations of the successive matrices M_i with $i < j$ for the construction of the matrix M_j. This trick will be used in a future implementation.

Table 7.1: Timings of computation of splitting fields (seconds)

group	$\|G\|$	$c(G)$	Tcheb.	p	Galois	Matrix/Solve	NF	Total
$6T_{12}$	60	126	0.13	929	0.06	0.22 / 017	0.04	0.66
$6T_{13}$	72	18	0.11	619	0.03	0.01 / 0.01	0	0.18
$6T_{14}$	120	126	0.15	1447	0.05	0.44 / 0.44	0.06	1.18
$6T_{15}$	360	366	0.22	2437	0.0	3.69 / 6.51	0.21	10.79
$7T_5$	168	45	0.19	1879	0.06	0.05 / 0.04	0.04	0.41
$8T_{32}$	96	208	0.34	3413	0.13	0.55 / 0.59	0.14	1.870
$8T_{33}$	96	136	0.23	2099	0.14	0.32 / 0.3	0.34	1.42
$8T_{34}$	96	152	0.09	229	0.14	0.34 / 0.24	0.09	0.99
$8T_{35}$	128	32	0.31	2909	0.06	0.01 / 0.01	0.01	0.45
$8T_{36}$	168	344	0.06	211	0.14	1.78 / 1.59	1.63	5.360
$8T_{37}$	168	344	0.31	2969	0.1	1.76 / 2.26	1.15	5.72
$8T_{38}$	192	112	0.26	2503	0.1	0.29 / 0.29	0.05	1.09
$8T_{39}$	192	208	0.16	947	0.06	1.14 / 1.44	0.2	3.11
$8T_{41}$	192	128	0.4	4271	0.13	0.33 / 0.32	0.06	1.32
$8T_{42}$	288	56	0.46	5051	0.1	0.05 / 0.02	0.02	0.71
$8T_{43}$	336	344	0.29	3209	0.12	3.48 / 6.09	3.84	14.0
$8T_{44}$	384	16	1.05	14071	0.06	0.01 / 0.01	0.05	1.24
$8T_{45}$	576	608	0.36	3719	0.06	10.21 / 22.87	1.18	35.1
$8T_{46}$	576	608	0.56	6269	0.1	10.25 / 23.72	1.1	36.14
$8T_{47}$	1152	32	1.27	17299	0.05	0.03 / 0.02	0.0	1.44
$8T_{48}$	1344	344	5.56	78497	0.08	3.56 / 8.56	20.33	38.3
$9T_{21}$	162	117	0.59	6047	1.08	0.2 / 0.16	0.54	2.72
$9T_{22}$	162	90	0.12	461	0.16	0.13 / 0.09	0.08	0.65
$9T_{23}$	297	216	0.16	727	0.31	3.13 / 5.17	1.37	10.4
$9T_{24}$	324	135	0.24	1801	1.07	0.4 / 0.38	2.23	4.45
$9T_{25}$	324	360	0.16	953	1.03	3.41 / 5.49	0.33	10.63
$9T_{26}$	432	81	0.98	10273	0.3	0.18 / 0.16	7.43	9.15
$9T_{27}$	504	513	0.79	10103	0.42	7.98 / 18.6	105.49	133.64
$9T_{28}$	648	36	0.33	3037	1.38	0.03 / 0.02	0.01	1.87
$9T_{29}$	648	675	0.75	7883	0.43	13.17 / 38.74	1.44	55.21
$9T_{31}$	1296	27	0.33	2801	1.0	0.01 / 0.01	0.03	1.53
$9T_{32}$	1512	3033	0.46	5167	0.27	142.17 / 608.1	1761.84	2523

Chapitre 8

Conclusions et perspectives

Le but de cette thèse était d'élaborer des algorithmes efficaces dans le cadre de la théorie de Galois effective.
Les résultats obtenus dans ce sens sont de trois types différents.

Théorique : nous avons étudié les idéaux de Galois et obtenu de nouveaux résultats. Ces derniers nous ont permis de mieux utiliser ces objets pour le calcul d'idéaux des relations.

Algorithmique : nous avons élaboré de nouveaux algorithmes et méthodes pour résoudre les problèmes qui nous intéressaient. Pour le calcul d'une représentation symétrique du groupe de Galois d'un polynôme f, ou plus généralement du groupe de décomposition d'un idéal triangulaire, nous avons appliqué un algorithme de *branch-and-cut*. Nous avons montré que dans le cas des idéaux de Galois purs, l'algorithme obtenu est de complexité polynomiale (en le nombre de formes normales calculées) et que cette dernière est meilleure que celle précédemment connue pour les idéaux de Galois maximaux.
Pour le calcul d'un idéal des relations d'un polynôme f, nous avons proposé différents algorithmes ayant des hypothèses de départ différentes. Leur point commun est l'utilisation des connaissances sur le groupe de Galois de f afin d'améliorer leur efficacité. Ces connaissances sont soit obtenues au fur et à mesure du calcul, soit obtenues à partir des entrées de l'algorithme. Dans ce dernier cas, nous fournissons un algorithme ayant pour hypothèse de départ le fait que le polynôme f soit de groupe de Galois dihédral et un autre ayant pour entrée l'action du groupe de Galois de f sur des approximations p-adiques de ses racines. Pour ces deux derniers algorithmes nous avons mené une étude de leur complexité.

Implantation : tous les algorithmes que nous avons élaborés ont fait l'objet d'un implantation à l'aide du logiciel Magma. Ces implantations se sont révélées de très bonne efficacité.

Même si les objectifs de départ ont été atteints, toute la recherche dans cette voie n'est pas terminée. En effet, d'après D. Lazard, les idéaux de Galois pourraient être utilisés pour donner une nouvelle description des solutions de systèmes polynomiaux présentant des symétries.

Les méthodes mises à jour pour améliorer l'efficacité de nos algorithmes (utilisation des connaissances sur le groupe de Galois) pourraient être utilisées conjointement au nouvel algorithme de factorisation dans les extensions (voir [17]) afin d'en étudier la

complexité et l'efficacité dans le cadre du calcul de l'idéal des relations.

On peut aussi se demander si l'utilisation des nouveaux ensembles proposés dans [32] pour représenter des idéaux triangulaires, améliorerait l'efficacité de nos algorithmes. Par exemple, il est fort possible que leur utilisation permette de réduire le nombre d'étapes de remontées henseliennes dans nos algorithmes modulaires.

Dans le cadre de l'implantation aussi il reste encore beaucoup à faire. Adapter nos implantations dans le cadre plus général des corps globaux, améliorer les calculs de formes normales ou encore développer une partie de notre travail dans un langage de plus bas niveau (en `C` par exemple) afin de mieux maîtriser les arithmétiques utilisées.

Annexe A

Implantations pour le calcul du groupe de décomposition

Dans cette annexe, nous présentons les implantations en MAGMA (version 2.10) permettant le calcul du groupe de décomposition d'un idéal triangulaire (voir Chapitre 3). Ces implantations ont été réalisées en collaboration avec S. Orange.

Cette première fonction prend en entrée une permutation σ et l'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action d'un sous-groupe G de S_n. Elle renvoie l'ensemble des orbites de $\{1,\ldots,n\}$ sous l'action de $\langle G,\sigma\rangle$. Elle correspond à l'implantation de l'algorithme 7.

```
/*************************************************************************/
function NouvellesOrbites (orbites,sigma);

nvorbites := {};
while not(IsEmpty(orbites)) do
    e := Random(orbites) ;
    p := e join Image(sigma,e) ;
    orbites := Exclude(orbites,e) ;
    while not(p eq e) do
        for oprime in orbites do
            if not(#(p meet oprime) eq 0) then
                e := e join oprime;
                orbites := Exclude(orbites,oprime) ;
            end if;
        end for;
        p := e join Image(sigma,e) ;
    end while ;
    nvorbites := Include(nvorbites,e) ;
end while;
return nvorbites;

end function;
/*************************************************************************/
```

Étant donné un ensemble triangulaire S de $\mathbb{Q}[x_1,\ldots,x_n]$ et un préfixe l, la fonction suivante calcule une permutation de $\mathrm{Dec}(S)$ de préfixe l si elle existe et l'identité sinon. Elle correspond à l'implantation de l'algorithme 5.

```
/*************************************************************************/
/**
```

```
  @param l une séquence d'entiers représentant le préfixe.
  @param S une séquence de polynômes représentant la base
     triangulaire d'un idéal.
  @param SP la séquence S modulo un premier compatible (pour le
     pré-test modulaire).
  @return s'il existe une permutation de préfixe l dans Dec(<S>) une
     d'entre elle est renvoyée sinon, c'est Id(S_n) qui est
     renvoyé.
*/
/*************************************************************************/
function UnePermutation(l,S,SP)
local r,Sn,n,boucle1,boucle2,a,ens,s,ll;
n := #S;
Sn := Sym(n);
r := n - #l;

boucle1 := true;
while (r gt 0) and boucle1 do
    ens:=Reverse(Sort(SetToSequence({1..n} diff Set(l))));
    boucle2 := true;

    while (r gt 0) and boucle2 do
          if #ens eq 0 then //BACKTRACK
                boucle1:=false;
                boucle2:=false;
          else
          a := ens[1];
          ens := ens[2 .. #ens];
          ll := [a] cat l;
          s:= Sn!(SetToSequence({1..n} diff Set(ll)) cat ll);
          if NormalForm((SP[r])^s ,SP) eq 0 then
                if NormalForm((S[r])^s,S) eq 0 then
                   r:=r-1;
                   boucle2 := false;
                   l := ll;
                end if;
          end if;
          end if;
    end while;
end while;

if r eq 0 then
   return s;
else //BACKTRACK
   return Id(Sn);
end if;

end function;
/*************************************************************************/
```

Les fonctions suivantes permettent le calcul du groupe de décomposition d'un idéal triangulaire. La seconde fonction prend en entrée un ensemble triangulaire `S` et un booléen `GalId`. Si ce dernier paramètre est initialisé à `true`, cette fonction calcule le prédicat "<S> est-il un idéal de Galois pur ?" et dans ce cas, l'ensemble triangulaire `S` est

supposé séparable. Le résultat du prédicat est donné en deuxième sortie et si ce prédicat est vraie, le groupe de décomposition est donné en première sortie. Dans le cas où `GalId` est initialisé à `false`, le groupe de décomposition est toujours calculé, l'ensemble `S` n'est pas supposé séparable et la deuxième sortie n'a pas de sens. La première fonction correspond à l'implantation de l'algorithme 8 et la seconde à l'algorithme 9 (voir aussi l'algorithme 10).

```
/*****************************************************************************/
/**
  Cette procedure détermine un système de générateurs G du fixateur de {k-1..n}
  du groupe de decomposition de l'ideal <S> en fonction d'un système
  de générateurs du fixateur de {k-1..n} de ce groupe. Un pré-test
  modulaire d'appartenance à l'idéal est utilisé pour améliorer l'efficacité.
  @param k un entier
  @param G paramètre d'e/s est une séquence de générateurs des
  fixateurs successifs.
  @param S base triangulaire.
  @param SP base triangulaire modulo p.
  @param n la longueur de S.
  @param sn le groupe symétrique.
  @param orbites paramètre d'e/s est l'ensemble des orbites de
  {1,...,n} selon l'action de <G>
  @param IsGalId paramètre d'e/s un booléen qui permet de savoir si
  l'on est de la cas de EstGaloisPur?.
  @return G l'ensemble des générateurs du fixateur calculé.
  @warn lorsque IsGalId est à TRUE la procédure s'arrête au moindre
  backtrack en renvoyant FALSE par l'intermédiaire de ce paramètre.
*/
/*****************************************************************************/
procedure deGkaGkm(k,~G,~S,~SP,~n,~sn,~orbites,~IsGalId)

elt:={1..(k-1)} meet {Max(o): o in orbites};
while (not(IsEmpty(elt))) do
    ak := Max(elt);
    elt := elt diff {ak};
    ll:= SetToSequence({1..k} diff {ak}) cat [ak] cat [(k+1)..n] ;
    if NormalForm((SP[k])^(sn! ll) ,SP) eq 0 then
        if NormalForm((S[k])^(sn! ll) ,S) eq 0 then

            sigma2:= UnePermutation([ak] cat [(k+1)..n],S,SP);

            if not (sigma2 eq Id(sn)) then
                G:=G cat [sigma2];
                orbites:=NouvellesOrbites(orbites,sigma2);
                elt:=elt meet {Max(o): o in orbites};
            else
                //Dans le cas de IsGaloisIdeal il faut sortir
                if IsGalId then
                    IsGalId := false;
                    print "BACKTRACK";
                    break;
                end if;
            end if;
        end if;
```

```
    end if;
end while;
end procedure;



/*************************************************************************/
/**
  @param S une base triangulaire donnée sous la forme d'une séquence.
     HYPOTHESE : Dans le cas où GalId est initialisé à true, S est séparable.
  @param GalId un booléen.
  @return le groupe de décomposition de <S>
  @return un booléen.
*/
/*************************************************************************/
function GroupeDeDecomposition(S,GalId)

S:=Reverse(Sort(S))
n:=Rank(Parent (S[1]));
sn:=Sym(n);
G:=[];
orbites := {{i}: i in {1..n}} ;

// On cherche un premier p compatible pour le test modulaire.

p:=2;
rep:=false;
while rep eq false do
    polmod:=PolynomialRing(FiniteField(p),n);
    k:=1;
    rep:=true;
    while (rep eq true) and (k le n) do
        rep:=IsCoercible(polmod,S[k]);
        k:=k+1;
    end while;
    if rep eq false then p:=NextPrime(p); end if;
end while;

polmod:=PolynomialRing(FiniteField(p),n);
SP := [(polmod ! S[i]) : i in [1..n]];

// Calcul du groupe de décomposition.

if GalId then
for k:= 2 to n do
    deGkaGkm(k,~G,~S,~SP,~n,~sn,~orbites,~GalId);
    if not(GalId) then
       break;
    end if;
end for;
else
for k:= 2 to n do
    deGkaGkm(k,~G,~S,~SP,~n,~sn,~orbites,~GalId);
```

```
end for;
end if;

// Calcul de Card(V(<S>))
// Dans le cas S est séparable, nous avons

card := &*[LeadingTotalDegree(f) : f in S];

// Fin

G:=PermutationGroup<n|G>
return G, (card eq #G) and GalId;
end function ;
/*****************************************************************************/
```

Annexe B

Base de données et implantations pour l'algorithme de Yokoyama revisité

Dans cette annexe, nous donnons les bases de données utilisées dans l'algorithme de Yokoyama revisité (voir Chapitre 7) et une implantation en MAGMA (version 2.10) de l'algorithme 13 dans le cas où l'entier premier choisi se décompose complètement.

B.1 Base de données

Nous avons calculé les bases de données pour les groupes transitifs de degré inférieur ou égal à 9. Ci-après, sont recensées celles pour les degrés 5 à 9. Ces informations ont été obtenues à l'aide du logiciel MAGMA (mais pourraient tout aussi bien être calculées avec `GAP` (voir [45])). Pour chaque groupe transitif de degré inférieur ou égal à 9, nous donnons un représentant symétrique et le schéma de calcul correspondant. Ce représentant G est donné comme conjugué du groupe de permutations obtenu à partir de la fonction `TransitiveGroup` de MAGMA. Pour un groupe G de degré d, le schéma de calcul correspondant est donné sous la forme d'un tableau de d lignes. Chaque ligne correspond à un polynôme d'une base triangulaire d'un idéal des relations d'un polynôme f de groupe de Galois G. Le polynôme de la ligne d correspond à $f(x_d)$ et celui de la ligne 1 au module de Cauchy de f linéaire en les variables $x_1, \ldots, x_d$. Pour chacune de ces lignes, le schéma indique comment calculer le polynôme de la base triangulaire correspondant. Trois types de calcul sont possibles :

$$C(i, L)$$

dans ce cas, le polynômes cherché est le module de Cauchy généralisé du polynômes f_i et ses variables sont numérotées par la liste L.

$$T(i, P)$$

ici, le polynôme cherché est obtenu en faisant agir sur le polynôme f_i la permutation donnée sous la forme du tableau P.

$$S(L, D)$$

dans ce dernier cas, on doit construire et résoudre un système linéaire à partir des approximation p-adiques des racines de f. Le système à construire dépend des variables numérotées par L et sont de degré borné par l'entier correspondant dans D.

Pour chaque représentant G, nous précisons sa taille $c(G)$. Il est à noter qu'il n'est pas prouvé que ces représentants soient c-minimaux (même s'il est fort probable qu'il en soit ainsi). Ils ont été trouvés en faisant une recherche exhaustive sur l'ensemble des conjugués des groupes transitifs et en utilisant des heuristiques pour limiter le calcul.

B.1.1 Degré 5

G =Conj($5T_1$, $[1,2,3,4,5]$)
$c(G) = 10$

1	$C(5,[5,4,3,2,1])$
2	$T(4,[4,5,1,2,3])$
3	$T(4,[5,1,2,3,4])$
4	$S([5,4],[5,1])$
5	$S([5],[5])$

G =Conj($5T_3$, $[1,2,3,4,5]$)
$c(G) = 25$

1	$C(5,[5,4,3,2,1])$
2	$T(3,[5,1,2,3,4])$
3	$S([5,4,3],[5,4,1])$
4	$C(5,[5,4])$
5	$S([5],[5])$

G =Conj($5T_4$, $[1,2,3,4,5]$)
$c(G) = 65$

1	$C(5,[5,4,3,2,1])$
2	$S([5,4,3,2],[5,4,3,1])$
3	$C(5,[5,4,3])$
4	$C(5,[5,4])$
5	$S([5],[5])$

G =Conj($5T_2$, $[1,2,3,4,5]$)
$c(G) = 25$

1	$C(5,[5,4,3,2,1])$
2	$T(3,[5,1,2,3,4])$
3	$S([5,4,3],[5,2,1])$
4	$S([5,4],[5,2])$
5	$S([5],[5])$

G =Conj($5T_5$, $[1,2,3,4,5]$)
$c(G) = 5$

1	$C(5,[5,4,3,2,1])$
2	$C(5,[5,4,3,2])$
3	$C(5,[5,4,3])$
4	$C(5,[5,4])$
5	$S([5],[5])$

B.1.2 Degré 6

G =Conj($6T_1$, $[1,2,3,4,5,6]$)
$c(G) = 12$

1	$C(6,[6,5,4,3,2,1])$
2	$T(5,[4,5,6,1,2,3])$
3	$T(5,[5,6,1,2,3,4])$
4	$T(5,[6,1,2,3,4,5])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_3$, $[1,5,3,4,2,6]$)
$c(G) = 24$

1	$C(6,[6,5,4,3,2,1])$
2	$T(3,[1,3,2,4,6,5])$
3	$S([6,3],[6,1])$
4	$C(5,[6,5,4])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_2$, $[1,2,3,4,5,6]$)
$c(G) = 18$

1	$C(6,[6,5,4,3,2,1])$
2	$T(4,[5,6,1,2,3,4])$
3	$T(5,[5,6,1,2,3,4])$
4	$S([6,4],[6,1])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_4$, $[1,6,3,4,2,5]$)
$c(G) = 30$

1	$C(6,[6,5,4,3,2,1])$
2	$T(4,[6,5,1,2,4,3])$
3	$C(5,[6,5,3])$
4	$S([6,5,4],[6,2,1])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_5$, $[1,4,3,6,2,5]$)
$c(G) = 12$

1	$C(6,[6,5,4,3,2,1])$
2	$T(5,[6,4,5,1,2,3])$
3	$C(6,[6,5,4,3])$
4	$T(5,[3,1,2,6,4,5])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_6$, $[1,3,2,6,4,5]$)
$c(G) = 18$

1	$C(6,[6,5,4,3,2,1])$
2	$C(5,[6,5,2])$
3	$C(4,[6,4,3])$
4	$T(5,[2,3,6,1,4,5])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_7$, $[1,2,6,3,4,5]$)
$c(G) = 36$

1	$C(6,[6,5,4,3,2,1])$
2	$T(5,[6,3,5,1,2,4])$
3	$S([6,4,3],[6,4,1])$
4	$C(6,[6,5,4])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_8$, $[1,2,5,3,4,6]$)
$c(G) = 36$

1	$C(6,[6,5,4,3,2,1])$
2	$T(5,[6,3,5,1,2,4])$
3	$S([6,4,3],[6,4,1])$
4	$C(6,[6,5,4])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_9$, $[1,4,3,5,2,6]$)
$c(G) = 54$

1	$C(6,[6,5,4,3,2,1])$
2	$S([6,5,3,2],[6,2,3,1])$
3	$C(6,[6,5,4,3])$
4	$C(5,[6,5,4])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_{10}$, $[1,4,3,5,2,6]$)
$c(G) = 54$

1	$C(6,[6,5,4,3,2,1])$
2	$S([6,5,3,2],[6,2,3,1])$
3	$C(6,[6,5,4,3])$
4	$C(5,[6,5,4])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_{11}$, $[1,3,5,2,4,6]$)
$c(G) = 12$

1	$C(6,[6,5,4,3,2,1])$
2	$C(6,[6,5,4,3,2])$
3	$T(5,[2,1,6,5,3,4])$
4	$C(6,[6,5,4])$
5	$S([6,5],[6,1])$
6	$S([6],[6])$

G =Conj($6T_{12}$, $[1,2,3,4,5,6]$)
$c(G) = 126$

1	$C(6,[6,5,4,3,2,1])$
2	$T(3,[1,6,2,5,3,4])$
3	$S([6,5,4,3],[6,5,2,1])$
4	$S([6,5,4],[6,5,2])$
5	$C(6,[6,5])$
6	$S([6],[6])$

G =Conj($6T_{13}$, $[1,4,3,5,2,6]$)
$c(G) = 18$

1	$C(6,[6,5,4,3,2,1])$
2	$C(6,[6,5,4,3,2])$
3	$C(6,[6,5,4,3])$
4	$C(5,[6,5,4])$
5	$S([6,5],[6,2])$
6	$S([6],[6])$

G =Conj($6T_{14}$, $[1,2,3,4,5,6]$)
$c(G) = 126$

1	$C(6,[6,5,4,3,2,1])$
2	$T(3,[1,6,2,5,3,4])$
3	$S([6,5,4,3],[6,5,4,1])$
4	$C(6,[6,5,4])$
5	$C(6,[6,5])$
6	$S([6],[6])$

G =Conj($6T_{15}$, $[1,2,3,4,5,6]$)
$c(G) = 366$

1	$C(6,[6,5,4,3,2,1])$
2	$S([6,5,4,3,2],[6,5,4,3,1])$
3	$C(6,[6,5,4,3])$
4	$C(6,[6,5,4])$
5	$C(6,[6,5])$
6	$S([6],[6])$

G =Conj($6T_{16}$, $[1,2,3,4,5,6]$)
$c(G) = 6$

1	$C(6,[6,5,4,3,2,1])$
2	$C(6,[6,5,4,3,2])$
3	$C(6,[6,5,4,3])$
4	$C(6,[6,5,4])$
5	$C(6,[6,5])$
6	$S([6],[6])$

B.1.3 Degré 7

G =Conj($7T_1$, $[1,2,3,4,5,6,7]$)
$c(G) = 14$

1	$C(7,[7,6,5,4,3,2,1])$
2	$T(6,[4,5,6,7,1,2,3])$
3	$T(6,[5,6,7,1,2,3,4])$
4	$T(6,[6,7,1,2,3,4,5])$
5	$T(6,[7,1,2,3,4,5,6])$
6	$S([7,6],[7,1])$
7	$S([7],[7])$

G =Conj($7T_2$, $[1,2,3,4,5,6,7]$)
$c(G) = 35$

1	$C(7,[7,6,5,4,3,2,1])$
2	$T(5,[5,6,7,1,2,3,4])$
3	$T(5,[6,7,1,2,3,4,5])$
4	$T(5,[7,1,2,3,4,5,6])$
5	$S([7,6,5],[7,2,1])$
6	$S([7,6],[7,2])$
7	$S([7],[7])$

G =Conj($7T_3$, $[1,2,3,4,5,6,7]$)
$c(G) = 49$

1	$C(7,[7,6,5,4,3,2,1])$
2	$T(5,[5,6,7,1,2,3,4])$
3	$C(6,[7,6,5,3])$
4	$T(5,[7,1,2,3,4,5,6])$
5	$S([7,6,5],[7,3,1])$
6	$S([7,6],[7,3])$
7	$S([7],[7])$

G =Conj($7T_4$, $[1,2,3,4,5,6,7]$)
$c(G) = 49$

1	$C(7,[7,6,5,4,3,2,1])$
2	$T(5,[3,1,6,4,2,7,5])$
3	$T(5,[2,4,6,1,3,5,7])$
4	$T(5,[7,1,2,3,4,5,6])$
5	$S([7,6,5],[7,6,1])$
6	$C(7,[7,6])$
7	$S([7],[7])$

G =Conj($7T_5$, $[1,2,3,6,5,4,7]$)
$c(G) = 49$

1	$C(7,[7,6,5,4,3,2,1])$
2	$T(5,[1,3,5,6,2,7,4])$
3	$T(5,[1,2,5,7,3,6,4])$
4	$C(7,[7,6,5,4])$
5	$S([7,6,5],[7,6,1])$
6	$C(7,[7,6])$
7	$S([7],[7])$

G =Conj($7T_6$, $[1,2,3,4,5,6,7]$)
$c(G) = 2527$

1	$C(7,[7,6,5,4,3,2,1])$
2	$S([7,6,5,4,3,2],[7,6,5,4,3,1])$
3	$C(7,[7,6,5,4,3])$
4	$C(7,[7,6,5,4])$
5	$C(7,[7,6,5])$
6	$C(7,[7,6])$
7	$S([7],[7])$

G =Conj($7T_7$, $[1,2,3,4,5,6,7]$)
$c(G) = 7$

1	$C(7,[7,6,5,4,3,2,1])$
2	$C(7,[7,6,5,4,3,2])$
3	$C(7,[7,6,5,4,3])$
4	$C(7,[7,6,5,4])$
5	$C(7,[7,6,5])$
6	$C(7,[7,6])$
7	$S([7],[7])$

B.1.4 Degré 8

G =Conj($8T_1$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 16$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[4,5,6,7,8,1,2,3])$
3	$T(7,[5,6,7,8,1,2,3,4])$
4	$T(7,[6,7,8,1,2,3,4,5])$
5	$T(7,[7,8,1,2,3,4,5,6])$
6	$T(7,[8,1,2,3,4,5,6,7])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_2$, $[1,3,5,8,2,4,7,6]$)
$c(G) = 24$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[5,7,6,8,1,3,2,4])$
3	$T(7,[8,6,2,1,4,7,3,5])$
4	$T(7,[6,8,1,2,3,5,4,7])$
5	$T(7,[2,1,4,3,7,8,5,6])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_3$, $[1,7,3,5,2,4,6,8]$)
$c(G) = 32$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[4,7,5,1,3,8,2,6])$
3	$T(6,[2,1,6,7,8,3,4,5])$
4	$T(7,[2,1,6,7,8,3,4,5])$
5	$S([8,5],[8,1])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_4$, $[1,2,4,7,8,3,5,6]$)
$c(G) = 24$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[4,6,7,1,8,2,3,5])$
3	$T(7,[4,6,7,1,8,2,3,5])$
4	$T(6,[6,1,8,2,3,4,5,7])$
5	$T(7,[6,1,8,2,3,4,5,7])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_5$, $[1,2,4,8,7,6,5,3]$)
$c(G) = 24$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[8,5,7,6,3,1,2,4])$
3	$T(4,[2,4,1,3,8,5,6,7])$
4	$S([8,4],[8,1])$
5	$T(7,[4,3,2,1,7,8,5,6])$
6	$T(7,[2,4,1,3,8,5,6,7])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_6$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[5,6,7,8,1,2,3,4])$
3	$T(6,[6,7,8,1,2,3,4,5])$
4	$T(6,[7,8,1,2,3,4,5,6])$
5	$T(6,[8,1,2,3,4,5,6,7])$
6	$S([8,7,6],[8,2,1])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_7$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 32$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[1,6,3,8,5,2,7,4])$
3	$C(7,[8,7,3])$
4	$T(6,[3,8,5,2,7,4,1,6])$
5	$T(6,[8,1,2,3,4,5,6,7])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_8$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[3,6,1,4,7,2,5,8])$
3	$T(6,[6,7,8,1,2,3,4,5])$
4	$T(6,[7,8,1,2,3,4,5,6])$
5	$C(7,[8,7,5])$
6	$S([8,7,6],[8,2,1])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_9$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[7,4,5,3,2,1,8,6])$
3	$S([8,3],[8,1])$
4	$T(5,[1,2,3,5,4,7,6,8])$
5	$S([7,5],[8,1])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{10}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[1,6,3,8,5,2,7,4])$
3	$C(7,[8,7,3])$
4	$T(5,[8,5,2,3,4,1,6,7])$
5	$S([7,5],[8,1])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{11}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 32$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[1,6,3,8,5,2,7,4])$
3	$C(7,[8,7,3])$
4	$T(6,[3,8,5,2,7,4,1,6])$
5	$T(6,[6,1,8,3,2,5,4,7])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{12}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[7,6,4,1,3,2,8,5])$
3	$T(6,[2,7,1,8,6,3,5,4])$
4	$T(6,[7,8,1,2,3,4,5,6])$
5	$T(6,[4,1,3,2,8,5,7,6])$
6	$S([8,7,6],[8,3,1])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{13}$, $[1,7,6,4,3,5,8,2]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[6,1,3,8,4,2,7,5])$
3	$T(6,[5,4,2,7,1,3,8,6])$
4	$T(6,[8,3,1,6,2,4,5,7])$
5	$T(6,[4,3,2,1,6,5,8,7])$
6	$S([8,7,6],[8,3,1])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{14}$, $[1,4,2,3,8,5,6,7]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(7,[8,7,4,2])$
3	$T(6,[1,7,5,2,6,3,4,8])$
4	$T(6,[3,5,2,8,1,4,6,7])$
5	$T(6,[2,4,3,1,8,5,7,6])$
6	$S([8,7,6],[8,3,1])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{15}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 72$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[1,6,3,8,5,2,7,4])$
3	$T(6,[2,7,4,1,6,3,8,5])$
4	$T(6,[7,8,1,2,3,4,5,6])$
5	$T(6,[8,1,2,3,4,5,6,7])$
6	$S([8,7,6],[8,4,1])$
7	$S([8,7],[8,4])$
8	$S([8],[8])$

G =Conj($8T_{16}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(6,[8,6,2])$
3	$C(7,[8,7,3])$
4	$T(5,[8,1,2,3,4,5,6,7])$
5	$S([8,7,6,5],[8,2,2,1])$
6	$T(7,[8,1,2,3,4,5,6,7])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{17}$, $[1,4,3,5,8,7,6,2]$)
$c(G) = 16$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[8,5,6,7,4,1,2,3])$
3	$T(7,[6,7,8,5,1,2,3,4])$
4	$C(8,[8,7,6,5,4])$
5	$T(7,[2,3,4,1,7,8,5,6])$
6	$T(7,[2,3,4,1,8,5,6,7])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{18}$, $[1,4,3,5,6,8,7,2]$)
$c(G) = 24$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[5,6,8,7,1,2,4,3])$
3	$T(7,[7,8,6,5,2,1,3,4])$
4	$C(8,[8,7,6,5,4])$
5	$T(7,[4,3,2,1,7,8,5,6])$
6	$S([8,6],[8,1])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{19}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 72$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[7,4,5,8,1,2,3,6])$
3	$T(6,[7,6,5,1,2,3,8,4])$
4	$C(7,[8,7,6,5,4])$
5	$T(6,[3,2,1,7,4,5,6,8])$
6	$S([8,7,6],[8,4,1])$
7	$S([8,7],[8,4])$
8	$S([8],[8])$

G =Conj($8T_{20}$, $[1,3,4,2,5,6,7,8]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[8,7,1,3,2,5,6,4])$
3	$C(6,[8,6,3])$
4	$C(7,[8,7,4])$
5	$S([8,7,6,5],[8,2,2,1])$
6	$T(7,[8,4,5,3,2,1,6,7])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{21}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 72$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(6,[8,6,2])$
3	$C(7,[8,7,3])$
4	$T(5,[8,3,2,1,4,7,6,5])$
5	$S([8,7,6,5],[8,2,2,1])$
6	$S([8,6],[8,2])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{22}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 72$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(3,[1,3,2,4,5,7,6,8])$
3	$S([8,7,5,3],[8,2,2,1])$
4	$C(5,[8,5,4])$
5	$S([8,5],[8,2])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{23}$, $[1,2,5,7,4,6,3,8]$)
$c(G) = 64$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[1,7,5,4,3,8,2,6])$
3	$T(7,[6,1,8,2,7,4,3,5])$
4	$T(5,[3,2,1,5,4,6,8,7])$
5	$S([8,6,5],[8,6,1])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{24}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[7,6,4,3,1,8,2,5])$
3	$T(7,[7,6,5,2,1,8,3,4])$
4	$C(6,[8,6,5,4])$
5	$C(6,[8,6,5])$
6	$S([8,6],[8,3])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{25}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 64$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[7,1,6,3,4,2,5,8])$
3	$T(6,[1,4,2,8,6,3,5,7])$
4	$T(6,[5,1,3,2,8,4,6,7])$
5	$T(6,[4,8,2,3,1,5,7,6])$
6	$S([8,7,6],[8,7,1])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{26}$, $[1,5,3,7,4,6,2,8]$)
$c(G) = 96$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[8,6,5,7,4,1,2,3])$
3	$S([8,6,4,3],[8,2,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$C(6,[8,6,5])$
6	$S([8,6],[8,2])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{27}$, $[1,3,5,2,8,4,6,7]$)
$c(G) = 24$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(7,[8,7,2])$
3	$C(4,[8,4,3])$
4	$T(7,[5,3,7,2,1,8,4,6])$
5	$C(6,[8,6,5])$
6	$T(7,[2,5,8,1,3,4,6,7])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{28}$, $[1,5,3,8,4,6,2,7]$)
$c(G) = 96$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[8,6,5,7,4,1,2,3])$
3	$S([8,6,4,3],[8,2,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$C(6,[8,6,5])$
6	$S([8,6],[8,2])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{29}$, $[1,2,3,5,7,8,6,4]$)
$c(G) = 96$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[8,6,5,7,2,3,1,4])$
3	$S([8,7,4,3],[8,2,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$S([8,5],[8,1])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{30}$, $[1,5,3,8,4,6,2,7]$)
$c(G) = 96$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[5,7,8,6,4,1,2,3])$
3	$S([8,6,4,3],[8,2,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$C(6,[8,6,5])$
6	$S([8,6],[8,2])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{31}$, $[1,6,3,2,8,7,4,5]$)
$c(G) = 40$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(5,[8,5,2])$
3	$C(4,[8,4,3])$
4	$T(7,[2,8,7,6,1,3,4,5])$
5	$S([8,5],[8,2])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,2])$
8	$S([8],[8])$

G =Conj($8T_{32}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 208$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(5,[8,6,5,2])$
3	$T(7,[8,2,6,1,5,7,3,4])$
4	$S([8,6,5,4],[8,6,2,1])$
5	$S([8,6,5],[8,6,2])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{33}$, $[1,4,6,2,5,3,8,7]$)
$c(G) = 136$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[1,5,8,4,2,6,7,3])$
3	$T(5,[7,2,8,1,3,6,4,5])$
4	$T(5,[3,1,7,2,4,8,5,6])$
5	$S([8,7,6,5],[8,4,3,1])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,4])$
8	$S([8],[8])$

G =Conj($8T_{34}$, $[1,2,4,5,6,7,8,3]$)
$c(G) = 152$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[5,6,8,7,1,2,4,3])$
3	$S([8,7,4,3],[8,3,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$S([8,7,6],[8,3,1])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{35}$, $[1,5,3,7,4,6,2,8]$)
$c(G) = 32$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(3,[4,3,2])$
3	$T(6,[5,7,8,6,2,3,1,4])$
4	$C(8,[8,7,6,5,4])$
5	$C(6,[8,6,5])$
6	$S([8,6],[8,2])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{36}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 344$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[8,1,5,6,2,3,7,4])$
3	$T(5,[2,1,4,6,3,8,5,7])$
4	$C(6,[8,7,6,5,4])$
5	$S([8,7,6,5],[8,7,3,1])$
6	$S([8,7,6],[8,7,3])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{37}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 344$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[7,6,1,4,2,5,3,8])$
3	$C(6,[8,7,6,5,3])$
4	$T(5,[1,3,7,2,4,8,6,5])$
5	$S([8,7,6,5],[8,7,3,1])$
6	$S([8,7,6],[8,7,3])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{38}$, $[1,2,7,4,5,3,8,6]$)
$c(G) = 112$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(3,[8,6,3,2])$
3	$T(5,[2,4,6,1,3,5,7,8])$
4	$T(7,[5,7,8,3,1,2,4,6])$
5	$S([8,6,5],[8,6,2])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{39}$, $[1,2,5,6,3,4,7,8]$)
$c(G) = 208$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(7,[8,1,4,7,6,5,2,3])$
3	$S([8,6,4,3],[8,6,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$T(7,[2,7,8,3,1,4,5,6])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{40}$, $[1,3,5,8,2,4,6,7]$)
$c(G) = 208$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$S([8,6,4,2],[8,6,4,1])$
3	$T(7,[1,2,6,5,8,7,3,4])$
4	$C(8,[8,7,6,5,4])$
5	$T(7,[8,7,2,1,4,3,5,6])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{41}$, $[1,2,3,5,7,8,6,4]$)
$c(G) = 128$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(3,[4,1,2,3,5,7,6,8])$
3	$S([8,7,4,3],[8,3,4,1])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{42}$, $[1,2,4,5,6,7,8,3]$)
$c(G) = 56$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(6,[8,5,7,6,1,2,3,4])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$S([8,7,6],[8,3,1])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{43}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 344$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[1,3,5,8,2,4,7,6])$
3	$T(5,[1,5,2,6,3,8,7,4])$
4	$T(5,[2,3,8,1,4,7,5,6])$
5	$S([8,7,6,5],[8,7,6,1])$
6	$C(8,[8,7,6])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{44}$, $[1,3,5,7,2,4,6,8]$)
$c(G) = 16$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(8,[8,7,6,5,4,3,2])$
3	$T(7,[5,6,8,7,1,2,3,4])$
4	$C(8,[8,7,6,5,4])$
5	$T(7,[3,4,2,1,8,7,5,6])$
6	$C(8,[8,7,6])$
7	$S([8,7],[8,1])$
8	$S([8],[8])$

G =Conj($8T_{45}$, $[1,2,3,5,6,7,8,4]$)
$c(G) = 608$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$S([8,7,6,4,3,2],[8,3,2,4,3,1])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{46}$, $[1,2,3,5,6,7,8,4]$)
$c(G) = 608$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$S([8,7,6,4,3,2],[8,3,2,4,3,1])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{47}$, $[1,2,3,5,6,7,8,4]$)
$c(G) = 32$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(8,[8,7,6,5,4,3,2])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(7,[8,7,6,5])$
6	$C(7,[8,7,6])$
7	$S([8,7],[8,3])$
8	$S([8],[8])$

G =Conj($8T_{48}$, $[1,2,3,5,6,7,8,4]$)
$c(G) = 344$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$T(5,[5,7,1,3,2,6,8,4])$
3	$T(5,[1,2,7,6,3,8,5,4])$
4	$C(8,[8,7,6,5,4])$
5	$S([8,7,6,5],[8,7,6,1])$
6	$C(8,[8,7,6])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{49}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 20168$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$S([8,7,6,5,4,3,2],[8,7,6,5,4,3,1])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(8,[8,7,6,5])$
6	$C(8,[8,7,6])$
7	$C(8,[8,7])$
8	$S([8],[8])$

G =Conj($8T_{50}$, $[1,2,3,4,5,6,7,8]$)
$c(G) = 8$

1	$C(8,[8,7,6,5,4,3,2,1])$
2	$C(8,[8,7,6,5,4,3,2])$
3	$C(8,[8,7,6,5,4,3])$
4	$C(8,[8,7,6,5,4])$
5	$C(8,[8,7,6,5])$
6	$C(8,[8,7,6])$
7	$C(8,[8,7])$
8	$S([8],[8])$

B.1.5 Degré 9

G =Conj($9T_{1}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 18$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(8,[4,5,6,7,8,9,1,2,3])$
3	$T(8,[5,6,7,8,9,1,2,3,4])$
4	$T(8,[6,7,8,9,1,2,3,4,5])$
5	$T(8,[7,8,9,1,2,3,4,5,6])$
6	$T(8,[8,9,1,2,3,4,5,6,7])$
7	$T(8,[9,1,2,3,4,5,6,7,8])$
8	$S([9,8],[9,1])$
9	$S([9],[9])$

G =Conj($9T_{2}$, $[1,2,8,4,5,9,7,6,3]$)
$c(G) = 27$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(8,[9,7,6,3,1,4,8,2,5])$
3	$T(8,[7,6,9,1,2,5,4,3,8])$
4	$T(8,[2,3,1,5,8,9,6,4,7])$
5	$T(8,[3,1,2,8,4,7,9,5,6])$
6	$T(7,[2,3,1,5,8,9,6,4,7])$
7	$S([9,7],[9,1])$
8	$S([9,8],[9,1])$
9	$S([9],[9])$

G =Conj($9T_3$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 45$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[5,6,7,8,9,1,2,3,4])$
3	$T(7,[6,7,8,9,1,2,3,4,5])$
4	$T(7,[7,8,9,1,2,3,4,5,6])$
5	$T(7,[8,9,1,2,3,4,5,6,7])$
6	$T(7,[9,1,2,3,4,5,6,7,8])$
7	$S([9,8,7],[9,2,1])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_4$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 36$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(6,[3,4,8,6,7,2,9,1,5])$
3	$T(6,[8,7,9,2,1,3,5,4,6])$
4	$T(6,[6,8,1,9,2,4,3,5,7])$
5	$T(6,[6,7,2,9,1,5,3,4,8])$
6	$S([9,6],[9,1])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_5$, $[1,2,9,7,5,6,3,4,8]$)
$c(G) = 45$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[5,7,4,3,1,6,2,9,8])$
3	$T(7,[7,5,1,2,4,8,3,9,6])$
4	$T(7,[2,1,5,7,3,9,4,8,6])$
5	$T(7,[4,3,2,1,7,8,5,6,9])$
6	$C(8,[9,8,6])$
7	$S([9,8,7],[9,2,1])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_6$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 63$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(8,[9,8,5,2])$
3	$T(7,[6,7,8,9,1,2,3,4,5])$
4	$T(7,[7,8,9,1,2,3,4,5,6])$
5	$T(7,[8,9,1,2,3,4,5,6,7])$
6	$T(7,[9,1,2,3,4,5,6,7,8])$
7	$S([9,8,7],[9,3,1])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_7$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 72$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[3,4,6,7,8,1,2,9,5])$
3	$T(7,[7,8,1,2,9,5,3,4,6])$
4	$T(7,[7,8,9,1,2,3,4,5,6])$
5	$S([9,8,5],[9,3,1])$
6	$C(8,[9,8,7,6])$
7	$S([8,7],[9,1])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_8$, $[1,4,2,3,9,5,7,8,6]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(6,[9,5,8,3,6,2,4,1,7])$
3	$T(6,[2,1,6,9,7,3,5,8,4])$
4	$C(8,[9,8,4])$
5	$C(7,[8,7,5])$
6	$S([9,7,6],[9,4,1])$
7	$S([8,7],[9,2])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_9$, $[1,6,3,5,2,7,4,9,8]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[1,7,9,5,4,8,2,6,3])$
3	$T(7,[5,2,1,6,7,8,3,9,4])$
4	$C(8,[9,8,7,5,4])$
5	$T(7,[2,3,6,8,4,1,5,7,9])$
6	$T(7,[4,3,2,1,5,7,6,9,8])$
7	$S([9,8,7],[9,4,1])$
8	$S([9,8],[9,4])$
9	$S([9],[9])$

G =Conj($9T_{10}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 117$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[8,1,3,5,7,9,2,4,6])$
3	$T(7,[9,5,1,6,2,7,3,8,4])$
4	$T(7,[1,6,2,7,3,8,4,9,5])$
5	$T(7,[8,9,1,2,3,4,5,6,7])$
6	$T(7,[9,1,2,3,4,5,6,7,8])$
7	$S([9,8,7],[9,6,1])$
8	$S([9,8],[9,6])$
9	$S([9],[9])$

G =Conj($9T_{11}$, $[1,6,3,2,8,9,4,5,7]$)
$c(G) = 117$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[8,9,5,1,6,3,2,4,7])$
3	$T(7,[2,4,9,1,6,8,3,5,7])$
4	$T(7,[5,1,7,3,2,9,4,6,8])$
5	$T(7,[4,3,2,6,1,9,5,8,7])$
6	$T(7,[1,4,5,2,3,7,6,9,8])$
7	$S([9,8,7],[9,6,1])$
8	$S([9,8],[9,6])$
9	$S([9],[9])$

G =Conj($9T_{12}$, $[1,6,2,5,4,7,9,8,3]$)
$c(G) = 72$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(8,[9,6,7,1,3,8,5,2,4])$
3	$T(8,[5,8,2,9,7,4,1,3,6])$
4	$T(8,[7,1,8,3,6,9,2,4,5])$
5	$S([9,6,5],[9,6,1])$
6	$C(9,[9,8,7,6])$
7	$T(8,[3,2,6,4,5,1,9,7,8])$
8	$S([9,8],[9,1])$
9	$S([9],[9])$

G =Conj($9T_{13}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 63$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(5,[6,7,9,1,2,4,5,3,8])$
3	$T(5,[2,1,5,4,3,7,6,8,9])$
4	$T(5,[2,1,3,5,4,6,8,7,9])$
5	$S([9,7,5],[9,3,1])$
6	$C(8,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_{14}$, $[1,2,3,7,5,6,8,4,9]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[5,7,9,8,1,6,2,4,3])$
3	$T(7,[6,4,7,2,5,1,3,9,8])$
4	$T(7,[2,1,6,7,8,3,4,5,9])$
5	$T(7,[3,6,2,8,4,1,5,7,9])$
6	$T(7,[2,3,5,4,1,9,6,7,8])$
7	$S([9,8,7],[9,8,1])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{15}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[9,5,8,1,3,6,2,4,7])$
3	$T(7,[6,7,2,9,1,5,3,4,8])$
4	$T(7,[5,7,1,3,8,2,4,6,9])$
5	$T(7,[4,2,8,3,1,7,5,9,6])$
6	$T(7,[1,4,2,5,8,3,6,9,7])$
7	$S([9,8,7],[9,8,1])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{16}$, $[1,5,3,2,9,4,8,6,7]$)
$c(G) = 117$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[6,9,1,8,7,3,2,5,4])$
3	$T(7,[9,8,6,1,2,5,3,7,4])$
4	$S([8,6,4],[9,4,1])$
5	$C(8,[9,8,7,6,5])$
6	$C(8,[9,8,7,6])$
7	$S([9,8,7],[9,4,1])$
8	$S([9,8],[9,4])$
9	$S([9],[9])$

G =Conj($9T_{17}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 45$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[3,4,7,8,6,1,2,9,5])$
3	$C(5,[9,5,4,3])$
4	$T(7,[6,7,1,2,9,3,4,5,8])$
5	$T(8,[7,8,1,2,9,3,4,5,6])$
6	$C(8,[9,8,7,6])$
7	$S([8,7],[9,1])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_{18}$, $[1,2,3,4,5,9,7,8,6]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(5,[5,4,1,6,2,3,7,9,8])$
3	$T(5,[7,8,4,5,3,9,6,1,2])$
4	$T(5,[1,2,5,3,4,6,8,9,7])$
5	$S([7,6,5],[9,6,1])$
6	$C(9,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_{19}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 225$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(5,[9,8,7,3,2,1,6,5,4])$
3	$T(5,[8,2,6,9,3,1,4,7,5])$
4	$T(5,[2,5,7,1,4,6,9,3,8])$
5	$S([9,7,5],[9,8,1])$
6	$C(7,[9,8,7,6])$
7	$S([9,8,7],[9,8,2])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{23}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 297$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(7,[9,8,7,3,2])$
3	$T(6,[2,5,1,4,7,3,6,9,8])$
4	$T(6,[6,5,7,3,2,4,9,8,1])$
5	$T(6,[2,4,1,3,8,5,7,9,6])$
6	$S([8,7,6],[9,8,1])$
7	$S([9,8,7],[9,8,3])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{20}$, $[1,3,4,6,5,7,9,8,2]$)
$c(G) = 18$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(8,[5,6,4,7,8,9,1,2,3])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$T(8,[7,8,9,3,1,2,6,4,5])$
5	$T(8,[7,8,9,3,1,2,4,5,6])$
6	$C(9,[9,8,7,6])$
7	$T(8,[5,6,4,2,3,1,9,7,8])$
8	$S([9,8],[9,1])$
9	$S([9],[9])$

G =Conj($9T_{24}$, $[1,2,4,6,5,7,8,9,3]$)
$c(G) = 135$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(5,[9,8,7,1,2,3,6,4,5])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$T(5,[3,2,1,5,4,6,9,8,7])$
5	$S([9,8,6,5],[9,2,6,1])$
6	$C(9,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_{21}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 117$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[5,3,6,7,8,1,2,9,4])$
3	$C(8,[9,8,7,6,5,4,3])$
4	$T(7,[8,6,9,1,2,3,4,5,7])$
5	$C(8,[9,8,7,6,5])$
6	$T(7,[1,2,3,4,5,8,6,7,9])$
7	$S([9,8,7],[9,6,1])$
8	$S([9,8],[9,6])$
9	$S([9],[9])$

G =Conj($9T_{25}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 360$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$S([9,8,7,5,4,2],[9,3,2,3,2,1])$
3	$C(5,[9,5,4,3])$
4	$C(5,[9,5,4])$
5	$T(8,[7,6,1,9,2,3,4,5,8])$
6	$C(8,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_{22}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 90$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(4,[7,8,1,2,9,3,4,5,6])$
3	$C(5,[9,5,4,3])$
4	$S([8,7,5,4],[9,2,3,1])$
5	$T(8,[6,7,1,2,9,3,4,5,8])$
6	$C(8,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_{26}$, $[1,2,3,6,8,4,9,5,7]$)
$c(G) = 81$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(7,[6,4,9,3,1,7,2,8,5])$
3	$T(7,[7,4,1,5,2,9,3,6,8])$
4	$T(7,[6,2,8,1,3,7,4,9,5])$
5	$T(7,[3,1,2,8,9,4,5,6,7])$
6	$C(9,[9,8,7,6])$
7	$S([9,8,7],[9,8,1])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{27}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 513$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$T(6,[6,4,5,7,1,2,8,9,3])$
3	$T(6,[8,1,2,5,9,3,4,7,6])$
4	$T(6,[7,3,1,5,2,4,8,9,6])$
5	$T(6,[2,3,4,8,1,5,6,9,7])$
6	$S([9,8,7,6],[9,8,7,1])$
7	$C(9,[9,8,7])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{28}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 36$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(9,[9,8,7,6,5,4,3,2])$
3	$C(5,[9,5,4,3])$
4	$C(5,[9,5,4])$
5	$T(8,[8,7,1,9,2,4,3,5,6])$
6	$C(8,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,3])$
9	$S([9],[9])$

G =Conj($9T_{29}$, $[1,2,4,5,6,7,8,9,3]$)
$c(G) = 675$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$S([9,8,6,5,3,2],[9,2,6,2,3,1])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$C(5,[6,5,4])$
5	$T(8,[1,2,3,7,8,9,4,5,6])$
6	$C(9,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_{30}$, $[1,2,4,5,6,7,8,9,3]$)
$c(G) = 675$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$S([9,8,6,5,3,2],[9,2,6,2,3,1])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$C(5,[6,5,4])$
5	$T(8,[7,9,8,1,3,2,4,5,6])$
6	$C(9,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_{31}$, $[1,2,4,5,6,7,8,9,3]$)
$c(G) = 27$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(9,[9,8,7,6,5,4,3,2])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$C(5,[6,5,4])$
5	$T(8,[9,8,7,1,3,2,4,5,6])$
6	$C(9,[9,8,7,6])$
7	$C(8,[9,8,7])$
8	$S([9,8],[9,2])$
9	$S([9],[9])$

G =Conj($9T_{32}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 3033$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(6,[9,8,7,6,3,2])$
3	$T(5,[8,1,7,2,3,5,9,6,4])$
4	$T(5,[2,1,3,9,4,5,8,6,7])$
5	$S([9,8,7,6,5],[9,8,7,3,1])$
6	$S([9,8,7,6],[9,8,7,3])$
7	$C(9,[9,8,7])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{33}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 181449$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$S([9,8,7,6,5,4,3,2],[9,8,7,6,5,4,3,1])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$C(9,[9,8,7,6,5,4])$
5	$C(9,[9,8,7,6,5])$
6	$C(9,[9,8,7,6])$
7	$C(9,[9,8,7])$
8	$C(9,[9,8])$
9	$S([9],[9])$

G =Conj($9T_{34}$, $[1,2,3,4,5,6,7,8,9]$)
$c(G) = 9$

1	$C(9,[9,8,7,6,5,4,3,2,1])$
2	$C(9,[9,8,7,6,5,4,3,2])$
3	$C(9,[9,8,7,6,5,4,3])$
4	$C(9,[9,8,7,6,5,4])$
5	$C(9,[9,8,7,6,5])$
6	$C(9,[9,8,7,6])$
7	$C(9,[9,8,7])$
8	$C(9,[9,8])$
9	$S([9],[9])$

B.2 Implantation

La fonction suivante prend un polynôme f à coefficients entiers en entrée et renvoie le plus petit premier p tel que f soit séparable et complètement décomposé modulo p.

Remarque B.2.1. Le polynôme $g = x^p - x$ de $\mathbb{F}[x]$ s'annule en les p éléments du corps $\mathbb{F}_p$. Ainsi, il suffit de trouver le premier p tel que f mod p divise g.

```
/*****************************************************************************/
```

```
function _Tchebotarev(f)
p:=1;
test:=true;
d:=Degree(f);

while test do
      p:=NextPrime(p);
      PR:=PolynomialRing(GaloisField(p));
      test:= not((PR.1^p mod PR!f eq PR.1))
end while;

return p;
end function;
/*************************************************************************/
```

La fonction qui suit, renvoie les racines dans $\mathbb{Z}/p^k\mathbb{Z}$ d'un polynôme f à coefficients entiers.

```
/*************************************************************************/
/** Calcul les racines p-adiques de $f$ modulo p^k. HYPOTHESE : $f$
est séparable et complètement décomposé modulo $p$.
@param f un polynome à coefficients entiers
@param rp les racines de $f$ modulo $p$
@param p l'entier premier
@param k la précision
@return l'ensemble des racines de $f$ modulo $p^k$.
*/

function _RacinesDansZpk(f,rp,p,k)

Qp := pAdicField(p,k);
rrp :=[r[1] : r in Roots(f,Qp)];
n := Degree(f);
Z:=Integers();

// On remet les racines dans le bon ordre

rrptmp:=[ Z!r mod p : r in rrp];
rrp2:=[rrp[Index(rrptmp,rp[i])] : i in [1 .. n]];
rrp := rrp2;
/** Fin pour l'ordre **/

// On passe dans Z/p^k.Z

_, pi := quo<Z| p^k>;

return [pi(Z!r) : r in rrp];

end function;
/*************************************************************************/
```

Les deux fonctions qui suivent permettent le calcul des modules de Cauchy généralisés d'un polynôme multivarié. La seconde prend en entrée un polynôme multivarié f, x_i sa variable dominante et L une liste d'entiers. Nous supposons que le polynôme f est

unitaire en x_i et que l'ensemble E des indices des variables de f est un sous-ensemble strict de L. Notant d le degré de f en x_i, cette fonction renvoie le module de Cauchy généralisé de f en les variables indicées par les entiers de L et de degré $d - |L| + |E|$ en sa variable dominante.

```
/*****************************************************************************/
function _CauchyUneEtape(rel,x_old,x_new)

return (Evaluate(rel,x_old,x_new) - rel) / (x_old - x_new);

end function;


function _CauchyGen(rel,x_old,x_ind)

PR := Parent(rel);
for j:=Index(x_ind,x_old)+1 to #x_ind do
    rel := PR!_CauchyUneEtape(rel,PR.x_ind[j-1],PR.x_ind[j]);
end for;

return rel;
end function;
/*****************************************************************************/
```

À l'aide de la ligne correspondant dans le schéma de calcul, cette fonction construit le système linéaire pour calculer un polynôme de la base triangulaire de l'idéal des relations du polynôme f. Pour ce faire, elle prend en entrée les racines de f dans $\mathbb{Z}/p^k\mathbb{Z}$ et la représentation symétrique de l'action de son groupe de Galois sur celles-ci.

```
/*****************************************************************************/
/**Construction de la matrice.
@param rr la liste des racines de f dans Z/p^k Z
@param G la représentation sym. du gp de Galois de f sur rr.
@param tti la ligne de la base de données correspondant à G.
@return la matrice Mi et le vecteur Vi
*/

function RYSystem(rr, G, tti)

local vi, di, tt, index, lcosets, d, sigma, un;

un := Parent(rr[1])!1; //l'unite dans z/p^kZ
vi := Reverse(tti[1]);
di := Reverse(tti[2]);

// Indices de decalage pour la boucle for du calcul de Mi

IndTab:=[];
IndTab[1]:=1;
for i:=2 to #di do
    IndTab[i]:=IndTab[i-1]*tti[2][i-1];
end for;
IndTab:=IndTab[2 .. #IndTab];
```

```
// Transversale correspondant au système

lcosets := RightTransversal(G,Stabilizer(G,vi));


//Produit cartesien pour les degrés des variables

cc := [[0 .. d-1] : d in di];
cc := CartesianProduct(cc);

// Construction de la matrice Mi et du vecteur Vi

M := [];
V := [];
i:=1;

for sigma in lcosets do
    NRac:=[v^sigma : v in vi];

    //Calcul de M[i]
    M[i]:=[];

    j:=1;

    for c in cc do
        if j eq 1 then
           Tab:=1;
           IRac:=#NRac;
           M[i][j]:=rr[NRac[IRac]]^0;
        else
           test:=Index(IndTab,j-1);
           if not(test eq 0) then
              Tab:=IndTab[test];
              IRac:=IRac-1;
           end if;

           M[i][j]:=rr[NRac[IRac]]*M[i][j-Tab];
        end if;

        j:=j+1;
    end for;
    V[i] := rr[vi[1]^sigma]^di[1];
    i:=i+1;
end for;


// Calcul des monômes du polynome solution

PR:=PolynomialRing(Rationals(),#rr);
rr:=[PR.i : i in [1 .. #rr]];

Ind:=[];
NRac:=vi;
```

```
j:=1;

for c in cc do
    if j eq 1 then
       Tab:=1;
       IRac:=#NRac;
       Ind[j]:=rr[NRac[IRac]]^0;
    else
       test:=Index(IndTab,j-1);
       if not(test eq 0) then
          Tab:=IndTab[test];
          IRac:=IRac-1;
       end if;

       Ind[j]:=rr[NRac[IRac]]*Ind[j-Tab];
    end if;
    j:=j+1;
end for;

// Fin

return Matrix(M), Vector(V), Ind;

end function;
/*****************************************************************************/
```

À partir des fonctions précédentes et de la base de données, la fonction qui suit permet le calcul de la base triangulaire réduite d'un idéal des relations d'un polynôme irréductible à coefficients entiers, unitaire et de degré inférieur ou égal à 9. Avec la base triangulaire T, cette fonction renvoie aussi le groupe de décomposition de T. On suppose que la variable `DB` représente la base de données sur les schémas de calcul. Ainsi, `DB[d,n]` contient les données pour le groupe transitif dT_n. L'entrée `DB[d,n]` correspond à un triplet. Le premier élément est la permutation par laquelle il faut conjuguer le groupe dT_n pour retrouver le bon représentant, le deuxième est un tableau contenant les variables et leur degré respectif pour construire les systèmes linéaires. Le dernier élément de ce triplet est un tableau contenant les informations nécessaires à l'application des techniques (éventuelles) permettant d'éviter les calculs de systèmes linéaires. Par exemple, l'entrée `DB[9,22]` est le triplet suivant

```
<Id(S), [
    <[ 9, 8, 7, 6, 5, 4, 3, 2, 1 ], []>,
    <[ 9, 8, 7, 2 ], [ 9, 3, 2, 1 ]>,
    <[ 9, 5, 4, 3 ], []>,
    <[ 8, 7, 5, 4 ], [ 9, 2, 3, 1 ]>,
    <[ 9, 5 ], [ 9, 3 ]>,
    <[ 9, 8, 7, 6 ], []>,
    <[ 9, 8, 7 ], []>,
    <[ 9, 8 ], [ 9, 3 ]>,
    <[ 9 ], [ 9 ]>
], [
    <9, Id(S)>,
```

```
    <4, S!(1, 7, 4, 2, 8, 5, 9, 6, 3)>,
    <5, Id(S)>,
    <0, Id(S)>,
    <8, S!(1, 6, 3)(2, 7, 4)(5, 9, 8)>,
    <8, Id(S)>,
    <8, Id(S)>,
    <0, Id(S)>,
    <0, Id(S)>
]>
```

où `S` est le groupe symétrique de degré 9.

```
/*************************************************************************/
function RelationsIdeal(f)

local p,G,S,k,tt,tt1,tt2;

n := Degree(f);
PR:=PolynomialRing(Rationals(),n);

// Calcul Tchebotarev
// Le premier nombre premier qui decompose totalement f

p := _Tchebotarev(f);

// Le groupe de Galois de f
// On utilise le premier que l'on vient de calculer

G, rp, _ := GaloisGroup(f:Prime:=p);
S := Generic(G);

// On récupère la numérotation de G selon Butler et McKay.

KayBut := TransitiveGroupIdentification(G);

// On récupère le schéma de calcul dans la base de données

tt:=DB[n,KayBut];
conj:=tt[1];
tt1 := tt[2];
tt2 := tt[3];
delete tt;

// On remet les racines dans le bon ordre et on change de conjugué pour G.
// De cette manière G est le représentant de la base.

rptmp:=[];
for i:=1 to #rp do
    rptmp[i] := rp[i^S!(conj^(-1))];
end for;
rp:=rptmp;
G:=G^conj;
```

```
//On calcule les racines de f dans Z/p^kZ

k:=10; // HEURISTIQUE
rrmodp := _RacinesDansZpk(f,rp,p,k);

// On calcule les modules de Cauchy de f.
// Ils seront utilisés pour les tests d'arrêt

BaseS:=[];
BaseS[n]:=Evaluate(f,PR.n);
for i := n-1 to 1 by -1 do
BaseS[i]:= _CauchyUneEtape(BaseS[i+1],PR.(i+1),PR.i);
end for;

// Initialisation des sorties

BaseRel:=[];
BaseRel_nr:=[];
BaseRel[n]:=Evaluate(f,PR.n);
BaseRel_nr[n]:=Evaluate(f,PR.n);

// Boucle principale

for i:=#tt1-1 to 1 by -1 do

if tt2[i][1] eq 0 then

// On construit et résout un système linéaire.

loop := true;
tmp_r :=PR!0;

while loop do
        loop :=false;
        X,W,ind:=RYSystem(rrmodp,G,tt1[i]);
        V:=Solution(Transpose(X),-W);

        // On essaie de reconstruire la solution à coefficients dans Q

        rat:=[];
        test:=true;
        for j in [1 .. Ncols(V)] do
                test_r, r := RationalReconstruction(V[j]);
                if test_r then
                   // Reconstrution possible
                   rat[j]:=r;
                else
                   // Reconstruction impossible
                   // On augmente la précision
                   k:=2*k;
                   rrmodp :=_RacinesDansZpk(f,rp,p,k);
                   loop:=true;
                   break;
```

```
                // On construit et resoud un nouveau système.
            end if;
        end for;

        if not(loop) then

        // La reconstruction était possible.
        // On réduit et on teste l'arrêt.

        ind:=[PR!e : e in ind];
        bb:=[g : g in BaseRel];
        BaseRel_nr[i]:=
            ((PR.i)^tt1[i][2][#tt1[i][2]])+(&+[rat[j]*ind[j]
            : j in [1 .. #ind]]);
        BaseRel[i]:=NormalForm(BaseRel_nr[i], Reverse(bb));
        delete bb;

        tmp_r:= BaseRel[i];

        // On teste l'arrêt avec les modules de Cauchy

        test:=NormalForm(BaseS[i],Reverse([BaseRel[j] : j in [i .. n]]));

        if test ne 0 then
                // Le test d'arrêt n'est pas passé.
                // On augmente la précision

                k:=2*k;
                rrmodp := _RacinesDansZpk(f,rp,p,k);
                loop := true;
                // On construit et resoud un nouveau système.
        end if;

        end if;
end while;

else

// Nous avons la relation sans calcul de système linéaire

        if S!tt2[i][2] eq Id(S) then
           // Module de Cauchy
           ind_old := tt2[i][1];
           BaseRel_nr[i]:=_CauchyGen(BaseRel[ind_old],ind_old,tt1[i][1]);
           BaseRel[i] := NormalForm(BaseRel_nr[i],Reverse([BaseRel[j] :
              j in [(i+1) .. n]]));

        else
           // Technique Transporteur
           ind_old := tt2[i][1];
           BaseRel_nr[i] := BaseRel_nr[ind_old]^tt2[i][2];
           BaseRel[i] := NormalForm(BaseRel_nr[i],Reverse([BaseRel[j] :
              j in [(i+1) .. n]]));
```

```
        end if;
end if;
end for;

// Fin

return BaseRel,G;
end function;
/*****************************************************************************/
```

Bibliographie

[1] J.A. Abbott. *On the factorisation of polynomials over algebraic fields*. PhD thesis, School of Math. Sci., University of Bath, 1989.

[2] I. Abdeljaouad. *Théorie des invariants et application à la théorie de Galois effective*. PhD thesis, Université Paris 6, 2000.

[3] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *AAECC*, 15(3-4) :279–294, 2004.

[4] N.-H. Abel. *Œuvres Mathématiques*. Grøendahl and Søøn, Christiania, 1881.

[5] V. Acciaro and J. Klüners. Computing automorphisms of abelian number fields. *Math. Comp.*, 68(227) :1179–1186, 1999.

[6] B. Allombert. An efficient algorithm for the computation of Galois automorphisms. *Math. Comp.*, 73(245) :359–375 (electronic), 2004.

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

[8] H. Anai and K. Yokoyama. Radical representation of polynomial roots. *Sūrikaisekikenkyūsho Kōkyūroku*, (920) :9–24, 1995. Research on the theory and applications of computer algebra (Japanese) (Kyoto, 1994).

[9] J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118 :23–40, 1997. Algorithms for algebra (Eindhoven, 1996).

[10] J.-M. Arnaudiès and A. Valibouze. *Cours de théorie de Galois*. DEA Algorithmique, Université Paris 6, 1998.

[11] Ph. Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris 6, 1999.

[12] Ph. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symbolic Comput.*, 28(1-2) :105–124, 1999. Polynomial elimination—algorithms and applications.

[13] Ph. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems : a comparative implementation of four methods. *J. Symbolic Comput.*, 28(1-2) :125–154, 1999. Polynomial elimination—algorithms and applications.

[14] Ph. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6) :635–651, 2000. Algorithmic methods in Galois theory.

[15] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[16] K. Belabas. A relative van Hoeij algorithm over number fields. *J. Symbolic Comput.*, 37(5), 2004.

[17] K. Belabas, M. van Hoeij, J. Klüners, and A. Steel. Factoring polynomials over global fields. 2005. Soumis.

[18] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24 :713–735, 1970.

[19] E. H. Berwick. On soluble sextic equations. *Proc. London Math. Soc.*, 29 :1–28, 1929.

[20] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4) :235–265, 1997. Computational algebra and number theory (London, 1993).

[21] N. Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7], Lecture Notes in Mathematics, 864.

[22] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, 4 :374–383, 1970.

[23] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 3–21. Springer, Berlin, 1979.

[24] G. Butler. *Fundamental algorithms for permutation groups*, volume 559 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 1991.

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

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

[27] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[28] A. Colin. *Théorie des invariants effective. Application à la théorie de Galois et à la résolution de système Algébrique. Implantation en AXIOM.* PhD thesis, École Polytechnique, 1997.

[29] D. Cox. *Galois Theory*. Wiley-Interscience, 2004.

[30] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[31] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24(3-4) :267–283, 1997. Computational algebra and number theory (London, 1993).

[32] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04 : Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 103–110, New York, NY, USA, 2004. ACM Press.

[33] H. Darmon and D. Ford. Computational verification of M_{11} and M_{12} as Galois groups over $\mathbf{Q}$. *Comm. Algebra*, 17(12) :2941–2943, 1989.

[34] J. H. Davenport, Y. Siret, and E. Tournier. *Computer algebra*. Academic Press Ltd., London, second edition, 1993. Systems and algorithms for algebraic computation, With a preface by Daniel Lazard, Translated from the French by A. Davenport and J. H. Davenport, With a foreword by Anthony C. Hearn.

[35] L. Ducos. Construction de corps de décomposition grâce aux facteurs de résolvantes. *Comm. Algebra*, 28(2) :903–924, 2000.

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

[37] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic), New York, 2002. ACM.

[38] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4) :329–344, 1993.

[39] P. Fernandez-Ferreiros, M. A. Gomez-Molleda, and L. Gonzalez-Vega. Partial solvability by radicals. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 84–91 (electronic), New York, 2002. ACM.

[40] *FGb, J.-C. Faugère*, 2004. http ://fgbrs.lip6.fr/jcf/Software/FGb/index.html.

[41] P. Flajolet, X. Gourdon, and D. Panario. The complete analysis of a polynomial factorization algorithm over finite fields. *J. Algorithms*, 40(1) :37–81, 2001.

[42] M. Fontet. Calcul de centralisateur d'un groupe de permutations. *Bull. Soc. Math. France Mém.*, (49-50) :53–63, 1977. Utilisation des calculateurs en mathématiques pures (Conf., Limoges, 1975).

[43] H.O. Foulkes. The resolvents of an equation of seventh degree. *Quart. J. Math. Oxford Ser.*, 2 :9–19, 1931.

[44] E. Galois. *Œuvres Mathématiques*. Gauthier-Villars, Paris, 1897.

[45] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (`http://www.gap-system.org`).

[46] K. Geissler. *Berechnung von Galoisgruppen über Zhal- und Funktionenkörpern.* PhD thesis, Universität Berlin, 2003.

[47] K. Geissler and J. Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6) :653–674, 2000. Algorithmic methods in Galois theory.

[48] K. Girstmair. On the computation of resolvents and Galois groups. *Manuscripta Math.*, 43(2-3) :289–307, 1983.

[49] K. Girstmair. On invariant polynomials and their application in field theory. *Math. Comp.*, 48(178) :781–797, 1987.

[50] Giulia. UMS MEDICIS. Intel - Pentium III 2 x 933 Mhz, 1024 Mo, Linux 2.4.1, http ://www.medicis.polytechnique.fr.

[51] M. A. Gómez Molleda. *Cálculo del Centro de un Grupo de Galois y Applicationes.* PhD thesis, Universidad de Cantabria, 2002.

[52] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM.

[53] C. U. Jensen, A. Ledet, and N. Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications.* Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem.

[54] M. Kalkbrener. Solving systems of algebraic equations by using Gröbner bases. In *EUROCAL '87 (Leipzig, 1987)*, volume 378 of *Lecture Notes in Comput. Sci.*, pages 282–292. Springer, Berlin, 1989.

[55] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symbolic Comput.*, 15(2) :143–167, 1993.

[56] E. Kaltofen and V. Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 184–188 (electronic), New York, 1997. ACM.

[57] J. Klüners. *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper.* PhD thesis, Technical University Berlin, 1997.

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

[59] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4 :182–196 (electronic), 2001.

[60] L. Kronecker. Grundzüge einer Arithmetischen Theorie der Algebraischen Grössen. *J. Reine Angew. Math.*, 92 :515–534, 1882.

[61] L. Kronecker. *Vorlesungen über Zahlentheorie*. Springer-Verlag, Berlin, 1978. Erster Band, Reprint.

[62] J.-L. Lagrange. Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*, 3 :205–421, 1770-1771.

[63] J.-L. Lagrange. *Œvres Complètes*. Gauthier-Villars, Paris, 1867-1892. 14 volumes.

[64] S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1) :184–195, 1985.

[65] S. Landau. Simplification of nested radicals. *SIAM J. Comput.*, 21(1) :85–110, 1992.

[66] S. Landau. How to tangle with a nested radical. *Math. Intelligencer*, 16(2) :49–55, 1994.

[67] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *J. Comput. System Sci.*, 30(2) :179–208, 1985.

[68] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[69] L. Langemyr. Algorithms for a multiple algebraic extension. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 235–248. Birkhäuser Boston, Boston, MA, 1991.

[70] L. Langemyr. Algorithms for a multiple algebraic extension. II. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 224–233. Springer, Berlin, 1991.

[71] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symbolic Comput.*, 13(2) :117–131, 1992.

[72] D. Lazard. Solving quintics by radicals. In *The legacy of Niels Henrik Abel*, pages 207–225. Springer, Berlin, 2004.

[73] F. Lehobey. *Calcul et factorisation interactive de résolvantes de Lagrange en théorie de Galois effective*. PhD thesis, Université de Rennes 1, 1999.

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

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

[76] F. Mertens. Ein Beweis des Galois'shen Fundamentalsatzes. *Akad. Wiss. Wien Math.-Natur. Kl. Sitzungsber. IIa*, 111 :17–37, 1902.

[77] M. Mignotte. *Mathématiques pour le calcul formel.* Mathématiques. [Mathematics]. Presses Universitaires de France, Paris, 1989.

[78] F. Morain. *Courbes elliptiques et tests de primalité.* PhD thesis, Université de Lyon I, 1990.

[79] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443. Springer, Berlin, 1999.

[80] B. Mourrain and Ph. Trébuchet. Solving projective complete intersection faster. In C. Traverso, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 231–238. New-York, ACM Press., 2000.

[81] P. Naudin and C. Quitté. Univariate polynomial factorization over finite fields. *Theoret. Comput. Sci.*, 191(1-2) :1–36, 1998.

[82] M. Noro and K. Yokoyama. Factoring polynomials over algebraic extension fields. *Josai Information Science Researches*, **9** :11–33, 1997.

[83] M. Noro and K. Yokoyama. Yet another practical implementation of polynomial factorization over finite fields. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 200–206 (electronic), New York, 2002. ACM.

[84] S. Orange, G. Renault, and A. Valibouze. Calcul efficace de corps de décomposition. *Soumis à Experiment. Math.*, 2003.

[85] S. Orange, G. Renault, and A. Valibouze. Calcul efficace d'un corps de décomposition. LIP6 Research Report 005, LIP6, Laboratoire d'Informatique de Paris 6, 2003. http ://www.lip6.fr/reports/lip6.2003.005.html.

[86] S. Orange, G. Renault, and A. Valibouze. Splitting tables for the degrees from 3d to 21th. *preprint*, 2004.

[87] S. Orange, G. Renault, and A. Valibouze. Note sur les relations entre les racines d'un polynôme réductible. *RAIRO- Theoritical Informatics and Applications*, to appear, 2005.

[88] *PARI/GP, version* `2.2.5`, 2003. http ://www.parigp-home.de.

[89] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Cambridge Univ. Press, Cambridge, 1989.

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

[91] *Risa/Asir, version 2003/05/07.* http ://www.asir.org.

[92] X.-F. Roblot. Polynomial factorization algorithms over number fields. *J. Symbolic Comput.*, 38(5) :1429–1443, 2004.

[93] F. Rouiller. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*. PhD thesis, Université de Rennes I, 1996.

[94] É. Schost. Complexity results for triangular sets. *J. Symbolic Comput.*, 36(3-4) :555–594, 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[95] Á. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[96] C. C. Sims. Computation with permutation groups. In *SYMSAC '71 : Proceedings of the second ACM symposium on Symbolic and algebraic manipulation*, pages 23–28. ACM Press, 1971.

[97] L. Soicher and J. McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3) :273–281, 1985.

[98] B. K. Spearman and K. S. Williams. Dihedral quintic polynomials and a theorem of Galois. *Indian J. Pure Appl. Math.*, 30(9) :839–845, 1999.

[99] R. Stauduhar. The determination of galois groups. *Math. Comp.*, 27 :981–996, 1973.

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

[101] B. Trager. Algebraic factoring and rational functiun integration. In *Proceedings of SYMSAC'76*, pages 219–226, 1976.

[102] Ph. Trébuchet. *Vers une résolution stable et rapide des équations algébriques*. PhD thesis, Université Paris 6, 2002.

[103] E. W. Tschirnhaus. Methodus auferendi omnes terminos intermedios ex data equatione. *Nieuw Arch. Wisk. (4)*, 11(1) :67–83, 1993. With translation and commentaries in Dutch by A. W. Grootendorst.

[104] M. Turrel Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Paris 6, 2004.

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

[106] 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.

[107] A. Valibouze. Généralisations de résultats sur les idéaux de Galois. Publication interne LIP6 2003.006, LIP6, Laboratoire d'Informatique de Paris 6, 2003. http ://www.lip6.fr/reports/lip6.2003.006.html.

[108] A. Valibouze. Corps de décomposition de groupe de Galois PSL(2,7). LIP6 Research Report 001, LIP6, Laboratoire d'Informatique de Paris 6, 2005. http ://www.lip6.fr/reports/lip6.2005.001.html.

[109] M. van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2) :167–189, 2002.

[110] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[111] A. Weil. *Fundations Of Algebraic Geometry*. A.M.S. Colloquium Publications. American Mathematical Society, New York, 1946.

[112] P. J. Weinberger and L. P. Rothschild. Factoring polynomials over algebraic number fields. *ACM Trans. Math. Software*, 2(4) :335–350, 1976.

[113] 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).